NEW EDITION

ISC2 CISSP Study Guide

9 Hour E-Learning Course Included

2025-2026

All in One Visual Exam Prep for the Certified Information Systems Security Professional Certification with 1250+ Practice Tests, In-Depth Reviews + 9 Hours Premium E-Learning Course

NewGrade Publication

ISC2 CISSP

Study Guide

2025-2026

All in One Visual Exam Prep for the Certified Information Systems Security Professional Certification with 1250+ Practice Tests, In-Depth Reviews + 9 Hours Premium E-Learning Course

NewGrade Publication

Disclaimer

Note: While we've made every effort to ensure the accuracy of this study guide, it's important to remember that it's a supplementary resource. Always consult your nursing program or official exam resources for the most up-to-date and comprehensive information.

This study guide is designed to help you enhance your understanding of exam and improve your chances of success. It provides practice questions, explanations, and strategies to aid in your preparation. However, it's not a substitute for professional guidance or official exam materials.

We recommend using this guide in conjunction with your nursing coursework and other study resources. If

you have any questions or concerns, please consult with your instructors or a qualified healthcare professional.

By using this study guide, you agree to use it at your own discretion and acknowledge that the authors and publishers are not responsible for any potential inaccuracies or any consequences that may arise from your use of the guide.

CONTENTS

HOW TO USE THIS BOOK?

Below is a detailed guide on how to effectively use the ISC2 CISSP Study Guide 2025-2026:

1. **Start with the Introduction**: Begin by carefully reading the introduction chapter. This will provide an overview of the CISSP exam, its structure, and what to expect. It will also outline the book's approach and how to best utilize its features.
2. **Review the Table of Contents**: Familiarize yourself with the book's layout and the topics covered in each chapter. This will help you plan your study schedule and identify areas you may need to focus on more.
3. **Read Each Chapter Thoroughly**:
    - Take notes on important points
    - Highlight or mark sections you find challenging for later review
4. **Complete Chapter Practice Questions**: At the end of each chapter, attempt all practice questions. These will help reinforce your learning and identify areas that need more study.
5. **Utilize the Visual Aids**: This guide emphasizes visual learning, so make sure to study the diagrams, charts, and infographics carefully. They often summarize complex concepts in an easy-to-understand format.
6. **Take Advantage of the 1250+ Practice Tests**:
    - Start with shorter practice sessions focusing on specific domains

- Gradually work up to full-length practice exams
- **Analyze your results** carefully to identify weak areas

7. **Utilize the Visual 9 Hours Premium E-Learning Course**:
    - This course complements the book content
    - Use it to reinforce concepts and gain additional perspectives
    - **Complete all interactive elements** for a more engaging learning experience
8. **Create a Study Schedule**: Plan your study time to cover all domains well before your exam date. Allocate more time to areas where you feel less confident.
9. **Implement Active Learning Techniques**:
    - Explain concepts in your own words
    - Create mind maps or flashcards for complex topics
    - Discuss concepts with study partners or in online forums

10. **Regular Review**: Periodically review earlier chapters to reinforce your understanding and maintain knowledge of all domains.
11. **Final Preparation**:
    - Take full-length practice exams under timed conditions
    - Review all incorrect answers and understand why you got them wrong

- Focus on your weak areas in the final days before the exam

12. **Utilize the Exam Preparation Strategies**: The book likely includes a section on exam strategies. Review these carefully and practice implementing them during your study sessions.

Remember, the key to success with this study guide is **active engagement** with the material and **consistent practice**. Good luck with your CISSP exam preparation!

Who's This Book For? Let's Find Out!

This ISC2 CISSP Study Guide 2025-2026 is intended for the following audiences:

Information Security Professionals: This comprehensive guide is primarily designed for experienced IT and cybersecurity professionals preparing to take the CISSP certification exam. It covers all 8 domains of the CISSP Common Body of Knowledge (CBK) in depth.

Aspiring CISSPs: Individuals looking to advance their careers in information security will find this an invaluable resource for exam preparation and building a strong foundation in cybersecurity concepts.

IT Managers and Executives: Those in leadership roles who want to gain a holistic understanding of information security principles and best practices to better manage their organization's security posture.

Security Consultants: Professionals who advise organizations on security matters will benefit from the comprehensive coverage of security domains and real-world applications.

System Administrators: IT professionals responsible for implementing and maintaining secure systems will find practical knowledge applicable to their daily work.

Risk Management Professionals: The guide's strong focus on risk management principles makes it relevant for those involved in assessing and mitigating organizational risks.

Compliance Officers: Individuals responsible for ensuring regulatory compliance will appreciate the coverage of legal and regulatory aspects of information security.

Students: Advanced cybersecurity students looking for a comprehensive study resource that goes beyond basic concepts.

Career Changers: Professionals transitioning into the cybersecurity field can use this guide to build a strong foundation in core security principles.

Key features that make this guide suitable for these audiences include:

- **1250+ Practice Tests**: Allowing readers to assess their knowledge and identify areas for improvement
- **In-Depth Reviews**: Providing comprehensive coverage of all CISSP domains
- **Visual Learning Aids**: Enhancing understanding through diagrams, charts, and infographics
- **9 Hours Premium E-Learning Course**: Offering additional interactive learning opportunities
- **All-in-One Format**: Serving as a complete resource for exam preparation and ongoing reference

This guide is designed to be accessible to those with some IT or security background, while still providing the depth of content required for CISSP certification.

INTRODUCTION

Have you ever wondered what separates top cybersecurity professionals from the rest? The Certified Information Systems Security Professional (CISSP) certification stands as the gold standard in the industry, but achieving it is no small feat. In fact, **the CISSP exam has a notoriously high failure rate of around 20-30%**, making it one of the most challenging professional certifications to obtain.

Imagine this scenario: A seasoned IT professional with over a decade of experience confidently walks into the testing center, ready to ace the CISSP exam. Six hours later, he emerge shell-shocked, having encountered questions and scenarios he never anticipated. This is a common experience for many CISSP candidates, regardless of their background or years in the field.

The **complexity and breadth of the CISSP exam** poses a significant challenge. Covering eight diverse domains of cybersecurity, from **Security and Risk Management** to **Software Development Security**, the exam demands not just technical knowledge, but also a deep understanding of how security integrates with business operations and strategy.

One of the **major problems** faced by exam takers is the **sheer volume of information** they need to master. The CISSP Common Body of Knowledge (CBK) is vast, encompassing topics that many IT professionals may not encounter in their day-to-day roles. This leads to a common pitfall: underestimating the exam's difficulty and the preparation required.

Another significant hurdle is the **exam's focus on applying knowledge to real-world scenarios**. It's not enough to memorize facts and definitions; candidates must demonstrate the ability to think critically and make sound decisions in complex security situations. This shift from theoretical knowledge to practical application catches many test-takers off guard.

The **time pressure** of the exam also presents a formidable challenge. With 100 to 150 questions to answer in just three hours for the English CAT version (or 250 questions in six hours for non-English linear exams), candidates must manage their time effectively while carefully analyzing each question.

Furthermore, the **adaptive nature of the computerized exam** means that the difficulty of questions adjusts based on the candidate's performance. This dynamic format can be psychologically taxing, as test-takers may find it difficult to gauge their progress during the exam.

Given these challenges, it's clear why comprehensive and targeted preparation is crucial for CISSP success. This is where the "ISC2 CISSP Study Guide 2025-2026" comes in. Designed to address the specific pain points of CISSP candidates, this guide offers:

- **1250+ Practice Tests** to familiarize you with the exam format and build your confidence
- **In-Depth Reviews** of all eight CISSP domains, ensuring comprehensive coverage of the CBK
- **Visual Learning Aids** to help you grasp and retain complex concepts more effectively
- **9 Hours of Premium E-Learning Content** to supplement your study and reinforce key topics

By combining these elements, this study guide aims to transform the daunting CISSP certification process into a structured, manageable journey. Whether you're a first-time candidate or retaking the exam, this all-in-one resource is crafted to equip you with the knowledge, skills, and confidence needed to join the elite ranks of CISSP-certified professionals.

As you embark on your CISSP preparation journey, remember that this certification is not just about passing an exam—it's about elevating your cybersecurity expertise to the highest level and positioning yourself as a leader in the field. With dedication, the right resources, and a strategic approach to learning, you can overcome the challenges of the CISSP exam and unlock new opportunities in your career.

Chapter 1: Security and Risk Management

Security and risk management forms the foundation of information security, encompassing the core principles, practices, and strategies organizations use to protect their assets and mitigate threats. This domain covers a wide range of topics essential for establishing and maintaining a robust security posture.

At its core, security and risk management is about understanding and addressing the various risks an organization faces. This includes identifying valuable assets, recognizing potential threats and vulnerabilities, and implementing appropriate controls and countermeasures. It requires a holistic approach that considers technical, operational, and administrative aspects of security.

Key concepts in this domain include the CIA triad of confidentiality, integrity, and availability - the fundamental goals of information security. Governance frameworks provide structure and guidance for security programs, while legal and regulatory compliance ensures organizations meet their obligations.

Risk management is a critical component, involving the continuous process of identifying, assessing, and responding to risks. This includes both qualitative and quantitative methods of analysis to prioritize risks and allocate resources effectively.

The human element is also crucial, addressed through professional ethics, security awareness training, and clearly defined policies and procedures. These provide guidance on

acceptable use of systems and handling of sensitive information.

Business continuity and disaster recovery planning ensure organizations can maintain critical functions and recover quickly from disruptive events. Threat modeling helps anticipate and prepare for potential attacks.

By mastering the concepts in this domain, security professionals can develop comprehensive strategies to protect their organizations' assets, meet compliance requirements, and build resilience against an ever-evolving threat landscape.

Information Security Concepts

Information security concepts provide the fundamental building blocks for protecting an organization's data and systems. At the core of these concepts is the idea that information is a valuable asset that must be safeguarded against various threats and vulnerabilities.

One of the primary information security concepts is the principle of least privilege. This principle states that users should only be granted the minimum level of access and permissions necessary to perform their job functions. By limiting access rights, organizations can reduce the potential impact of a security breach or insider threat. For example, a customer service representative may only need read access to customer records, while a database administrator would require full access to manage the database system.

Another key concept is defense in depth, which involves implementing multiple layers of security controls to protect assets. This approach recognizes that no single security measure is perfect, and by combining various defenses, an organization can create a more robust security posture.

Layers might include firewalls, intrusion detection systems, encryption, access controls, and security awareness training for employees.

The concept of separation of duties is crucial for preventing fraud and reducing the risk of errors or malicious actions. This principle ensures that no single individual has complete control over a critical process or system. For instance, in financial systems, the person who approves payments should be different from the one who initiates them.

Data classification is another important concept that helps organizations determine the appropriate level of protection for different types of information. By categorizing data based on its sensitivity and importance, security teams can allocate resources more effectively and implement suitable controls. Common classification levels might include public, internal use only, confidential, and restricted.

The principle of non-repudiation is essential in ensuring accountability and preventing individuals from denying their actions. This is often achieved through the use of digital signatures, audit logs, and other mechanisms that provide proof of a user's actions within a system.

Security through obscurity is a controversial concept that suggests keeping system details secret can enhance security. While this approach can provide some benefits, it should not be relied upon as a primary security measure. Instead, it should be used in conjunction with other, more robust security controls.

The concept of security awareness emphasizes the importance of educating all members of an organization about security risks and best practices. This includes regular training sessions, simulated phishing exercises, and clear communication of security policies and procedures.

Incident response and management is a critical concept that focuses on how organizations detect, respond to, and

recover from security incidents. This involves having a well-defined plan in place, including roles and responsibilities, communication protocols, and steps for containment and recovery.

The principle of least common mechanism suggests limiting the number of shared resources between users or systems to reduce potential attack surfaces. This concept is particularly relevant in multi-tenant environments or shared computing resources.

Asset management is a fundamental concept that involves identifying, tracking, and protecting an organization's valuable assets. This includes not only physical assets but also intangible assets such as intellectual property and data.

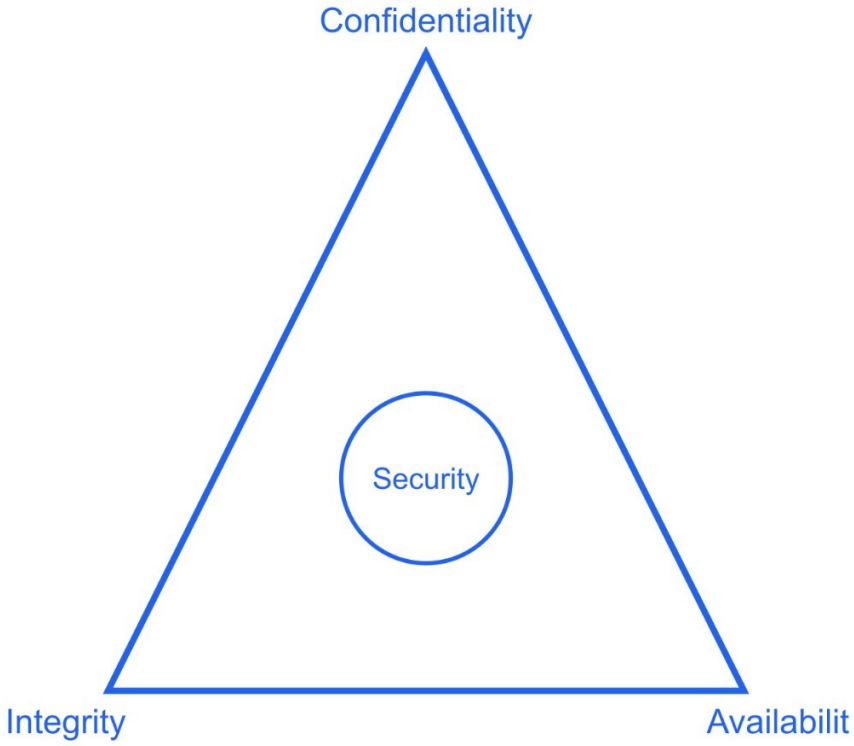
The concept of risk management underpins many information security practices. It involves identifying potential threats and vulnerabilities, assessing their potential impact, and implementing appropriate controls to mitigate risks to an acceptable level.

Security metrics and measurements are important for evaluating the effectiveness of security controls and demonstrating compliance with regulations. These might include key performance indicators (KPIs) such as mean time to detect (MTTD) or mean time to respond (MTTR) for security incidents.

The principle of fail-safe defaults ensures that when a system fails, it does so in a secure state. For example, if an authentication system fails, it should deny access rather than grant it by default.

Finally, the concept of privacy by design emphasizes the importance of considering privacy implications throughout the entire system development lifecycle, rather than as an afterthought. This approach helps organizations comply with data protection regulations and build trust with their customers and stakeholders.

CIA Triad and Security Governance



The CIA triad and security governance are fundamental concepts in information security that provide a framework for protecting an organization's assets and ensuring the effectiveness of its security program.

The CIA triad consists of three core principles: Confidentiality, Integrity, and Availability. These principles form the foundation of information security and guide the development of security policies and controls.

Confidentiality refers to the protection of sensitive information from unauthorized access or disclosure. This principle ensures that data is only accessible to those who have the right to view it. Techniques to maintain confidentiality include encryption, access controls, and

secure communication protocols. For example, a healthcare organization might use encryption to protect patient records during transmission and implement strict access controls to ensure only authorized personnel can view sensitive medical information.

Integrity focuses on maintaining the accuracy and consistency of data throughout its lifecycle. This principle ensures that information remains unaltered by unauthorized parties and that any changes are detectable. Methods to preserve integrity include digital signatures, checksums, and version control systems. For instance, a financial institution might use digital signatures to verify the authenticity of transactions and implement checksums to detect any unauthorized modifications to financial records.

Availability ensures that information and resources are accessible to authorized users when needed. This principle is crucial for maintaining business operations and user productivity. Techniques to ensure availability include redundancy, load balancing, and disaster recovery planning. An e-commerce company, for example, might implement redundant servers and load balancers to ensure their website remains accessible during high-traffic periods or in the event of hardware failures.

Security governance provides the structure and oversight necessary to implement and maintain an effective information security program. It involves aligning security strategies with business objectives, managing risks, and ensuring compliance with relevant laws and regulations.

One key aspect of security governance is the establishment of a clear organizational structure for security management. This typically includes defining roles and responsibilities, such as appointing a Chief Information Security Officer (CISO) to oversee the security program. The CISO is responsible for developing and implementing security

policies, managing security operations, and reporting to senior management on the organization's security posture.

Security policies play a crucial role in governance by providing guidelines for acceptable use of information systems, data handling procedures, and security requirements. These policies should be regularly reviewed and updated to address new threats and changes in the business environment. For example, a company might have policies covering password requirements, data classification, and incident response procedures.

Risk management is an integral part of security governance. This involves identifying potential threats and vulnerabilities, assessing their potential impact on the organization, and implementing appropriate controls to mitigate risks. Regular risk assessments help organizations prioritize their security efforts and allocate resources effectively.

Compliance management ensures that the organization adheres to relevant laws, regulations, and industry standards. This might include regulations such as the General Data Protection Regulation (GDPR) for data privacy or industry-specific standards like the Payment Card Industry Data Security Standard (PCI DSS) for organizations handling credit card information. Compliance management involves regular audits, documentation of security practices, and reporting to regulatory bodies as required.

Security awareness and training programs are essential components of governance, ensuring that all employees understand their role in maintaining the organization's security. This might include regular training sessions on topics such as identifying phishing emails, proper handling of sensitive information, and reporting security incidents.

Incident management and response planning are critical aspects of security governance. Organizations should have

well-defined procedures for detecting, responding to, and recovering from security incidents. This includes establishing an incident response team, defining communication protocols, and regularly testing response plans through simulations or tabletop exercises.

Performance measurement and reporting are necessary to evaluate the effectiveness of the security program and demonstrate its value to stakeholders. This might involve tracking key performance indicators (KPIs) such as the number of security incidents, time to detect and respond to threats, and compliance with security policies.

Third-party risk management is an increasingly important aspect of security governance, as organizations often rely on vendors and partners who may have access to sensitive information or systems. This involves assessing the security practices of third parties, establishing contractual security requirements, and monitoring their compliance.

Continuous improvement is a key principle of security governance. As the threat landscape evolves and new technologies emerge, organizations must regularly review and update their security practices. This might involve conducting regular security assessments, staying informed about new threats and vulnerabilities, and adapting security controls as needed.

Legal and Regulatory Issues

Legal and regulatory issues play a crucial role in shaping the information security landscape, imposing requirements on organizations to protect sensitive data and maintain privacy. Understanding and complying with these laws and regulations is essential for organizations to avoid legal penalties, maintain customer trust, and protect their reputation.

One of the most significant regulations in recent years is the General Data Protection Regulation (GDPR), which came into effect in the European Union in 2018. GDPR sets strict requirements for the collection, processing, and storage of personal data of EU residents. It introduces concepts such as the right to be forgotten, data portability, and mandatory breach notification. Organizations must obtain explicit consent from individuals before collecting their data and implement appropriate security measures to protect this information. Non-compliance with GDPR can result in substantial fines of up to 4% of global annual turnover or €20 million, whichever is higher.

In the United States, various sector-specific laws govern data protection and privacy. The Health Insurance Portability and Accountability Act (HIPAA) sets standards for protecting patient health information in the healthcare industry. HIPAA requires healthcare providers, insurers, and their business associates to implement safeguards to ensure the confidentiality, integrity, and availability of protected health information (PHI). Violations of HIPAA can lead to significant fines and reputational damage.

The Gramm-Leach-Bliley Act (GLBA) applies to financial institutions and requires them to explain their information-sharing practices to customers and protect sensitive data. The act mandates that financial institutions implement comprehensive information security programs and regularly assess and address risks to customer information.

The Sarbanes-Oxley Act (SOX) focuses on corporate governance and financial reporting for public companies. While not specifically a cybersecurity law, SOX has implications for information security as it requires companies to maintain effective internal controls over financial reporting, which often involves IT systems and data protection measures.

The California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), provide California residents with enhanced privacy rights and consumer protection. These laws give consumers the right to know what personal information is being collected about them, the right to delete this information, and the right to opt-out of the sale of their personal information. While these are state laws, they have far-reaching implications for businesses operating in California or dealing with California residents' data.

The Payment Card Industry Data Security Standard (PCI DSS) is not a law but an industry standard that applies to all organizations that handle credit card information. It sets out specific security requirements to protect cardholder data, including encryption, access controls, and regular security testing. While not legally binding, many contracts between merchants and payment processors require compliance with PCI DSS.

The Federal Information Security Management Act (FISMA) applies to federal agencies and their contractors, mandating the development and implementation of agency-wide information security programs. FISMA requires agencies to categorize their information systems based on risk levels and implement appropriate security controls.

Internationally, many countries have their own data protection laws. For example, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) sets rules for how private sector organizations collect, use, and disclose personal information. Australia's Privacy Act 1988 and subsequent amendments regulate the handling of personal information by government agencies and private sector organizations.

The Children's Online Privacy Protection Act (COPPA) in the United States imposes certain requirements on operators of

websites or online services directed to children under 13 years of age. It regulates the collection and use of personal information from children, requiring parental consent and implementing measures to protect children's privacy online.

Intellectual property laws, such as copyright, patent, and trademark laws, also have implications for information security. Organizations must ensure they respect intellectual property rights and implement measures to protect their own intellectual property from theft or unauthorized use.

Export control regulations, such as the U.S. Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR), place restrictions on the export of certain technologies, including encryption software. Organizations dealing with controlled technologies must implement appropriate security measures and obtain necessary licenses.

As the digital landscape continues to evolve, new laws and regulations are being introduced to address emerging technologies and threats. For example, the Internet of Things (IoT) Cybersecurity Improvement Act in the U.S. aims to establish security standards for IoT devices used by federal agencies. Similarly, various jurisdictions are developing regulations around artificial intelligence and machine learning to address privacy and ethical concerns.

Professional Ethics

Professional ethics in information security is a critical aspect of maintaining trust, integrity, and accountability in the field. It encompasses a set of moral principles and standards that guide the behavior of security professionals in their daily work and decision-making processes.

One of the fundamental ethical principles in information security is confidentiality. Security professionals often have

access to sensitive information about their organizations, clients, and individuals. They must maintain strict confidentiality and not disclose this information to unauthorized parties. This principle extends beyond just technical data to include business strategies, personal information, and any other sensitive details encountered in the course of their work.

Integrity is another cornerstone of professional ethics in information security. This involves being honest and truthful in all professional interactions and communications. Security professionals must provide accurate information about security risks, vulnerabilities, and incidents, even when doing so might be uncomfortable or potentially damaging to their organization's reputation. They should resist pressure to downplay or conceal security issues and always strive to present an accurate picture of the security landscape.

The principle of due care and due diligence is crucial in information security ethics. Professionals have a responsibility to stay current with the latest security trends, threats, and best practices. They should continuously update their knowledge and skills to ensure they can provide the best possible protection for their organizations. This includes pursuing relevant certifications, attending conferences, and engaging in ongoing professional development activities.

Respect for privacy is an essential ethical consideration, especially given the vast amounts of personal data that organizations collect and process. Security professionals must balance the need for security with individuals' right to privacy. This involves implementing privacy-enhancing technologies, advocating for data minimization practices, and ensuring compliance with relevant privacy laws and regulations.

The ethical use of security tools and techniques is another important aspect. While security professionals often have access to powerful tools that can be used to test and assess systems, these tools must be used responsibly and only with proper authorization. Engaging in unauthorized penetration testing or using security tools for personal gain or curiosity is a serious ethical breach.

Conflict of interest is a significant ethical concern in the information security field. Professionals must be aware of potential conflicts and disclose them when they arise. For example, a security consultant should not recommend products or services from companies in which they have a financial interest without full disclosure.

Professionalism and respect for colleagues and clients are essential ethical principles. This includes treating others with respect, avoiding discriminatory behavior, and maintaining a professional demeanor in all interactions. Security professionals should also respect the work and contributions of others in the field, giving credit where it's due and avoiding plagiarism or unauthorized use of others' work.

The principle of non-maleficence, or "do no harm," is particularly relevant in information security. While security testing and incident response may sometimes require actions that could potentially disrupt systems or services, professionals must always strive to minimize harm and avoid unnecessary damage or disruption.

Ethical reporting of vulnerabilities and security issues is a critical responsibility. When security professionals discover vulnerabilities in systems or products, they have an ethical obligation to report these issues through appropriate channels. This often involves following responsible disclosure practices, giving vendors or organizations time to address the issues before public disclosure.

Social responsibility is an increasingly important ethical consideration in information security. Professionals should consider the broader societal impacts of their work and strive to use their skills and knowledge for the greater good. This might involve volunteering for non-profit organizations, participating in cybersecurity education initiatives, or advocating for policies that enhance overall cybersecurity.

Ethical decision-making in complex situations is a skill that security professionals must develop. They often face situations where different ethical principles may conflict, requiring careful consideration and balanced judgment. For example, the need for transparency might conflict with the requirement to maintain confidentiality in certain situations.

Whistleblowing is a challenging ethical issue in information security. Professionals may encounter situations where they become aware of unethical or illegal practices within their organizations. They must carefully consider their ethical obligations to report such issues, balancing this against potential personal and professional risks.

Ethical considerations in emerging technologies, such as artificial intelligence and machine learning in cybersecurity, present new challenges. Security professionals must grapple with issues like algorithmic bias, privacy implications of big data analytics, and the ethical use of automated decision-making systems. As AI and machine learning become more prevalent in cybersecurity tools and processes, security professionals must consider the following ethical issues:

1. Algorithmic bias: AI systems can inadvertently perpetuate or amplify biases present in their training data or algorithms. Security professionals must work to identify and mitigate these biases to ensure fair and equitable security practices.

2. Privacy concerns: Machine learning models often require large datasets to function effectively. Security professionals must balance the need for data with individuals' privacy rights, ensuring that data collection and analysis comply with relevant regulations and ethical standards.
3. Transparency and explainability: Many AI and machine learning models operate as "black boxes," making it difficult to understand how they arrive at decisions. Security professionals should strive for transparency in AI-driven security systems and be able to explain their functioning to stakeholders.
4. Accountability: As AI systems take on more decision-making roles in cybersecurity, questions of accountability arise. Security professionals must establish clear lines of responsibility for AI-driven decisions and their consequences.
5. Job displacement: The increasing use of AI in cybersecurity may lead to job displacement for some security professionals. The ethical implications of this shift must be considered, including retraining and reskilling opportunities for affected workers.
6. Autonomous systems: As AI-powered security systems become more autonomous, security professionals must grapple with the ethical implications of machines making critical security decisions without human intervention.
7. Dual-use concerns: AI and machine learning technologies developed for cybersecurity purposes may have potential malicious applications. Security professionals must consider the ethical implications of their work and take steps to prevent misuse.

8. Ethical hacking and penetration testing: The use of AI in offensive security testing raises questions about the boundaries of ethical hacking and the potential for unintended consequences.
9. Data retention and deletion: Security professionals must consider the ethical implications of storing large amounts of data for AI and machine learning purposes, including data retention policies and the right to be forgotten.
10. Informed consent: When collecting and analyzing data for AI-driven security systems, security professionals must ensure that individuals are properly informed about how their data will be used and have given meaningful consent.
11. Cross-border data flows: The global nature of cybersecurity and AI technologies raises questions about data sovereignty and the ethical implications of transferring data across national borders.
12. Ethical decision-making frameworks: Security professionals should work to develop and implement ethical frameworks for AI and machine learning in cybersecurity, ensuring that these technologies are deployed in a manner consistent with organizational and societal values.

By addressing these ethical considerations, security professionals can help ensure that the integration of AI and machine learning into cybersecurity practices aligns with ethical principles and promotes trust in these emerging technologies.

Security Policies, Standards, and Procedures

Security policies, standards, and procedures form the foundation of an organization's information security program. These documents provide guidance, set expectations, and define requirements for protecting information assets.

Security policies are high-level statements of management intent that define the overall security goals and objectives of an organization. They provide a framework for making decisions about security and set the tone for the organization's security culture. Key characteristics of effective security policies include:

- Alignment with business objectives and risk appetite
- Clear definition of roles and responsibilities
- Approval and support from senior management
- Regular review and updates
- Concise and easy to understand language
- Enforceable and realistic requirements

Some common types of security policies include:

- Acceptable Use Policy: Defines appropriate use of IT systems and data
- Information Classification Policy: Establishes data classification levels and handling requirements
- Access Control Policy: Specifies access management principles and procedures

- Incident Response Policy: Outlines the process for responding to security incidents
- Business Continuity Policy: Defines the approach for maintaining critical operations during disruptions

Security standards provide specific, mandatory rules that support the implementation of security policies. They define minimum baseline requirements and technical specifications. For example, a password standard may specify minimum length, complexity, and expiration requirements. Standards help ensure consistency across the organization.

Security procedures are step-by-step instructions for performing specific security-related tasks or processes. They provide the operational details for implementing policies and standards. Procedures should be clear, concise and regularly updated to reflect changes in technology or processes.

The hierarchy of these documents is typically:

Policies (high-level) > Standards (specific rules) > Procedures (detailed steps)

When developing security policies, standards and procedures, organizations should:

- Involve key stakeholders from across the business
- Align with industry regulations and best practices
- Consider the organization's risk profile and tolerance
- Make documents easily accessible to employees
- Provide training on key policies and procedures
- Establish a process for regular review and updates
- Ensure policies are enforceable and violations have consequences

Effective implementation requires:

- Leadership support and setting the right "tone at the top"
- Integration into business processes and daily operations
- Ongoing security awareness training for all employees
- Monitoring and measurement of policy compliance
- A process for exceptions with appropriate approvals
- Regular audits and assessments

Some key policy areas organizations should address include:

- Information classification and handling
- Access control and identity management
- Network security and remote access
- Physical security and environmental controls
- Human resources security (e.g. background checks)
- Asset management
- Cryptography
- Third party security
- Incident management
- Business continuity and disaster recovery

Organizations may also develop topic-specific policies for areas like mobile device security, cloud computing, social media use, etc. The specific policies needed depend on the organization's risk profile and regulatory requirements.

Policies should be written in clear, concise language avoiding technical jargon. They should focus on the "what" rather than the "how". Standards and procedures can provide more technical details on implementation.

Regular review and updates are critical as threats, technologies and business needs evolve. Many organizations review policies annually and update as needed. Major changes in the business or threat landscape may require more frequent updates.

Proper documentation and version control of policies is important. Many organizations use a policy management system to maintain policies and track employee acknowledgements.

Policy exceptions should be formally documented, approved by management, and regularly reviewed. Too many exceptions may indicate the policy needs to be updated.

Measuring policy effectiveness can be challenging but is important. Some approaches include:

- Compliance audits and assessments
- Security metrics and KPIs
- Incident and near-miss analysis
- Employee surveys and feedback
- Benchmarking against industry peers

Overall, well-crafted and consistently enforced security policies, standards and procedures are essential for establishing clear expectations, driving secure behaviors, and protecting an organization's information assets. They provide the foundation for an effective information security program.

Risk Management Concepts

Risk management is a critical component of information security and involves identifying, assessing, and mitigating risks to an organization's assets and operations. The goal is to reduce risk to an acceptable level in a cost-effective manner.

Key risk management concepts include:

1. Asset: Anything of value to the organization (e.g. data, systems, people, facilities)
2. Threat: A potential cause of an unwanted event that may result in harm to a system or organization
3. Vulnerability: A weakness that can be exploited by a threat
4. Risk: The potential for loss or damage when a threat exploits a vulnerability

5. Impact: The magnitude of harm that could be caused by a threat exploiting a vulnerability
6. Likelihood: The probability of a threat exploiting a vulnerability

The risk management process typically involves the following steps:

1. Asset Identification and Valuation: Identify and catalog critical assets and determine their value to the organization.
2. Threat Assessment: Identify potential threats to assets, both internal and external.
3. Vulnerability Assessment: Identify and analyze weaknesses in systems, processes, and controls that could be exploited by threats.
4. Risk Assessment: Analyze the likelihood and potential impact of identified risks. This can be done using qualitative or quantitative methods.
5. Risk Treatment: Determine how to address identified risks through various strategies:
    - Risk Avoidance: Eliminate the risk by removing the asset or related process
    - Risk Mitigation: Implement controls to reduce the likelihood or impact of the risk
    - Risk Transfer: Shift the risk to another party (e.g. through insurance)
    - Risk Acceptance: Acknowledge and accept the risk if it falls within the organization's risk tolerance
6. Monitoring and Review: Continuously monitor risks and the effectiveness of controls, adjusting as needed.

Risk assessment can be performed using qualitative or quantitative methods:

Qualitative Risk Assessment:

- Uses descriptive scales (e.g. high, medium, low) to rate likelihood and impact
- Based on expert judgment and experience
- Faster and easier to perform, but less precise
- Useful for prioritizing risks and identifying areas for further analysis

Quantitative Risk Assessment:

- Uses numerical values to calculate risk
- More precise but requires more data and effort
- Allows for cost-benefit analysis of controls
- Key formulas include:
    - Single Loss Expectancy (SLE) = Asset Value x Exposure Factor
    - Annual Rate of Occurrence (ARO) = Expected frequency of loss event per year
    - Annual Loss Expectancy (ALE) = SLE x ARO

Many organizations use a hybrid approach, combining qualitative and quantitative methods.

Risk management frameworks and standards provide structured approaches to managing risk. Some common ones include:

- ISO 31000: Provides principles and guidelines for risk management
- NIST Risk Management Framework: Integrates risk management into the system development lifecycle
- COSO ERM: Focuses on enterprise risk management

- FAIR (Factor Analysis of Information Risk): Quantitative model for information security risk

Key risk management concepts also include:

Inherent Risk: The level of risk before any controls are applied

Residual Risk: The level of risk remaining after controls are implemented

Risk Appetite: The amount and type of risk an organization is willing to accept in pursuit of its objectives

Risk Tolerance: The acceptable variation relative to the achievement of objectives

Risk Register: A document used to record identified risks, their assessment, and treatment plans

Risk Owner: The person or entity responsible for managing a particular risk

Control: A measure that modifies risk (e.g. policies, procedures, technical solutions)

Effective risk management requires:

- Strong governance and leadership support
- Integration into business processes and decision-making
- Clear communication of risks to stakeholders
- Regular review and updates to risk assessments
- A culture of risk awareness throughout the organization

Challenges in risk management include:

- Accurately quantifying risks, especially for intangible assets

- Keeping pace with evolving threats and technologies
- Balancing security with business needs and usability
- Managing risks in complex, interconnected systems
- Addressing risks from third-party vendors and partners

Emerging areas in risk management include:

- Cyber insurance to transfer certain information security risks
- Artificial intelligence and machine learning for risk analysis
- Integration of security and privacy risk management
- Managing risks related to cloud computing and IoT devices

Overall, effective risk management is essential for organizations to make informed decisions about protecting their assets and achieving their objectives in the face of uncertainty and evolving threats.

Threat Modeling

Threat modeling is a structured approach to identifying, quantifying, and addressing security risks associated with an application, system, or business process. It is an essential practice in secure system design and risk management, allowing organizations to proactively identify and mitigate potential security threats.

Key components of threat modeling include:

1. Asset Identification: Determine what needs to be protected (e.g. data, systems, processes)
2. System Decomposition: Break down the system into its components and understand data flows
3. Threat Identification: Identify potential threats to the system and its assets
4. Vulnerability Analysis: Identify weaknesses that could be exploited by threats
5. Risk Assessment: Evaluate the likelihood and impact of identified threats
6. Mitigation Strategies: Develop and prioritize countermeasures to address risks

Common threat modeling methodologies include:

STRIDE: Developed by Microsoft, STRIDE categorizes threats into six types:

- Spoofing: Impersonating something or someone else
- Tampering: Modifying data or code
- Repudiation: Claiming to have not performed an action
- Information Disclosure: Exposing information to unauthorized individuals
- Denial of Service: Denying service to valid users
- Elevation of Privilege: Gaining capabilities without proper authorization

DREAD: Another Microsoft model used to quantify, compare and prioritize the amount of risk presented by each evaluated threat. It considers:

- Damage potential

- Reproducibility
- Exploitability
- Affected users
- Discoverability

PASTA (Process for Attack Simulation and Threat Analysis): A risk-centric methodology that aligns business objectives with technical requirements.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Focuses on organizational risk and strategic, practice-related issues.

TRIKE: A conceptual framework for security auditing from a risk management perspective.

VAST (Visual, Agile, and Simple Threat modeling): Emphasizes scalability and integration into an Agile development process.

The threat modeling process typically involves the following steps:

1. Define the Scope: Determine what is being modeled and the objectives of the analysis.
2. Create a System Model: Develop a high-level overview of the system, including its components, data flows, and trust boundaries.
3. Identify Threats: Use techniques like brainstorming, threat libraries, or methodologies like STRIDE to identify potential threats.
4. Analyze Threats: Evaluate the likelihood and potential impact of each identified threat.
5. Mitigate Risks: Develop strategies to address identified threats, such as implementing security controls or redesigning parts of the system.

6. Validate: Review the threat model and mitigation strategies for completeness and effectiveness.
7. Document and Communicate: Record findings and share with relevant stakeholders.

Threat modeling tools can assist in the process, such as:

- Microsoft Threat Modeling Tool
- OWASP Threat Dragon
- IriusRisk
- ThreatModeler

Best practices for effective threat modeling include:

- Start early in the development lifecycle
- Involve cross-functional teams (developers, security experts, business stakeholders)
- Focus on assets and business impact, not just technical vulnerabilities
- Use a consistent, repeatable process
- Update models as the system evolves or new threats emerge
- Integrate with other security practices (e.g. penetration testing, code review)

Challenges in threat modeling include:

- Keeping models up-to-date as systems change
- Balancing depth of analysis with time and resource constraints
- Addressing complex, interconnected systems
- Quantifying and prioritizing risks
- Integrating threat modeling into fast-paced development processes

Emerging trends in threat modeling include:

- Automated threat modeling tools using AI/ML
- Cloud-specific threat modeling techniques
- Threat modeling for IoT and embedded systems
- Integration with DevSecOps practices
- Threat modeling for privacy risks

Threat modeling for specific domains:

Application Security: Focus on identifying threats to web and mobile applications, such as injection attacks, cross-site scripting, and insecure authentication.

Network Security: Model threats to network infrastructure, including unauthorized access, denial of service attacks, and man-in-the-middle attacks.

Cloud Security: Address threats specific to cloud environments, such as data breaches, account hijacking, and shared technology vulnerabilities.

IoT Security: Consider threats to connected devices and their ecosystems, including device tampering, data privacy issues, and botnet recruitment.

Overall, threat modeling is a powerful technique for proactively identifying and addressing security risks. When integrated into the development lifecycle and risk management processes, it can significantly improve an organization's security posture and resilience against evolving threats.

Business Continuity Planning

Business Continuity Planning (BCP) is a proactive process that helps organizations prepare for, respond to, and recover from disruptive events. The goal is to ensure that critical business functions can continue during and after a disaster or major disruption, minimizing downtime and financial losses.

Key components of a Business Continuity Plan include:

1. Business Impact Analysis (BIA): Identifies critical business functions and the potential impact of their disruption. Key elements include:
    - Recovery Time Objective (RTO): The maximum acceptable time to restore a business function
    - Recovery Point Objective (RPO): The maximum acceptable data loss measured in time
    - Maximum Tolerable Downtime (MTD): The longest time a business function can be unavailable without causing significant harm
2. Risk Assessment: Identifies potential threats and vulnerabilities that could disrupt business operations.

3. Business Continuity Strategies: Develops approaches to maintain critical functions during a disruption. This may include:
    - Alternate work sites
    - Remote work capabilities
    - Data backup and recovery systems
    - Redundant IT infrastructure
    - Supply chain diversification
4. Incident Response Plan: Outlines immediate actions to be taken during a disruptive event.
5. Recovery Plans: Detailed procedures for restoring business functions and IT systems.
6. Communication Plan: Procedures for notifying and updating stakeholders during a disruption.
7. Testing and Exercises: Regular drills and simulations to validate the effectiveness of the plan.
8. Plan Maintenance: Ongoing review and updates to keep the plan current.

The BCP development process typically involves:

1. Project Initiation: Gain management support, define scope, and assemble a BCP team.
2. Business Impact Analysis: Identify critical functions, dependencies, and impact of disruptions.
3. Recovery Strategy Development: Determine strategies to maintain or quickly resume critical functions.
4. Plan Development: Create detailed procedures for response and recovery.
5. Testing and Training: Conduct exercises and train personnel on their roles.

6. Plan Maintenance: Regularly review and update the plan.

Types of Business Continuity Tests:

- Tabletop Exercises: Discussion-based sessions where team members walk through their responses to various scenarios.
- Walkthrough Test: Physical rehearsal of specific recovery procedures.
- Simulation Test: Full-scale exercise that mimics a real disaster scenario.
- Parallel Test: Recovery systems are activated alongside primary systems.
- Full Interruption Test: Primary systems are shut down and recovery systems are fully activated.

Key considerations for effective Business Continuity Planning:

- Senior Management Support: Ensure leadership commitment and resource allocation.
- Cross-functional Involvement: Include representatives from all critical business areas.
- Regular Testing and Updates: Conduct exercises at least annually and update plans as needed.
- Clear Roles and Responsibilities: Define who does what during a disruption.
- Vendor Management: Assess and plan for disruptions to critical vendors and partners.
- Communication Strategies: Develop multi-channel approaches for internal and external communication.

- Data Backup and Recovery: Implement robust backup systems with off-site storage.
- Compliance Requirements: Ensure the plan meets relevant regulatory standards.

Challenges in Business Continuity Planning:

- Keeping plans up-to-date as the business evolves
- Balancing cost of preparedness with potential risks
- Addressing complex, interdependent systems and processes
- Managing global operations with diverse regulatory requirements
- Maintaining employee awareness and readiness

Emerging trends in Business Continuity:

- Cloud-based recovery solutions
- Integration with cybersecurity incident response
- AI and machine learning for predictive analysis and automated response
- Mobile apps for BCP access and communication
- Increased focus on supply chain resilience

Related concepts:

Disaster Recovery (DR): Often considered a subset of BCP, DR focuses specifically on restoring IT systems and infrastructure after a disruption.

Crisis Management: Addresses the broader organizational response to a disruptive event, including public relations and stakeholder management.

IT Service Continuity Management (ITSCM): Part of ITIL, focuses on managing risks that could seriously impact IT services.

Operational Resilience: A broader concept that encompasses BCP, focusing on an organization's ability to adapt to and recover from any type of disruption.

Standards and frameworks related to Business Continuity include:

- ISO 22301: International standard for Business Continuity Management Systems
- NIST SP 800-34: Contingency Planning Guide for Federal Information Systems
- NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs
- FFIEC Business Continuity Planning Booklet: Guidance for financial institutions
- COBIT 5: Framework that includes business continuity management
- ITIL: Includes IT Service Continuity Management as part of Service Design

Key benefits of implementing a formal Business Continuity Management System include:

- Improved organizational resilience
- Faster recovery times after disruptions
- Reduced financial impact of incidents
- Enhanced stakeholder confidence
- Compliance with legal and regulatory requirements

To be effective, Business Continuity Planning must be an ongoing process that is regularly tested, reviewed, and updated. It requires commitment from senior management and should be integrated into the organization's overall risk management strategy.

Chapter 2: Asset Security

Asset security forms a critical foundation for protecting an organization's valuable resources and information. This domain focuses on the proper identification, classification, and protection of assets throughout their lifecycle. Organizations must implement robust processes to inventory and categorize their assets, assign appropriate ownership and access controls, and ensure proper handling from creation through disposal.

Key aspects of asset security include developing comprehensive asset inventories, implementing data classification schemes, defining clear ownership and custodianship roles, and establishing policies for securely managing assets. Organizations need to balance security controls with business needs, implementing protection measures commensurate with an asset's value and sensitivity. Privacy considerations are also paramount, especially for personally identifiable information and other regulated data types.

Proper data retention and destruction practices are essential to minimize risks. Organizations must have processes to securely store data for required periods and then properly dispose of it when no longer needed. This includes securely erasing electronic media and physically destroying assets containing sensitive information.

Asset handling requirements provide guidance on how different types of assets should be used, stored, transmitted, and protected based on their classification level. This ensures consistent security practices are applied across the organization.

By implementing a comprehensive asset security program aligned with business objectives and risk tolerance, organizations can more effectively safeguard their critical information and resources. The following sections explore key elements of asset security in more detail.

Information and Asset Classification

Classification	Characteristics
Restricted	• Highest sensitivity • Severe impact if disclosed
Confidential	• Business sensitive • Limited distribution
Internal Use	• Day-to-day operations • Staff access only
Public	• No restrictions • Approved for release

Information and asset classification provide a structured approach for organizations to identify and categorize their assets based on value, sensitivity, and criticality. This process allows appropriate security controls to be applied to protect assets commensurate with their importance to the organization.

The first step in classification is to conduct a thorough asset inventory. This involves identifying and documenting all

information assets, including data, systems, applications, hardware, and other resources. The inventory should capture key details like asset type, owner, location, and purpose.

Once assets are inventoried, they can be classified into defined categories. Common classification levels for commercial organizations include:

Public: Information that can be freely shared externally with no adverse impact if disclosed.

Internal Use Only: Information intended for use within the organization but not highly sensitive. Unauthorized disclosure may cause minor damage.

Confidential: Sensitive information that if disclosed could negatively impact the organization's competitive position, finances, or reputation.

Restricted: Highly sensitive information that if compromised could cause severe damage to the organization. Access is limited to a small number of authorized individuals.

Military and government organizations typically use classification levels like Unclassified, Confidential, Secret, and Top Secret. The specific levels used should align with the organization's needs and risk tolerance.

When classifying assets, several factors should be considered:

Value: The asset's importance to business operations and potential impact if compromised.

Sensitivity: The level of protection required based on privacy, legal, or contractual obligations.

Criticality: How essential the asset is for business continuity.

Regulations: Any relevant laws or industry standards that mandate certain handling requirements.

The data owner is typically responsible for determining the appropriate classification level, with input from relevant stakeholders. Classification decisions should be documented and periodically reviewed as sensitivity may change over time.

Proper labeling is crucial to ensure assets are easily identifiable and handled appropriately. Labels should clearly indicate the classification level and any special handling instructions. For electronic documents, this may involve metadata tags or visual markings. Physical assets may require tamper-evident labels.

Classification schemes should be formally defined in organizational policies and procedures. These should outline the classification levels, criteria for assigning levels, roles and responsibilities, labeling requirements, and handling procedures for each level. Regular training helps ensure employees understand and adhere to classification policies.

It's important to strike a balance with classification. Over-classifying assets can lead to unnecessary restrictions and costs, while under-classification leaves sensitive information vulnerable. The goal is to apply appropriate protections without overly impeding business operations.

Automated tools can assist with discovering and classifying large volumes of data, especially unstructured data stored across various repositories. However, human review is still important to validate classifications and handle edge cases.

As the volume and variety of data grows, many organizations are moving towards more granular data classification rather than broad categories. This allows for more precise application of security controls. For example, specific fields within a database may be classified and protected differently based on sensitivity.

Regular audits should be conducted to verify assets are properly classified and labeled. This helps identify any gaps

or inconsistencies in the classification process. Audits may involve manual spot checks as well as automated scans to detect potentially misclassified information.

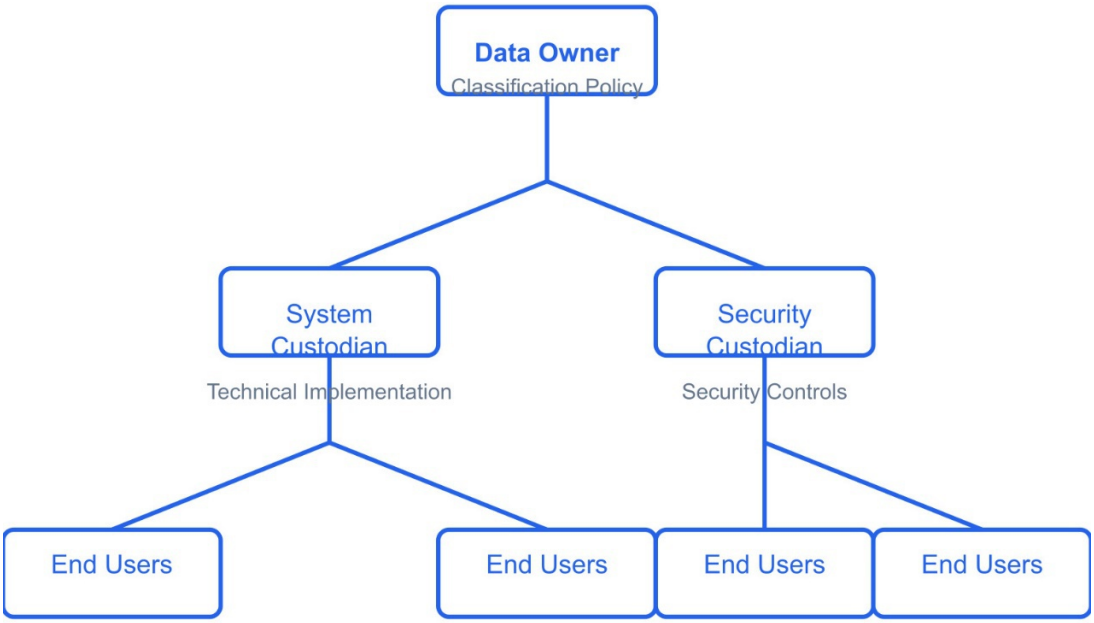
Classification also plays a key role in access control by defining who should have access to what information. Role-based access control can be aligned with classification levels to streamline permissions management.

When sharing information with external parties, the classification level helps determine what protections are required, such as encryption or confidentiality agreements. De-classification and downgrading processes should be defined for when assets no longer require their original level of protection.

Proper classification is essential for effective data loss prevention. DLP tools can be configured to monitor and control the flow of sensitive information based on classification tags.

Overall, a well-designed classification program provides the foundation for applying appropriate security controls across the organization. It enables more efficient and consistent protection of information assets aligned with their business value and sensitivity.

Ownership and Data Security Controls



Establishing clear ownership and implementing robust data security controls are essential components of an effective asset security program. This ensures accountability for protecting information assets and applies appropriate safeguards based on classification and risk.

Data ownership refers to assigning responsibility for specific information assets to designated individuals or groups within the organization. The data owner is typically a senior manager or executive in the business unit most closely associated with the information. Key responsibilities of data owners include:

Determining and periodically reviewing the classification level
Defining access rights and privileges
Ensuring appropriate security controls are in place
Approving requests for access
Reviewing access periodically to ensure it remains appropriate
Participating in risk assessments related to the data

While data owners have overall accountability, day-to-day management is often delegated to data custodians. These are typically IT staff responsible for implementing and maintaining the technical controls to protect the data. Custodian duties may include:

Implementing access controls based on owner-defined requirements
Performing backups and ensuring recoverability
Monitoring for security events and incidents
Applying patches and updates to systems hosting the data
Providing reports on access and usage to data owners

Users granted access to data also have responsibilities for proper handling and protection in line with its classification. This should be clearly communicated through policies, procedures, and regular security awareness training.

Data security controls encompass the full range of administrative, technical, and physical safeguards implemented to protect information confidentiality, integrity, and availability. Controls should be selected and applied based on the asset's classification level and associated risks.

Common data security controls include:

Access Control: Restricting data access to authorized users based on the principle of least privilege. This may involve authentication mechanisms, role-based access control, and access monitoring.

Encryption: Protecting data confidentiality both at rest and in transit. Strong encryption algorithms and proper key management are essential.

Data Loss Prevention: Monitoring for and preventing unauthorized data exfiltration through various channels like email, web, or removable media.

Auditing and Logging: Recording access attempts and changes to sensitive data for detection of unauthorized activity and forensic purposes.

Backup and Recovery: Ensuring data can be restored in case of loss or corruption. This includes defining retention periods and secure off-site storage.

Physical Security: Protecting the facilities and hardware where data is stored and processed. This may include measures like access control systems, surveillance, and environmental controls.

Network Security: Implementing firewalls, intrusion detection/prevention systems, and network segmentation to protect data as it traverses networks.

Application Security: Ensuring applications that handle sensitive data have appropriate security controls built-in, such as input validation and secure coding practices.

Data Masking: Obscuring sensitive data elements in non-production environments to reduce exposure.

Database Security: Implementing controls specific to database platforms, such as encryption, access monitoring, and vulnerability management.

The specific controls applied should be commensurate with the data's classification level and value to the organization. A defense-in-depth approach using multiple complementary controls is recommended.

Regular risk assessments should be conducted to evaluate the effectiveness of existing controls and identify any gaps. This allows for continuous improvement of the data security program.

As data increasingly moves to cloud environments, additional considerations come into play. Organizations must carefully evaluate cloud provider security capabilities and implement supplementary controls where needed. Clear delineation of security responsibilities between the organization and the cloud provider is crucial.

Data discovery and classification tools can help organizations identify where sensitive data resides across their environment. This visibility is essential for applying appropriate controls, especially for unstructured data stored in various repositories.

Data security policies should clearly define roles, responsibilities, and requirements for protecting information assets. These policies should be regularly reviewed and updated to address evolving threats and business needs.

Security awareness training is crucial to ensure all employees understand their role in protecting sensitive data. This should cover topics like proper data handling, recognizing phishing attempts, and reporting security incidents.

Incident response plans should be developed and tested to enable quick and effective action in case of a data breach or other security incident. This includes defining escalation procedures and communication protocols.

Third-party risk management is an important consideration, as sensitive data is often shared with vendors and partners. Appropriate contractual clauses, security assessments, and monitoring should be implemented for third parties with access to organizational data.

Data security controls should be designed with privacy requirements in mind, especially for personally identifiable information. This includes implementing data minimization, purpose limitation, and other privacy principles.

Regular audits and assessments help verify that data security controls are functioning as intended and identify any areas for improvement. This may involve both internal audits and external compliance assessments.

Ultimately, effective data ownership and security controls require ongoing collaboration between business units, IT, security, legal, and other stakeholders. By clearly defining responsibilities and implementing appropriate safeguards, organizations can better protect their valuable information assets.

Privacy Protection

Privacy protection has become increasingly critical as organizations collect, process, and store growing volumes of personal data. Effective privacy measures not only help comply with regulations but also build trust with customers and stakeholders. Privacy protection encompasses a range of practices to ensure personal information is handled responsibly and securely throughout its lifecycle.

A fundamental principle of privacy protection is data minimization. This involves collecting and retaining only the personal information necessary for specific, legitimate business purposes. Organizations should regularly review their data collection practices to ensure they are not gathering excessive or unnecessary personal information.

Purpose limitation is another key privacy principle. Personal data should only be used for the specific purposes for which it was collected, unless explicit consent is obtained for new

uses. Clear privacy notices should inform individuals about how their data will be used and shared.

Implementing strong access controls is crucial for privacy protection. Access to personal data should be restricted to authorized personnel with a legitimate need, following the principle of least privilege. Role-based access control and regular access reviews help ensure appropriate limitations.

Data anonymization and pseudonymization techniques can enhance privacy by removing or obscuring identifying information. This allows organizations to analyze and use data while reducing privacy risks. However, care must be taken as re-identification may still be possible in some cases.

Privacy by design is an approach that incorporates privacy considerations throughout the system development lifecycle. This proactive approach helps ensure privacy protections are built into new products, services, and processes from the outset rather than added as an afterthought.

Data subject rights are a key component of many privacy regulations. Organizations must have processes in place to handle requests from individuals to access, correct, delete, or port their personal data. Timely and accurate responses to these requests are essential for regulatory compliance.

Consent management is crucial for many aspects of privacy protection. Organizations should obtain and manage consent for collecting and using personal data where required. This includes providing clear opt-in mechanisms and the ability to withdraw consent.

Data retention policies should be established to ensure personal information is not kept longer than necessary. This involves defining retention periods based on legal requirements and business needs, and securely disposing of data when it is no longer needed.

Privacy impact assessments (PIAs) are valuable tools for evaluating privacy risks associated with new projects, systems, or processes involving personal data. PIAs help identify potential privacy issues early on and inform the selection of appropriate controls.

Employee training on privacy principles and practices is essential. All staff handling personal data should understand their responsibilities for protecting privacy, including recognizing and reporting potential breaches.

Incident response plans should include procedures specific to privacy breaches. This includes processes for assessing the impact of a breach, notifying affected individuals and regulators if required, and taking steps to mitigate any harm.

When sharing personal data with third parties, organizations must ensure appropriate contractual safeguards are in place. This includes conducting due diligence on vendors' privacy practices and implementing monitoring mechanisms.

Privacy-enhancing technologies like encryption, access controls, and secure communication channels play a crucial role in protecting personal data from unauthorized access or disclosure.

Regular privacy audits help verify compliance with internal policies and external regulations. These audits may involve reviewing data handling practices, access controls, consent mechanisms, and other privacy-related processes.

Cross-border data transfers require special attention due to varying privacy regulations in different jurisdictions. Organizations must ensure appropriate safeguards are in place when transferring personal data internationally, such as standard contractual clauses or binding corporate rules.

Data mapping and inventory exercises help organizations understand what personal data they hold, where it resides, and how it flows through the organization. This visibility is crucial for effective privacy management and compliance efforts.

Privacy governance structures should be established, defining roles and responsibilities for privacy management across the organization. This may include appointing a Data Protection Officer or Chief Privacy Officer to oversee privacy efforts.

Privacy policies and notices should be clear, concise, and easily accessible to individuals. These should accurately reflect the organization's data handling practices and be regularly reviewed and updated.

Privacy considerations should be incorporated into vendor management processes. This includes assessing vendors' privacy practices during selection and ongoing monitoring of their compliance with privacy requirements.

Data de-identification techniques can be valuable for using data for analytics or research while protecting individual privacy. However, the effectiveness of de-identification must be carefully evaluated given advances in re-identification techniques.

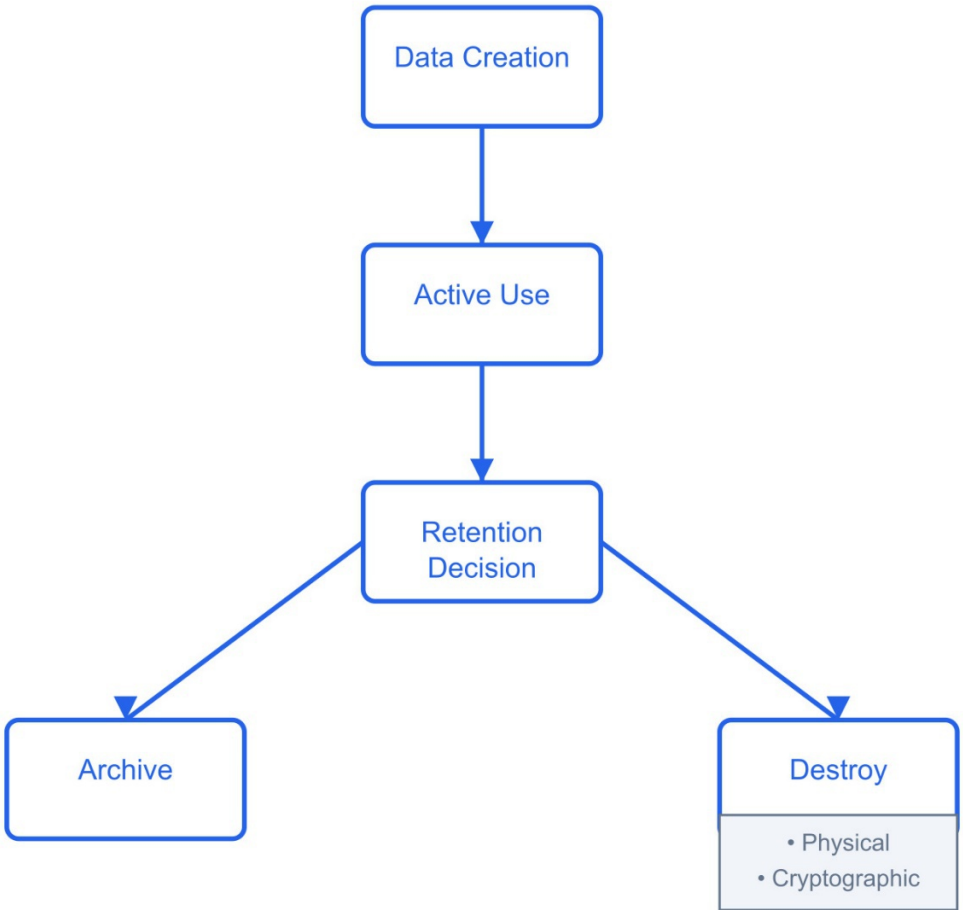
Privacy-preserving computation techniques, such as homomorphic encryption and secure multi-party computation, offer promising approaches for analyzing sensitive data while maintaining privacy. These advanced techniques may become more prevalent as privacy concerns grow.

Balancing privacy protection with other business objectives can be challenging. Organizations must carefully weigh privacy risks against potential benefits when considering new data uses or sharing arrangements.

As privacy regulations continue to evolve globally, organizations must stay informed about changing requirements and adapt their practices accordingly. This may involve monitoring regulatory developments and participating in industry groups focused on privacy issues.

Ultimately, effective privacy protection requires a comprehensive approach that addresses technical, organizational, and legal aspects. By implementing robust privacy practices, organizations can better protect individuals' rights, comply with regulations, and build trust with their stakeholders.

Data Retention and Destruction



Proper data retention and destruction practices are crucial components of an organization's information lifecycle management strategy. These processes help ensure compliance with legal and regulatory requirements, manage storage costs, and minimize security and privacy risks associated with retaining unnecessary data.

Data retention involves storing information for a specified period to meet business, legal, or regulatory needs. Key considerations for developing a data retention policy include:

Legal and regulatory requirements: Many industries have specific mandates for how long certain types of data must be retained. For example, financial records may need to be kept for several years to comply with tax laws.

Business needs: Some data may need to be retained to support ongoing operations, historical analysis, or potential future legal actions.

Privacy regulations: Laws like GDPR require organizations to retain personal data only as long as necessary for the purposes for which it was collected.

Storage costs: Retaining large volumes of data indefinitely can lead to significant storage and management costs.

Security risks: Keeping data longer than necessary increases the potential impact of a data breach.

A comprehensive data retention schedule should be developed, specifying retention periods for different types of data based on these factors. This schedule should be regularly reviewed and updated to reflect changing requirements and business needs.

Implementing effective data retention practices requires collaboration between legal, IT, business units, and records management teams. Clear policies and procedures should

be established to guide employees on proper data handling and retention.

Automated tools can assist with enforcing retention policies by automatically archiving or deleting data based on predefined rules. However, human oversight is still important to handle exceptions and ensure compliance.

For data stored in cloud environments, organizations must ensure their retention policies can be effectively implemented by the cloud provider. This may involve using specific features or APIs provided by the cloud platform.

Regular audits should be conducted to verify compliance with retention policies. This helps identify any gaps or inconsistencies in retention practices across the organization.

When the retention period for data expires, it must be securely destroyed to prevent unauthorized access or recovery. Simply deleting files or formatting storage media is often insufficient, as the data may still be recoverable using forensic techniques.

Secure data destruction methods include:

Physical destruction: For physical media like hard drives or tapes, this may involve shredding, crushing, or incinerating the devices.

Degaussing: Using strong magnetic fields to erase data from magnetic storage media.

Overwriting: Writing patterns of data over existing information multiple times to make it unrecoverable. The DoD 5220.22-M standard specifies a 3-pass overwrite process.

Cryptographic erasure: For encrypted data, securely destroying the encryption keys renders the data unreadable.

The appropriate destruction method depends on factors like the sensitivity of the data, the type of storage media, and any applicable regulatory requirements.

For electronic data, specialized software tools can be used to securely erase files or entire storage devices. These tools typically use multiple overwrite passes to ensure data cannot be recovered.

When disposing of physical assets like computers or mobile devices, it's crucial to ensure all storage media are properly sanitized or physically destroyed before the assets leave organizational control.

Third-party destruction services can be engaged for secure disposal of large volumes of data or specialized media. These services offer several advantages:

- Specialized equipment and expertise for securely destroying different types of media
- Documented chain of custody and certificates of destruction
- Compliance with regulatory requirements for data destruction
- Ability to handle large volumes efficiently
- On-site mobile shredding options for sensitive data

When using a third-party service, organizations should:

- Verify the service provider's credentials and security practices
- Ensure proper employee background checks and security clearances
- Review the destruction methods used and ensure they meet required standards
- Maintain an inventory of media sent for destruction

- Witness the destruction process when possible, especially for highly sensitive data
- Obtain detailed destruction certificates and documentation

For ongoing data destruction needs, organizations may want to consider implementing their own secure destruction capabilities. This could include:

- Installing industrial shredders or degaussers
- Implementing secure erase software for electronic media
- Training staff on proper data destruction procedures
- Establishing a secure area for storing media awaiting destruction
- Implementing tracking systems to maintain chain of custody

Regardless of whether destruction is handled internally or externally, organizations should have clear policies and procedures governing the entire data destruction process. This includes identifying what data requires secure destruction, approved destruction methods, documentation requirements, and verification procedures. Regular audits should be conducted to ensure destruction policies are being followed.

Proper data destruction is a critical part of the overall data lifecycle. By implementing robust destruction practices, organizations can minimize the risk of data breaches or unauthorized access to sensitive information after it is no longer needed.

Asset Handling Requirements

Asset handling requirements define how different types of assets should be used, stored, transmitted, and protected based on their classification level. These requirements ensure consistent security practices are applied across the organization to safeguard assets according to their sensitivity and value.

Key aspects of asset handling requirements include:

Access Controls: Access to assets should be restricted based on the principle of least privilege. Only authorized personnel with a legitimate business need should be granted access. This may involve:

- Physical access controls like locks, security guards, and biometric systems for physical assets
- Logical access controls like user authentication, access control lists, and encryption for digital assets

Different levels of access may be defined for various roles and responsibilities. For example, some users may have read-only access while others have full read/write permissions.

Storage Requirements: Assets must be stored securely when not in use. This could involve:

- Locked cabinets or safes for physical documents and media
- Encrypted storage for digital assets
- Off-site secure storage facilities for backups and archives

Transmission Controls: When assets need to be moved or transmitted, appropriate safeguards must be in place:

- Secure courier services for physical asset transport
- Encryption for electronic transmission of sensitive data
- Secure file transfer protocols
- Virtual private networks (VPNs) for remote access

Labeling and Marking: Assets should be clearly labeled with their classification level to ensure proper handling. This may include:

- Confidential/Secret stamps on physical documents
- Digital watermarks on electronic files
- Metadata tags indicating sensitivity level

Retention and Destruction: Policies should define how long different types of assets need to be retained and how they should be securely destroyed when no longer needed:

- Retention periods based on legal/regulatory requirements and business needs
- Secure shredding for physical documents
- Certified destruction services for electronic media
- Data wiping procedures for reusable storage devices

Auditing and Monitoring: Asset handling activities should be logged and monitored to detect unauthorized access or misuse:

- Access logs for sensitive systems and data
- Video surveillance of secure areas

- Regular audits to ensure compliance with handling procedures

Incident Reporting: Procedures should be in place for reporting any suspected loss, theft, or unauthorized disclosure of assets.

Training and Awareness: All personnel who handle sensitive assets should receive regular training on proper handling procedures and security awareness.

Third-Party Requirements: When assets need to be shared with external parties, appropriate agreements and controls must be in place to ensure they are handled securely.

Business Continuity: Critical assets should have appropriate backup and recovery procedures to ensure availability in case of disruption.

Asset handling requirements should be documented in formal policies and procedures. These should be regularly reviewed and updated to address changes in technology, business needs, and the threat landscape. Compliance with asset handling requirements should be monitored and enforced to maintain the security of the organization's valuable assets.

Different classification levels typically have different handling requirements. For example:

Public assets may have minimal restrictions on handling and distribution.

Internal/Private assets may require encryption when transmitted externally but can be freely shared within the organization.

Confidential assets may require encryption both at rest and in transit, with access restricted to specific authorized individuals.

Top Secret/Highly Confidential assets may have very strict handling requirements, such as storage in secure facilities, transmission only via approved encrypted channels, and extremely limited access.

Organizations should develop a clear matrix mapping classification levels to specific handling requirements. This ensures consistent application of controls across the enterprise.

Asset handling requirements should also consider the full lifecycle of assets, from creation or acquisition through to eventual destruction or decommissioning. At each stage, appropriate controls need to be in place.

Regular risk assessments should be conducted to evaluate the effectiveness of asset handling procedures and identify any gaps or areas for improvement. As new technologies emerge and business processes evolve, handling requirements may need to be updated.

It's important that asset handling requirements strike a balance between security and usability. Overly restrictive controls can impede business operations and may lead to users trying to circumvent security measures. Requirements should be risk-based and proportional to the sensitivity of the assets involved.

Clear accountability should be established for asset handling. Asset owners are typically responsible for defining handling requirements, while custodians are responsible for implementing and maintaining controls. End users need to understand and follow proper handling procedures in their day-to-day work.

Automated tools can help enforce and monitor asset handling requirements. For example, data loss prevention (DLP) systems can detect and prevent unauthorized transmission of sensitive data. Rights management systems can control access to and use of digital assets.

Encryption plays a key role in asset handling, especially for digital assets. Organizations should have clear policies on when encryption is required and what encryption standards should be used. Key management procedures are critical to ensure encrypted assets remain accessible when needed.

Physical asset handling is equally important. This includes secure transport procedures, proper storage facilities, and controlled disposal methods for paper documents, computer equipment, and other physical assets containing sensitive information.

Asset handling requirements should align with broader organizational policies on information security, acceptable use, and data privacy. They should also comply with any relevant legal and regulatory requirements for data protection and information handling.

Regular audits and assessments help ensure asset handling requirements are being followed consistently across the organization. This may include both internal audits and external compliance assessments.

Incident response plans should address scenarios involving improper handling or compromise of sensitive assets. This includes procedures for containing the incident, assessing the impact, and taking corrective actions.

As organizations increasingly rely on cloud services and mobile devices, asset handling requirements need to evolve to address these new paradigms. This may involve additional controls for data stored in the cloud or accessed via personal devices.

Employee training is crucial for effective implementation of asset handling requirements. All personnel who work with sensitive assets should receive regular training on proper procedures and the importance of following security protocols.

Comprehensive asset handling requirements are essential for protecting an organization's valuable information assets throughout their lifecycle. By implementing appropriate controls based on asset classification and sensitivity, organizations can significantly reduce the risk of data breaches, intellectual property theft, and other security incidents.

Chapter 3: Security Architecture and Engineering

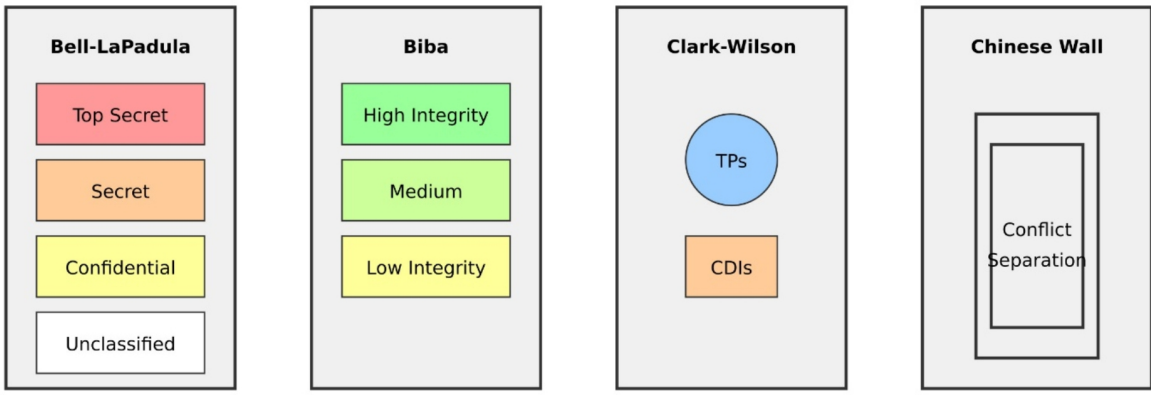
Security architecture and engineering form the foundation for designing and implementing secure systems and networks. This domain covers the fundamental models, principles, and practices used to build security into information systems from the ground up. It encompasses formal security models that provide a theoretical basis for access control and information flow, as well as practical approaches for secure system design and implementation.

Key areas include security models like Bell-LaPadula and Biba that define how subjects and objects should interact to maintain confidentiality and integrity. Evaluation models such as the Common Criteria provide frameworks for assessing the security of IT products and systems. The security capabilities of hardware, operating systems, and applications are examined, along with secure architecture principles like defense-in-depth and least privilege.

Cryptography plays a crucial role in protecting data confidentiality and integrity, so this domain covers cryptographic concepts, algorithms, and protocols. Physical security is also addressed, including facility design considerations and physical access controls.

By understanding these core concepts and principles, security professionals can architect robust systems that are inherently secure by design rather than trying to bolt on security as an afterthought. This domain provides the building blocks for creating a comprehensive security

architecture that aligns with business objectives while protecting critical assets.



Security models provide a formal, abstract representation of security policies and mechanisms. They serve as a blueprint for designing and analyzing secure systems by defining how subjects (users, processes) can access and manipulate objects (files, resources) while preserving key security properties. Some of the most influential security models include:

The Bell-LaPadula model focuses on preserving confidentiality in systems handling classified information. It enforces two key properties: the Simple Security Property, which prevents subjects from reading objects at a higher classification level (no read up), and the *-Property, which prevents subjects from writing to objects at a lower level (no write down). This model maps well to military and government classification schemes.

The Biba model addresses integrity concerns by preventing low-integrity subjects from modifying high-integrity objects.

It implements the Simple Integrity Axiom (no read down) and the *-Integrity Axiom (no write up). This helps maintain data integrity in commercial systems where preventing unauthorized modifications is critical.

The Clark-Wilson model is tailored for commercial environments and emphasizes both integrity and separation of duties. It defines constrained data items (CDIs) that can only be manipulated by certified transformation procedures (TPs). This model maps well to financial systems and other transactional environments.

The Brewer and Nash model, also known as the Chinese Wall model, addresses conflicts of interest in consulting firms and financial institutions. It dynamically adjusts access rights to prevent users from accessing information from competing companies.

The Graham-Denning model focuses on secure creation and deletion of subjects and objects, as well as granting and revoking access rights. It defines eight primitive protection operations that form the basis for securely managing system entities and their permissions.

The Harrison-Ruzzo-Ullman model examines how access rights can be passed between subjects, addressing the safety problem of determining if a subject can eventually gain unauthorized access to an object through a series of allowed operations.

Non-interference models like Goguen-Meseguer ensure that actions performed by high-level subjects do not affect what low-level subjects can observe about the system state, preventing covert channels.

While these formal models provide a theoretical foundation, real-world systems often implement a hybrid approach combining elements from multiple models to address specific security requirements.

Evaluation models provide frameworks for assessing the security of IT products and systems. The most widely recognized is the Common Criteria for Information Technology Security Evaluation (CC). The CC defines seven Evaluation Assurance Levels (EAL1 to EAL7) that indicate the depth and rigor of the security evaluation. Higher EALs require more extensive documentation, testing, and formal verification.

The CC process involves creating a Protection Profile (PP) that defines security requirements for a class of products, and a Security Target (ST) that specifies how a particular product meets those requirements. The evaluation examines the product's design, implementation, and documentation against the ST claims.

Other evaluation models include TCSEC (Trusted Computer System Evaluation Criteria), also known as the Orange Book, which was a precursor to the CC. It defined levels from D (minimal protection) to A1 (verified design). The ITSEC (Information Technology Security Evaluation Criteria) was a European standard that influenced the development of the CC.

These models provide a common language and methodology for vendors to make security claims about their products and for consumers to compare security features across different offerings. However, it's important to note that these evaluations assess products against their stated security targets - a high EAL does not necessarily mean a product is more secure in absolute terms, only that it has undergone more rigorous evaluation.

Understanding these security and evaluation models is crucial for security architects and engineers. They provide a theoretical foundation for designing secure systems, analyzing potential vulnerabilities, and selecting appropriate security controls. By applying these models, organizations

can build systems that enforce their security policies consistently and verifiably, rather than relying on ad-hoc security measures.

Security Capabilities of Information Systems

Information systems encompass a wide range of components, including hardware, operating systems, applications, and networks. Each of these elements contributes to the overall security posture of the system. Understanding their security capabilities is crucial for designing and implementing robust security architectures.

Hardware security capabilities form the foundation of a secure system. Trusted Platform Modules (TPMs) provide a hardware-based root of trust, offering secure storage for cryptographic keys and the ability to attest to the system's integrity. Secure boot mechanisms ensure that only authorized firmware and operating system components are loaded during the boot process, preventing malware from compromising the system before security controls are in place.

Hardware-based encryption, such as self-encrypting drives, offloads cryptographic operations from the CPU and provides protection against physical theft of storage devices. Some processors offer features like Intel SGX (Software Guard Extensions) or AMD SEV (Secure Encrypted Virtualization) that create isolated execution environments to protect sensitive computations from other processes, even if the operating system is compromised.

Operating systems provide a wide array of security capabilities. Access control mechanisms enforce the principle of least privilege by restricting users and processes to the minimum permissions necessary to perform their

functions. This can be implemented through discretionary access control (DAC), where owners determine access rights, or mandatory access control (MAC), where system-wide policies govern access.

Memory protection features like Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) make it more difficult for attackers to exploit memory corruption vulnerabilities. Process isolation ensures that separate processes cannot interfere with each other's memory space, while user/kernel separation provides a higher level of protection for critical system components.

Secure communication channels between processes, such as those provided by SELinux's Multi-Level Security (MLS) implementation, allow for fine-grained control over information flow. Auditing and logging capabilities provide a trail of system events for forensic analysis and compliance purposes.

Many operating systems now include built-in encryption capabilities for both data at rest (full disk encryption) and data in transit (VPN clients). Secure update mechanisms ensure that security patches can be applied reliably without introducing new vulnerabilities.

Application security capabilities vary widely depending on the type of application, but common features include authentication mechanisms to verify user identities, authorization controls to enforce access policies, and input validation to prevent injection attacks. Secure coding practices and frameworks help developers build applications that are resistant to common vulnerabilities like SQL injection, cross-site scripting, and buffer overflows.

Web applications often implement security features like Content Security Policy (CSP) to mitigate cross-site scripting attacks, and HTTP Strict Transport Security (HSTS) to enforce the use of HTTPS. API security capabilities include

rate limiting to prevent abuse, OAuth for secure authorization, and JSON Web Tokens (JWT) for maintaining secure sessions.

Database management systems offer features like row-level security, which allows for fine-grained access control to data, and transparent data encryption to protect sensitive information at rest. Many also provide auditing capabilities to track access and changes to data.

Network security capabilities are crucial for protecting data in transit and controlling access to resources. Firewalls filter traffic based on predefined rules, while intrusion detection and prevention systems (IDS/IPS) monitor for and block malicious activity. Virtual Private Networks (VPNs) create secure tunnels for remote access, and network segmentation techniques like VLANs help contain potential breaches.

Secure protocols like TLS/SSL provide encryption and authentication for network communications. Network access control (NAC) systems ensure that only authorized and compliant devices can connect to the network. Software-defined networking (SDN) offers more flexible and granular control over network traffic, allowing for dynamic security policies.

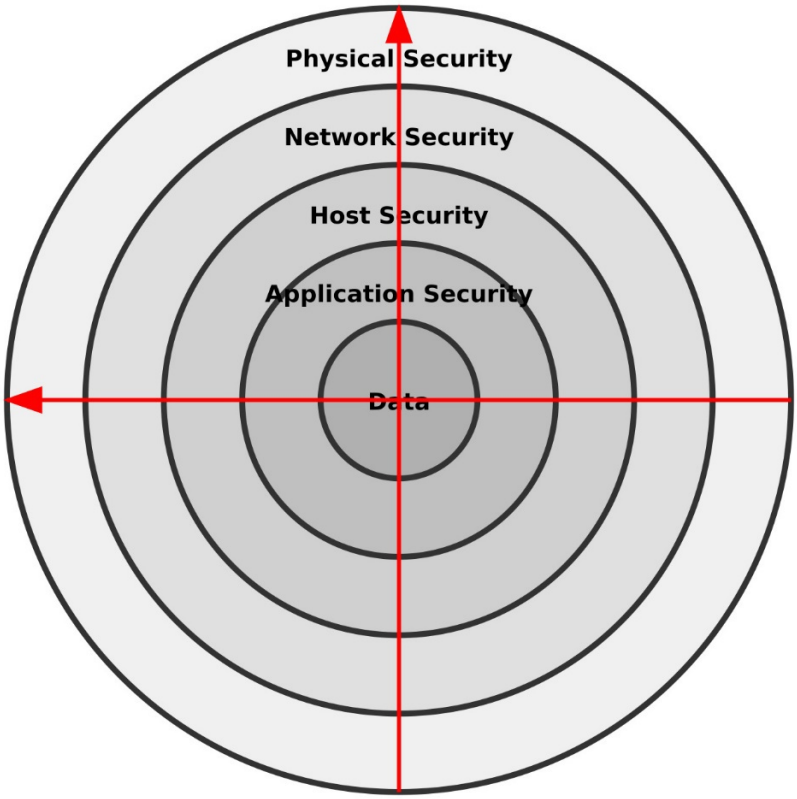
Cloud computing introduces additional security capabilities. Multi-tenancy isolation ensures that different customers' data and resources are kept separate. Identity and Access Management (IAM) services provide centralized control over user permissions across multiple cloud resources. Cloud providers often offer advanced threat detection and DDoS mitigation services that can be difficult for individual organizations to implement on their own.

When designing secure systems, it's important to consider how these various security capabilities can be integrated and layered to provide defense in depth. No single security

feature or component can provide complete protection, but by combining multiple layers of security controls, organizations can create a more resilient security architecture.

It's also crucial to understand the limitations and potential vulnerabilities of these security capabilities. For example, while TPMs provide a hardware root of trust, they are not immune to all attacks. Similarly, encryption protects data confidentiality but does not guarantee integrity or availability. By understanding both the strengths and weaknesses of different security capabilities, security architects can make informed decisions about how to best protect their information systems.

Secure System Architecture and Design



Secure system architecture and design is the process of creating information systems that are inherently secure, resilient to attacks, and capable of protecting the confidentiality, integrity, and availability of data and resources. This process involves applying security principles and best practices throughout the system development lifecycle, from initial requirements gathering to implementation and maintenance.

One of the fundamental principles of secure design is defense in depth. This approach involves implementing multiple layers of security controls so that if one layer is compromised, others are still in place to protect the system. For example, a secure network architecture might include perimeter firewalls, network segmentation, host-based firewalls, intrusion detection systems, and encryption for data in transit. Each layer provides additional protection and increases the difficulty for an attacker to reach sensitive assets.

The principle of least privilege is another cornerstone of secure design. This principle states that users, processes, and systems should be granted only the minimum level of access rights necessary to perform their functions. Implementing least privilege helps contain the potential damage from compromised accounts or malicious insiders. It often involves role-based access control (RBAC) systems that assign permissions based on job functions rather than individual users.

Separation of duties is a related principle that prevents any single individual from having complete control over a critical process. For example, in a financial system, the person who initiates a payment should not be the same person who approves it. This principle helps prevent fraud and reduces the risk of errors or malicious actions.

Secure system design also emphasizes the importance of simplicity and minimalism. Complex systems with unnecessary features or components increase the attack surface and make security analysis more difficult. By keeping designs as simple as possible while still meeting functional requirements, architects can reduce the potential for vulnerabilities and make systems easier to secure and maintain.

Fail-safe defaults are another key principle. Systems should be designed so that the default state is secure, and access is granted only after explicit authorization. For example, a firewall should by default block all incoming traffic and only allow specific, approved connections. This approach ensures that misconfigurations or oversights don't accidentally expose sensitive resources.

Complete mediation is the principle that every access to every object must be checked for authorization. This means implementing access controls consistently across all access paths, including direct access, network access, and API calls. Caching of access decisions should be done carefully to avoid introducing vulnerabilities.

Open design, also known as Kerckhoffs's principle in cryptography, states that the security of a system should not depend on the secrecy of its design. Instead, security should rely on the strength of algorithms, protocols, and keys. This principle encourages peer review and scrutiny of security mechanisms, which can help identify and fix vulnerabilities.

Psychological acceptability is an often-overlooked principle that emphasizes the importance of making security mechanisms user-friendly. If security controls are too cumbersome or disruptive, users may try to bypass them, undermining the overall security of the system. Designing security features that are intuitive and align with users' workflows can improve compliance and effectiveness.

When it comes to specific architectural patterns, the use of security gateways or reverse proxies can provide a centralized point for implementing security controls like authentication, access control, and traffic filtering. This pattern can simplify security management and provide a clear separation between external and internal networks.

Microservices architecture, while primarily an approach for building scalable and maintainable systems, can also enhance security by providing better isolation between components. Each microservice can be secured independently, and compromises can be more easily contained. However, this approach also introduces challenges in managing distributed security and ensuring consistent policy enforcement across services.

Secure communication patterns are crucial for protecting data in transit. This includes using encrypted protocols like TLS for all network communications, implementing mutual authentication where both client and server verify each other's identities, and using secure key exchange mechanisms to establish shared secrets.

Data protection patterns focus on securing information at rest and in use. This includes implementing encryption for stored data, using secure enclaves for processing sensitive information, and applying data masking or tokenization techniques to protect personally identifiable information (PII) in non-production environments.

Identity and access management (IAM) architectures are a critical component of secure systems. Centralized IAM services can provide consistent authentication and authorization across multiple applications and services. Federated identity systems allow for single sign-on (SSO) capabilities while maintaining separation between different security domains.

Secure logging and monitoring architectures are essential for detecting and responding to security incidents. This involves collecting logs from multiple sources, ensuring the integrity of log data, and implementing real-time analysis and alerting systems. Security information and event management (SIEM) systems often form the core of these architectures.

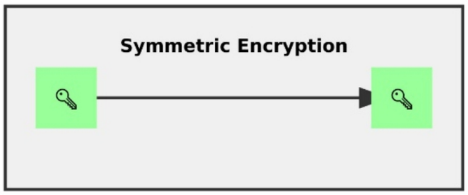
When designing secure systems, it's important to consider the entire lifecycle of data and components. This includes secure provisioning of new resources, ongoing patch management and vulnerability assessment processes, and secure decommissioning procedures to ensure sensitive data is properly destroyed when systems are retired.

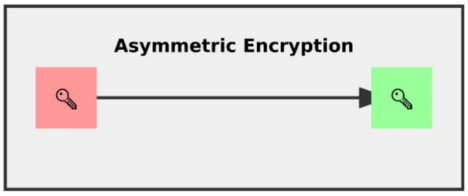
Threat modeling is an integral part of secure system design. By systematically identifying potential threats and vulnerabilities, architects can make informed decisions about which security controls to implement and where to focus resources. Techniques like STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) provide structured approaches to threat analysis.

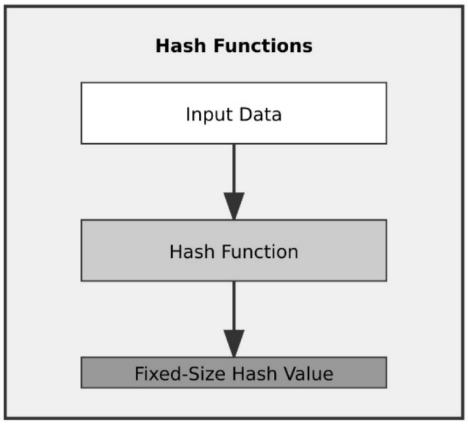
Finally, it's crucial to design systems with resilience and recoverability in mind. This includes implementing redundancy for critical components, designing for graceful degradation in the face of partial failures, and having well-defined incident response and disaster recovery procedures.

Secure system architecture and design is not a one-time activity but an ongoing process. As threats evolve and new vulnerabilities are discovered, architectures must be reviewed and updated to maintain their security posture. Regular security assessments, penetration testing, and code reviews are essential for identifying weaknesses and ensuring that security controls are functioning as intended.

Cryptography Fundamentals







Cryptography is a fundamental building block of information security, providing mechanisms for protecting the confidentiality, integrity, and authenticity of data. Understanding cryptographic principles and their practical applications is crucial for designing secure systems and implementing effective security controls.

At its core, cryptography involves transforming plaintext (readable data) into ciphertext (encrypted data) using an algorithm and a key. The strength of a cryptographic system typically relies on the secrecy of the key rather than the secrecy of the algorithm itself, a principle known as Kerckhoffs's principle.

There are two main types of cryptographic systems: symmetric and asymmetric. Symmetric cryptography, also known as secret key cryptography, uses the same key for both encryption and decryption. Common symmetric algorithms include AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple DES). Symmetric algorithms are generally faster and more

efficient for encrypting large amounts of data, but they face challenges in key distribution and management, especially in large-scale systems.

Asymmetric cryptography, also called public key cryptography, uses a pair of mathematically related keys: a public key that can be freely distributed, and a private key that must be kept secret. Data encrypted with the public key can only be decrypted with the corresponding private key, and vice versa. Common asymmetric algorithms include RSA, DSA, and elliptic curve cryptography (ECC). Asymmetric cryptography solves the key distribution problem of symmetric systems and enables digital signatures, but it is computationally more intensive.

In practice, many systems use a hybrid approach, using asymmetric cryptography to securely exchange a symmetric session key, which is then used for bulk data encryption. This combines the key management advantages of asymmetric cryptography with the performance benefits of symmetric encryption.

Cryptographic hash functions are another essential component of modern cryptography. These functions take an input of arbitrary length and produce a fixed-length output (hash) with several important properties: they are one-way functions (it's computationally infeasible to derive the input from the hash), they produce a dramatically different hash for even small changes in the input (avalanche effect), and it's extremely unlikely to find two different inputs that produce the same hash (collision resistance). Common hash functions include SHA-256, SHA-3, and BLAKE2.

Digital signatures combine asymmetric cryptography and hash functions to provide authentication, non-repudiation, and integrity. They work as follows:

1. The sender creates a hash of the message using a cryptographic hash function like SHA-256.
2. The sender encrypts the hash using their private key.
3. The encrypted hash is attached to the message as the digital signature.
4. The recipient decrypts the signature using the sender's public key to obtain the original hash.
5. The recipient independently hashes the received message.
6. If the decrypted hash matches the independently generated hash, the signature is valid.

This process provides:

- Authentication: Only the holder of the private key could have created the signature.
- Non-repudiation: The sender cannot deny signing the message.
- Integrity: Any changes to the message would result in a different hash.

Key management is crucial for the security of cryptographic systems. This includes secure generation, storage, distribution, and destruction of cryptographic keys. Best practices include:

- Using hardware security modules (HSMs) for key generation and storage
- Implementing key rotation policies
- Separating duties for key management tasks
- Using strong key derivation functions
- Protecting key backups

- Securely destroying keys at end-of-life

Public key infrastructure (PKI) provides a framework for managing digital certificates and public key encryption. It typically includes:

- Certificate authorities (CAs) that issue and revoke certificates
- Registration authorities (RAs) that verify certificate requestor identities
- Certificate repositories for storing and distributing certificates
- Certificate revocation lists (CRLs) for publishing revoked certificates

PKI enables secure communication and authentication in large-scale systems by providing a trusted mechanism for verifying the binding between public keys and identities.

Cryptographic protocols combine various cryptographic primitives to provide security services for specific applications. Examples include:

- TLS/SSL for secure web communications
- IPsec for virtual private networks (VPNs)
- SSH for secure remote access
- S/MIME and PGP for secure email

These protocols address challenges like key exchange, mutual authentication, and session key establishment in practical networked environments.

Quantum cryptography and post-quantum cryptography are emerging fields addressing potential threats from quantum computers. Quantum key distribution uses quantum mechanical properties to securely distribute keys, while

post-quantum algorithms aim to resist attacks by both classical and quantum computers.

As cryptographic systems become more complex, formal security models and proofs play an increasingly important role in analyzing their security properties and identifying potential vulnerabilities. This mathematical approach helps ensure that cryptographic protocols achieve their intended security goals.

Site and Facility Security Design

Site and facility security design is a critical component of an organization's overall security strategy. It involves planning and implementing physical security measures to protect assets, people, and information from various threats. Effective site and facility security design requires a holistic approach that considers multiple layers of protection.

The first step in site and facility security design is conducting a thorough risk assessment. This involves identifying potential threats, vulnerabilities, and the impact of security breaches. Common threats to consider include unauthorized access, theft, vandalism, terrorism, natural disasters, and insider threats. The risk assessment should also take into account the specific needs and operations of the organization, as well as any regulatory requirements or industry standards that must be met.

Once risks are identified, the next step is to develop a comprehensive security plan. This plan should outline the security objectives, strategies, and specific measures to be implemented. It's important to apply the principle of defense in depth, which involves using multiple layers of security controls to provide redundancy and make it more difficult for potential attackers to breach the facility.

The outermost layer of security typically begins with the perimeter of the property. This may include fencing, walls, or natural barriers to define the boundaries and deter casual intruders. Perimeter security measures might include:

- Security fencing with appropriate height and anti-climb features
- Crash-resistant barriers to prevent vehicle ramming attacks
- Landscaping designed to eliminate hiding spots and maintain clear lines of sight
- Exterior lighting to illuminate the perimeter and discourage intruders

Access control is a crucial aspect of site security. This involves managing how people, vehicles, and materials enter and exit the facility. Common access control measures include:

- Gated entrances with security personnel or automated systems
- Vehicle inspection areas for delivery trucks and visitor vehicles
- Turnstiles or mantraps to control pedestrian access
- Visitor management systems to track and authorize guests

The building envelope itself forms another important layer of security. This includes the walls, roof, doors, and windows of the facility. Security considerations for the building envelope include:

- Reinforced walls and roof structures to resist forced entry or explosive attacks

- Blast-resistant windows or window films to mitigate the effects of explosions
- High-security doors with multi-point locking systems
- Intrusion detection systems on doors, windows, and other potential entry points

Inside the facility, space planning and interior design play a role in security. This might involve:

- Creating secure zones with varying levels of access restrictions
- Designing circulation paths that funnel visitors through controlled areas
- Implementing open floor plans to improve visibility and reduce hiding spots
- Securing critical assets in hardened rooms or vaults

Environmental design is another important aspect of facility security. Crime Prevention Through Environmental Design (CPTED) principles can be applied to create spaces that naturally deter criminal activity. CPTED strategies include:

- Natural surveillance: Designing spaces that maximize visibility and the ability to observe activities
- Natural access control: Using physical elements to guide people and vehicles through the site
- Territorial reinforcement: Clearly defining public, semi-public, and private spaces
- Maintenance: Keeping the facility well-maintained to demonstrate active management and discourage disorder

Technology plays a significant role in modern facility security design. Key technological components might include:

- Video surveillance systems with analytics capabilities
- Electronic access control systems using cards, biometrics, or mobile credentials
- Intrusion detection and alarm systems
- Mass notification systems for emergency communications

When designing secure facilities, it's also important to consider emergency response and evacuation procedures. This includes:

- Designing clear and accessible evacuation routes
- Installing fire suppression systems and smoke detectors
- Creating secure assembly points for employees during emergencies
- Establishing command and control centers for managing incidents

For organizations with particularly sensitive operations or assets, additional security measures might be necessary. These could include:

- Radio Frequency (RF) shielding to prevent electronic eavesdropping
- Faraday cages to protect against electromagnetic pulse (EMP) attacks
- Positive air pressure systems to prevent chemical or biological contamination

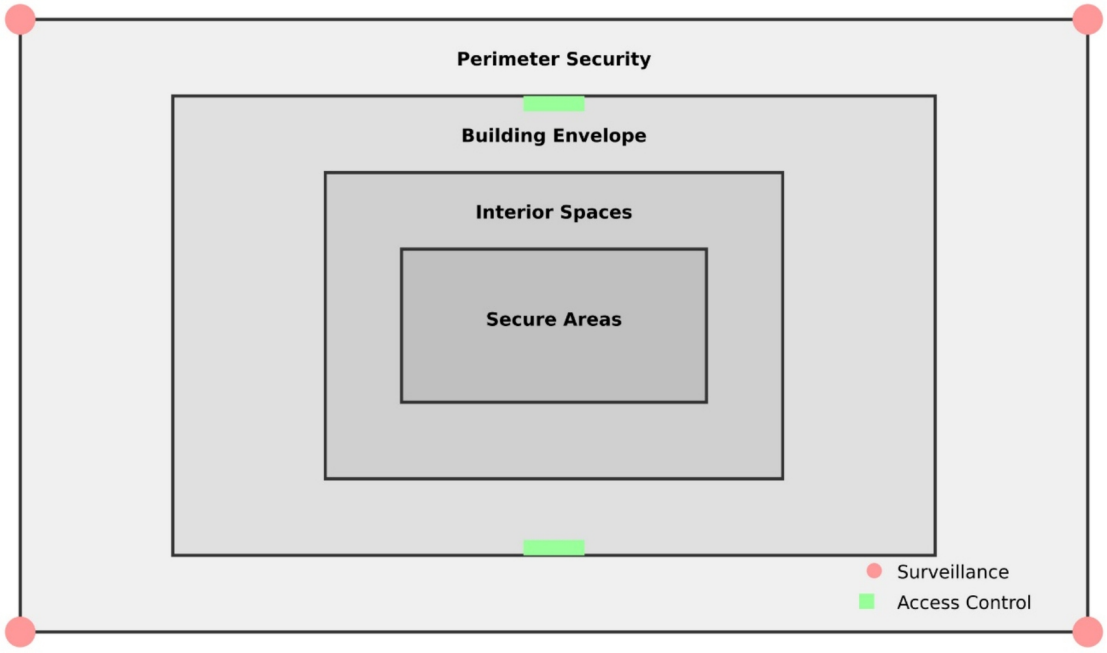
- Redundant utility systems to ensure continuity of operations

When implementing security measures, it's crucial to balance security needs with usability and aesthetics. Overly intrusive or intimidating security measures can negatively impact employee morale and productivity. The goal should be to create a secure environment that still feels welcoming and supports the organization's operations.

Regular security audits and assessments should be conducted to ensure that the implemented measures remain effective. As threats evolve and organizational needs change, the security design should be updated accordingly.

Collaboration between security professionals, architects, engineers, and other stakeholders is essential for successful site and facility security design. By working together, these teams can create integrated solutions that protect assets while supporting the organization's mission and culture.

Physical Security



Physical security is a fundamental component of an organization's overall security strategy, focusing on the protection of people, assets, and information through tangible measures and controls. It encompasses a wide range of elements designed to deter, detect, delay, and respond to physical threats.

The foundation of physical security is the concept of layered defense, also known as defense in depth. This approach involves implementing multiple security measures to create overlapping layers of protection. If one layer is breached, subsequent layers continue to provide security. The typical layers of physical security include:

1. Perimeter Security: This outermost layer defines the boundaries of the protected area. It may include:
    - Fencing or walls
    - Gates and barriers
    - Surveillance cameras
    - Security lighting
    - Intrusion detection systems
2. External Security: This layer focuses on the area immediately surrounding buildings and facilities. It may include:
    - Parking lot controls
    - Landscaping designed for security (e.g., clear lines of sight)
    - External lighting
    - Bollards or other vehicle barriers
3. Building Security: This layer protects the structure itself and may include:
    - Access control systems for doors and entrances
    - Security guards or reception staff

- Visitor management systems
- Reinforced doors and windows
- Intrusion alarms

4. Internal Security: This innermost layer protects specific areas or assets within a building. It may include:
    - Internal access control systems
    - Safes and vaults
    - Security cameras in sensitive areas
    - Mantraps or security airlocks

Access control is a critical aspect of physical security. It involves managing who can enter specific areas and when. Common access control methods include:

- ID badges or access cards
- Biometric systems (e.g., fingerprint, retinal scan)
- PIN codes or passwords
- Keys and locks

These methods can be combined for multi-factor authentication, increasing security for sensitive areas.

Surveillance is another key component of physical security. This typically involves the use of security cameras (CCTV) to monitor and record activities in and around a facility. Modern surveillance systems often incorporate advanced features such as:

- Motion detection
- Facial recognition
- License plate recognition
- Integration with access control systems
- Remote monitoring capabilities

Intrusion detection systems (IDS) are designed to detect unauthorized entry attempts. These may include:

- Door and window sensors
- Glass break detectors
- Motion sensors
- Pressure mats
- Vibration sensors

When an intrusion is detected, these systems typically trigger an alarm and notify security personnel or law enforcement.

Physical security also involves protecting against environmental threats and disasters. This may include:

- Fire detection and suppression systems
- Flood detection systems
- Earthquake-resistant construction
- Lightning protection systems
- Backup power systems

Asset protection is a crucial aspect of physical security. This involves safeguarding valuable or sensitive items such as:

- Cash and negotiable instruments
- Sensitive documents
- Intellectual property
- Computer equipment and data storage devices

Methods of asset protection may include:

- Safes and vaults
- Secure storage rooms
- Asset tracking systems

- Destruction methods for sensitive materials (e.g., shredders, degaussers)

Human factors play a significant role in physical security. This includes:

- Security awareness training for employees
- Background checks for personnel
- Visitor management procedures
- Contractor and vendor management

Physical security policies and procedures are essential for ensuring consistent implementation of security measures. These should cover areas such as:

- Access control policies
- Key management
- Visitor and contractor management
- Incident response procedures
- Emergency evacuation plans

Regular security audits and assessments are crucial for maintaining effective physical security. These helps identify vulnerabilities, ensure compliance with policies and regulations, and keep security measures up-to-date with evolving threats.

Integration of physical and logical security is becoming increasingly important. This involves linking physical access control systems with IT systems to provide a more comprehensive security approach. For example, an employee's building access card might also be used for computer login, providing a single credential for both physical and logical access.

Emerging technologies are also shaping the future of physical security. These include:

- Internet of Things (IoT) devices for security applications
- Artificial Intelligence and Machine Learning for threat detection and response
- Drones for aerial surveillance and perimeter monitoring
- Robotics for security patrols

As with all security measures, physical security must balance protection with usability and cost-effectiveness. Overly restrictive measures can impede business operations and create a negative work environment. The goal is to implement security that effectively protects assets while supporting the organization's mission and culture.

Physical security is a multifaceted discipline that requires careful planning, implementation, and ongoing management. By employing a layered approach and integrating various security measures, organizations can create a robust physical security posture that protects their people, assets, and information from a wide range of threats.

Chapter 4: Communication and Network Security

Communication and network security form the backbone of modern information systems, ensuring the confidentiality, integrity, and availability of data as it traverses networks. This domain encompasses the design, implementation, and maintenance of secure network architectures, as well as the protection of data in transit.

Key areas include secure network architecture design, which focuses on creating resilient and defensible network structures. This involves segmentation, access controls, and the implementation of security zones. Secure network components, such as firewalls, intrusion detection systems, and virtual private networks, play crucial roles in protecting network boundaries and monitoring traffic.

Secure communication channels are essential for protecting data as it moves between systems. This includes encryption protocols, secure routing mechanisms, and methods for ensuring the authenticity of network connections. Understanding common network attacks and their countermeasures is vital for defending against threats like denial of service, man-in-the-middle attacks, and various forms of network-based exploitation.

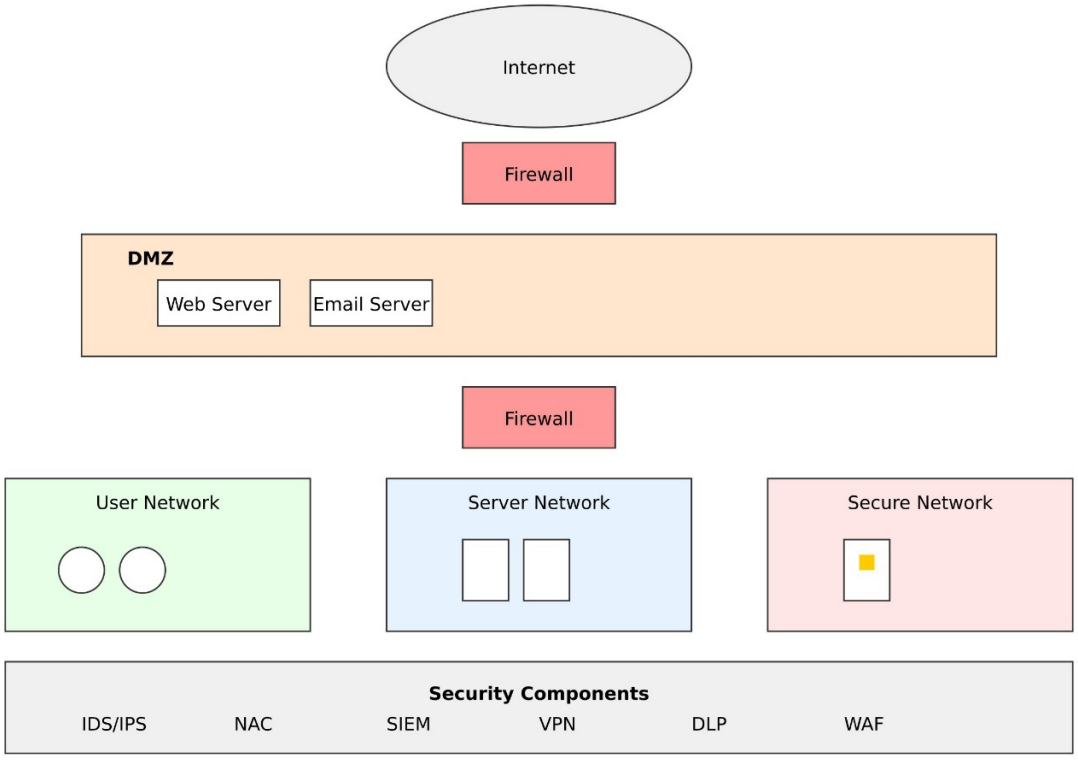
The growing prevalence of wireless networks and mobile devices introduces additional security challenges. This domain addresses the unique security considerations for Wi-Fi networks, cellular communications, and the protection of mobile endpoints.

By mastering these concepts, security professionals can design and maintain networks that are resilient to attacks,

protect sensitive data in transit, and support secure communications across diverse and distributed environments.

Secure Network Architecture Design

Secure network architecture design is the foundation of a robust and defensible network infrastructure. It involves creating a network structure that not only supports business operations but also incorporates security principles from the ground up. The goal is to develop an architecture that can effectively resist attacks, contain breaches, and facilitate secure communication and data flow.



One of the primary principles of secure network design is segmentation. This involves dividing the network into distinct zones or segments, each with its own security requirements and access controls. Segmentation helps contain potential breaches by limiting lateral movement within the network. For example, a typical enterprise network might be divided into segments for general office use, sensitive financial systems, customer-facing web services, and industrial control systems. Each segment would have its own security policies and access restrictions.

The concept of defense in depth is crucial in network architecture. This approach involves implementing multiple layers of security controls throughout the network, so that if one layer is compromised, others are still in place to protect assets. This might include perimeter firewalls, internal firewalls between segments, intrusion detection systems at various points, and host-based security controls on individual systems.

Implementing a demilitarized zone (DMZ) is a common practice in secure network design. The DMZ is a segment that sits between the internal network and the public internet, typically hosting services that need to be accessible from outside the organization, such as web servers or email gateways. By placing these services in a DMZ, organizations can apply strict controls on traffic between the DMZ and the internal network, reducing the risk of external attacks compromising internal systems.

Network access control (NAC) is another key component of secure architecture. NAC systems verify the security posture of devices before allowing them to connect to the network. This might include checking for up-to-date antivirus software, required security patches, or other security configurations. Devices that don't meet the security requirements can be quarantined or given limited access until they are brought into compliance.

Secure network design also involves careful planning of routing and switching infrastructure. This includes implementing secure routing protocols that can resist attacks and maintain the integrity of routing information. Virtual LANs (VLANs) can be used to further segment traffic at the switch level, providing additional isolation between different types of network traffic.

Incorporating redundancy and high availability into the network design is crucial for maintaining security and business continuity. This might involve implementing redundant network paths, load balancers, and failover systems to ensure that critical services remain available even if some components fail or come under attack.

Security monitoring and logging are essential aspects of network architecture. This involves strategically placing sensors and log collection points throughout the network to provide visibility into network activity and potential security events. Security information and event management (SIEM) systems can be used to aggregate and analyze this data, providing a holistic view of the network's security posture.

As organizations increasingly adopt cloud services, secure network architecture must extend beyond the traditional perimeter. This involves designing secure connections to cloud providers, implementing cloud access security brokers (CASBs) to monitor and control cloud usage, and ensuring that security policies are consistently applied across on-premises and cloud environments.

Software-defined networking (SDN) and network function virtualization (NFV) are emerging technologies that can enhance network security. SDN allows for more dynamic and granular control over network traffic, enabling rapid response to security threats. NFV can be used to quickly deploy and scale security functions like firewalls and intrusion detection systems as needed.

Zero Trust architecture is a modern approach to network security that assumes no user or device should be trusted by default, even if they are inside the network perimeter. This model requires continuous authentication and authorization for all users and devices, regardless of their location. Implementing Zero Trust principles often involves microsegmentation, strong identity management, and continuous monitoring and analytics.

When designing secure network architectures, it's important to consider the principle of least privilege. This means granting users and systems only the minimum level of access and permissions necessary to perform their functions. This principle should be applied not only to user access but also to network communication paths, allowing only necessary traffic flows between network segments.

Data flow analysis is a crucial step in secure network design. This involves mapping out how data moves through the network, identifying where sensitive information is stored and processed, and ensuring that appropriate security controls are in place along these paths. This analysis can help identify potential vulnerabilities and inform decisions about where to place security controls.

Secure network architecture should also account for remote access needs. This might involve implementing virtual private networks (VPNs) for secure remote connections, or more advanced solutions like software-defined perimeters (SDPs) that provide granular access control for remote users.

As networks become more complex and distributed, automation and orchestration tools play an increasingly important role in maintaining security. These tools can help ensure that security policies are consistently applied across the network, quickly respond to security events, and

manage the configuration of numerous network devices and security controls.

Finally, it's important to recognize that secure network architecture is not a one-time design task but an ongoing process. Regular security assessments, penetration testing, and architecture reviews are necessary to ensure that the network design remains effective against evolving threats and changing business requirements. The architecture should be flexible enough to adapt to new technologies and security challenges while maintaining a strong security posture.

Secure Network Components

Secure network components are the building blocks of a robust and resilient network infrastructure. These components work together to protect the network from various threats, control access, monitor for suspicious activity, and ensure the confidentiality and integrity of data in transit. Understanding the functions and proper configuration of these components is crucial for maintaining a secure network environment.

Firewalls are one of the most fundamental security components in any network. They act as a barrier between trusted internal networks and untrusted external networks, such as the internet. Firewalls filter incoming and outgoing network traffic based on predetermined security rules. There are several types of firewalls, each with its own strengths:

Packet filtering firewalls examine packets based on predefined rules, typically looking at source and destination IP addresses, port numbers, and protocols. While simple and fast, they lack the ability to understand the context of the traffic.

Stateful inspection firewalls build upon packet filtering by keeping track of the state of network connections. This allows them to make more intelligent decisions about which packets to allow or block based on the context of the connection.

Application layer firewalls, also known as proxy firewalls, operate at the application layer of the OSI model. They can inspect the content of the traffic and make decisions based on the specific application protocols being used. This allows for more granular control but can introduce latency.

Next-generation firewalls (NGFWs) combine traditional firewall capabilities with additional features like intrusion prevention, application awareness, and integration with threat intelligence feeds. They provide more comprehensive protection against modern, sophisticated threats.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are crucial for identifying and responding to potential security breaches. An IDS monitors network traffic for suspicious activity and generates alerts when potential threats are detected. An IPS goes a step further by actively blocking or preventing detected threats.

There are two main types of IDS/IPS:

Network-based IDS/IPS (NIDS/NIPS) monitor traffic on the network itself, typically deployed at key points like network boundaries or between segments.

Host-based IDS/IPS (HIDS/HIPS) are installed on individual systems to monitor for suspicious activity specific to that host.

These systems use various detection methods, including signature-based detection (looking for known patterns of malicious activity) and anomaly-based detection (identifying deviations from normal behavior).

Virtual Private Networks (VPNs) are essential for securing communications over untrusted networks, such as the internet. VPNs create encrypted tunnels between endpoints, allowing for secure remote access to network resources or connecting geographically dispersed office locations. There are several types of VPNs:

Site-to-site VPNs connect entire networks, typically used to link branch offices to a main corporate network.

Remote access VPNs allow individual users to connect securely to a network from remote locations.

SSL/TLS VPNs use web browsers as the client interface, providing easier access for remote users without requiring specialized software.

IPsec VPNs operate at the network layer and are often used for site-to-site connections due to their strong security and wide support in network devices.

Network Access Control (NAC) systems manage access to a network based on the identity and security posture of devices attempting to connect. NAC can enforce security policies by checking factors like:

- Device authentication and authorization
- Presence of up-to-date antivirus software
- Operating system patch levels
  Compliance with organizational security policies

Devices that don't meet the required security standards can be quarantined or given limited access until they are brought into compliance.

Secure switches and routers play a crucial role in network security. Modern switches offer features like:

- Port security to limit which devices can connect to specific switch ports

- VLANs for network segmentation at the data link layer
- Access Control Lists (ACLs) to filter traffic
- Spanning Tree Protocol (STP) security to prevent attacks on the network topology

Secure routers incorporate features such as:

- Secure routing protocols (e.g., OSPF with authentication)
- Control plane policing to protect the router itself from attacks
- VPN termination for site-to-site and remote access VPNs
- Quality of Service (QoS) to ensure critical security traffic is prioritized

Load balancers, while primarily used to distribute traffic across multiple servers for performance and availability, also contribute to security. They can provide features like:

- SSL/TLS offloading to centralize encryption processing
- Web application firewall functionality to protect against application-layer attacks
- DDoS protection by absorbing and filtering malicious traffic

Security Information and Event Management (SIEM) systems are central to network security monitoring and incident response. SIEM systems collect and analyze log data from various network devices and security components, providing:

- Real-time analysis of security alerts
- Correlation of events from different sources to identify complex attack patterns

- Long-term storage of log data for compliance and forensic purposes
- Automated incident response workflows

Secure DNS servers are critical for protecting against DNS-based attacks and ensuring the integrity of name resolution. Features of secure DNS include:

- DNSSEC to verify the authenticity of DNS responses
- DNS filtering to block access to known malicious domains
- Response policy zones (RPZ) to customize DNS responses based on security policies

Web Application Firewalls (WAFs) specifically protect web applications from various attacks. They inspect HTTP traffic and can prevent common web application attacks like SQL injection, cross-site scripting (XSS), and CSRF.

Data Loss Prevention (DLP) systems monitor data in use, in motion, and at rest to prevent unauthorized transmission of sensitive information. Network DLP components can inspect traffic for sensitive data patterns and enforce policies to prevent data exfiltration.

Honeypots and honeynets are deception technologies used to detect, deflect, or study attack attempts. By mimicking vulnerable systems, they can attract attackers, allowing security teams to study their techniques and gather threat intelligence.

Network Behavior Analysis (NBA) tools monitor network traffic to establish baselines of normal behavior and detect anomalies that could indicate security threats. This can be particularly effective for identifying novel or zero-day attacks that might evade signature-based detection.

Each of these components plays a specific role in network security, and their effectiveness depends on proper configuration, regular updates, and integration into a

comprehensive security strategy. By understanding the capabilities and limitations of each component, network security professionals can design and implement robust, layered defenses that protect against a wide range of threats.

Secure Communication Channels

Secure communication channels are essential for protecting the confidentiality, integrity, and authenticity of data as it travels across networks. These channels ensure that sensitive information remains protected from interception, tampering, and unauthorized access. Implementing secure communication channels involves a combination of cryptographic protocols, network configurations, and security best practices.

One of the most fundamental technologies for securing communication channels is encryption. Encryption transforms readable data (plaintext) into an unreadable format (ciphertext) that can only be decrypted by authorized parties with the correct key. There are two main types of encryptions used in secure communications:

Symmetric encryption uses the same key for both encryption and decryption. It's fast and efficient, making it suitable for encrypting large amounts of data. However, the challenge lies in securely distributing the shared key to all parties. Common symmetric encryption algorithms include AES (Advanced Encryption Standard) and ChaCha20.

Asymmetric encryption, also known as public-key cryptography, uses a pair of mathematically related keys: a public key for encryption and a private key for decryption. This solves the key distribution problem of symmetric encryption but is computationally more intensive. RSA and

Elliptic Curve Cryptography (ECC) are widely used asymmetric algorithms.

In practice, many secure communication protocols use a hybrid approach, using asymmetric encryption to securely exchange a symmetric session key, which is then used for bulk data encryption.

The Transport Layer Security (TLS) protocol, and its predecessor Secure Sockets Layer (SSL), are the most widely used protocols for securing communications on the internet. TLS provides:

Confidentiality through encryption
Integrity through message authentication codes (MACs)
Authentication using digital certificates

TLS is commonly used to secure web traffic (HTTPS), email communications (SMTP over TLS), and many other application-layer protocols. The latest version, TLS 1.3, offers improved security and performance over previous versions.

When implementing TLS, it's crucial to:

- Use strong cipher suites and disable weak or outdated ciphers
- Implement proper certificate management, including regular renewal and revocation checking
- Enable features like HTTP Strict Transport Security (HSTS) to prevent downgrade attacks

For securing network-layer communications, Internet Protocol Security (IPsec) is widely used. IPsec can operate in two modes:

- Transport mode, which encrypts only the payload of IP packets
- Tunnel mode, which encrypts the entire IP packet and is commonly used in VPN implementations

IPsec provides:

1. Confidentiality through encryption protocols like ESP (Encapsulating Security Payload)
2. Integrity and authentication through protocols like AH (Authentication Header)
3. Key management through the Internet Key Exchange (IKE) protocol

Secure Shell (SSH) is another crucial protocol for secure communications, primarily used for remote administration of systems. SSH provides:

1. Encrypted command-line access to remote systems
2. Secure file transfers through SFTP or SCP
3. Port forwarding for tunneling other protocols securely

When implementing SSH, best practices include:

1. Using strong key exchange algorithms and ciphers
2. Disabling password authentication in favor of public key authentication
3. Implementing two-factor authentication for additional security

For email communications, several protocols and standards contribute to security:

- S/MIME (Secure/Multipurpose Internet Mail Extensions) provides end-to-end encryption and digital signatures for email messages.
- PGP (Pretty Good Privacy) and its open-source implementation, GPG, offer similar functionality with a decentralized trust model.
- DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), and DMARC (Domain-based Message Authentication, Reporting, and

Conformance) work together to authenticate email senders and prevent email spoofing.

Virtual Private Networks (VPNs) create secure tunnels over untrusted networks, allowing remote users or branch offices to securely connect to corporate networks. Common VPN protocols include:

- IPsec VPNs, which operate at the network layer and are often used for site-to-site connections
- SSL/TLS VPNs, which operate at higher layers and are often used for remote access, leveraging web browsers as clients
- WireGuard, a newer protocol that aims to be simpler and more performant than traditional VPN protocols

When implementing VPNs, consider:

- Strong authentication methods, preferably multi-factor authentication
- Regular updates and patching of VPN software and appliances
- Proper segmentation of VPN traffic within the internal network

For wireless networks, several protocols provide security:

WPA3 (Wi-Fi Protected Access 3) is the latest standard for securing Wi-Fi networks, offering stronger encryption and protection against password guessing attacks.

802.1X provides port-based network access control, often used in enterprise Wi-Fi deployments for strong authentication.

Secure communication in Internet of Things (IoT) environments presents unique challenges due to the limited resources of many IoT devices. Protocols like MQTT (Message Queuing Telemetry Transport) with TLS can

provide a lightweight yet secure method for IoT devices to communicate. MQTT uses a publish/subscribe model and can be secured using TLS for encryption and authentication.

Other approaches for securing IoT communications include:

Datagram Transport Layer Security (DTLS): A version of TLS designed for unreliable transport protocols like UDP, which is common in IoT.

Constrained Application Protocol (CoAP): An application layer protocol designed for resource-constrained devices that can be secured with DTLS.

Lightweight cryptography: Algorithms specifically designed for low-power devices with limited processing capabilities.

Hardware security modules (HSMs): Dedicated crypto processors that can offload encryption tasks from resource-limited IoT devices.

Secure boot and firmware updates: Ensuring the integrity and authenticity of IoT device software.

Network segmentation: Isolating IoT devices on separate network segments to limit potential attack surfaces.

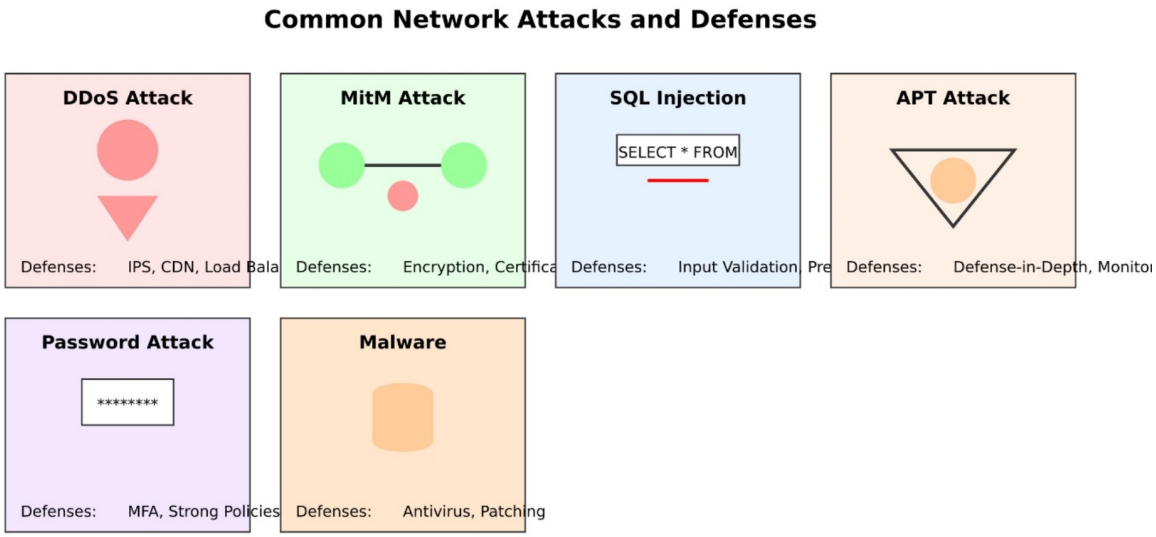
Device authentication: Using certificates, pre-shared keys, or other methods to verify device identities.

Access control: Implementing fine-grained policies to restrict what IoT devices can access and communicate with.

Monitoring and anomaly detection: Watching for unusual behavior that could indicate compromised devices.

The key is to implement security measures that provide adequate protection without overwhelming the limited resources of IoT devices. This often requires a careful balance and may involve specialized protocols and lightweight cryptographic algorithms designed specifically for constrained environments.

Network Attacks and Countermeasures



Network attacks pose a significant threat to organizations of all sizes. Understanding common attack vectors and implementing appropriate countermeasures is crucial for maintaining a robust security posture. Some of the most prevalent network attacks include:

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks aim to overwhelm network resources and make services unavailable to legitimate users. These attacks can take various forms, such as TCP SYN floods, UDP floods, or application layer attacks. Countermeasures include implementing intrusion prevention systems (IPS), using content delivery networks (CDNs) for traffic distribution, and configuring firewalls to filter suspicious traffic patterns.

Man-in-the-Middle (MitM) attacks occur when an attacker intercepts communication between two parties, potentially eavesdropping on or altering the data in transit. To mitigate MitM attacks, organizations should enforce the use of

encrypted protocols like HTTPS, implement certificate pinning, and use virtual private networks (VPNs) for remote access.

SQL injection attacks target vulnerabilities in web applications by inserting malicious SQL code into input fields. This can lead to unauthorized data access or manipulation. Countermeasures include input validation, parameterized queries, and the principle of least privilege for database accounts.

Cross-Site Scripting (XSS) attacks involve injecting malicious scripts into web pages viewed by other users. This can lead to session hijacking or credential theft. Defenses include input sanitization, content security policies, and using frameworks that automatically escape user input.

Password attacks attempt to gain unauthorized access by guessing or cracking user credentials. Common techniques include brute force attacks, dictionary attacks, and credential stuffing. Countermeasures include enforcing strong password policies, implementing multi-factor authentication, and using account lockout mechanisms.

Malware infections, including viruses, worms, and trojans, can compromise network security by stealing data, establishing backdoors, or spreading to other systems. Defense strategies include deploying antivirus software, keeping systems patched and updated, and implementing application whitelisting.

Insider threats pose a unique challenge as they originate from within the organization. These can be malicious actors or negligent employees. Countermeasures include implementing the principle of least privilege, monitoring user activities, and conducting regular security awareness training.

Advanced Persistent Threats (APTs) are sophisticated, long-term attacks often conducted by nation-states or well-

funded groups. They typically involve multiple attack vectors and aim to maintain long-term access to targeted networks. Defending against APTs requires a comprehensive approach, including threat intelligence, network segmentation, and continuous monitoring.

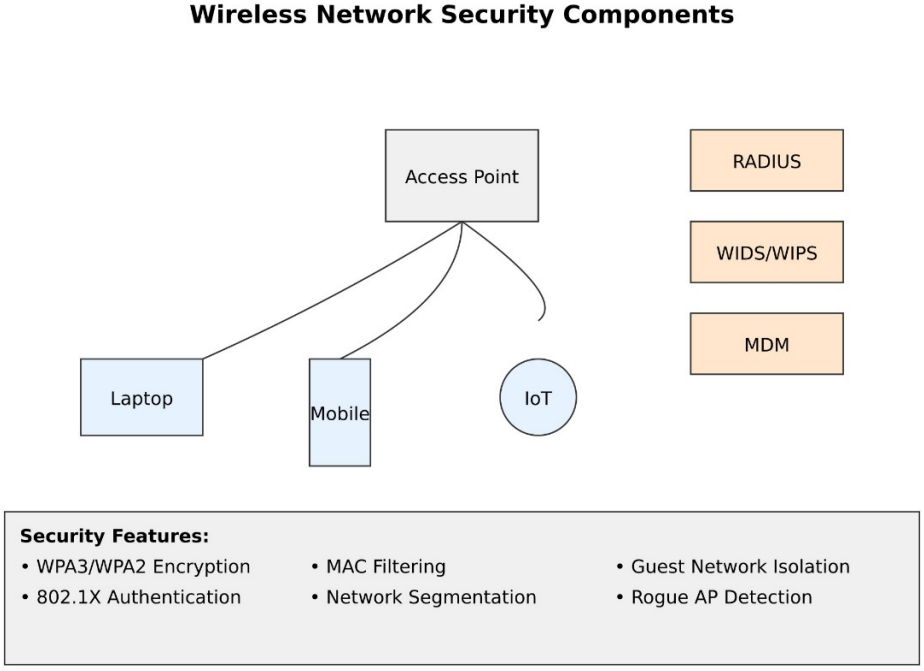
To effectively counter these and other network attacks, organizations should implement a defense-in-depth strategy that includes:

1. Perimeter security: Firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways.
2. Network segmentation: Dividing the network into smaller, isolated segments to limit the spread of potential breaches.
3. Access controls: Implementing strong authentication mechanisms and enforcing the principle of least privilege.
4. Encryption: Protecting data in transit and at rest using robust encryption protocols.
5. Vulnerability management: Regular scanning, patching, and updating of systems and applications.
6. Security information and event management (SIEM): Centralized logging and analysis of security events across the network.
7. Incident response planning: Developing and regularly testing procedures for detecting, containing, and mitigating security incidents.
8. User awareness training: Educating employees about security best practices and potential threats.
9. Third-party risk management: Assessing and monitoring the security posture of vendors and partners with network access.

10. Continuous monitoring: Implementing tools and processes for real-time threat detection and response.

By understanding common network attacks and implementing appropriate countermeasures, organizations can significantly improve their ability to detect, prevent, and respond to security threats effectively.

Wireless Networks and Mobile Security



Wireless networks and mobile devices have become integral to modern business operations, but they also introduce unique security challenges. Organizations must implement robust security measures to protect sensitive data and maintain the integrity of their networks.

Wireless Network Security:

1. Encryption: Use strong encryption protocols like WPA3 or WPA2 with AES encryption. Avoid older, vulnerable protocols like WEP.
2. Network segmentation: Isolate wireless networks from critical internal networks using VLANs or physical separation.
3. Strong authentication: Implement 802.1X authentication with RADIUS servers for enterprise environments.
4. Guest network isolation: Provide separate, restricted networks for guests and visitors.
5. Rogue access point detection: Regularly scan for and remove unauthorized access points.
6. Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS): Deploy these systems to detect and respond to wireless-specific threats.
7. MAC address filtering: While not foolproof, it can add an extra layer of access control.
8. Disable WPS: Wi-Fi Protected Setup can be vulnerable to brute-force attacks.
9. Regular security assessments: Conduct wireless penetration testing and vulnerability scans.

Mobile Device Security:

1. Mobile Device Management (MDM): Implement MDM solutions to enforce security policies, manage apps, and remotely wipe lost or stolen devices.
2. Encryption: Enforce full-device encryption and secure communication channels.

3. Strong authentication: Require complex passcodes, biometrics, or multi-factor authentication.
4. Application control: Use whitelisting or blacklisting to control which apps can be installed and used.
5. Data loss prevention: Implement controls to prevent unauthorized data transfer or storage on personal cloud services.
6. Remote wipe capabilities: Enable the ability to remotely erase sensitive data from lost or stolen devices.
7. Regular updates: Ensure devices receive timely security patches and OS updates.
8. Secure container solutions: Separate personal and corporate data using containerization technologies.
9. VPN usage: Enforce VPN connections for accessing corporate resources over public networks.
10. BYOD policies: Develop and enforce clear policies for personal device usage in the workplace.

Emerging Wireless Technologies:

1. 5G security: As 5G networks become more prevalent, organizations must address new security challenges such as network slicing and edge computing vulnerabilities.
2. IoT device security: Implement strong authentication and encryption for IoT devices connected to wireless networks.
3. Bluetooth security: Be aware of Bluetooth vulnerabilities and implement security measures like disabling unnecessary services and using the latest Bluetooth security features.

4. NFC security: For organizations using Near Field Communication, implement proper encryption and access controls.

Common Wireless and Mobile Attacks:

1. Evil Twin attacks: Rogue access points that mimic legitimate networks to intercept traffic.
2. Jamming: Disrupting wireless signals to cause denial of service.
3. Bluejacking and Bluesnarfing: Exploiting Bluetooth vulnerabilities to send unsolicited messages or steal data.
4. Man-in-the-Middle attacks: Intercepting wireless communications to eavesdrop or modify data.
5. Mobile malware: Malicious applications that can compromise device and data security.
6. Phishing and smishing: Social engineering attacks targeting mobile users via email or SMS.

Best Practices for Wireless and Mobile Security:

1. Regular security audits and penetration testing of wireless infrastructure.
2. Continuous monitoring of wireless networks for anomalies and potential threats.
3. Employee education on wireless and mobile security best practices.
4. Implementing a formal incident response plan for wireless and mobile security incidents.
5. Keeping abreast of emerging wireless technologies and their associated security implications.
6. Regularly reviewing and updating wireless and mobile security policies to address new threats and

technologies.

By implementing comprehensive security measures for wireless networks and mobile devices, organizations can mitigate risks associated with these technologies while reaping their benefits in terms of productivity and flexibility.

Chapter 5: Identity and Access Management (IAM)

Identity and Access Management (IAM) is a critical component of information security that focuses on controlling and managing digital identities and access to resources within an organization. IAM encompasses the processes, policies, and technologies used to create, maintain, and terminate user identities, as well as govern their access rights to systems, applications, and data.

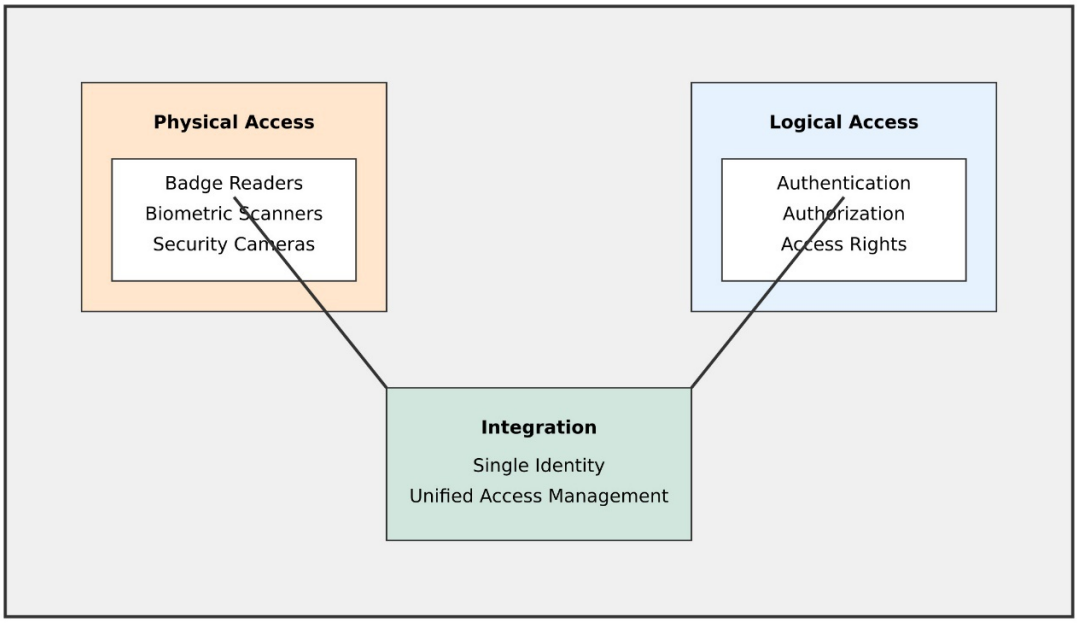
The core objectives of IAM are to ensure that the right individuals have the appropriate access to the right resources at the right times, while preventing unauthorized access and maintaining compliance with security policies and regulations. This involves managing the entire lifecycle of user identities, from initial creation through changes in roles and responsibilities, to eventual termination.

Key aspects of IAM include authentication (verifying a user's identity), authorization (determining what resources a user can access), and accountability (tracking user activities). These functions are implemented through various mechanisms such as password management, multi-factor authentication, access control lists, and role-based access control.

IAM systems must balance security with usability, ensuring that legitimate users can efficiently access the resources they need while maintaining strong protection against unauthorized access. As organizations increasingly rely on cloud services and support remote work, IAM has become more complex, necessitating solutions that can manage identities and access across diverse and distributed environments.

This chapter explores the fundamental concepts and technologies of IAM, including physical and logical access control, identification and authentication methods, identity management processes, access control models, and advanced concepts like single sign-on and federation. Understanding these topics is crucial for designing and implementing effective IAM strategies that protect an organization's assets while enabling productivity and innovation.

Physical and Logical Access Control



Physical and logical access control are two interconnected aspects of security that work together to protect an organization's assets, information, and resources. While physical access control focuses on securing physical spaces and assets, logical access control deals with protecting digital resources and systems. Both are essential components of a comprehensive security strategy.

Physical Access Control

Physical access control involves managing and restricting access to physical locations, buildings, rooms, and assets. The primary goal is to prevent unauthorized individuals from gaining physical access to sensitive areas or resources. Key components of physical access control include:

1. **Perimeter Security**: This is the outermost layer of physical security, often including fences, gates, and security guards. It defines the boundary between public and private spaces.
2. **Building Access**: Control measures at building entrances, such as locked doors, turnstiles, and reception desks, regulate who can enter the premises.
3. **Internal Access Control**: Within a building, different areas may have varying levels of security. For example, server rooms or executive offices might require additional authentication.
4. **Asset Protection**: Securing physical assets like computers, servers, and sensitive documents through locks, safes, or secure storage areas.

Common physical access control mechanisms include:

- **Keys and Locks**: Traditional mechanical locks and keys, though increasingly being replaced by electronic alternatives.
- **Access Cards**: Magnetic stripe or proximity cards that can be swiped or tapped to gain entry.
- **Biometric Systems**: Using unique physical characteristics like fingerprints, retinal scans, or facial recognition for authentication.
- **Security Personnel**: Human guards who verify identities and control access.
- **Mantrap**: A small space with two sets of interlocking doors, allowing only one person to enter at a time.

Physical access control also involves monitoring and logging entry and exit activities, often through surveillance cameras and access logs. These measures not only prevent

unauthorized access but also provide an audit trail for investigations if a security breach occurs.

Logical Access Control

Logical access control focuses on managing access to digital resources, including computer systems, networks, applications, and data. It ensures that users can only access the resources they are authorized to use. Key aspects of logical access control include:

1. **User Authentication**: Verifying the identity of users before granting access to systems or applications.
2. **Authorization**: Determining what resources and actions a user is allowed to access or perform.
3. **Access Rights Management**: Assigning, modifying, and revoking access rights based on user roles and responsibilities.
4. **Audit and Monitoring**: Tracking user activities and access attempts for security and compliance purposes.

Common logical access control mechanisms include:

- **Passwords**: Still the most widely used form of authentication, though often combined with other factors for increased security.
- **Multi-Factor Authentication (MFA)**: Requiring two or more forms of authentication, such as something you know (password), something you have (token), and something you are (biometric).
- **Access Control Lists (ACLs)**: Specifying which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

- **Role-Based Access Control (RBAC)**: Assigning access rights based on job functions or roles within an organization.
- **Firewalls and Network Segmentation**: Controlling access between different network segments or between the internal network and external networks.

Integration of Physical and Logical Access Control

In modern security architectures, physical and logical access control systems are often integrated to provide more comprehensive security. For example:

- A user's physical access card might also be used for computer login, providing a single credential for both physical and logical access.
- Biometric data used for physical access control can be linked to logical access rights.
- Physical location can be used as a factor in logical access decisions. For instance, a user might only be allowed to access certain systems when physically present in a secure facility.

Challenges and Considerations

Implementing effective physical and logical access control presents several challenges:

1. **Balancing Security and Usability**: Overly restrictive controls can hinder productivity, while lax controls expose the organization to risks.
2. **Scalability**: As organizations grow and change, access control systems must be able to adapt and scale accordingly.
3. **Integration**: Ensuring seamless integration between various physical and logical access control

systems can be complex.

4. **Compliance**: Access control measures must often comply with various regulations and standards, such as GDPR, HIPAA, or PCI DSS.
5. **Insider Threats**: Access control systems must account for the possibility of threats from within the organization.
6. **Remote Work**: The increase in remote work has complicated access control, requiring secure methods for remote access to resources.

Best Practices

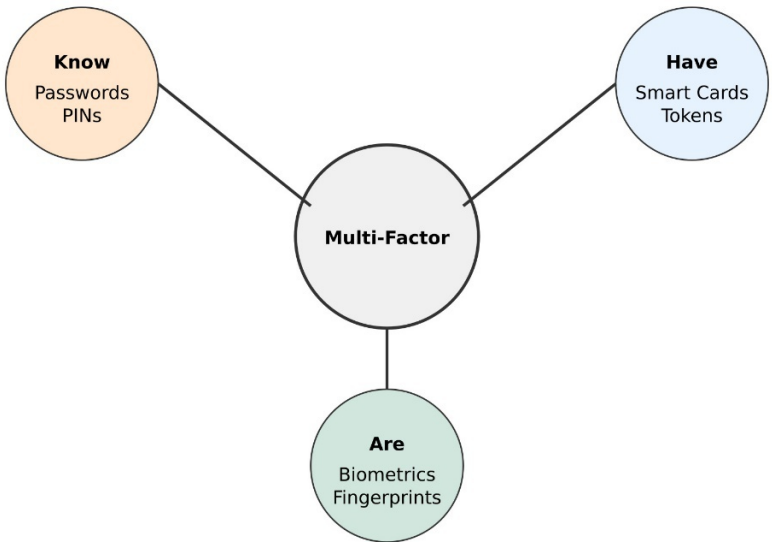
To implement effective physical and logical access control, organizations should consider the following best practices:

- Implement the principle of least privilege, granting users only the minimum access rights necessary for their roles.
- Regularly review and update access rights, especially when employees change roles or leave the organization.
- Use multi-factor authentication for sensitive systems and data.
- Implement strong password policies and consider using password managers.
- Regularly audit and monitor access logs for both physical and logical access.
- Provide security awareness training to all employees about the importance of access control.
- Implement a formal process for requesting, approving, and revoking access rights.
- Regularly test and update access control systems to address new threats and vulnerabilities.

By implementing comprehensive physical and logical access control measures, organizations can significantly reduce the risk of unauthorized access to their assets and information. However, it's important to remember that access control is just one part of a broader security strategy. It should be complemented by other security measures such as encryption, network security, and security awareness training to create a robust, multi-layered defense against potential threats.

Identification and Authentication

Identification and authentication are fundamental concepts in information security that form the foundation of access control systems. These processes work together to verify the identity of users or entities attempting to access a system or resource, ensuring that only authorized individuals can gain entry.



Identification

Identification is the process by which a user or entity claims a specific identity within a system. It's the first step in the access control process, where the user declares who they are. Common forms of identification include:

- **Usernames**: A unique identifier assigned to each user.
- **Employee ID numbers**: Often used in corporate environments.
- **Email addresses**: Frequently used as identifiers, especially for online services.
- **Smart cards or tokens**: Physical devices that contain identification information.

The identification process doesn't verify that the claimed identity is genuine; it merely establishes the identity that the user is asserting. Verification of this claim is the role of authentication.

Authentication

Authentication is the process of verifying that the claimed identity is genuine. It answers the question, "Are you really who you say you are?" Authentication typically relies on one or more of the following factors:

1. **Something you know** (Knowledge factor):
    - Passwords
    - PINs
    - Security questions
2. **Something you have** (Possession factor):
    - Smart cards
    - Security tokens
    - Mobile devices (for SMS or app-based authentication)

3. **Something you are** (Inherence factor):
    - Biometrics (fingerprints, retinal scans, facial recognition)
    - Behavioral biometrics (typing patterns, gait analysis)
4. **Somewhere you are** (Location factor):
    - GPS location
    - Network location
5. **Something you do** (Behavior factor):
    - Signature analysis
    - Voice recognition

Authentication Methods

1. **Password-based Authentication**:
   Despite known vulnerabilities, passwords remain the most common form of authentication. Best practices for password security include:
    - Enforcing strong password policies (length, complexity, expiration)
    - Implementing account lockout after multiple failed attempts
    - Using salted hashes to store passwords
    - Encouraging the use of password managers
2. **Multi-Factor Authentication (MFA)**:
   MFA combines two or more authentication factors, significantly enhancing security. Common implementations include:
    - Password + SMS code
    - Password + authenticator app
    - Smart card + PIN
    - Biometric + password

3. **Biometric Authentication**:
   Biometrics offer a high level of security but come with unique challenges:
   - Advantages: Difficult to forge, can't be forgotten or lost
   - Challenges: Privacy concerns, potential for false positives/negatives, difficulty in changing if compromised
4. **Token-based Authentication**:
   Tokens can be physical devices or software-based:
   - Hardware tokens: Generate time-based one-time passwords (TOTP)
   - Software tokens: Mobile apps that generate authentication codes
   - JSON Web Tokens (JWT): Used for authentication in web applications
5. **Certificate-based Authentication**:
   Digital certificates, often used in conjunction with Public Key Infrastructure (PKI), provide a robust method of authentication:
   - Commonly used in SSL/TLS for secure web communications
   - Can be stored on smart cards for physical access control
6. **Risk-based Authentication**:

This adaptive approach considers contextual factors to determine the level of authentication required:

- Factors may include location, device, time of access, and behavior patterns
- Can trigger additional authentication steps if suspicious activity is detected

Challenges in Authentication

1. **Balancing Security and Usability**:
   Stronger authentication methods often come at the cost of user convenience. Finding the right balance is crucial for user adoption and overall security effectiveness.
2. **Managing Multiple Identities**:
   Users often have numerous accounts across various systems, leading to password fatigue and potentially risky behaviors like password reuse.
3. **Account Recovery**:
   Secure and user-friendly account recovery mechanisms are essential, especially for systems using strong authentication methods.
4. **Privacy Concerns**:

Biometric authentication and location-based methods raise privacy issues that must be carefully addressed.

5. **Scalability**:
   Authentication systems must be able to handle large numbers of users and authentication requests efficiently.
6. **Integration with Legacy Systems**:
   Implementing modern authentication methods in environments with legacy systems can be challenging.

Emerging Trends in Authentication

1. **Passwordless Authentication**:
   Moving away from traditional passwords towards methods like biometrics, hardware tokens, or magic links sent via email.
2. **Continuous Authentication**:
   Constantly verifying user identity throughout a

session based on behavioral patterns and other contextual factors.

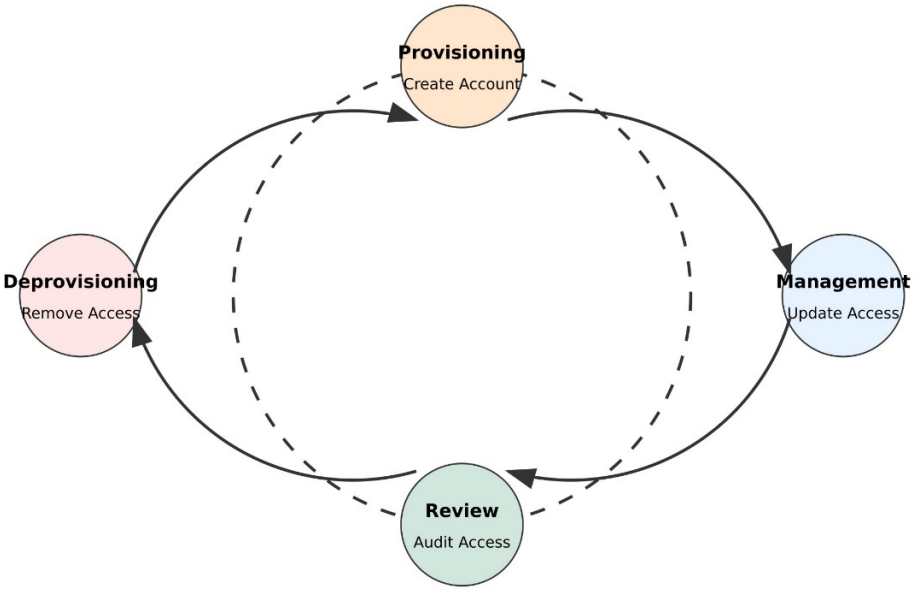
3. **Adaptive Authentication**:
   Dynamically adjusting authentication requirements based on risk assessment of each access attempt.
4. **Blockchain-based Identity**:
   Using blockchain technology to create decentralized, user-controlled digital identities.
5. **AI and Machine Learning**:
   Enhancing authentication systems with AI to detect anomalies and improve accuracy in biometric and behavioral authentication.

Best Practices for Implementing Authentication

1. Implement multi-factor authentication, especially for sensitive systems and privileged accounts.
2. Regularly review and update authentication policies and mechanisms.
3. Educate users about the importance of strong authentication and potential risks.
4. Monitor authentication logs for suspicious activities.
5. Implement secure password reset and account recovery procedures.
6. Consider the specific needs and risk profile of your organization when choosing authentication methods.
7. Ensure compliance with relevant regulations and standards (e.g., GDPR, PCI DSS) in authentication implementations.
8. Regularly test the security of authentication systems through penetration testing and security audits.

ffective identification and authentication are critical components of a robust security strategy. By implementing strong, multi-layered authentication methods and staying abreast of emerging trends and best practices, organizations can significantly enhance their security posture and protect against unauthorized access to sensitive resources and data.

Identity Management



Identity Management (IdM), also known as Identity and Access Management (IAM), is a comprehensive framework of policies, processes, and technologies used to manage digital identities and control access to resources within an organization. It encompasses the entire lifecycle of user identities, from creation to termination, and ensures that the right individuals have the appropriate access to the right resources at the right times for the right reasons.

Key Components of Identity Management

1. **Identity Lifecycle Management**:
    - User Provisioning: Creating and setting up new user accounts
    - Account Maintenance: Updating user information and access rights as roles change
    - De-provisioning: Removing or disabling accounts when users leave or change roles
2. **Authentication**:
    - Verifying user identities through various methods (passwords, biometrics, tokens, etc.)
    - Implementing multi-factor authentication for enhanced security
3. **Authorization**:
    - Determining what resources and actions a user is allowed to access or perform
    - Implementing access control models (e.g., Role-Based Access Control)
4. **Directory Services**:
    - Centralized storage of user identities and attributes
    - Examples include Active Directory, LDAP, and cloud-based directory services
5. **Single Sign-On (SSO)**:
    - Allowing users to access multiple applications with a single set of credentials
    - Enhancing user experience and reducing password fatigue
6. **Federation**:
    - Enabling users to access resources across different organizations or domains

- Implementing standards like SAML, OAuth, and OpenID Connect

7. **Audit and Compliance**:
   - Monitoring and logging user activities and access attempts
   - Generating reports for compliance and security analysis
8. **Self-Service Capabilities**:
   - Allowing users to manage their own accounts, reset passwords, and request access

Identity Lifecycle Management

The identity lifecycle encompasses several stages:

1. **Joiner Process**:
   - Account creation based on HR or other authoritative sources
   - Assignment of initial access rights and roles
   - Provisioning of necessary resources (email, applications, etc.)
2. **Mover Process**:
   - Updating access rights as users change roles within the organization
   - Revoking unnecessary access and granting new permissions
   - Ensuring compliance with the principle of least privilege
3. **Leaver Process**:
   - Promptly disabling or deleting accounts when users leave the organization
   - Revoking all access rights and recovering company assets

- Archiving user data as required for compliance or business needs

Identity Governance

Identity Governance is a crucial aspect of IdM that focuses on ensuring that access rights are appropriate and compliant with organizational policies and regulations. Key components include:

1. **Access Certification**:
   - Periodic reviews of user access rights
   - Involving managers or resource owners in the review process
2. **Segregation of Duties (SoD)**:
   - Preventing conflicts of interest by separating critical functions
   - Implementing controls to detect and prevent SoD violations
3. **Policy Enforcement**:
   - Automating the enforcement of access policies
   - Ensuring compliance with regulatory requirements (e.g., GDPR, HIPAA)
4. **Risk-Based Access Control**:
   - Dynamically adjusting access rights based on risk factors
   - Considering contextual information like location, time, and device

Challenges in Identity Management

1. **Integration with Legacy Systems**:
   - Many organizations struggle to integrate modern IdM solutions with older systems that may lack robust identity capabilities.

2. **Cloud and Hybrid Environments**:
    - Managing identities across on-premises and cloud-based resources can be complex.
3. **Scalability**:
    - IdM systems must be able to handle growing numbers of users, devices, and applications.
4. **User Experience**:
    - Balancing security requirements with user convenience is an ongoing challenge.
5. **Insider Threats**:
    - IdM systems must account for the possibility of malicious actions by authorized users.
6. **Compliance and Regulations**
    - IdM systems must ensure compliance with various data protection and privacy regulations like GDPR, HIPAA, SOX, etc.
    - This involves implementing appropriate access controls, audit trails, and reporting capabilities.
    - Regular compliance audits and assessments are necessary to verify adherence to regulatory requirements.

7. **Integration Challenges:**
    - Integrating IdM systems with legacy applications and diverse IT environments can be complex.
    - **Ensuring seamless user experience across multiple systems and platforms is crucial.**
8. **Identity Lifecycle Management:**

- Managing identities throughout their lifecycle, from creation to deactivation, requires robust processes and automation.
- **This includes handling role changes, transfers, and departures efficiently.**

9. **Privileged Access Management:**
    - Securing and monitoring privileged accounts is critical, as these pose the highest risk if compromised.
    - **Implementing just-in-time privileged access and session monitoring are important controls.**
10. **Emerging Technologies:**
    - Adapting IdM systems to new technologies like cloud services, IoT devices, and blockchain presents ongoing challenges.
    - **Balancing security with the flexibility needed for digital transformation initiatives is key.**

Best Practices for Identity Management:

1. Implement the principle of least privilege
2. Use multi-factor authentication for sensitive systems and privileged accounts
3. Regularly review and audit access rights
4. Automate identity lifecycle processes where possible
5. Implement strong password policies and consider passwordless authentication methods

6. Maintain detailed logs and audit trails of identity-related activities
7. Provide ongoing security awareness training for users
8. Implement a formal process for access requests and approvals
9. Regularly test and update IdM systems to address new threats
10. Integrate IdM with other security systems like SIEM for better threat detection

By addressing these challenges and following best practices, organizations can build robust identity management systems that enhance security, improve user experience, and meet compliance requirements. However, IdM is an ongoing process that requires continuous evaluation and improvement to keep pace with evolving threats and business needs.

Access Control Models and Access Control Systems

Access control models and systems are fundamental components of identity and access management, providing frameworks and mechanisms to regulate access to resources. These models define how subjects (users or processes) can interact with objects (files, databases, systems) based on predefined rules and policies.

Discretionary Access Control (DAC) is one of the most common access control models. In DAC, the owner of a resource has the discretion to grant or revoke access rights to other users. This model is flexible but can lead to security issues if owners make poor decisions about access rights.

DAC is often implemented through access control lists (ACLs) attached to objects.

Mandatory Access Control (MAC) is a more rigid model where access decisions are made by the system based on security labels assigned to subjects and objects. In a MAC system, users cannot override or modify these access rules. This model is commonly used in high-security environments, such as military systems.

Role-Based Access Control (RBAC) assigns access rights based on roles within an organization. Users are assigned to roles, and roles are assigned permissions. This model simplifies access management, especially in large organizations with frequent personnel changes. RBAC aligns well with the principle of least privilege, ensuring users have only the access necessary for their job functions.

Attribute-Based Access Control (ABAC) is a more flexible and granular model that makes access decisions based on attributes of the user, resource, action, and environment. ABAC can implement complex access policies that consider multiple factors, making it suitable for dynamic and context-aware access control scenarios.

Rule-Based Access Control uses predefined rules to determine access rights. These rules can be based on various factors such as time of day, location, or system status. Rule-based systems can be used to implement both DAC and MAC models.

Access Control Systems are the practical implementations of these models. They typically include the following components:

- **Authentication mechanisms**: These verify the identity of users or systems attempting to access resources. Common methods include passwords,

biometrics, smart cards, and multi-factor authentication.

- **Authorization systems**: Once authenticated, these systems determine what actions the user is allowed to perform based on the access control model in use.
- **Auditing and logging**: These components record access attempts and activities for security monitoring and compliance purposes.
- **Policy administration**: Tools and interfaces for managing access control policies, user accounts, and permissions.

Physical Access Control Systems are also crucial, controlling entry to buildings, rooms, and other physical spaces. These can include:

- **Badge systems**: Using ID cards with magnetic strips or RFID chips.
- **Biometric systems**: Utilizing fingerprints, retinal scans, or facial recognition.
- **Mantrap doors**: Creating secure entry points with interlocking doors.

Logical Access Control Systems protect digital resources and can include:

- **Firewalls**: Controlling network traffic based on predefined security rules.
- **Virtual Private Networks (VPNs)**: Providing secure remote access to network resources.
- **Database access controls**: Managing access to specific data within databases.

Privileged Access Management (PAM) is a critical aspect of access control systems, focusing on securing,

controlling, and monitoring access to critical assets by privileged users. PAM systems often include features like password vaulting, session recording, and just-in-time privilege elevation.

Network Access Control (NAC) systems enforce security policies on devices attempting to connect to a network. They can check for compliance with security standards before granting network access.

Implementing effective access control requires a balance between security and usability. Overly restrictive controls can hinder productivity, while lax controls expose organizations to security risks. Regular audits and reviews of access rights are essential to maintain the principle of least privilege and ensure that access controls remain aligned with organizational needs and security policies.

Single Sign-On and Federation

Single Sign-On (SSO) and federation are advanced identity and access management concepts that aim to simplify user authentication and authorization across multiple systems or organizations while maintaining security.

Single Sign-On (SSO) is an authentication scheme that allows a user to log in once and gain access to multiple applications or systems without the need to re-enter credentials. The key benefits of SSO include:

- **Improved user experience**: Users only need to remember one set of credentials.
- **Increased productivity**: Less time spent on login processes.
- **Enhanced security**: Reduced risk of password fatigue leading to weak passwords.

- **Simplified administration**: Centralized user management and access control.

There are several types of SSO implementations:

1. **Enterprise SSO (E-SSO)**: Works at the application level, often using a password vault to store and automatically input credentials for legacy applications.
2. **Web SSO**: Utilizes web-based authentication protocols like SAML, OAuth, or OpenID Connect to provide SSO for web applications.
3. **Kerberos-based SSO**: Uses the Kerberos protocol to authenticate users and provide tickets for accessing various services.
4. **Smart card SSO**: Employs physical smart cards for authentication, often used in high-security environments.

Federation extends the concept of SSO across multiple organizations or security domains. It allows users from one domain (the identity provider) to access resources in another domain (the service provider) without the need for separate accounts or credentials. Key aspects of federation include:

- **Trust relationships**: Established between participating organizations to accept each other's authentication assertions.
- **Identity provider (IdP)**: The entity responsible for authenticating users and issuing security tokens or assertions.
- **Service provider (SP)**: The entity that relies on the identity provider's assertions to grant access to its resources.

- **Claims**: Statements about the user (such as role, department, or access rights) that are passed from the IdP to the SP.

Federation protocols are standardized methods for implementing SSO and federation:

1. **Security Assertion Markup Language (SAML)**: An XML-based open standard for exchanging authentication and authorization data between parties. SAML is widely used for web-based SSO and federation.
2. **OAuth**: An authorization framework that allows applications to obtain limited access to user accounts on other services. While not primarily an authentication protocol, OAuth is often used in conjunction with OpenID Connect for SSO scenarios.
3. **OpenID Connect**: Built on top of OAuth 2.0, OpenID Connect adds an identity layer, providing user authentication and basic profile information.
4. **WS-Federation**: Part of the WS-* set of web service specifications, used primarily in Microsoft environments.

Benefits of federation include:

- **Improved collaboration**: Easier sharing of resources across organizational boundaries.
- **Cost reduction**: Eliminates the need for managing separate accounts for external users.
- **Enhanced security**: Reduces the attack surface by centralizing authentication.
- **Compliance**: Can help meet regulatory requirements for access control and data protection.

Challenges and considerations for implementing SSO and federation:

- **Single point of failure**: If the SSO system goes down, it can affect access to multiple applications.
- **Increased impact of compromised credentials**: A single set of compromised credentials can grant access to multiple systems.
- **Complexity**: Implementing and maintaining federation across organizations can be technically challenging.
- **Trust management**: Establishing and maintaining trust relationships between federated entities requires ongoing effort.
- **Privacy concerns**: Sharing user information across organizational boundaries may raise privacy issues.

To address these challenges, organizations implementing SSO and federation should:

- Implement strong authentication methods, preferably multi-factor authentication.
- Regularly audit and review access rights and trust relationships.
- Use encryption for all communication between federated entities.
- Implement robust monitoring and logging to detect and respond to suspicious activities.
- Develop clear policies and agreements governing the sharing and use of identity information.

By carefully implementing SSO and federation, organizations can significantly improve their identity and access management capabilities, enhancing both security and user experience across their digital ecosystems.

Chapter 6: Security Assessment and Testing

Security assessment and testing are critical components of an organization's overall security program. This domain focuses on the strategies, processes, and techniques used to evaluate the effectiveness of security controls and identify vulnerabilities in systems, networks, and applications. The goal is to provide a comprehensive view of an organization's security posture and drive continuous improvement.

Key aspects include developing assessment and test strategies that align with business objectives and risk tolerance. This involves planning various types of security tests, from vulnerability scans to full-scale penetration testing. Security process data plays a crucial role, as it provides the metrics and information needed to measure the effectiveness of security controls and identify areas for improvement.

Security control testing encompasses a wide range of activities, including configuration reviews, code analysis, and social engineering tests. These assessments help verify that implemented controls are functioning as intended and identify any gaps in security.

Test outputs are essential for communicating findings to stakeholders and driving remediation efforts. This includes developing clear, actionable reports that prioritize risks and provide recommendations for addressing vulnerabilities.

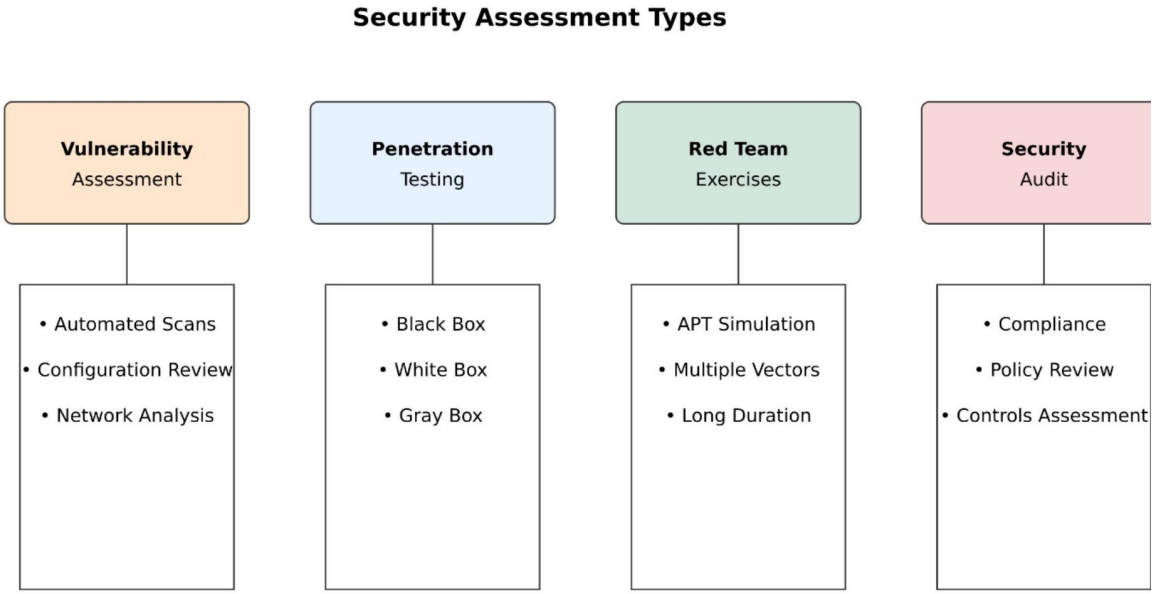
Finally, understanding security architecture vulnerabilities is crucial for building robust defenses. This involves analyzing how different components of the security architecture

interact and identifying potential weak points that could be exploited by attackers.

By mastering these concepts, security professionals can develop comprehensive assessment programs that provide valuable insights into their organization's security posture and drive continuous improvement in their overall security strategy.

Assessment and Test Strategies

Assessment and test strategies form the foundation of an effective security evaluation program. These strategies outline the approach, scope, and methodologies used to assess an organization's security posture and identify vulnerabilities. A well-designed strategy ensures that security assessments are comprehensive, aligned with business objectives, and provide actionable insights for improving overall security.



Key Components of Assessment Strategies

1. **Objectives and Scope**: Clearly define the goals of the assessment and what systems, networks, or processes will be evaluated. This should align with the organization's risk management strategy and compliance requirements.
2. **Methodology Selection**: Choose appropriate assessment methodologies based on the objectives.

This may include vulnerability scanning, penetration testing, code review, or social engineering tests.

3. **Resource Allocation**: Determine the personnel, tools, and time required to conduct the assessment effectively.
4. **Scheduling and Frequency**: Establish a timeline for assessments, including the frequency of recurring tests. This should balance the need for regular evaluation with operational impact.
5. **Stakeholder Involvement**: Identify key stakeholders and their roles in the assessment process, including management, IT teams, and third-party vendors if applicable.
6. **Compliance Considerations**: Ensure the strategy addresses relevant regulatory and industry standards, such as PCI DSS, HIPAA, or ISO 27001.

Types of Security Assessments

1. **Vulnerability Assessments**: These scans identify known vulnerabilities in systems, networks, and applications. They provide a broad overview of potential weaknesses but typically do not involve active exploitation.
2. **Penetration Testing**: This involves simulating real-world attacks to identify vulnerabilities and test the effectiveness of security controls. Penetration tests can be categorized as:
    - **Black Box**: Testers have no prior knowledge of the target systems.
    - **White Box**: Testers are provided with detailed information about the target environment.

- **Gray Box**: A combination of black and white box approaches.

3. **Red Team Exercises**: These are more comprehensive than typical penetration tests, often involving multiple attack vectors and lasting for extended periods to simulate advanced persistent threats (APTs).
4. **Social Engineering Tests**: These assess human vulnerabilities through techniques like phishing, pretexting, or physical security breaches.
5. **Code Reviews**: Systematic examination of source code to identify security flaws and ensure adherence to secure coding practices.
6. **Configuration Reviews**: Evaluation of system and network configurations against security best practices and organizational standards.
7. **Compliance Audits**: Assessments specifically designed to verify compliance with regulatory requirements or industry standards.

Developing an Effective Test Strategy

1. **Risk-Based Approach**: Prioritize assessment efforts based on the criticality of assets and potential impact of vulnerabilities. This ensures resources are focused on the most significant risks.
2. **Continuous Assessment**: Move beyond point-in-time assessments to implement continuous monitoring and testing processes. This helps identify new vulnerabilities and changes in the security posture more quickly.
3. **Automation**: Leverage automated tools and processes where appropriate to increase efficiency and coverage of assessments.

4. **Diversity of Techniques**: Employ a variety of assessment methods to gain a comprehensive view of the security posture. Relying on a single technique may leave blind spots.
5. **Scenario-Based Testing**: Develop realistic attack scenarios based on current threat intelligence to test specific aspects of the security program.
6. **Metrics and Benchmarking**: Establish key performance indicators (KPIs) to measure the effectiveness of the security program over time and compare against industry benchmarks.
7. **Remediation Planning**: Include processes for prioritizing and addressing identified vulnerabilities as part of the overall strategy.

Challenges and Considerations

1. **Operational Impact**: Balance the need for thorough testing with minimizing disruption to business operations. This may involve scheduling tests during off-hours or using staged environments.
2. **Scope Creep**: Clearly define and maintain boundaries for assessments to prevent unintended expansion of scope, which can lead to increased costs and delays.
3. **False Positives**: Implement processes to validate and prioritize findings to avoid wasting resources on non-issues.
4. **Skill Gap**: Ensure the assessment team has the necessary expertise to conduct thorough evaluations across various technologies and attack vectors.

5. **Evolving Threat Landscape**: Regularly update assessment strategies to address new threats and attack techniques.
6. **Cloud and Third-Party Assessments**: Develop strategies for assessing security in cloud environments and evaluating the security posture of third-party vendors and partners.
7. **Legal and Ethical Considerations**: Ensure all assessment activities comply with legal requirements and ethical standards, including obtaining proper authorization and protecting sensitive data.

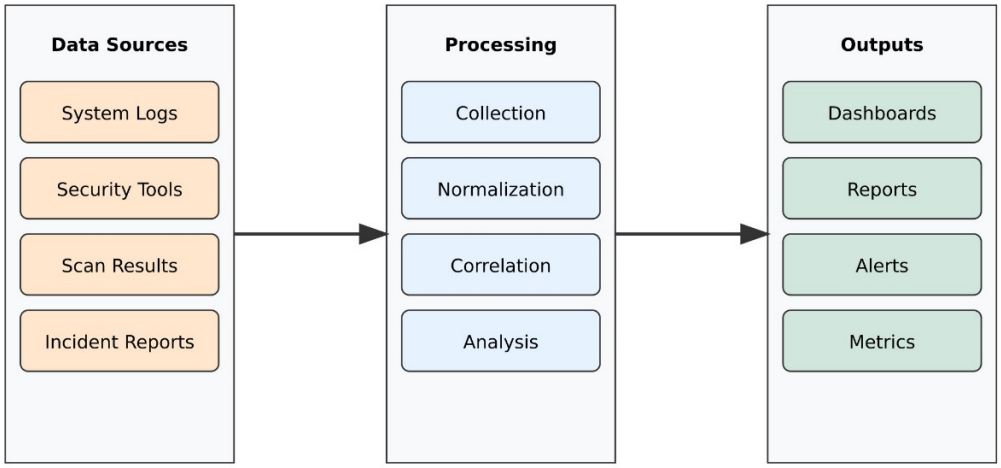
Communicating Assessment Strategies

Effective communication of assessment strategies is crucial for gaining support from stakeholders and ensuring smooth execution:

1. **Executive Summary**: Provide a high-level overview of the strategy, its objectives, and expected outcomes for senior management.
2. **Detailed Planning Documents**: Develop comprehensive plans outlining methodologies, timelines, and resource requirements for technical teams.
3. **Stakeholder Briefings**: Conduct briefings with relevant departments to explain the assessment process and address concerns.
4. **Reporting Templates**: Establish standardized reporting formats to ensure consistent and clear communication of findings across different assessments.

By developing comprehensive and well-communicated assessment and test strategies, organizations can systematically evaluate their security posture, identify vulnerabilities, and drive continuous improvement in their overall security program. These strategies should be living documents, regularly reviewed and updated to address changes in the threat landscape, technology environment, and business objectives.

Security Process Data



Security process data plays a crucial role in assessing and improving an organization's security posture. This data encompasses a wide range of information collected from various security processes, tools, and activities. Properly collecting, analyzing, and interpreting this data is essential for making informed decisions about security investments, identifying trends, and measuring the effectiveness of security controls.

Types of Security Process Data

1. **Log Data**: Logs from various systems, applications, and security devices provide valuable information about events, access attempts, and potential security incidents. Key sources include:
    - Firewall logs
    - Intrusion Detection/Prevention System (IDS/IPS) logs

- Authentication logs
- Application logs
- System logs

2. **Vulnerability Scan Results**: Data from regular vulnerability scans, including:
    - Identified vulnerabilities
    - Severity ratings
    - Affected systems and applications
    - Remediation recommendations
3. **Patch Management Data**: Information related to the patching process:
    - Patch levels of systems
    - Patch deployment status
    - Time to patch critical vulnerabilities
4. **Incident Response Metrics**: Data collected during and after security incidents:
    - Number and types of incidents
    - Time to detect and respond
    - Root cause analysis results
    - Impact assessments
5. **Access Control Data**: Information about user access and privileges:
    - User account creation, modification, and deletion
    - Access attempts (successful and failed)
    - Privilege escalation events
6. **Security Awareness Training Metrics**: Data related to employee security training:
    - Training completion rates
    - Test scores

- Phishing simulation results

7. **Asset Inventory Data**: Information about the organization's IT assets:
    - Hardware and software inventory
    - Asset configurations
    - End-of-life and support status
8. **Threat Intelligence Data**: Information about current and emerging threats:
    - Indicators of compromise (IoCs)
    - Threat actor tactics, techniques, and procedures (TTPs)
    - Vulnerability intelligence

Collecting and Managing Security Process Data

Effective collection and management of security process data involve several key considerations:

1. **Data Collection Tools**: Implement appropriate tools to gather data from various sources, such as:
    - Security Information and Event Management (SIEM) systems
    - Log management solutions
    - Vulnerability management platforms
    - Governance, Risk, and Compliance (GRC) tools
2. **Data Quality**: Ensure the accuracy, completeness, and timeliness of collected data:
    - Implement data validation processes
    - Regularly audit data collection mechanisms
    - Address any gaps in data collection
3. **Data Retention**: Establish policies for data retention that balance security needs with legal and

regulatory requirements:
    - Define retention periods for different types of data
    - Implement secure storage and archiving processes
    - Ensure proper data destruction when retention periods expire
4. **Data Normalization**: Standardize data from various sources to enable effective analysis:
    - Use common formats and taxonomies
    - Correlate data across different systems and tools
5. **Access Control**: Implement appropriate access controls to protect sensitive security data:
    - Apply the principle of least privilege
    - Use role-based access control (RBAC)
    - Implement strong authentication for accessing security data

Analyzing Security Process Data

Effective analysis of security process data is crucial for deriving actionable insights:

1. **Trend Analysis**: Identify patterns and trends over time:
    - Monitor changes in the number and types of security events
    - Track improvements in key security metrics
    - Identify emerging threats or vulnerabilities
2. **Correlation Analysis**: Connect data from different sources to gain a more comprehensive view:
    - Correlate log data with vulnerability scan results

    - Link security events to specific assets or users
3. **Anomaly Detection**: Identify unusual patterns or behaviors that may indicate security issues:
    - Use statistical analysis or machine learning techniques
    - Establish baselines for normal behavior
4. **Risk Assessment**: Use security process data to inform risk assessments:
    - Identify high-risk assets or processes
    - Quantify potential impact of vulnerabilities
5. **Compliance Monitoring**: Analyze data to ensure compliance with security policies and regulations:
    - Track compliance with patching policies
    - Monitor access control compliance
6. **Performance Measurement**: Use data to measure the effectiveness of security controls and processes:
    - Calculate mean time to detect (MTTD) and mean time to respond (MTTR) for incidents
    - Measure the effectiveness of security awareness training

Reporting and Visualization

Effective communication of security process data is essential for driving action and improvement:

1. **Executive Dashboards**: Provide high-level overviews of key security metrics for senior management:
    - Overall risk posture
    - Compliance status
    - Trend analysis of critical metrics

2. **Operational Reports**: Detailed reports for security teams and IT staff:
    - Vulnerability reports
    - Incident response summaries
    - Patch compliance reports
3. **Data Visualization**: Use charts, graphs, and other visual representations to make data more accessible and understandable:
    - Heat maps for vulnerability distribution
    - Time series graphs for trend analysis
    - Network diagrams for visualizing security events
4. **Automated Alerting**: Implement systems to automatically alert relevant personnel when specific thresholds or conditions are met:
    - Critical vulnerability detections
    - Unusual access patterns
    - Compliance violations

Challenges in Managing Security Process Data

1. **Data Volume**: The sheer amount of security data generated can be overwhelming. Implementing effective data management and analysis strategies is crucial.
2. **Data Silos**: Security data often resides in different systems and departments. Breaking down these silos is essential for comprehensive analysis.
3. **False Positives**: Security tools can generate a high number of false positives. Developing processes to validate and prioritize alerts is important.
4. **Skill Gap**: Analyzing security process data often requires specialized skills. Organizations may need

to invest in training or hire data analysis experts.

5. **Privacy Concerns**: Security process data may contain sensitive information. Ensuring proper data protection and compliance with privacy regulations is crucial.

By effectively collecting, analyzing, and leveraging security process data, organizations can gain valuable insights into their security posture, identify areas for improvement, and make data-driven decisions to enhance their overall security program. This data-driven approach is essential for adapting to the ever-evolving threat landscape and demonstrating the value of security investments to stakeholders.

Security Control Testing

Security control testing is a critical component of an organization's overall security program. It involves systematically evaluating the effectiveness of implemented security measures to ensure they are functioning as intended and providing adequate protection against potential threats. This process helps identify vulnerabilities, gaps in security coverage, and areas for improvement in the organization's security posture.

Types of Security Controls

Before discussing testing methods, it's important to understand the different types of security controls:

1. **Technical Controls**: Hardware and software mechanisms used to protect assets and enforce security policies. Examples include firewalls, intrusion detection systems, and encryption.
2. **Administrative Controls**: Policies, procedures, and guidelines that define security practices and expectations. These include security policies,

employee training programs, and incident response plans.

3. **Physical Controls**: Measures to protect physical assets and prevent unauthorized physical access. Examples include locks, security cameras, and access control systems.

Security Control Testing Methodologies

1. **Vulnerability Assessments**: Systematic examination of systems, networks, and applications to identify known vulnerabilities. This typically involves using automated scanning tools to detect misconfigurations, missing patches, and other security weaknesses.
2. **Penetration Testing**: Simulated attacks conducted by skilled security professionals to identify vulnerabilities that could be exploited by malicious actors. Penetration tests can be categorized as:
    - **External**: Testing from outside the organization's network
    - **Internal**: Testing from within the internal network
    - **Web Application**: Focused on identifying vulnerabilities in web-based applications
3. **Configuration Reviews**: Detailed examination of system and network configurations to ensure they align with security best practices and organizational policies.
4. **Code Reviews**: Systematic inspection of application source code to identify security flaws and ensure adherence to secure coding practices.

5. **Social Engineering Tests**: Assessments designed to evaluate human vulnerabilities and the effectiveness of security awareness training. These may include phishing simulations, pretexting, or physical security tests.
6. **Red Team Exercises**: Comprehensive, multi-faceted simulations that test an organization's detection and response capabilities across multiple attack vectors.
7. **Compliance Audits**: Assessments specifically designed to verify compliance with regulatory requirements or industry standards, such as PCI DSS, HIPAA, or ISO 27001.

Planning and Executing Security Control Tests

1. **Scope Definition**: Clearly define the systems, networks, and processes to be tested. This should align with the organization's risk assessment and prioritization.
2. **Methodology Selection**: Choose appropriate testing methodologies based on the scope and objectives of the assessment.
3. **Resource Allocation**: Determine the personnel, tools, and time required to conduct the tests effectively.
4. **Authorization and Communication**: Obtain proper authorization for testing activities and communicate plans to relevant stakeholders to minimize disruption and avoid false alarms.
5. **Test Execution**: Conduct tests according to the defined methodology, ensuring proper documentation of all activities and findings.

6. **Result Analysis**: Carefully analyze test results to identify vulnerabilities, assess their potential impact, and prioritize remediation efforts.
7. **Reporting**: Develop clear, actionable reports that communicate findings to both technical and non-technical stakeholders.

Specific Testing Techniques

1. **Network Security Testing**:
    - Port scanning to identify open ports and services
    - Firewall rule testing to verify proper configuration
    - Wireless network security assessments
    - VPN security testing
2. **Application Security Testing**:
    - Static Application Security Testing (SAST) to analyze source code
    - Dynamic Application Security Testing (DAST) to test running applications
    - Interactive Application Security Testing (IAST) combining elements of SAST and DAST
    - API security testing
3. **Cloud Security Testing**:
    - Assessing security configurations in cloud environments
    - Testing identity and access management controls
    - Evaluating data protection measures in the cloud
4. **Mobile Device Security Testing**:

- Testing mobile device management (MDM) solutions
- Assessing security of mobile applications
- Evaluating mobile device encryption

Additional mobile security testing considerations include:

- **Network security testing**: Assessing the security of Wi-Fi, cellular, and Bluetooth connections on mobile devices.
- **Authentication testing**: Evaluating the strength of authentication mechanisms like passcodes, biometrics, and multi-factor authentication.
- **Data leakage testing**: Checking for unintended data exposure through clipboard contents, temporary files, or app caches.
- **Malware detection**: Testing the effectiveness of anti-malware solutions on mobile platforms.
- **Jailbreak/root detection**: Assessing the ability to detect compromised devices that may bypass security controls.
- **Secure communication**: Evaluating the use of VPNs, SSL/TLS, and certificate pinning for secure data transmission.
- **Privacy controls**: Testing features that protect user privacy, such as app permissions and location services management.
- **Secure boot and firmware**: Assessing the integrity of the device's boot process and firmware to prevent low-level attacks.

Mobile security testing requires a comprehensive approach that addresses the unique challenges of mobile platforms

while considering the organization's specific risk profile and compliance requirements.

Test Outputs

Test outputs are critical components of the security assessment and testing process. They provide valuable insights into the security posture of an organization and help drive remediation efforts. The key outputs from security testing typically include:

Vulnerability Reports: These detailed reports list all vulnerabilities discovered during testing, often categorized by severity level (e.g., critical, high, medium, low). Each vulnerability entry usually includes:

- A description of the vulnerability
- The affected systems or components
- Potential impact if exploited
- Steps to reproduce the vulnerability
- Recommendations for remediation

Risk Assessment: Based on the vulnerabilities discovered, a risk assessment is often provided to help prioritize remediation efforts. This may include:

- Likelihood of exploitation
- Potential business impact
- Overall risk rating

Executive Summary: A high-level overview of the testing results, suitable for management and stakeholders. This typically includes:

- Scope of the assessment

- Key findings and themes
- Overall risk posture
- High-priority recommendations

Technical Details: In-depth technical information about the vulnerabilities, often including:

- Exploit code or proof-of-concept demonstrations
- System configurations
- Network diagrams
- Raw scan data

Remediation Plan: A proposed plan for addressing the identified vulnerabilities, including:

- Prioritized list of actions
- Estimated effort and timelines
- Potential compensating controls

Compliance Status: If applicable, an assessment of the organization's compliance with relevant standards or regulations based on the test results.

Metrics and Trends: Quantitative data on the security posture, which may include:

- Number of vulnerabilities by severity
- Comparison to industry benchmarks
- Trends over time if historical data is available

Evidence and Artifacts: Supporting documentation such as screenshots, log files, and other data collected during testing.

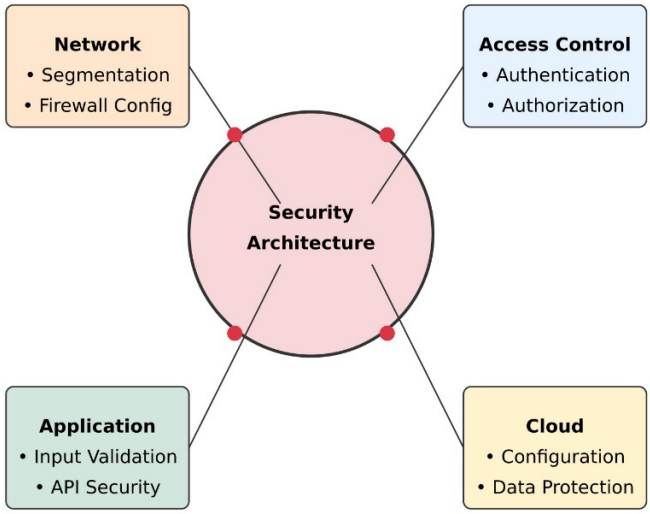
To ensure test outputs are effective:

- Use clear, concise language appropriate for the intended audience

- Provide actionable recommendations
- Prioritize findings based on risk and business impact
- Include both technical and non-technical summaries
- Use visualizations (charts, graphs) to convey key points
- Ensure reports are delivered securely to protect sensitive information

Properly formatted and comprehensive test outputs are essential for helping organizations understand their security posture and make informed decisions about risk management and resource allocation.

Security Architectures Vulnerabilities



Security architecture vulnerabilities are weaknesses or flaws in the design and implementation of an organization's overall security structure. Identifying and addressing these vulnerabilities is crucial for maintaining a robust security posture. Key areas of focus include:

Network Design Vulnerabilities:

- Lack of network segmentation
- Improper firewall configuration
- Insecure wireless networks

- Inadequate intrusion detection/prevention systems

Access Control Weaknesses:

- Overly permissive access rights
- Weak authentication mechanisms
- Lack of multi-factor authentication
- Inadequate privileged access management

Cryptographic Flaws:

- Use of weak or outdated encryption algorithms
- Poor key management practices
- Insufficient encryption of sensitive data at rest and in transit

Application Security Issues:

- Lack of input validation
- Cross-site scripting (XSS) vulnerabilities
- SQL injection flaws
- Insecure API implementations

Physical Security Weaknesses:

- Inadequate physical access controls
- Insufficient environmental controls (e.g., fire suppression, temperature regulation)
- Poor asset management and tracking

Cloud Security Concerns:

- Misconfigurations in cloud services
- Inadequate data protection in multi-tenant environments

- Lack of visibility into cloud provider security practices

Identity and Access Management (IAM) Flaws:

- Weak password policies
- Inadequate user provisioning and de-provisioning processes
- Lack of centralized identity management

Monitoring and Logging Deficiencies:

- Insufficient logging of security events
- Lack of real-time monitoring
- Inadequate log retention and protection

Incident Response and Business Continuity Weaknesses:

- Lack of formal incident response plans
- Inadequate disaster recovery procedures
- Insufficient testing of business continuity plans

Third-Party and Supply Chain Risks:

- Lack of vendor security assessments
- Insufficient contractual security requirements
- Poor integration of third-party systems

Compliance and Regulatory Gaps:

- Failure to meet industry-specific compliance requirements
- Inadequate data privacy controls
- Lack of regular compliance audits

Human Factors:

- Insufficient security awareness training
- Lack of clear security policies and procedures
- Inadequate enforcement of security practices

To address security architecture vulnerabilities:

1. Conduct regular security assessments and penetration tests
2. Implement a robust vulnerability management program
3. Adopt a defense-in-depth approach to security
4. Regularly update and patch systems and applications
5. Implement strong access controls and authentication mechanisms
6. Encrypt sensitive data both at rest and in transit
7. Conduct regular security awareness training for all employees
8. Implement and maintain comprehensive security policies and procedures
9. Regularly review and update the security architecture to address emerging threats
10. Engage in threat modeling to proactively identify potential vulnerabilities

By systematically addressing these vulnerabilities, organizations can significantly improve their overall security posture and reduce the risk of successful attacks or data breaches.

Chapter 7: Security Operations

Security operations encompass the day-to-day activities and processes that maintain an organization's security posture. This domain focuses on the practical implementation of security controls, incident response, disaster recovery, and ongoing monitoring to detect and mitigate threats. It covers a wide range of topics essential for maintaining the confidentiality, integrity, and availability of information assets.

Key areas include investigations and incident management, which involve detecting, responding to, and analyzing security incidents to minimize their impact and prevent future occurrences. Disaster recovery planning ensures business continuity in the face of major disruptions, outlining strategies to restore critical systems and data.

Logging and monitoring form the backbone of security operations, providing visibility into system activities and potential security events. Resource protection encompasses the measures taken to safeguard an organization's assets, including physical security, access controls, and data protection.

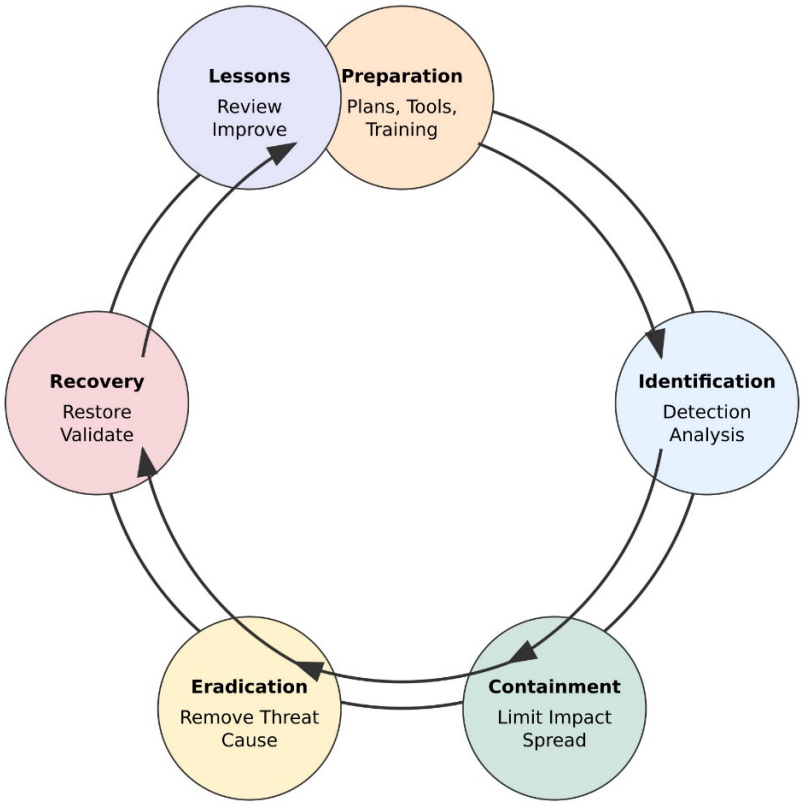
Foundational security operations concepts provide the framework for implementing effective security practices across the organization. This includes principles like least privilege, separation of duties, and defense in depth.

Change management is crucial for maintaining security in dynamic environments, ensuring that modifications to systems and processes are properly evaluated, tested, and implemented without introducing new vulnerabilities.

By mastering these concepts, security professionals can develop comprehensive operational security programs that effectively protect their organizations from a wide range of threats while supporting business objectives.

Investigations and Incident Management

Investigations and incident management are critical components of an organization's security operations. They involve the systematic approach to detecting, responding to, and analyzing security incidents to minimize their impact, prevent future occurrences, and maintain the overall security posture of the organization.



Incident Response Process

The incident response process typically follows a structured approach:

1. **Preparation**: This phase involves developing incident response plans, establishing a team, and ensuring necessary tools and resources are in place.
2. **Identification**: Detecting and confirming that a security incident has occurred. This often involves analyzing logs, alerts, and other indicators of compromise.
3. **Containment**: Taking immediate actions to limit the damage and prevent further spread of the incident. This may include isolating affected systems or revoking compromised credentials.
4. **Eradication**: Removing the root cause of the incident, such as malware or vulnerabilities that were exploited.
5. **Recovery**: Restoring affected systems to normal operation and ensuring they are free from compromise.
6. **Lessons Learned**: Conducting a post-incident review to identify areas for improvement in the incident response process and overall security posture.

Incident Response Team

An effective incident response team typically includes members with diverse skills:

- **Incident Response Manager**: Oversees the incident response process and coordinates team activities.
- **Security Analysts**: Investigate and analyze incidents, often specializing in areas like network security or malware analysis.

- **System Administrators**: Provide technical expertise on affected systems and assist with containment and recovery.
- **Legal Counsel**: Advises on legal implications and ensures compliance with relevant regulations.
- **Public Relations**: Manages communication with stakeholders and the public if necessary.

Digital Forensics

Digital forensics plays a crucial role in incident investigations. It involves the collection, preservation, and analysis of digital evidence to reconstruct events and support potential legal proceedings. Key aspects include:

- **Evidence Collection**: Gathering data from various sources while maintaining its integrity and chain of custody.
- **Forensic Analysis**: Examining collected data to identify relevant information and reconstruct the incident timeline.
- **Reporting**: Documenting findings in a clear, concise manner suitable for both technical and non-technical audiences.

Incident Classification and Triage

Not all incidents are equal in severity or impact. Effective incident management requires a system for classifying and prioritizing incidents:

- **Severity Levels**: Typically ranging from low to critical, based on factors like impact on operations, data sensitivity, and potential financial losses.
- **Triage Process**: Quickly assessing incoming incident reports to determine their severity and required response.

Communication and Reporting

Clear communication is essential throughout the incident management process:

- **Internal Communication**: Keeping stakeholders informed about the incident status, required actions, and potential impacts.
- **External Communication**: Managing communication with customers, partners, and regulatory bodies when necessary.
- **Incident Reports**: Documenting each incident, including its cause, impact, and resolution, to support future analysis and improvements.

Threat Intelligence

Incorporating threat intelligence into the incident management process can enhance an organization's ability to detect and respond to threats:

- **Indicators of Compromise (IoCs)**: Using known malicious IP addresses, file hashes, or other indicators to identify potential incidents.
- **Threat Feeds**: Subscribing to external threat intelligence sources to stay informed about emerging threats and attack techniques.

Automation and Orchestration

As the volume and complexity of security incidents increase, many organizations are turning to automation and orchestration tools to improve their incident response capabilities:

- **Security Orchestration, Automation, and Response (SOAR)**: Platforms that integrate

various security tools and automate routine incident response tasks.

- **Playbooks**: Predefined sequences of actions for responding to common types of incidents, which can be partially or fully automated.

Continuous Improvement

The incident management process should be subject to ongoing review and refinement:

- **Metrics and KPIs**: Tracking key performance indicators like mean time to detect (MTTD) and mean time to respond (MTTR) to measure and improve incident response effectiveness.
- **Tabletop Exercises**: Conducting simulated incident scenarios to test and improve the incident response process.
- **Post-Incident Reviews**: Thoroughly analyzing each significant incident to identify lessons learned and areas for improvement.

Regulatory Considerations

Many industries are subject to regulations that mandate specific incident reporting and handling requirements:

- **Data Breach Notification Laws**: Requirements for notifying affected individuals and authorities in case of data breaches.
- **Industry-Specific Regulations**: Such as HIPAA for healthcare or PCI DSS for organizations handling payment card data.

By implementing a comprehensive approach to investigations and incident management, organizations can effectively detect, respond to, and learn from security

incidents, ultimately strengthening their overall security posture and resilience against future threats.

Disaster Recovery

Disaster recovery (DR) is a critical component of an organization's business continuity strategy, focused on restoring IT systems and infrastructure following a major disruption. The goal of disaster recovery is to minimize downtime and data loss, ensuring that critical business operations can resume as quickly as possible after a disaster.

Disaster Recovery Planning

A comprehensive disaster recovery plan typically includes the following elements:

1. **Risk Assessment**: Identifying potential threats and vulnerabilities that could lead to disasters, such as natural disasters, cyberattacks, or equipment failures.
2. **Business Impact Analysis (BIA)**: Determining the potential effects of disasters on business operations, including financial losses, reputational damage, and regulatory compliance issues.
3. **Recovery Objectives**: Establishing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical systems and data.
    - RTO: The maximum acceptable time to restore a system or process after a disaster.
    - RPO: The maximum acceptable amount of data loss measured in time.
4. **Recovery Strategies**: Developing detailed plans for restoring systems, data, and infrastructure. This

may include:
    - Data backup and replication strategies
    - Alternate site preparations
    - Cloud-based recovery solutions
5. **Documentation**: Creating and maintaining comprehensive documentation of the DR plan, including contact information, system configurations, and step-by-step recovery procedures.
6. **Testing and Maintenance**: Regularly testing the DR plan and updating it to reflect changes in the IT environment and business needs.

Types of Disaster Recovery Sites

Organizations often establish alternate sites to support their disaster recovery efforts:

- **Hot Site**: A fully equipped facility with hardware, software, and data backups, ready for immediate operation.
- **Warm Site**: A partially equipped facility that requires some setup before it can support operations.
- **Cold Site**: A basic facility with power and environmental controls, but minimal equipment. Requires significant setup time.
- **Mobile Site**: A portable, self-contained unit that can be quickly deployed to a desired location.
- **Cloud-based DR**: Utilizing cloud services to provide scalable, on-demand recovery capabilities.

Data Backup and Replication

Effective data protection is crucial for successful disaster recovery:

- **Backup Methods**: Including full, incremental, and differential backups.
- **Offsite Storage**: Securely storing backup media at a separate location to protect against site-wide disasters.
- **Data Replication**: Continuously copying data to a secondary site or cloud environment for near-real-time recovery capabilities.

High Availability and Fault Tolerance

Implementing high availability and fault-tolerant systems can reduce the need for full-scale disaster recovery:

- **Redundant Systems**: Deploying duplicate hardware and software components to eliminate single points of failure.
- **Load Balancing**: Distributing workloads across multiple systems to improve performance and resilience.
- **Clustering**: Grouping servers to work together, providing continuous availability even if individual nodes fail.

Crisis Management and Communication

Effective communication is crucial during a disaster:

- **Crisis Communication Plan**: Outlining procedures for notifying employees, customers, and other stakeholders.
- **Emergency Contact Lists**: Maintaining up-to-date contact information for key personnel and external resources.
- **Media Relations**: Preparing strategies for managing public communications during and after a disaster.

Regulatory Compliance

Many industries have specific requirements for disaster recovery and business continuity:

- **HIPAA**: Mandates specific backup and disaster recovery requirements for healthcare organizations.
- **SOX**: Requires public companies to have controls in place to protect financial data, including disaster recovery capabilities.
- **GDPR**: Emphasizes the importance of data protection and availability, impacting disaster recovery strategies for organizations handling EU citizens' data.

Emerging Technologies in Disaster Recovery

New technologies are shaping the future of disaster recovery:

- **Containerization**: Using container technologies to package applications and dependencies for easier recovery and portability.
- **Artificial Intelligence and Machine Learning**: Enhancing disaster prediction, automated recovery processes, and anomaly detection.
- **Software-Defined Data Centers**: Providing greater flexibility and automation in disaster recovery operations.

Testing and Continuous Improvement

Regular testing is essential to ensure the effectiveness of a disaster recovery plan:

- **Tabletop Exercises**: Discussing hypothetical scenarios to evaluate the plan's completeness and team readiness.

- **Functional Tests**: Verifying the operation of specific systems or processes at the recovery site.
- **Full-Scale Simulations**: Conducting comprehensive tests that simulate a complete disaster and recovery process.

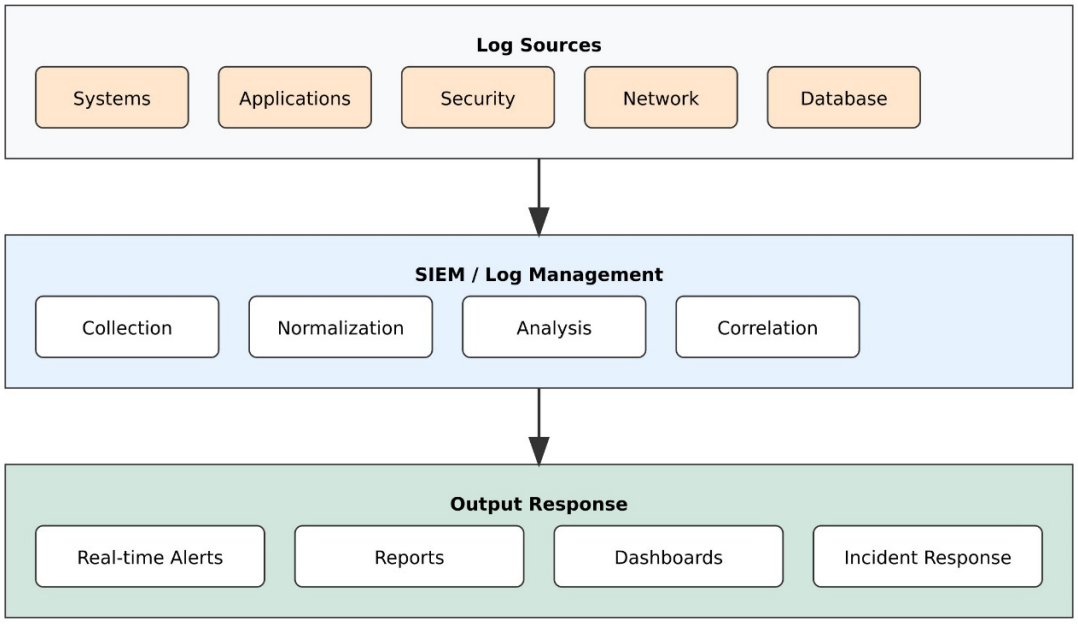
Challenges in Disaster Recovery

Organizations face several challenges in implementing effective disaster recovery:

- **Cost**: Balancing the need for robust DR capabilities with budget constraints.
- **Complexity**: Managing increasingly complex IT environments and interdependencies.
- **Data Growth**: Dealing with exponential growth in data volumes and the associated backup and recovery challenges.
- **Evolving Threats**: Adapting DR strategies to address new types of disasters, such as sophisticated cyberattacks.

By developing and maintaining a comprehensive disaster recovery strategy, organizations can significantly improve their resilience against a wide range of potential disruptions, ensuring business continuity and protecting critical assets in the face of disasters.

Logging and Monitoring



Logging and monitoring are fundamental components of an organization's security operations, providing visibility into system activities, user behaviors, and potential security events. These processes are crucial for detecting and responding to security incidents, maintaining compliance, and supporting forensic investigations.

Importance of Logging and Monitoring

Effective logging and monitoring serve several critical purposes:

1. **Threat Detection**: Identifying potential security incidents in real-time or near-real-time.
2. **Incident Response**: Providing valuable information for investigating and responding to security events.

3. **Compliance**: Meeting regulatory requirements for data protection and privacy.
4. **Forensics**: Supporting post-incident analysis and potential legal proceedings.
5. **Performance Monitoring**: Tracking system health and identifying operational issues.

Types of Logs

Organizations typically collect and analyze various types of logs:

- **System Logs**: Recording operating system events, errors, and warnings.
- **Application Logs**: Capturing application-specific events and user activities.
- **Security Logs**: Documenting security-related events such as authentication attempts and access control changes.
- **Network Logs**: Recording network traffic, connections, and device activities.
- **Database Logs**: Tracking database queries, modifications, and access attempts.

Log Management Process

An effective log management process typically includes the following steps:

1. **Log Generation**: Configuring systems and applications to produce relevant log data.
2. **Log Collection**: Gathering logs from various sources into a centralized location.
3. **Log Storage**: Securely storing logs for a defined retention period.

4. **Log Analysis**: Examining logs to identify patterns, anomalies, and potential security events.
5. **Log Reporting**: Generating reports and alerts based on log analysis findings.

Security Information and Event Management (SIEM)

SIEM systems play a crucial role in modern logging and monitoring practices:

- **Log Aggregation**: Collecting and normalizing logs from diverse sources.
- **Correlation**: Analyzing relationships between different log events to identify potential security incidents.
- **Real-time Alerting**: Generating notifications for predefined security events or anomalies.
- **Dashboards and Reporting**: Providing visual representations of security data and trends.

Monitoring Techniques

Organizations employ various monitoring techniques to detect and respond to security events:

- **Network Monitoring**: Observing network traffic patterns and identifying anomalies.
- **Host-based Monitoring**: Tracking activities on individual systems, including file integrity and process behaviors.
- **User Behavior Analytics (UBA)**: Analyzing user activities to detect insider threats and compromised accounts.
- **Application Performance Monitoring (APM)**: Tracking application performance and identifying potential security-related issues.

Log Retention and Protection

Proper log management includes considerations for retention and protection:

- **Retention Policies**: Defining how long different types of logs should be kept, based on operational needs and regulatory requirements.
- **Log Integrity**: Implementing measures to prevent unauthorized modification of log data.
- **Access Controls**: Restricting access to log data and log management systems to authorized personnel only.

Continuous Monitoring

Implementing a continuous monitoring strategy helps organizations maintain ongoing awareness of their security posture:

- **Asset Discovery**: Continuously identifying and tracking assets on the network.
- **Vulnerability Scanning**: Regularly assessing systems for known vulnerabilities.
- **Configuration Monitoring**: Tracking changes to system and application configurations.
- **Threat Intelligence Integration**: Incorporating external threat data to enhance monitoring capabilities.

Challenges in Logging and Monitoring

Organizations face several challenges in implementing effective logging and monitoring:

- **Data Volume**: Managing and analyzing the large volumes of log data generated by modern IT environments.

- **False Positives**: Distinguishing between genuine security events and benign anomalies.
- **Skills Gap**: Finding and retaining personnel with the expertise to effectively analyze and respond to security events.
- **Tool Sprawl**: Managing multiple monitoring and analysis tools across the organization.

Emerging Technologies

New technologies are shaping the future of logging and monitoring:

- **Machine Learning and AI**: Enhancing anomaly detection and predictive analytics capabilities.
- **Cloud-native Monitoring**: Adapting monitoring practices for cloud and containerized environments.
- **Extended Detection and Response (XDR)**: Integrating data from multiple security layers for improved threat detection and response.

Regulatory Considerations

Many regulations have specific requirements for logging and monitoring:

- **PCI DSS**: Mandates specific logging requirements for organizations handling payment card data.
- **HIPAA**: Requires healthcare organizations to implement audit controls and regularly review system activity records.
- **GDPR**: Emphasizes the importance of being able to demonstrate compliance through appropriate logging and monitoring practices.

Best Practices

To maximize the effectiveness of logging and monitoring efforts, organizations should consider the following best practices:

1. **Define Clear Objectives**: Establish specific goals for logging and monitoring activities aligned with business and security needs.
2. **Implement Proper Log Management**: Ensure logs are collected, stored, and protected in a manner that maintains their integrity and usefulness.
3. **Develop Incident Response Procedures**: Create clear processes for responding to alerts and potential security incidents identified through monitoring.
4. **Regularly Review and Tune**: Continuously assess and adjust logging and monitoring practices to address evolving threats and business changes.
5. **Automate Where Possible**: Leverage automation to handle routine analysis tasks and focus human expertise on complex issues.
6. **Maintain Context**: Ensure that logs contain sufficient contextual information to support effective analysis and investigation.
7. **Integrate with Other Security Processes**: Align logging and monitoring activities with broader security operations, including vulnerability management and incident response.

By implementing comprehensive logging and monitoring practices, organizations can significantly enhance their ability to detect, respond to, and mitigate security threats, while also supporting compliance efforts and operational efficiency.

Resource Protection

Resource protection is a fundamental aspect of security operations, encompassing the measures and controls implemented to safeguard an organization's assets, including physical resources, data, and intellectual property. Effective resource protection requires a comprehensive approach that addresses various types of assets and potential threats.

Types of Resources

Organizations typically need to protect several categories of resources:

- **Physical assets**: Buildings, equipment, computers, etc.
- **Information assets**: Data, databases, files, etc.
- **Software assets**: Applications, operating systems, etc.
- **Human resources**: Employees, contractors, etc.
- **Intangible assets**: Reputation, intellectual property, etc.

Key aspects of resource protection include:

- **Access control**: Limiting who can access resources and what they can do with them
- **Data classification**: Categorizing information based on sensitivity and value
- **Encryption**: Protecting data confidentiality
- **Backup and recovery**: Ensuring availability of critical resources
- **Physical security**: Safeguarding tangible assets

- **Personnel security**: Vetting and monitoring employees/contractors
- **Vendor management**: Securing the supply chain
- **Compliance**: Meeting regulatory requirements for protecting certain types of data
- **Monitoring and auditing**: Detecting and investigating unauthorized access attempts
- **Incident response**: Having plans in place to address security breaches

Effective resource protection requires a comprehensive approach that addresses people, processes, and technology. Organizations should implement defense-in-depth with multiple layers of controls to protect their most valuable assets.

Foundational Security Operations Concepts

Foundational security operations concepts provide the framework for implementing effective security practices across an organization. These concepts include:

Defense in Depth: This strategy uses multiple layers of security controls to protect assets. If one layer fails, others are still in place to provide protection.

Least Privilege: Users should be given the minimum level of access rights necessary to perform their job functions. This limits potential damage from accidents or malicious actions.

Separation of Duties: No single individual should have control over an entire critical process. This helps prevent fraud and errors.

Need to Know: Access to information should be restricted to only those who require it for their work.

Job Rotation: Periodically moving employees between different roles helps prevent fraud and ensures cross-training.

Mandatory Vacations: Requiring employees to take time off allows their work to be reviewed by others, potentially uncovering malicious activities.

Dual Control: Requiring two people to complete a sensitive task reduces the risk of fraud or errors.

Accountability: All actions and events should be traceable to an individual user.

Fail-Safe: Systems should default to a secure state in case of failure.

Complete Mediation: Access rights should be checked every time a resource is accessed, not just the first time.

Economy of Mechanism: Security designs should be as simple as possible to reduce potential vulnerabilities.

Open Design: Security should not rely on secrecy of design, but rather on the strength of its implementation.

Psychological Acceptability: Security mechanisms should be user-friendly to encourage adoption.

Weakest Link: Security is only as strong as the weakest component in the system.

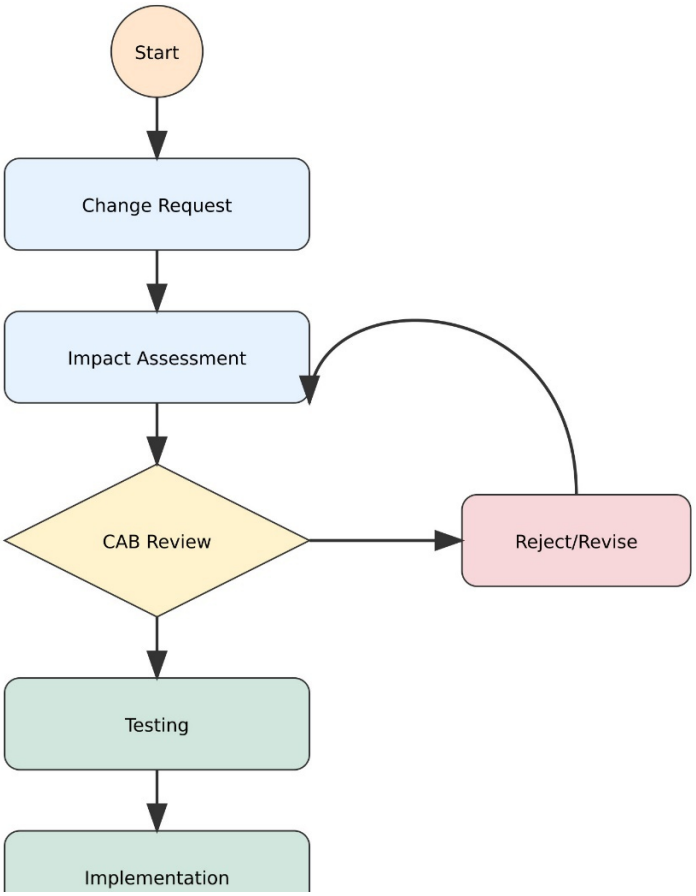
Single Point of Failure: Avoid having any single component whose failure would compromise the entire system.

Implementing these concepts requires:

- **Security Awareness Training**: Educating all employees about security risks and best practices.

- **Incident Response Planning**: Developing procedures for detecting, responding to, and recovering from security incidents.
- **Continuous Monitoring**: Regularly assessing systems and networks for vulnerabilities and suspicious activities.
- **Asset Management**: Maintaining an inventory of all hardware, software, and data assets.
- **Configuration Management**: Ensuring systems are configured securely and changes are properly controlled.
- **Patch Management**: Regularly updating systems with security patches.
- **Access Control**: Implementing strong authentication and authorization mechanisms.
- **Logging and Auditing**: Recording and reviewing security-relevant events.

Change Management



Change management is a critical process for maintaining security in dynamic IT environments. It ensures that modifications to systems and processes are properly evaluated, tested, and implemented without introducing new vulnerabilities. Key components of effective change management include:

Change Control Process: A formal, documented procedure for requesting, evaluating, approving, and implementing changes. This typically involves:

1. **Change Request**: Initiating a formal request for a change, including justification and potential impact.

2. **Impact Assessment**: Evaluating the potential effects of the change on security, operations, and other systems.
3. **Approval**: Getting sign-off from appropriate stakeholders based on the impact assessment.
4. **Testing**: Verifying the change in a non-production environment to ensure it works as intended and doesn't introduce new issues.
5. **Implementation**: Applying the change in the production environment according to a planned schedule.
6. **Documentation**: Updating relevant documentation to reflect the change.
7. **Review**: Post-implementation evaluation to ensure the change achieved its objectives and didn't cause unintended consequences.

Change Advisory Board (CAB): A group of stakeholders responsible for reviewing and approving changes. The CAB typically includes representatives from IT, security, and relevant business units.

Emergency Change Procedures: A streamlined process for implementing critical changes quickly, while still maintaining some level of control and documentation.

Change Windows: Designated time periods when changes can be implemented to minimize disruption to business operations.

Rollback Plans: Procedures for reverting changes if unexpected issues arise during or after implementation.

Configuration Management Database (CMDB): A central repository of information about all configuration items (CIs) in the IT environment, including their relationships and dependencies.

Version Control: Tracking different versions of software, configurations, and documentation to maintain a history of changes and enable rollback if needed.

Change Classification: Categorizing changes based on their potential impact and urgency to determine the appropriate level of scrutiny and approval required.

Automated Change Management Tools: Software that helps streamline the change management process, enforce workflows, and maintain audit trails.

Effective change management helps organizations:

- Reduce the risk of security incidents caused by unauthorized or poorly implemented changes
- Maintain compliance with regulatory requirements
- Improve system stability and reliability
- Enhance visibility into the IT environment
- Facilitate faster and more efficient implementation of necessary changes

By implementing a robust change management process, organizations can balance the need for agility with the requirement to maintain a secure and stable IT environment.

Chapter 8: Software Development Security

Software development security is a critical aspect of creating and maintaining secure applications and systems. This domain focuses on integrating security practices throughout the software development lifecycle to produce more resilient and trustworthy software. It encompasses a wide range of techniques, tools, and methodologies aimed at identifying and mitigating security vulnerabilities early in the development process.

The chapter begins by examining security in the software development lifecycle, exploring how security considerations can be incorporated into each phase of development, from requirements gathering to deployment and maintenance. This includes secure coding practices, threat modeling, and security testing methodologies.

Next, the chapter delves into development environment security controls, which are essential for protecting the tools, systems, and processes used in software creation. This includes securing source code repositories, implementing access controls, and ensuring the integrity of development and testing environments.

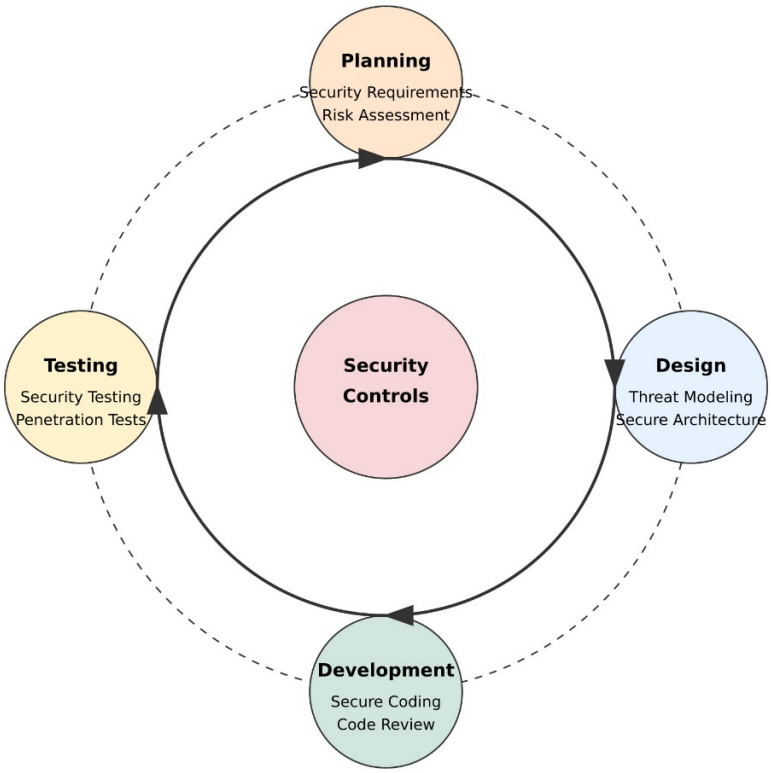
The effectiveness of software security measures is a crucial topic, covering methods for evaluating and measuring the security of software products. This includes various testing techniques, metrics for assessing security posture, and approaches for continuous security improvement.

Finally, the chapter addresses the security impact of acquired software, recognizing that many organizations rely on third-party or commercial off-the-shelf (COTS) software.

This section explores strategies for evaluating the security of acquired software, managing supply chain risks, and integrating external components securely into an organization's environment.

By mastering these concepts, security professionals can play a vital role in ensuring that software development processes produce secure, reliable applications that protect an organization's assets and data.

Security in the Software Development Lifecycle



Security in the Software Development Lifecycle (SDLC) is a comprehensive approach to integrating security practices throughout the entire process of creating, deploying, and maintaining software. This approach aims to identify and address security vulnerabilities early in the development process, reducing the cost and effort required to fix issues later.

The **traditional SDLC** typically consists of several phases: planning, requirements analysis, design, implementation, testing, deployment, and maintenance. Incorporating

security into each of these phases is crucial for developing secure software.

In the **planning phase**, security considerations should be factored into project scope, timelines, and resource allocation. This includes identifying potential security risks associated with the project and planning for necessary security activities throughout the development process.

During **requirements analysis**, security requirements should be explicitly defined alongside functional requirements. This involves identifying regulatory compliance needs, data protection requirements, and specific security features that the software must implement. **Threat modeling** is a valuable technique at this stage, helping teams identify potential threats and design appropriate countermeasures.

The **design phase** is critical for establishing a secure architecture. This includes designing secure authentication and authorization mechanisms, implementing proper input validation and output encoding, and ensuring secure data storage and transmission. **Secure design principles** such as least privilege, defense in depth, and fail-safe defaults should be applied.

In the **implementation phase**, developers should follow **secure coding practices** to prevent common vulnerabilities such as injection flaws, cross-site scripting (XSS), and buffer overflows. This involves using secure coding standards, leveraging security-focused libraries and frameworks, and implementing proper error handling and logging.

Static Application Security Testing (SAST) tools can be integrated into the development environment to identify potential security issues in the source code as it's being written. These tools can provide immediate feedback to developers, allowing them to fix issues quickly.

The **testing phase** should include dedicated security testing alongside functional testing. This encompasses various techniques:

- **Dynamic Application Security Testing (DAST)** involves testing the running application to identify vulnerabilities that may not be apparent in the source code.
- **Interactive Application Security Testing (IAST)** combines elements of both SAST and DAST, providing real-time analysis of application behavior.
- **Penetration testing** simulates real-world attacks to identify vulnerabilities that automated tools might miss.
- **Fuzz testing** involves providing invalid, unexpected, or random data as input to identify potential crash scenarios or security vulnerabilities.

During the **deployment phase**, secure configuration management is crucial. This includes hardening the production environment, implementing proper access controls, and ensuring secure communication channels. **Continuous monitoring** and **logging** should be set up to detect and respond to potential security incidents.

The **maintenance phase** involves ongoing security activities such as patch management, vulnerability assessments, and security updates. Regular security audits and assessments should be conducted to ensure the software remains secure as the threat landscape evolves.

DevSecOps is an approach that integrates security practices into the DevOps workflow, emphasizing collaboration between development, operations, and security teams throughout the SDLC. This approach aims to make security a shared responsibility and automate security processes where possible.

Key principles of DevSecOps include:

- **Shift Left**: Moving security earlier in the development process to identify and address issues sooner.
- **Automation**: Implementing automated security testing and controls to reduce manual effort and increase consistency.
- **Continuous Security**: Integrating security practices into continuous integration and continuous deployment (CI/CD) pipelines.
- **Security as Code**: Treating security configurations and policies as code, allowing them to be version-controlled and automatically deployed.

Secure Software Development Frameworks provide structured approaches to incorporating security into the SDLC. Examples include:

- **Microsoft Security Development Lifecycle (SDL)**: A set of practices that emphasize security and privacy considerations throughout the development process.
- **OWASP Software Assurance Maturity Model (SAMM)**: An open framework to help organizations formulate and implement a strategy for software security.

Agile and Security: Integrating security into Agile development methodologies presents unique challenges due to the rapid, iterative nature of Agile processes. Strategies for addressing this include:

- Incorporating security user stories into sprint planning
- Conducting regular security stand-ups

- Integrating automated security testing into each sprint
- Implementing security champions within development teams

Secure Code Reviews are an essential practice in secure software development. These reviews involve examining source code for security vulnerabilities and coding best practices. Effective code reviews can be facilitated by:

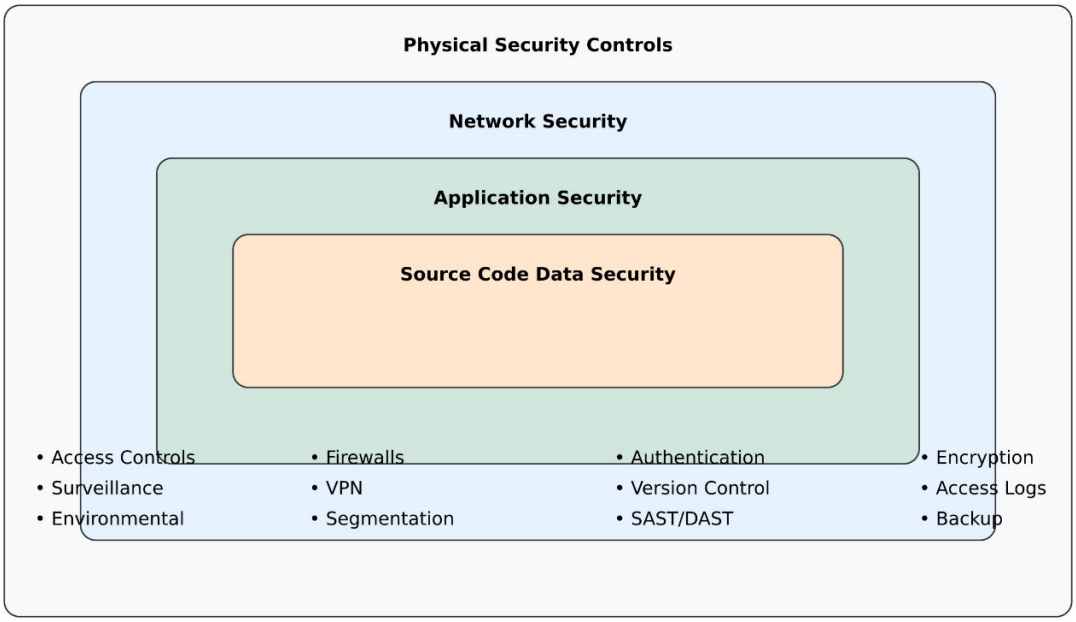
- Using checklists of common security issues to look for
- Leveraging automated tools to assist in identifying potential vulnerabilities
- Conducting pair programming sessions with a focus on security
- Implementing a "four eyes" principle where at least two people review all code changes

Security Training for Developers is crucial for building a culture of security within development teams. This training should cover:

- Common security vulnerabilities and how to prevent them
- Secure coding practices specific to the programming languages and frameworks used
- Threat modeling techniques
- Use of security tools in the development process

By integrating security throughout the SDLC, organizations can significantly reduce the risk of vulnerabilities in their software products. This proactive approach not only enhances the security of the final product but also can lead to cost savings by identifying and addressing security issues early in the development process.

Development Environment Security Controls



Development environment security controls are essential measures implemented to protect the tools, systems, and processes used in software creation. These controls aim to maintain the integrity, confidentiality, and availability of code, development tools, and related assets throughout the software development lifecycle.

Access Control is a fundamental aspect of securing the development environment. This involves implementing strong authentication mechanisms and enforcing the principle of least privilege. Developers should only have access to the resources necessary for their specific roles and responsibilities. **Multi-factor authentication (MFA)** should be implemented for accessing critical systems and sensitive code repositories.

Source Code Management (SCM) systems play a crucial role in development environment security. These systems, such as Git, SVN, or Mercurial, should be configured with appropriate access controls and auditing capabilities. Key security considerations for SCM include:

- Implementing strong authentication for repository access
- Enforcing code review processes before merging changes
- Using signed commits to verify the authenticity of code changes
- Regularly backing up repositories and storing backups securely
- Implementing branch protection rules to prevent unauthorized changes to critical branches

Secure Configuration Management ensures that development tools and environments are set up securely. This includes:

- Hardening operating systems and applications used in the development environment
- Regularly updating and patching all software components
- Disabling unnecessary services and features
- Implementing secure communication protocols (e.g., HTTPS, SSH) for all network connections
- Configuring firewalls to restrict network access to development systems

Secrets Management is crucial for protecting sensitive information such as API keys, passwords, and encryption keys. Secure practices include:

- Using dedicated secrets management tools or vaults
- Avoiding hardcoding secrets in source code
- Implementing rotation policies for secrets
- Providing developers with temporary, limited-scope credentials when necessary

Secure Build and Deployment Pipelines are essential for maintaining the integrity of the software throughout the development process. This involves:

- Implementing integrity checks on build artifacts
- Using reproducible builds to ensure consistency
- Scanning dependencies for known vulnerabilities
- Implementing secure code signing processes
- Ensuring the security of Continuous Integration/Continuous Deployment (CI/CD) tools and workflows

Isolation of Development Environments helps prevent unauthorized access and reduces the risk of cross-contamination between different projects or stages of development. This can be achieved through:

- Using separate physical or virtual machines for development, testing, and production environments
- Implementing network segmentation to isolate development networks from production and corporate networks
- Using containerization technologies to create isolated development environments

Secure Communication Channels ensure that data transmitted between development tools and systems remains confidential and intact. This includes:

- Encrypting all network traffic using protocols like TLS/SSL
- Implementing Virtual Private Networks (VPNs) for remote access to development resources
- Using secure file transfer protocols for sharing code and other assets

Monitoring and Logging in the development environment are crucial for detecting and responding to security incidents. Key aspects include:

- Implementing centralized logging for all development systems and tools
- Setting up alerts for suspicious activities or unauthorized access attempts
- Regularly reviewing logs and access patterns
- Using Security Information and Event Management (SIEM) systems to correlate and analyze security events

Secure Development Workstations are essential for protecting the endpoints where developers write and test code. Security measures for workstations include:

- Implementing endpoint protection solutions (antivirus, anti-malware)
- Enforcing disk encryption
- Restricting administrative privileges
- Regularly updating and patching operating systems and applications
- Implementing application whitelisting to prevent execution of unauthorized software

Third-Party Component Management is crucial given the widespread use of open-source libraries and frameworks

in modern software development. Security considerations include:

- Maintaining an inventory of all third-party components used in projects
- Regularly scanning dependencies for known vulnerabilities
- Implementing policies for approving and integrating new third-party components
- Monitoring for updates and security patches in used components

Secure Testing Environments ensure that security testing can be conducted effectively without risking production systems. This involves:

- Creating isolated environments that mimic production settings
- Populating test environments with sanitized or synthetic data to protect sensitive information
- Implementing access controls to restrict access to testing environments
- Regularly refreshing and resetting test environments to maintain their integrity

Data Protection in Development is essential, especially when working with sensitive or regulated data. Measures include:

- Implementing data masking or anonymization techniques for production data used in development
- Enforcing strict controls on the use and storage of sensitive data in development environments

- Implementing data loss prevention (DLP) solutions to prevent unauthorized data exfiltration

Security Training and Awareness for development teams is crucial for maintaining a secure development environment. This should cover:

- Best practices for secure use of development tools and environments
- Recognition and reporting of security incidents
- Understanding of relevant security policies and procedures

Incident Response Planning specific to the development environment ensures that teams can quickly and effectively respond to security breaches or incidents. This includes:

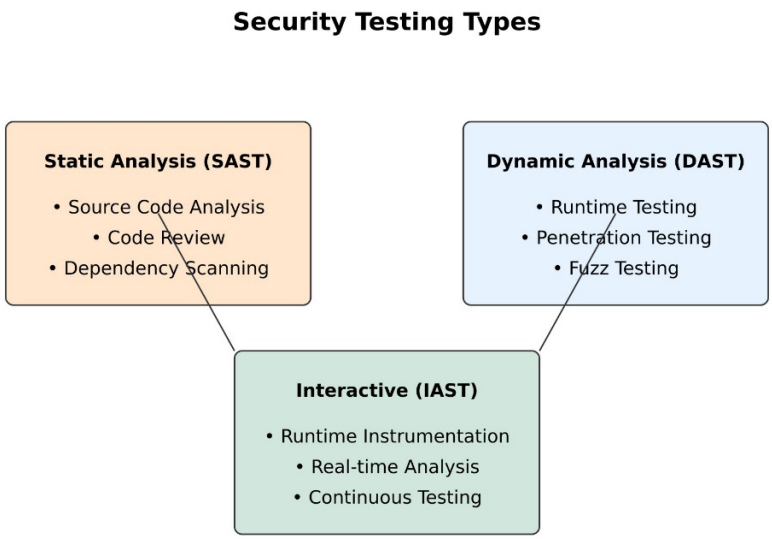
- Developing and maintaining an incident response plan tailored to development environment risks
- Conducting regular drills or tabletop exercises to test the plan
- Establishing clear communication channels and escalation procedures

By implementing comprehensive security controls in the development environment, organizations can significantly reduce the risk of security breaches, protect their intellectual property, and ensure the integrity of their software development process. These controls form a crucial foundation for producing secure and reliable software products.

Software Security Effectiveness

Software security effectiveness refers to the degree to which security measures implemented in software

successfully protect against threats and vulnerabilities. Evaluating and improving software security effectiveness is crucial for ensuring that applications can withstand attacks and maintain the confidentiality, integrity, and availability of data and resources.



Security Testing is a fundamental aspect of assessing software security effectiveness. Various types of security testing provide different perspectives on the security posture of an application:

- **Penetration Testing** involves simulating real-world attacks to identify vulnerabilities that could be exploited by malicious actors. This type of testing can uncover complex vulnerabilities that might be missed by automated tools.
- **Vulnerability Scanning** uses automated tools to identify known vulnerabilities in the application and its dependencies. Regular vulnerability scans can help catch common security issues quickly.
- **Fuzz Testing** involves providing invalid, unexpected, or random data as input to the

application to identify potential crash scenarios or security vulnerabilities. This technique is particularly effective at finding input validation and handling issues.

- **Static Application Security Testing (SAST)** analyzes source code or compiled versions of code to identify potential security vulnerabilities. SAST tools can be integrated into the development process to catch issues early.
- **Dynamic Application Security Testing (DAST)** involves testing a running application to find vulnerabilities. This type of testing can identify runtime issues that might not be apparent from static code analysis.
- **Interactive Application Security Testing (IAST)** combines elements of both SAST and DAST, providing real-time analysis of application behavior during manual or automated testing.

Metrics and Measurements play a crucial role in quantifying software security effectiveness. Key metrics might include:

- **Number of vulnerabilities**: Tracked by severity and type, this metric can help gauge the overall security posture of the application.
- **Time to fix**: Measuring how long it takes to address identified vulnerabilities can indicate the efficiency of the security process.
- **Security debt**: Similar to technical debt, this metric represents the effort required to address accumulated security issues.
- **Code coverage**: In the context of security testing, this measures what percentage of the codebase has been analyzed for security issues.

- **False positive rate**: Tracking the accuracy of security tools and processes helps refine and improve testing efforts.

Threat Modeling is an essential practice for understanding and evaluating potential threats to an application. Effective threat modeling can:

- Identify potential attack vectors and security risks
- Prioritize security efforts based on the likelihood and impact of threats
- Guide the design of security controls and countermeasures

Security Architecture Reviews assess the overall design of an application from a security perspective. These reviews can identify architectural flaws that might lead to security vulnerabilities, such as improper segregation of duties or insecure data flow.

Code Reviews with a focus on security are crucial for identifying vulnerabilities and ensuring adherence to secure coding practices. Effective security code reviews involve:

- Using checklists of common vulnerabilities to guide the review process
- Leveraging automated tools to assist in identifying potential issues
- Involving security experts in the review process

Runtime Application Self-Protection (RASP) technologies can enhance software security effectiveness by providing real-time protection against certain types of attacks. RASP tools integrate with an application to detect and prevent attacks at runtime.

Continuous Monitoring of applications in production environments is essential for maintaining security

effectiveness over time. This involves:

- Implementing logging and monitoring solutions to detect potential security incidents
- Using intrusion detection and prevention systems (IDS/IPS) to identify and block attacks
- Regularly analyzing logs and security events to identify trends or anomalies

Security Benchmarking involves comparing an application's security posture against industry standards or best practices. This can help identify areas for improvement and ensure that security measures meet or exceed industry norms.

Vulnerability Management processes are crucial for addressing identified security issues effectively. This includes:

- Prioritizing vulnerabilities based on risk and potential impact
- Implementing a systematic approach to tracking and resolving security issues
- Regularly reassessing the application to ensure vulnerabilities have been properly addressed

Security Awareness and Training for development teams can significantly impact software security effectiveness. Ongoing education should cover:

- Common vulnerabilities and how to prevent them
- Secure coding practices specific to the technologies in use
- Understanding of the threat landscape and emerging security risks

Third-Party Component Management is increasingly important given the prevalence of open-source and third-party libraries in modern applications. Effective management includes:

- Maintaining an inventory of all third-party components
- Regularly scanning for known vulnerabilities in these components
- Implementing processes for quickly updating or replacing vulnerable components

Security by Design principles should be embedded throughout the development process to enhance overall security effectiveness. This approach involves:

- Considering security requirements from the earliest stages of design
- Implementing security controls as fundamental components of the application architecture
- Regularly reassessing and updating security measures as the application evolves

Automated Security Testing integrated into the development and deployment pipeline can significantly improve security effectiveness by:

- Providing rapid feedback on potential security issues
- Ensuring consistent application of security checks across all code changes
- Reducing the likelihood of security vulnerabilities being introduced into production

Bug Bounty Programs can complement internal security efforts by leveraging external expertise to identify

vulnerabilities. These programs can:

- Provide fresh perspectives on application security
- Identify complex or novel vulnerabilities that might be missed by internal testing
- Offer a cost-effective way to enhance security testing coverage

Security Governance

Security governance refers to the system by which an organization directs and controls security, encompassing the leadership, organizational structures, and processes that ensure information security aligns with and supports business objectives. Key aspects of security governance include:

- Establishing clear roles and responsibilities for security
- Developing and maintaining security policies, standards, and procedures
- Ensuring compliance with relevant laws and regulations
- Implementing risk management processes
- Allocating resources for security initiatives
- Monitoring and measuring security performance

Effective security governance requires strong leadership and commitment from senior management. The board of directors and executive management should be actively involved in:

- Setting the overall security strategy and risk appetite

- Approving key security policies
- Ensuring adequate resources are allocated to security
- Receiving regular reports on the security posture and major risks

Some common security governance frameworks and standards include:

- COBIT (Control Objectives for Information and Related Technologies)
- ISO/IEC 27014 - Governance of Information Security
- NIST Cybersecurity Framework

A governance structure typically includes:

- Board of Directors - Provides oversight and sets strategic direction
- Executive Management - Responsible for implementing security strategy
- Chief Information Security Officer (CISO) - Leads security program
- Information Security Steering Committee - Provides guidance and coordination
- Business Unit Leaders - Responsible for security in their areas

Key governance activities include:

- Developing security strategy aligned with business goals
- Establishing security policies and standards
- Defining security roles and responsibilities
- Implementing risk management processes

- Allocating budget and resources for security
- Monitoring security metrics and KPIs
- Conducting security awareness training
- Ensuring regulatory compliance

Effective security governance helps ensure that security is treated as a business issue, not just a technical one. It provides the framework for managing security in a consistent, business-aligned manner across the organization.

Acquired Software Security Impact

Acquired software, whether commercial off-the-shelf (COTS) products or open-source solutions, can introduce significant security risks to an organization. Understanding and managing these risks is crucial for maintaining a robust security posture. Key factors to consider include:

Supply Chain Security: The security of acquired software begins with the supply chain. Organizations must assess the security practices of their software vendors and suppliers. This includes:

- **Vendor security assessments**: Evaluating the security posture and practices of software providers.
- **Software composition analysis**: Identifying and assessing the security of third-party components and libraries used in the acquired software.
- **Secure software development lifecycle (SSDLC)**: Ensuring vendors follow secure development practices throughout the software lifecycle.

Vulnerability Management: Acquired software may contain known or unknown vulnerabilities. Organizations should:

- Implement a **vulnerability scanning** process for all acquired software.
- Establish procedures for **timely patching and updates**.
- Monitor **vulnerability databases** and **security advisories** for newly discovered issues in acquired software.

Integration and Configuration: Securely integrating acquired software into existing environments is critical:

- **Secure configuration**: Implementing security best practices and hardening guidelines for the acquired software.
- **Integration testing**: Assessing the security impact of the acquired software on existing systems and applications.
- **Access control**: Ensuring proper access controls and authentication mechanisms are in place for the acquired software.

Licensing and Compliance: Organizations must manage legal and compliance aspects of acquired software:

- **License management**: Tracking and complying with software licenses to avoid legal issues.
- **Regulatory compliance**: Ensuring acquired software meets relevant regulatory requirements (e.g., GDPR, HIPAA).

Security Features and Capabilities: Evaluate the security features provided by the acquired software:

- **Built-in security controls**: Assessing and leveraging native security features.
- **Encryption capabilities**: Ensuring proper data protection mechanisms are available and implemented.
- **Logging and auditing**: Verifying that the software provides adequate logging and auditing capabilities for security monitoring.

Third-Party Access: Consider the implications of vendor access to systems and data:

- **Remote access policies**: Establishing secure protocols for vendor support and maintenance.
- **Data sharing agreements**: Defining clear terms for data access and protection by third parties.

End-of-Life and Support: Plan for the entire lifecycle of acquired software:

- **Support agreements**: Ensuring ongoing security support and updates from the vendor.
- **End-of-life planning**: Developing strategies for securely decommissioning or replacing software when vendor support ends.

Open Source Software Considerations: For open-source solutions, additional factors include:

- **Community support**: Assessing the activity and responsiveness of the open-source community.
- **Code review**: Conducting or obtaining independent security reviews of the open-source code.
- **Contribution policies**: Understanding how security issues are reported and addressed in the

open-source project.

Security Testing: Conduct thorough security testing of acquired software:

- **Penetration testing**: Identifying potential vulnerabilities through simulated attacks.
- **Code review**: When possible, reviewing source code or obtaining third-party code review results.
- **Functional security testing**: Verifying that security features work as intended.

Documentation and Training: Ensure proper documentation and training for secure use of the acquired software:

- **Security documentation**: Obtaining and reviewing security-related documentation from the vendor.
- **User training**: Providing training on secure usage of the acquired software to relevant personnel.

Continuous Monitoring: Implement ongoing monitoring of acquired software:

- **Security information and event management (SIEM)**: Integrating acquired software logs into centralized security monitoring systems.
- **Behavioral analysis**: Monitoring for unusual behavior or activity related to the acquired software.

By carefully considering these factors, organizations can significantly reduce the security risks associated with acquired software and maintain a strong overall security posture. It's important to remember that the security impact of acquired software extends beyond the initial

implementation and requires ongoing management throughout its lifecycle within the organization.

Practice Tests Sections

Welcome to the **Practice Test** section of the ISC2 CISSP Study Guide 2025-2026. This comprehensive exam simulation is designed to **assess your knowledge** and **readiness** for the actual CISSP certification exam. The practice test consists of **carefully crafted questions** that cover all eight domains of the CISSP Common Body of Knowledge (CBK).

To get the most benefit from this practice test, we strongly recommend that you **attempt all questions without referring to any external resources**. Treat this as a **real exam scenario** to gauge your current understanding and identify areas that may require further study.

Important: Do not check the answers or explanations until you have completed the entire practice test. This approach will help you **simulate actual exam conditions** and provide a more accurate assessment of your preparedness. Once you've finished, review your responses alongside the provided explanations to **reinforce your learning** and address any knowledge gaps.

Good luck, and remember - this is an opportunity to **learn and improve** your cybersecurity expertise!

Practice Tests 1

Question 1

A database security administrator at a military contractor is concerned about employees with lower security clearances potentially discovering classified mission information by observing aircraft movements. What type of security issue is this administrator worried about?

A) Inference

B) Aggregation

C) Multilevel security

D) SQL injection

Question 2

An information security analyst is evaluating whether to upgrade a data center's fire suppression system. The facility costs $2 million to replace, and a typical fire would cause $750,000 in damage. Fires are expected once every 50 years. What is the Exposure Factor for a fire at this data center?

A) 7.5%

B) 37.5%

C) 15.0%

D) 27.5%

Question 3

Which of the following best describes a set of rules or restrictions commonly found on security devices like firewalls and proxies?

A) Element

B) Filter

C) Field

D) Range

Question 4

An employee received an email with an unfamiliar attachment named "smime.p7s". What is the most probable explanation for this attachment?

A) It's part of a phishing attack

B) It's a spoofing attempt

C) It contains embedded malware

D) It's an encrypted email message

Question 5

Which software testing approach is considered the most rigorous and formal?

A) Fuzzing

B) Fagan

C) Over-the-shoulder

D) Pair programming

Question 6

What is the primary weakness associated with using pre-set questions for cognitive passwords?

A) The answers may be easily found online

B) They require users to think, which not all can do

C) They don't support long passwords

D) They prevent the use of tokens

Question 7

An information security analyst is assessing the risk of fire at a data center. The facility costs $2 million to replace, a typical fire would cause $750,000 in damage, and fires are

expected once every 50 years. What is the annualized rate of occurrence for a fire at this data center?

A) 0.002

B) 0.02

C) 0.05

D) 0.002

Question 8

In the context of database security, which of the following is not necessarily an attribute of an aircraft's tail number used as a unique identifier?

A) Candidate key

B) Database field

C) Primary key

D) Foreign key

Question 9

What type of access control restricts data access based on the contents or payload of an object?

A) Composition-Contingent Access Control

B) Content-Dependent Access Control

C) Provisory-Context Access Control

D) Subject-Matter Reliant Access Control

Question 10

A network administrator is dealing with issues where data packets are becoming corrupted during transmission. What term best describes this problem?

A) Packet loss

B) Interference

C) Jitter

D) Latency

Question 11

What is the most effective method to address concerns about a high False Acceptance Rate (FAR) in a biometric system?

A) Adjust the CER

B) Add a second authentication factor

C) Lower the False Rejection Rate (FRR)

D) Replace the entire biometric system

Question 12

Which RAID level is commonly referred to as disk mirroring?

A) RAID 1

B) RAID 10

C) RAID 5

D) RAID 0

Question 13

What type of cryptography offers security similar to established public key systems but with smaller key sizes?

A) Elliptic Curve Cryptography

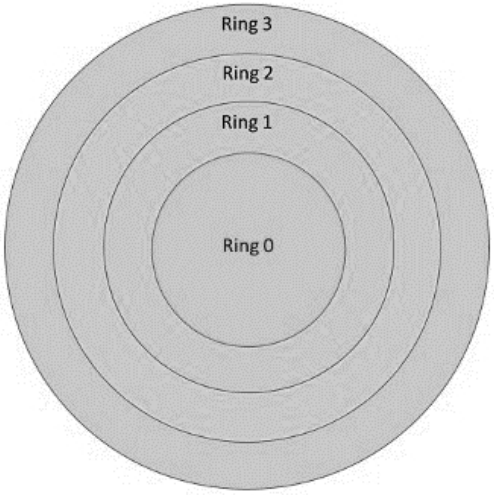
B) Symmetric Key Cryptography

C) Hash Cryptography

D) Blockchain Cryptography

Question 14

In a ring protection model, which ring typically contains user programs and applications?



A) Ring 1

B) Ring 3

C) Ring 0

D) Ring 2

Question 15

What term is used to describe a system whose security has been breached?

A) Violated

B) Compromised

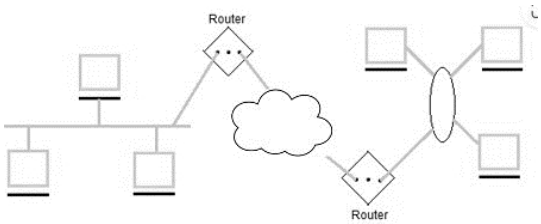
C) Jeopardized

D) Cracked

Question 16

What type of network is designed to cover an entire city, potentially connecting multiple LANs?

And looking at the image below, What type of network is displayed in the image?



A) LAN

B) MAN

C) WAN

D) CAN

Question 17

Which form of multiprocessing involves processors operating independently, each with its own OS and/or task instruction set?

A) Blockchain Multi-Processing (BMP)

B) Decryption Multi-Processing (DMP)

C) Symmetric Multi-Processing (SMP)

D) Asymmetric Multi-Processing (AMP)

Question 18

What action transforms a zero-day vulnerability into a less critical security threat?

A) Release of a security patch

B) Implementation of transport-layer encryption

C) Discovery of the vulnerability

D) Reconfiguration of a firewall

Question 19

Which of the following is most effective in preventing session hijacking attacks?

A) Complex session cookies

B) SSL

C) Frequently expiring cookies

D) TLS

Question 20

What type of encryption creates a cryptographic code that cannot be reversed when applied to passwords, messages, or CRCs?

A) SHA1256

B) Symmetric Encryption

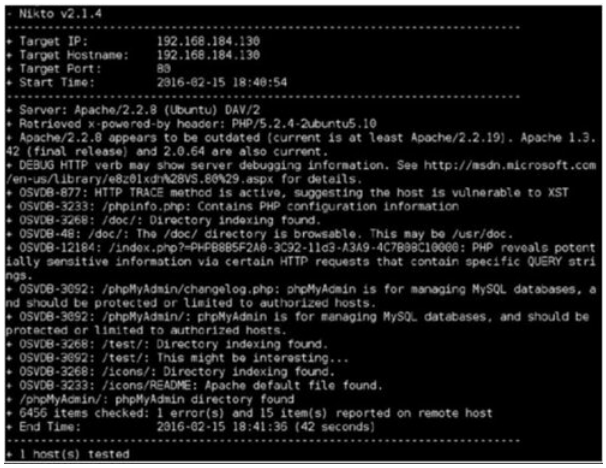
C) Cell-Level Encryption

D) One-Way Encryption

Question 21

During a web vulnerability scan, a tester discovers potential cross-site tracing issues. Which of the following is most relevant to this type of vulnerability?

Which of the following relate to this type of issue?



A) Stealing user cookies

B) Countering SQL tracing

C) A PSQL tracing problem

D) Modifying users' TRACE information

Question 22

What kind of attack involves submitting database expressions and script code to bypass authentication and interact directly with the DBMS or underlying operating system?

A) SQL Injection

B) DoS Manipulation

C) Man-in-the-Middle Engineering

D) Brute Force Assault

Question 23

Which backup method stores all files that have been modified since the most recent full backup?

A) Remote backup

B) Partial backup

C) Incremental backup

D) Differential backup

Question 24

What term describes an attack where a large number of messages are directed to a single user's inbox or through a specific SMTP server to cause a denial of service?

A) Malware Attack

B) Mail-Bombing

C) Drive-By Attack

D) Phishing and Spear Phishing Attack

Question 25

What is the term for the measurement of wave oscillations within a specific time, typically expressed in Hertz (Hz)?

A) Frequency

B) Harmonic

C) Transverse

D) Vibration

Question 26

What is the process of dividing a network into smaller units to improve various aspects such as performance, security, and traffic isolation?

A) Locking

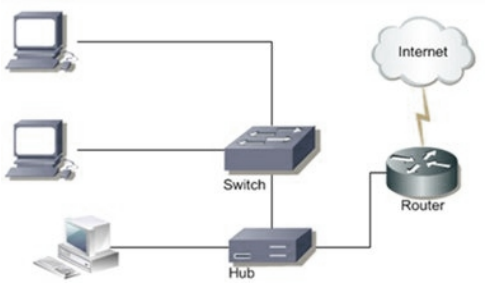
B) Stacking

C) Threading

D) Segmentation

Question 27

What type of smart card is used by US government personnel that includes a picture and can function as both a badge and a smart card?



A) General Admission Card (GAC)

B) Multiple-Entry Pass (MEP)

C) Common Access Card (CAC)

D) Dual-Interface Cards (DIC)

Question 28

In which cloud computing model do multiple organizations collaborate to build a shared environment for their own use?

A) Public Cloud

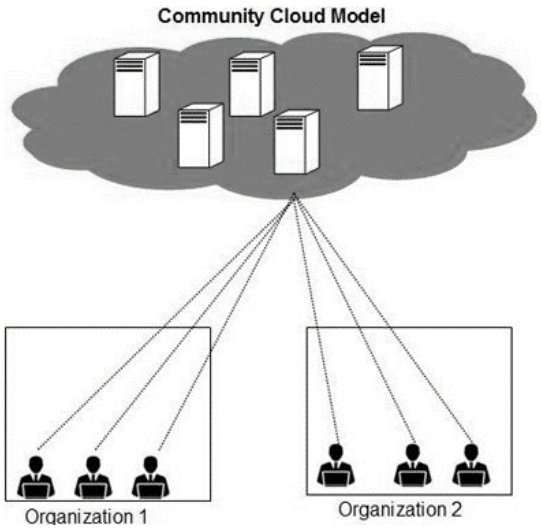
B) Community Cloud

C) Shared Cloud

D) Private Cloud

Question 29

A web server log shows a user entered "Smith' ; DROP TABLE orders;--" as their last name when placing an order. What type of attack does this indicate?



A) Cross-site request forgery

B) Cross-site scripting

C) Buffer overflow

D) SQL injection

Question 30

What network service provides voice communication by transporting voice traffic's network packets over an IP network?

A) DSL

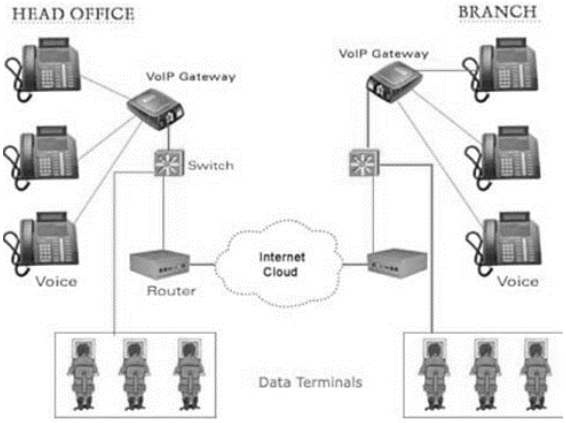
B) VoIP

C) PBX

D) 5G

Question 31

Which class of fire extinguishers is suitable for combating electrical fires?



A) Class B

B) Class D

C) Class A

D) Class C

Question 32

What legislation criminalizes the act of stealing or assuming another person's identity, with penalties including up to 15 years in prison and/or a $250,000 fine?

A) Identity Theft and Assumption Deterrents Act

B) Impersonation and Identity Theft Act

C) Identity Falsification Prohibition Act

D) Misrepresentation of Identity Act

Question 33

What is the maximum distance a Category 6 cable can be run according to the standard?

A) 200 metres

B) 50 metres

C) 100 metres

D) 300 metres

Question 34

When labeling a system that handles Secret, Confidential, and Unclassified information in a US government context, what classification should be applied?

A) Confidential

B) Top secret

C) Secret

D) Mixed classification

Question 35

What type of policy defines acceptable performance and behavior expectations for employees, with potential consequences for non-compliance?

A) ARP

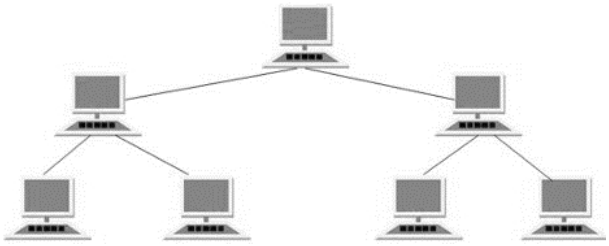
B) APP

C) AUP

D) AAP

Question 36

What network topology features a root node with all other nodes connected to it in a hierarchy?



A) Bus

B) Hybrid

C) Tree

D) Mesh

Question 37

What security measure is typically employed when purchasing tickets online to protect credit card and personal information during transmission?

A) Identification

B) Authorization

C) Encryption

D) Authentication

Question 38

What term describes the process of breaking into telephone company computers to place free calls?

A) Phreaking

B) Swishing

C) Pharming

D) Phishing

Question 39

In a relational database, what is a column within a table called?

A) Attribute

B) List

C) Vertical

D) Sub-Section

Question 40

What type of virus modifies its own code as it spreads from system to system, maintaining its core functions but altering its signature?

A) Polyalphabetic Virus

B) Pigpen Virus

C) Monoalphabetic Virus

D) Polymorphic Virus

Question 41

Using a trusted channel and link encryption are methods to prevent what type of access control attack?

A) Brute Force Attacks

B) Dictionary Attacks

C) Man-in-the-Middle Attacks

D) Spoofed Login Screens

Question 42

Which principle states that an individual should strive to complete their responsibilities accurately and in a timely manner?

A) Due Care

B) Separation of Duties

C) Due Diligence

D) Least Privilege

Question 43

What US law establishes baseline security requirements for all federal agencies?

A) Patriot Security Act (PAS)

B) Consumer Safety Act (CSA)

C) Electronic Safeguards and Measures Act (ESMA)

D) Computer Security Act (CSA)

Question 44

What protocols are used to provide the transport mechanism for login credentials?

A) HTML Server Protocols

B) Authentication Protocols

C) SSL Server Protocols

D) Application Programming Interface

Question 45

How many possible keys exist in a cryptographic algorithm using 6-bit encryption keys?

A) 32

B) 64

C) 16

D) 12

Question 46

What property in database transactions ensures that each transaction is processed independently and simultaneously without interference from others?

A) Durability

B) Consistency

C) Isolation

D) Atomicity

Question 47

What is a secret value used to encrypt or decrypt messages or database fields called?

A) Hash

B) Key

C) Cipher

D) Algorithm

Question 48

Which of the following are characteristics of alpha testing?

- Testing performed by internal employees
- Conducted at the developer's site
- Involves both white box and black box techniques
- Requires a testing environment
- May have a long execution cycle
- Critical issues can be addressed immediately by developers

A) Delta Testing

B) Beta Testing

C) Omega Testing

D) Alpha Testing

Question 49

What level of RAID is known as disk striping with parity?

A) RAID 1

B) RAID 10

C) RAID 5

D) RAID 0

Question 50

In the context of information security, what term describes the act of subdividing a network into numerous smaller units to improve various aspects such as performance, congestion, and security?

A) Locking

B) Stacking

C) Threading

D) Segmentation

Question 51

Identify the missing term in this Information Systems Security context:

[?] is considered an intangible asset, such as confidential recipes or manufacturing methods.

A. Registered Trademarks

B. Proprietary Assets

C. Intellectual Property

D. Copyrighted Material

Question 52

In Information Systems Security, what is described as the art and science of concealing the meaning or purpose of communication from unintended recipients?

A. Encryption

B. Hashing

C. Salting

D. Decryption

Question 53

In wireless networking, what type of packet announces a network's presence by broadcasting its SSID or name?

A. Probe Response

B. CF End + CF ACK

C. Beacon Frame

D. Association Response

Question 54

What credit card-sized device contains embedded information about the authorized user for identification and authentication purposes?

A. Prestocard

B. Gocard

C. Smartcard

D. Passcard

Question 55

Kabuki, a system administrator, notices systems across the office suddenly showing signs of infection. What type of malware is likely responsible?

A. Trojan horse

B. Virus

C. Worm

D. Logic bomb

Question 56

What standardized protocol should Cable use to interface with the National Vulnerability Database and ensure compatibility?

A. XACML

B. SCAP

C. VSM

D. SCML

Question 57

What term describes a network limited to a specific geographic area like an office, building, or city block?

A. FAN

B. YAN

C. LAN

D. WAN

Question 58

What structure defines or describes a database and is written using a Data Definition Language (DDL)?

A. Catalog

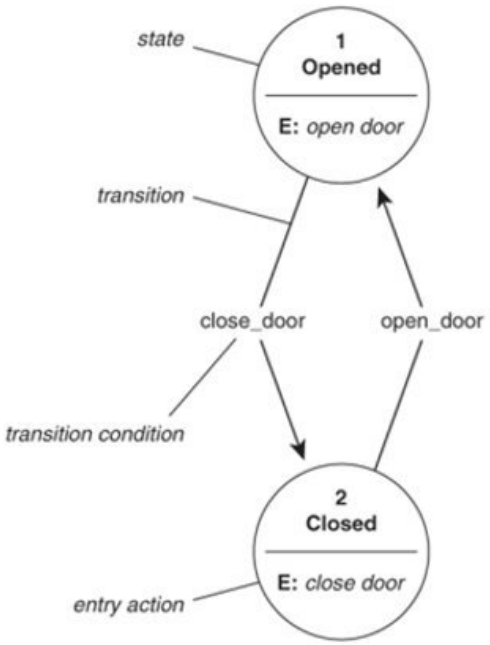
B. Stack

C. Schema

D. Protocol

Question 59

Which model, based on the machine shown in the figure, defines behaviors for a finite number of states, transitions, and actions?



A. Non-interference Model

B. Information Flow Model

C. State Machine Model

D. Bell-LaPadula Model

Question 60

Hope Pym wants a disaster recovery facility balancing cost and recovery time, activating about a week after disaster declaration. What type should she choose?

A. Cold site

B. Warm site

C. Hot site

D. Mutual assistance agreement

Question 61

In the OSI Model, which layer allows applications to access network services?

A. Human-Computer Interaction

B. Presentation

C. Circuit Level Gateway Firewall

D. Transport

Question 62

What is the most severe penalty an (ISC)2 peer review board can impose for an ethics violation?

A. Suspension of certification

B. Revocation of certification

C. Financial penalty

D. Termination of employment

Question 63

Which authentication factor refers to something you possess, like a smartcard or token device?

A. Type 3

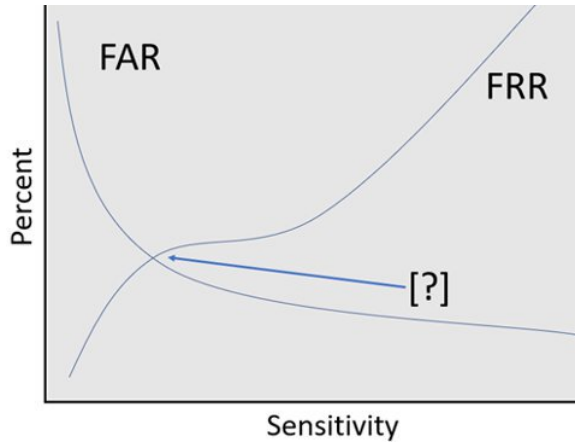
B. Type 4

C. Type 2

D. Type 1

Question 64

What term describes the point where the False Acceptance Rate (FAR) equals the False Rejection Rate (FRR)?



A. FAR/FRR

B. UAR

C. CER

D. COP

Question 65

During which biometric scanning process is low-beam infrared light cast onto the eye, with blood vessels absorbing the light to generate a unique pattern?

A. Iris Scanning

B. Eye Recognition

C. Retinal Scanning

D. Iris Recognition

Question 66

In keystroke dynamics biometrics, what term describes the time between releasing one key and pressing the next?

A. Flight Time

B. Rest Time

C. Transient Time

D. Dwell Time

Question 67

What security element, stored separately from salted passwords, is used to enhance their protection?

A. Pepper

B. Spice

C. Vinegar

D. Chili

Question 68

What process involves adding headers and footers to a PDU as it moves down the OSI model layers?

A. Propagation

B. Decapsulation

C. Encapsulation

D. Rendering

Question 69

When a web application retrieves user information from a database, what role does the application play?

A. A token

B. A user

C. An object

D. A subject

Question 70

What term, also known as sniffing, encompasses capturing network traffic, audio communications, faxes, and radio signals?

A. Hijacking

B. Scrubbing

C. Eavesdropping

D. Isolating

Question 71

What approach to threat modeling occurs after product deployment and forms the basis for ethical hacking and penetration testing?

A. Reactive Approach

B. Peer Approach

C. Genesis Approach

D. Proactive Approach

Question 72

In Kerberos authentication, what component acts as both an Authentication Server and a Ticket Granting Server?

A. Permission Allocation Matrix (PAX)

B. Key Distribution Centre (KDC)

C. Secure Verification Protocol (SVP)

D. Trusted Permission Vehicle (TPV)

Question 73

Which alternate processing facility can restore operations within minutes by including all necessary hardware and data?

A. Warm site

B. Mobile site

C. Cold site

D. Hot site

Question 74

What change management process can help Bethany address issues arising from system administrators updating libraries without informing developers?

A. Request control

B. Change control

C. Configurational control

D. Release control

Question 75

What term describes the risk associated with specific threats to assets that management chooses not to safeguard against?

A. Human Risk

B. Residual Risk

C. Physical Risk

D. Strategic Risk

Question 76

In Hunter's scenario, what is the Exposure Factor (EF) for flood impact on the data center valued at $100 million with potential $20 million damage?

A. 2%

B. 200%

C. 20%

D. 100%

Question 77

What type of access control uses measures like locks, security badges, and awareness training to discourage security policy violations?

A. Role-Based Access Control

B. Discretionary Access Control

C. Detective Access Control

D. Deterrent Access Control

Question 78

Which capability is not typically included in Mobile Device Management (MDM) solutions?

A. Enforcing device encryption

B. Assuming control of non-registered BYOD devices

C. Managing device backups

D. Remotely wiping device contents

Question 79

Which SOC report type provides general-use information on controls related to compliance and operations?

A. SOC 1, Type 1

B. SOC 2

C. SOC 1, Type 2

D. SOC 3

Question 80

In keystroke dynamics biometrics, what term describes the duration between key presses?

A. Typographic Measure

B. Liveness Detection

C. Crossover

D. Flight Time

Question 81

What type of single sign-on allows authentication between separate secure domains without relying on a master authentication server?

A. Kerberos-based SSO

B. Cross-domain SSO

C. Form-filling SSO

D. SPNEGO-based SSO

Question 82

Which risk analysis method uses scenario-oriented analysis for ranking and grading exposure ratings and decisions?

A. Quantitative Risk Analysis

B. Qualitative Risk Analysis

C. Pareto Chart

D. SWOT Analysis

Question 83

What method assures a recipient that a message is authentic and unaltered during transmission?

A. Digital Signature

B. Hash

C. Asymmetric Encryption

D. Symmetric Encryption

Question 84

What type of database consists of tables containing sets of related records?

A. Centralized Database

B. Relational Database

C. SQL Database

D. Non-Relational Database

Question 85

What testing approach involves checking systems on the fly without pre-created test cases?

A. Exploratory Testing

B. Scripted Testing

C. Start-To-End Testing

D. End-To-End Testing

Question 86

What term describes the variation in packet delay from source to destination?

A. Packet loss

B. Latency

C. Jitter

D. Interference

Question 87

Which security model uses limited interfaces or programs to control and maintain object integrity?

A. Clark-Wilson Model

B. Bell-Lapadula Model

C. Brewer and Nash Model

D. Open Systems Interconnection (OSI) Model

Question 88

What term describes mobile code that attempts to perform unwanted or malicious activities?

A. Worm

B. Jumping-Jack Applet

C. Hostile Applet

D. Trojan Horse

Question 89

What U.S. law imposes specific requirements on websites catering to or knowingly collecting information from children?

A. Online Privacy Protection Act (OPPA)

B. Global Internet Protection Act (GIPA)

C. Minor's Protection on Internet Activity (MPIA)

D. Children's Online Privacy Protection Act (COPPA)

Question 90

In Harry Osborn's scenario involving a potential SQL injection attack, what represents the vulnerability?

A. Web defacement

B. Hacker

C. Unpatched web application

D. Operating system

Question 91

What mobile device policy involves an organization purchasing and providing devices to employees?

A. BYOD

B. COPE

C. COD

D. CODE

Question 92

Which IPSec component provides authentication, integrity, and non-repudiation?

A. Encryption Security Header

B. Encapsulating Security Payload

C. L2TP

D. Authentication Header

Question 93

Which classification level is not typically found in commercial data classification schemes?

A. Public

B. Confidential

C. Secret

D. Sensitive

Question 94

What type of testing focuses on performance, reliability, scalability, and other non-functional aspects of a software system?

A. Non-Functional Testing

B. Functional Testing

C. Generic Testing

D. Focused Testing

Question 95

What term describes the use of multiple wireless access points to support a single network over a larger area?

A. WiFi

B. Local Area Network (LAN)

C. Wide Area Network (WAN)

D. Enterprise Extended Mode

Question 96

What type of Industrial Control System (ICS) is a single-purpose digital computer used for managing industrial electromechanical operations?

A. Smart Relay

B. Embedded Controller

C. Programmable Logic Controller (PLC)

D. Remote Telemetry Unit (RTU)

Question 97

Which combination provides the most assurance that data won't be lost if a mobile device is stolen?

A. Mandatory passcodes and application management

B. Full device encryption and mandatory passcodes

C. Enabling GPS tracking and full device encryption

D. Remote wipe and GPS tracking

Question 98

What authentication factor type refers to something you know?

A. Type 1

B. Type 3

C. Type 4

D. Type 2

Question 99

Based on the image of a network-connected web camera, what type of devices likely compose the botnet?

A. IoT

B. SCADA

C. Web Servers

D. Cloud infrastructure

Question 100

What type of error occurs when a valid subject using biometric authentication is not authenticated?

A. A Type 2 error

B. A Type 1 error

C. A Type 3 error

D. A Type 4 error

Question 101:

In the context of Information Systems Security, what comprises the three essential security principles of confidentiality, integrity, and availability?

A) RCMP Triad

B) FBI Triad

C) INTERPOL Triad

D) CIA Triad

Question 102:

What term describes a highly detailed and specific level of control over an object's security settings in Information Systems Security?

A) Specific Object Control

B) Granular Object Control

C) Precise Object Control

D) Detailed Object Control

Question 103:

In a scenario where Harry wants to access a document owned by Sally on a file server, what is considered the object of the resource request according to the subject/object model?

A) Harry

B) Document

C) Sally

D) File server

Question 104:

What is the term for connecting or linking two devices over Bluetooth in Information Systems Security?

A) Pairing

B) Coupling

C) Teaming

D) Mating

Question 105:

Which type of attack overwhelms a system's resources, preventing it from responding to service requests?

A) Denial-of-Service

B) Drive-By Attack

C) Man-in-the-Middle

D) SQL Injection Attack

Question 106:

What is the name of the DoS attack that exploits a bug in an operating system's packet reassembly routines, causing the system to freeze or crash when specifically formatted fragmented packets are sent?

A) Fragmented HTTP Flood

B) Zero-Day Attack

C) Teardrop Attack

D) Ping-of-Death Attack

Question 107:

Which testing method validates the software system according to requirements specifications, checks system functionalities and features, considers both functional and non-functional testing, is executed after Integration Testing, and can be performed manually or through automation?

A) Iterative Testing

B) End-To-End Testing

C) Start-To-End Testing

D) System Testing

Question 108:

Regarding a document titled "Forensic Response Guidelines" provided to a new system engineer, which statement is incorrect?

A) The employee must comply with the information in this document.

B) The document contains information about forensic examinations.

C) The employee should read the document thoroughly.

D) The document is likely based on industry best practices.

Question 109:

If someone who recently took the CISSP certification exam writes a blog post including the text of many exam questions they encountered, which aspect of the (ISC)2 code of ethics is most directly violated?

A) Provide diligent and competent service to principles.

B) Protect society, the common good, necessary public trust.

C) Act honourably, honest, justly, responsibly, and legally.

D) Advance and protect the profession.

Question 110:

According to HIPAA, how is data related to past, present, or future payment for an individual's health care provision classified?

A) PHI

B) Personal billing data

C) PCI

D) Personally Identifiable Information (PII)

Question 111:

What category does the IP address 201.19.7.45 fall under?

A) A loopback address

B) An RFC 1918 address

C) A public IP address

D) An APIPA address

Question 112:

Which of the following is an example of a biometric factor that uses a physiological characteristic unique to an individual?

A) Face Scan

B) Signature Recognition

C) Voice Pattern Recognition

D) Typing Recognition

Question 113:

What term describes a checksum used to verify the integrity of a transmission in Information Systems Security?

A) Validator Sum

B) Hash Total

C) Reverse Lookup

D) Key-Sum Value

Question 114:

In Information Systems Security, what term refers to the minimum security level that all systems within an organization must meet?

A) Guideline

B) Threshold

C) Baseline

D) Control

Question 115:

During which phase of the incident response process do administrators design new security controls to prevent a recurrence of the incident?

A) Lessons learned

B) Recovery

C) Remediation

D) Reporting

Question 116:

What term describes the process of grouping similar elements into classes or roles for assigning security controls, restrictions, or permissions collectively?

A) Aggregation

B) Assimilation

C) Abstraction

D) Arbitration

Question 117:

Which software development lifecycle model is characterized by a series of sequential steps with a feedback loop allowing the process to return to the previous step when necessary?

A) Boehm

B) Agile

C) Waterfall

D) Spiral

Question 118:

What is the term for the practice of sending emails that appear to be from trusted sources with the goal of obtaining personal information or influencing users' actions?

A) SQL Injection Attack

B) Password Attack

C) Birthday Attack

D) Spear Phishing Attacks

Question 119:

In the OSI model, when a packet transitions from a datastream to a segment or datagram, which layer has it traversed?

A) The Physical layer

B) The Data Link layer

C) The Transport layer

D) The Application layer

Question 120:

How does single sign-on enhance security in an organization?

A) It decreases the number of accounts required for a subject.

B) It provides better encryption for authentication data.

C) It helps decrease the likelihood users will write down their passwords.

D) It provides blocking for each system that it is connected to.

Question 121:

When a user attempts to log into their online account and Google sends a text message with a code to their cell phone, what type of verification is this?

A) Risk-based identity proofing

B) Dynamic knowledge-based authentication

C) Out-of-band identity proofing

D) Knowledge based authentication

Question 122:

What term describes the act of redirecting workload or traffic to a backup system when the primary system fails?

A) Failover

B) Failsafe

C) Failclosed

D) Failopen

Question 123:

In wireless networks, what connection scheme allows communications as long as a radio signal can be transmitted between the client and WAP, without requiring real authentication?

A) Open Relays

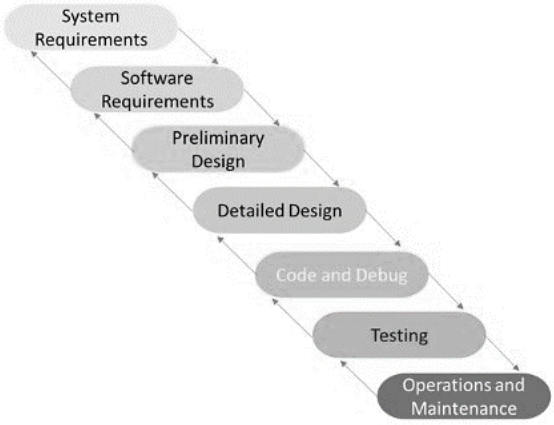
B) Open System Authentication (OSA)

C) Public Use Mail Relays (PUMR)

D) Open Source Mail Services (OSMS)

Question 124:

For a mission-critical application with a direct impact on human safety, where time and cost are less important than correctly functioning software, which software development methodology is most appropriate?



A) Agile

B) Waterfall

C) DevOps

D) Spiral

Question 125:

The CIA Triad consists of three essential security principles. Which of the following is not one of these principles?

A) Confidentiality

B) Integrity

C) Availability

D) Accountability

Question 126: What security system employs video cameras and recording devices for surveillance purposes?

A) Security System Entry Detection (SSED)

B) Commercial Security Automation Equipment (CSAE)

C) Closed-Circuit Television (CCTV)

D) Security System Threat Detection (SSTD)

Question 127: Which communication medium can only support one signal at a time?

A) Twisted Pair

B) Coaxial Cable

C) 3G

D) Baseband

Question 128: What process is used to transform a message into ciphertext?

A) Salt

B) Hash

C) Decrypt

D) Encrypt

Question 129: What type of password changes with each use and is considered a dynamic variant?

A) One-Time Password (OTP)

B) Biometric Access Control (BAC)

C) Password Resetting

D) Multifactor Authentication (MA)

Question 130: In the sequence of physical security controls, which objective is typically addressed first?

A) Deterrence

B) Detection

C) Denial

D) Delay

Question 131: Which solution is most appropriate for addressing the log management challenges outlined in NIST Special Publication 800-92?

A) Implement a SIEM

B) Enable logging on all endpoints using native formats and set local time correctly

C) Implement SNMP for all logging devices

D) Standardize on Windows event log format and use NTP

Question 132: Which identification tool is commonly used but not suitable as an authenticator?

A) Token

B) Password

C) Retinal scan

D) Username

Question 133: What authentication method, often used in mobile device management systems, considers factors like user location, time of day, and device type?

A) Content-Aware Authentication

B) System-Rights Authentication

C) User-Specific Authentication

D) Permission-Based Authentication

Question 134: Which Single Sign-On (SSO) method is used when the client and server are unsure of each other's supported authentication types?

A) Cookie-based SSO

B) Kerberos-based SSO

C) Form-filling SSO

D) SPNEGO-based SSO

Question 135: In the OSI Model, which layer is responsible for transmitting raw bitstream over the physical medium?

A) Presentation

B) Application

C) Transport

D) Physical

Question 136: Which RAID configuration is also known as disk striping?

A) RAID 5

B) RAID 0

C) RAID 1

D) RAID 10

Question 137: What type of inbound packet is typically associated with a Ping Flood Attack?

A) ICMP echo reply

B) ICMP route changed

C) ICMP echo request

D) ICMP destination unreachable

Question 138: What technology creates a secure network connection between two systems over an existing network, providing confidentiality and integrity through encryption?

A) Validation of Parent Netmask (VPN)

B) Valid Parallel Network (VPN)

C) Virtual Private Network (VPN)

D) Vertical Patch Nonce (VPN)

Question 139: Under which category do preventative, detective, corrective, recovery, deterrent, and compensation controls fall?

A) Permission Control

B) Anti-malware Control

C) Virus Control

D) Access Control

Question 140: What should be investigated when needing to share identity information with a business partner in an identity management implementation?

A) IDaaS

B) Federation

C) Single Sign-on

D) Multi-factor Authentication

Question 141: When building a disaster recovery plan, what metric determines the acceptable amount of data loss following an outage?

A) MTD

B) RTO

C) RPO

D) SLA

Question 142: Which type of alternate processing site has the necessary hardware for restoring operations but lacks current data copies?

A) Warm site

B) Cold site

C) Mobile site

D) Hot site

Question 143: Which encryption algorithm would be most efficient for key management in a large organization with 10,000 employees?

A) 3DES

B) Skipjack

C) RSA

D) IDEA

Question 144: What term describes the decrease in signal strength and integrity in a cable due to its length?

A) Fatigue

B) Attenuation

C) Sarcopenia

D) Asthenia

Question 145: What is a read-only version of a certificate authority that can distribute CRLs and verify certificates but cannot create new ones?

A) Secure Sockets Layer Authority (SSLA)

B) Registration Authority (RA)

C) Certificate Revocation Authority (CRA)

D) Certificate Authority (CA)

Question 146: What technique is often employed on honeypot systems and critical resources to simulate known operating system vulnerabilities?

A) Apparition

B) Pseudo Flaw

C) Poltergeist

D) Pirate Trap

Question 147: What term describes a system's response to failure that results in a default "deny" posture?

A) Fail-Closed

B) Fail-Over

C) Fail-Safe

D) Fail-Open

Question 148: After conducting automated functional testing with 100% coverage on an application, which type of error is most likely to persist?

A) Runtime errors

B) Input validation errors

C) Business logic errors

D) Error handling errors

Question 149: In an asymmetric cryptosystem, what key should be used to encrypt a private message when communicating with another party?

A) CA's private key

B) Recipient's private key

C) Recipient's public key

D) CA's public key

Question 150: Which programming language can be directly executed by a computer without further translation?

A) Scripting Language

B) Assembly Language

C) Machine Language

D) Object-Oriented Language

Correct Answers & Explanations

Question 1

A) Inference (Correct Answer)

Explanation: The security administrator is concerned about inference, which is the process of deducing sensitive information from seemingly innocuous data. In this case, employees with lower security clearances might infer classified mission information by observing aircraft movements. Inference is a significant security issue in multilevel security environments, where users with different clearance levels have access to the same system.

Question 2

B) 37.5% (Correct Answer)

Explanation: The Exposure Factor (EF) is the percentage of asset value that would be lost in a single occurrence of a threat. In this case, the total asset value is $2 million, and the potential damage from a fire is $750,000. To calculate the EF, we divide the potential loss by the total asset value: $750,000 / $2,000,000 = 0.375 or 37.5%.

Question 3

B) Filter (Correct Answer)

Explanation: A filter is a set of rules or restrictions commonly used in security devices like firewalls and proxies. Filters are designed to control network traffic by allowing or blocking specific types of data packets based on predefined criteria such as source IP address, destination port, or protocol type.

Question 4

D) It's an encrypted email message (Correct Answer)

Explanation: The attachment named "smime.p7s" is typically associated with S/MIME (Secure/Multipurpose Internet Mail Extensions) encrypted email messages. S/MIME is a widely used protocol for sending digitally signed and encrypted messages. The ".p7s" file extension indicates a PKCS#7 signature file, which is used to verify the authenticity and integrity of the email.

Question 5

B) Fagan (Correct Answer)

Explanation: The Fagan inspection, developed by Michael Fagan at IBM, is considered the most rigorous and formal software testing approach. It involves a structured process of preparation, inspection meeting, rework, and follow-up. This method is known for its thoroughness and effectiveness in identifying defects early in the software development lifecycle.

Question 6

A) The answers may be easily found online (Correct Answer)

Explanation: The primary weakness of using pre-set questions for cognitive passwords is that the answers to these questions can often be easily found online, especially with the prevalence of social media and public records. This makes it relatively simple for attackers to guess or research the correct answers, compromising the security of the authentication system.

Question 7

B) 0.02 (Correct Answer)

Explanation: The Annualized Rate of Occurrence (ARO) is the estimated frequency with which a threat is expected to occur in a year. In this case, fires are expected once every 50 years. To calculate the ARO, we divide 1 by the number of years between occurrences: 1 / 50 = 0.02. This means there's a 2% chance of a fire occurring in any given year.

Question 8

D) Foreign key (Correct Answer)

Explanation: In database security, an aircraft's tail number used as a unique identifier would typically be a candidate key, a primary key, and a database field. However, it is not necessarily a foreign key. A foreign key is used to establish a relationship between two tables by referencing the primary key of another table, which may not be the case for the tail number in all database designs.

Question 9

B) Content-Dependent Access Control (Correct Answer)

Explanation: Content-Dependent Access Control is a type of access control that restricts data access based on the contents or payload of an object. This approach examines the actual content of the data, rather than just relying on predefined access rules or user roles, to determine whether access should be granted or denied.

Question 10

B) Interference (Correct Answer)

Explanation: Interference best describes the problem where data packets are becoming corrupted during transmission. Interference occurs when external signals or noise disrupt the transmission of data, leading to errors or corruption in the packets. This can be caused by various factors such as electromagnetic interference, radio frequency interference, or physical obstacles in the transmission path.

Question 11

B) Add a second authentication factor (Correct Answer)

Explanation: To address concerns about a high False Acceptance Rate (FAR) in a biometric system, adding a second authentication factor is the most effective method. This approach, known as multi-factor authentication,

combines the biometric factor with another form of authentication (e.g., a password or token). This significantly reduces the likelihood of unauthorized access, even if the biometric system occasionally accepts an impostor.

Question 12

A) RAID 1 (Correct Answer)

Explanation: RAID 1, commonly referred to as disk mirroring, is a configuration where data is written identically to two or more drives. This creates a redundant copy of the data, providing fault tolerance and improved read performance. In the event of a drive failure, the system can continue to operate using the mirrored drive without data loss.

Question 13

A) Elliptic Curve Cryptography (Correct Answer)

Explanation: Elliptic Curve Cryptography (ECC) offers security similar to established public key systems but with smaller key sizes. ECC uses the mathematics of elliptic curves to create cryptographic keys. It provides the same level of security as traditional methods like RSA but with significantly shorter keys, making it more efficient for resource-constrained devices and faster computations.

Question 14

B) Ring 3 (Correct Answer)

Explanation: In a ring protection model, Ring 3 typically contains user programs and applications. The ring protection model is a hierarchical approach to system security, with Ring 0 being the most privileged (usually containing the kernel) and outer rings having progressively less privilege. Ring 3 is the least privileged ring where user-mode applications run, providing a separation between user space and more critical system components.

Question 15

B) Compromised (Correct Answer)

Explanation: The term "compromised" is used to describe a system whose security has been breached. When a system is compromised, it means that an unauthorized party has gained access or control, potentially exposing sensitive data or functionality. This term is widely used in information security to indicate that the integrity, confidentiality, or availability of a system has been negatively impacted.

Question 16

B) MAN (Correct Answer)

Explanation: A Metropolitan Area Network (MAN) is designed to cover an entire city, potentially connecting multiple Local Area Networks (LANs). MANs typically span a larger geographical area than LANs but are smaller than Wide Area Networks (WANs). They are often used by organizations with multiple locations within a city or by municipal governments to connect various departments and services across a metropolitan area.

Question 17

D) Asymmetric Multi-Processing (AMP) (Correct Answer)

Explanation: Asymmetric Multi-Processing (AMP) involves processors operating independently, each with its own operating system and/or task instruction set. In AMP, different processors may be assigned specific tasks or run different operating systems, allowing for specialized processing and potentially more efficient use of resources in certain scenarios. This is in contrast to Symmetric Multi-Processing (SMP), where all processors share the same resources and run the same operating system.

Question 18

A) Release of a security patch (Correct Answer)

Explanation: The release of a security patch transforms a zero-day vulnerability into a less critical security threat. A zero-day vulnerability is a software flaw that is unknown to the vendor and has no available fix. Once a patch is released, the vulnerability is no longer "zero-day" as a solution exists. However, it's important to note that the threat is not completely eliminated until the patch is widely deployed.

Question 19

D) TLS (Correct Answer)

Explanation: Transport Layer Security (TLS) is most effective in preventing session hijacking attacks. TLS, the successor to SSL, provides end-to-end encryption for data in transit, ensuring the confidentiality and integrity of the communication between the client and server. It also includes mechanisms for authentication, making it difficult for attackers to intercept or manipulate the session data. While SSL also offers protection, TLS is the more current and secure protocol.

Question 20

D) One-Way Encryption (Correct Answer)

Explanation: One-Way Encryption, also known as hashing, creates a cryptographic code that cannot be reversed when applied to passwords, messages, or CRCs. This type of encryption transforms input data into a fixed-size string of characters, which is designed to be irreversible. It's particularly useful for storing passwords securely, as the original input cannot be derived from the hash, enhancing security even if the hash is compromised.

Question 21

A) Stealing user cookies (Correct Answer)

Explanation: In the context of cross-site tracing (XST) vulnerabilities, stealing user cookies is the most relevant

concern. XST is a type of attack that exploits the HTTP TRACE method to capture sensitive information, particularly cookies. Attackers can use this vulnerability to bypass security measures like HttpOnly flags and gain access to session cookies, potentially leading to session hijacking or other forms of unauthorized access.

Question 22

A) SQL Injection (Correct Answer)

Explanation: SQL Injection is an attack that involves submitting database expressions and script code to bypass authentication and interact directly with the Database Management System (DBMS) or underlying operating system. Attackers exploit vulnerabilities in input validation to inject malicious SQL statements, which can allow them to read, modify, or delete database contents, execute administrative operations, or even issue commands to the operating system.

Question 23

C) Incremental backup (Correct Answer)

Explanation: An incremental backup stores all files that have been modified since the most recent backup, whether it was a full backup or another incremental backup. This method is efficient as it only backs up changes, resulting in smaller backup sizes and faster backup times compared to full or differential backups. However, restoration can be more complex as it requires the last full backup and all subsequent incremental backups.

Question 24

B) Mail-Bombing (Correct Answer)

Explanation: Mail-Bombing describes an attack where a large number of messages are directed to a single user's inbox or through a specific SMTP server to cause a denial of service. This flood of messages can overwhelm the

recipient's email system, potentially causing it to crash or become unresponsive. Mail-bombing can also be used to fill up the target's storage quota, preventing legitimate emails from being received.

Question 25

A) Frequency (Correct Answer)

Explanation: Frequency is the term for the measurement of wave oscillations within a specific time, typically expressed in Hertz (Hz). In the context of waves, including sound and electromagnetic waves, frequency refers to the number of cycles or vibrations that occur in one second. It is a fundamental characteristic of waves and plays a crucial role in various fields, including communications, audio engineering, and signal processing.

Question 26

D) Segmentation (Correct Answer)

Explanation: Network segmentation is the process of dividing a network into smaller units or subnetworks to improve various aspects such as performance, security, and traffic isolation. This technique allows for better control over network traffic, limits the spread of security threats, and can enhance overall network performance by reducing congestion in any one segment.

Question 27

C) Common Access Card (CAC) (Correct Answer)

Explanation: The Common Access Card (CAC) is a smart card used by US government personnel that includes a picture and functions as both a badge and a smart card. It serves as the standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. The CAC is used for both physical access to buildings and controlled

spaces, and for logical access to computer networks and systems.

Question 28

B) Community Cloud (Correct Answer)

Explanation: In a community cloud model, multiple organizations with shared concerns (e.g., mission, security requirements, policy, and compliance considerations) collaborate to build a shared environment for their own use. This model allows organizations with similar needs to pool their resources and share infrastructure, reducing costs while maintaining more control and privacy than a public cloud offering.

Question 29

D) SQL injection (Correct Answer)

Explanation: The input "Smith' ; DROP TABLE orders;--" is a clear indicator of an SQL injection attack. In this case, the attacker is attempting to manipulate the database query by inserting a malicious SQL command (DROP TABLE orders) into the input field. The single quote (') is used to close the original query, the semicolon (;) separates commands, and the double dash (--) comments out the rest of the original query to prevent syntax errors.

Question 30

B) VoIP (Correct Answer)

Explanation: Voice over Internet Protocol (VoIP) is the network service that provides voice communication by transporting voice traffic's network packets over an IP network. VoIP converts analog voice signals into digital data packets and transmits them over the internet or other IP-based networks. This technology allows for voice calls to be made using internet connections rather than traditional phone lines, often resulting in lower costs and increased flexibility.

Question 31

D) Class C (Correct Answer)

Explanation: Class C fire extinguishers are specifically designed and suitable for combating electrical fires. These extinguishers use non-conductive agents, typically dry chemical powders, to suppress fires involving energized electrical equipment without risking electric shock to the user. It's crucial to use the correct class of extinguisher for electrical fires to ensure safety and effectiveness in fire suppression.

Question 32

A) Identity Theft and Assumption Deterrents Act (Correct Answer)

Explanation: The Identity Theft and Assumption Deterrence Act of 1998 is the U.S. federal law that criminalizes the act of stealing or assuming another person's identity, with penalties including up to 15 years in prison and/or a $250,000 fine. This act made identity theft a federal crime and provided for enhanced penalties for aggravated identity theft. It also recognized the individual victim in identity theft cases, allowing them to seek restitution.

Question 33

C) 100 metres (Correct Answer)

Explanation: According to the TIA/EIA-568-B standard, the maximum distance a Category 6 (Cat6) cable can be run is 100 meters (328 feet). This distance includes 90 meters of solid "horizontal" cabling between the patch panel and the wall jack, plus 10 meters of stranded patch cable between the jack and the attached device, and the switch and the patch panel. This limitation is due to signal attenuation and crosstalk over longer distances.

Question 34

C) Secret (Correct Answer)

Explanation: When labeling a system that handles Secret, Confidential, and Unclassified information in a US government context, the highest classification level should be applied, which in this case is Secret. This practice, known as the "high water mark" principle, ensures that the system is protected at the level of its most sensitive information. Secret classification requires stricter security measures than Confidential or Unclassified, thus providing adequate protection for all levels of information in the system.

Question 35

C) AUP (Correct Answer)

Explanation: AUP stands for Acceptable Use Policy, which defines acceptable performance and behavior expectations for employees, with potential consequences for non-compliance. An AUP typically outlines the permitted uses of an organization's IT resources, including computers, networks, and internet access. It may cover topics such as email usage, social media behavior, data protection, and security practices. AUPs are crucial for maintaining security, productivity, and legal compliance within an organization.

Question 36

C) Tree (Correct Answer)

Explanation: A tree network topology features a root node with all other nodes connected to it in a hierarchy. This structure resembles an inverted tree, with the root node at the top and branches extending downward. Each node in the tree can have multiple child nodes, but only one parent node. This topology is often used in wide area networks and is efficient for organizing hierarchical data structures or network management systems.

Question 37

C) Encryption (Correct Answer)

Explanation: Encryption is the security measure typically employed when purchasing tickets online to protect credit card and personal information during transmission. Encryption converts sensitive data into a coded format that can only be deciphered with the correct decryption key. This process ensures that even if the data is intercepted during transmission, it remains unreadable and secure. Common encryption protocols used in online transactions include SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security).

Question 38

A) Phreaking (Correct Answer)

Explanation: Phreaking is the term that describes the process of breaking into telephone company computers to place free calls. This practice originated in the 1960s and 1970s when "phone phreaks" discovered ways to manipulate the telephone system's signaling tones to make free long-distance calls or access special phone company functions. While modern digital telephone systems have made traditional phreaking techniques largely obsolete, the term is still used to describe various forms of telephone system exploitation.

Question 39

A) Attribute (Correct Answer)

Explanation: In a relational database, a column within a table is called an attribute. Each attribute represents a specific piece of data or characteristic of the entity that the table represents. For example, in a "Customers" table, attributes might include "CustomerID," "FirstName," "LastName," and "Email." Attributes define the structure of the table and the type of data that can be stored in each column.

Question 40

D) Polymorphic Virus (Correct Answer)

Explanation: A polymorphic virus is a type of malware that modifies its own code as it spreads from system to system, maintaining its core functions but altering its signature. This self-modification capability allows the virus to evade detection by traditional signature-based antivirus software. Each time the virus replicates, it encrypts itself differently or changes its code structure, making it challenging for security systems to identify and remove. Despite these changes, the virus retains its original malicious functionality.

Question 41

C) Man-in-the-Middle Attacks (Correct Answer)

Explanation: Using a trusted channel and link encryption are methods primarily designed to prevent Man-in-the-Middle (MitM) attacks. In a MitM attack, an attacker intercepts communication between two parties, potentially eavesdropping on or altering the data being exchanged. A trusted channel ensures that the communication path between parties is secure and authenticated, while link encryption protects the data as it travels across the network. Together, these methods make it extremely difficult for an attacker to insert themselves between the communicating parties or to intercept and decipher the transmitted data.

Question 42

A) Due Care (Correct Answer)

Explanation: The principle of Due Care states that an individual should strive to complete their responsibilities accurately and in a timely manner. In the context of information security, due care refers to taking reasonable steps to protect assets and information, fulfill job responsibilities, and meet legal and regulatory requirements. It implies that individuals and organizations

should act responsibly and diligently in carrying out their duties, especially when it comes to protecting sensitive information and systems.

Question 43

D) Computer Security Act (CSA) (Correct Answer)

Explanation: The Computer Security Act of 1987 (CSA) established baseline security requirements for all federal agencies in the United States. This act was a landmark piece of legislation that required federal agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. It also gave the National Institute of Standards and Technology (NIST) the responsibility for developing standards and guidelines for federal computer systems, except for national security systems.

Question 44

B) Authentication Protocols (Correct Answer)

Explanation: Authentication protocols are used to provide the transport mechanism for login credentials. These protocols define the process and methods by which a user's identity is verified and access is granted to a system or network. Common authentication protocols include Kerberos, LDAP (Lightweight Directory Access Protocol), RADIUS (Remote Authentication Dial-In User Service), and OAuth. These protocols ensure that login credentials are securely transmitted and verified, protecting against unauthorized access and maintaining the integrity of the authentication process.

Question 45

B) 64 (Correct Answer)

Explanation: In a cryptographic algorithm using 6-bit encryption keys, there are 64 possible keys. This is because the number of possible combinations for a binary key is

2^n, where n is the number of bits. In this case, 2^6 = 64. Each bit in the key can be either 0 or 1, and with 6 bits, we have 2 choices for each of the 6 positions, resulting in 2 * 2 * 2 * 2 * 2 * 2 = 64 possible unique key combinations.

Question 46

C) Isolation (Correct Answer)

Explanation: Isolation is the property in database transactions that ensures each transaction is processed independently and simultaneously without interference from others. This ACID (Atomicity, Consistency, Isolation, Durability) property guarantees that concurrent execution of transactions results in a system state that would be obtained if transactions were executed sequentially. Isolation prevents intermediate or partial results of one transaction from becoming visible to other transactions, maintaining data integrity and consistency in multi-user database systems.

Question 47

B) Key (Correct Answer)

Explanation: In cryptography, a key is a secret value used to encrypt or decrypt messages or database fields. The key is a crucial component in cryptographic algorithms, determining how plaintext is converted into ciphertext (during encryption) or how ciphertext is converted back into plaintext (during decryption). The security of many cryptographic systems relies on keeping the key secret, even if the details of the algorithm are known. Keys can be symmetric (same key for encryption and decryption) or asymmetric (different keys for encryption and decryption).

Question 48

D) Alpha Testing (Correct Answer)

Explanation: Alpha testing is characterized by the following:

- It is performed by internal employees, typically developers or testers within the organization.
- It is conducted at the developer's site in a controlled environment.
- It involves both white box (testing internal structures) and black box (testing functionality) techniques.
- It requires a testing environment that closely mimics the production environment.
- It may have a long execution cycle as it's often the first comprehensive testing phase.
- Critical issues can be addressed immediately by developers due to their proximity and involvement.
- Alpha testing is crucial for identifying and resolving major issues before the software is released for beta testing or to end-users.

Question 49

C) RAID 5 (Correct Answer)

Explanation: RAID 5 is known as disk striping with parity. In this RAID configuration, data is striped across multiple drives, and parity information is distributed across all drives in the array. This arrangement provides both improved performance (due to striping) and fault tolerance. If one drive fails, the parity information can be used to reconstruct the lost data. RAID 5 requires a minimum of three drives and offers a good balance between performance, storage efficiency, and data protection.

Question 50

D) Segmentation (Correct Answer)

Explanation: In the context of information security, segmentation describes the act of subdividing a network into numerous smaller units to improve various aspects such as performance, congestion, and security. Network segmentation involves creating subnetworks or VLANs

(Virtual Local Area Networks) that isolate different parts of the network. This practice enhances security by limiting the potential spread of malware or breaches, improves performance by reducing network congestion, and allows for more granular access control policies. Segmentation is a fundamental principle in designing secure and efficient network architectures.

Question 51

C) Intellectual Property (Correct Answer)

Explanation: Intellectual Property refers to intangible creations of the human intellect, such as confidential recipes or manufacturing methods. It includes patents, trademarks, copyrights, and trade secrets. In Information Systems Security, protecting intellectual property is crucial as it often represents a company's most valuable assets.

Question 52

A) Encryption (Correct Answer)

Explanation: Encryption is the process of converting information or data into a code to prevent unauthorized access. It is indeed the art and science of concealing the meaning or purpose of communication from unintended recipients. Encryption uses complex algorithms to scramble data, making it unreadable without the correct decryption key.

Question 53

C) Beacon Frame (Correct Answer)

Explanation: In wireless networking, a Beacon Frame is a type of management frame that contains all the information about the network. It is periodically transmitted by access points to announce the presence of a wireless LAN and to synchronize the members of the service set. The Beacon Frame includes the network's SSID (Service Set Identifier) or name, among other important parameters.

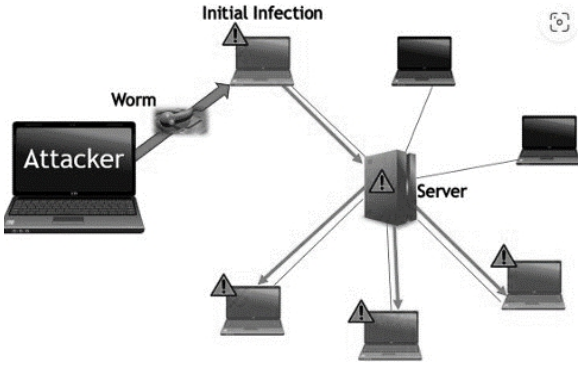
Question 54

C) Smartcard (Correct Answer)

Explanation: A Smartcard is a credit card-sized device that contains an embedded integrated circuit chip. This chip stores and processes data, including information about the authorized user for identification and authentication purposes. Smartcards are widely used in various applications, including secure identity verification, financial transactions, and access control systems.

Question 55

C) Worm (Correct Answer)



Explanation: A worm is a type of malware that replicates itself and spreads to other computers over a network without any user interaction. The scenario described, where systems across the office are suddenly showing signs of infection, is characteristic of a worm attack. Worms can spread rapidly, causing widespread damage and disruption to network operations.

Question 56

B) SCAP (Correct Answer)

Explanation: SCAP (Security Content Automation Protocol) is the correct standardized protocol for interfacing with the National Vulnerability Database. SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate software

flaw and security configuration information. It ensures compatibility and consistency in vulnerability management across different systems and tools.

Question 57

C) LAN (Correct Answer)

Explanation: LAN stands for Local Area Network. It is a computer network that interconnects computers within a limited area such as an office, building, or small group of buildings. LANs are used for sharing resources like files, printers, games or other applications. They are characterized by high-speed data transfer rates and are typically owned, controlled, and managed by a single organization.

Question 58

C) Schema (Correct Answer)

Explanation: A schema is the structure that defines or describes a database. It is written using a Data Definition Language (DDL) and serves as a blueprint of how the database is constructed. The schema defines the tables, fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, and other elements that make up a database.

Question 59

C) State Machine Model (Correct Answer)

Explanation: The State Machine Model defines behaviors for a finite number of states, transitions between those states, and actions. It is based on the concept that a system can be in only one state at a time, transitioning from one state to another when triggered by a specific event or condition. This model is particularly useful for describing systems with discrete states and well-defined transitions.

Question 60

B) Warm site (Correct Answer)

Explanation: A warm site is a disaster recovery facility that balances cost and recovery time. It typically includes the necessary hardware and infrastructure but may not have all the data and applications fully configured. A warm site can be activated within a few days to a week after a disaster declaration, which aligns with Hope Pym's requirements. It offers a middle ground between the more expensive, faster-to-activate hot site and the cheaper, slower-to-activate cold site.

Question 61

D) Transport (Correct Answer)

Explanation: In the OSI (Open Systems Interconnection) Model, the Transport layer (Layer 4) is responsible for providing reliable data transfer services to the upper layers. It allows applications to access network services by establishing, maintaining, and terminating connections between applications. The Transport layer ensures end-to-end communication, flow control, and error recovery, effectively bridging the gap between application-specific higher layers and the more network-oriented lower layers.

Question 62

B) Revocation of certification (Correct Answer)

Explanation: The most severe penalty that an (ISC)² peer review board can impose for an ethics violation is the revocation of certification. This means the individual's certification is permanently withdrawn, and they are no longer recognized as a certified professional by (ISC)². This severe action is typically taken for the most serious ethical breaches, as it effectively ends the individual's status as a certified professional in their field.

Question 63

C) Type 2 (Correct Answer)

Explanation: In authentication factor categorization, Type 2 refers to something you possess. This includes physical objects like smartcards, token devices, or key fobs. These items are unique to the user and serve as a means of verifying identity. Type 2 factors are often used in combination with other factor types (like passwords - Type 1, or biometrics - Type 3) to create multi-factor authentication systems, enhancing security.

Question 64

C) CER (Correct Answer)

Explanation: CER stands for Crossover Error Rate. It is the point where the False Acceptance Rate (FAR) equals the False Rejection Rate (FRR) in a biometric system. The CER is an important metric in evaluating the overall accuracy of a biometric system. A lower CER indicates a more accurate system. At this point, the system's tolerance is optimally set to balance the trade-off between falsely accepting unauthorized users and falsely rejecting authorized users.

Question 65

C) Retinal Scanning (Correct Answer)

Explanation: Retinal scanning is a biometric technique that uses low-beam infrared light to map the unique patterns of a person's retina. The retina, located at the back of the eye, contains a complex network of blood vessels. When infrared light is cast onto the eye, these blood vessels absorb the light at a higher rate than surrounding tissue, creating a unique pattern. This pattern is then captured and converted into a digital signature for identification purposes. Retinal scans are considered one of the most accurate and secure biometric methods due to the uniqueness and stability of retinal patterns.

Question 66

A) Flight Time (Correct Answer)

Explanation: In keystroke dynamics biometrics, Flight Time refers to the duration between releasing one key and pressing the next. This measure is part of a user's typing pattern and can be used as a biometric identifier. Flight time, along with other metrics like dwell time (how long a key is pressed), forms a unique typing signature for each individual. This can be used as an additional layer of authentication or continuous verification in cybersecurity applications.

Question 67

A) Pepper (Correct Answer)

Explanation: In the context of password security, a pepper is a secret value that is added to passwords before hashing. Unlike a salt, which is typically stored with the password hash, a pepper is kept separate and secret. The purpose of a pepper is to add an extra layer of protection against rainbow table attacks and to make it significantly more difficult for an attacker to crack passwords even if they gain access to the password database. By keeping the pepper secret and separate from the salted passwords, it adds an additional security barrier that an attacker would need to overcome.

Question 68

C) Encapsulation (Correct Answer)

Explanation: Encapsulation is the process of adding headers and footers (collectively called overhead) to a Protocol Data Unit (PDU) as it moves down the OSI model layers. Each layer adds its own layer-specific information to the data received from the layer above, wrapping it in a new layer of protocol information. This process continues until the data reaches the physical layer for transmission. Encapsulation ensures that each layer can perform its designated

functions and that the data can be properly routed and interpreted as it travels across the network.

Question 69

D) A subject (Correct Answer)

Explanation: When a web application retrieves user information from a database, it acts as a subject. In information security, a subject is an active entity that requests access to an object or the data within an object. In this scenario, the web application is actively requesting and accessing data (the object) stored in the database. The application is performing an action (retrieving information) on behalf of a user, making it a subject in the context of access control and information security models.

Question 70

C) Eavesdropping (Correct Answer)

Explanation: Eavesdropping, also known as sniffing, is the act of secretly listening to or intercepting private communications without the consent of the participants. In the context of information security, this term encompasses the unauthorized capture and monitoring of various forms of electronic communications, including network traffic, audio communications, faxes, and radio signals. Eavesdropping can be passive (just listening) or active (injecting data into the communication). It's a significant security concern as it can lead to the compromise of sensitive information.

Question 71

A) Reactive Approach (Correct Answer)

Explanation: The Reactive Approach to threat modeling occurs after a product has been deployed. This approach forms the basis for ethical hacking and penetration testing. Unlike proactive approaches that try to anticipate threats during the development phase, the reactive approach involves analyzing and testing the system in its live

environment. Ethical hackers and penetration testers use this approach to identify vulnerabilities that may have been overlooked during development or that have emerged due to changes in the threat landscape. This approach helps in continuously improving the security posture of deployed systems.

Question 72

B) Key Distribution Centre (KDC) (Correct Answer)

Explanation: In Kerberos authentication, the Key Distribution Centre (KDC) acts as both an Authentication Server (AS) and a Ticket Granting Server (TGS). The KDC is a trusted third party that manages secret keys for all clients and servers within its realm. As an Authentication Server, it verifies the initial identity of users and provides them with a Ticket Granting Ticket (TGT). As a Ticket Granting Server, it issues service tickets to authenticated users, allowing them to access specific services. This dual role makes the KDC a central component in the Kerberos authentication process, facilitating secure communication in distributed environments.

Question 73

D) Hot site (Correct Answer)

Explanation: A hot site is an alternate processing facility that can restore operations within minutes by including all necessary hardware and data. It is a fully equipped duplicate of the original site, with up-to-date copies of data. Hot sites maintain a constant state of readiness, with systems running and data continuously replicated from the primary site. This makes them capable of taking over operations almost immediately in the event of a disaster. While hot sites are the most expensive disaster recovery option, they offer the fastest recovery time, which is critical for organizations that cannot tolerate extended downtime.

Question 74

B) Change control (Correct Answer)

Explanation: Change control is the process that would best help Bethany address issues arising from system administrators updating libraries without informing developers. Change control is a systematic approach to managing all changes made to a product or system. It ensures that no unnecessary changes are made, all changes are documented, services are not unnecessarily disrupted, and resources are used efficiently. In this scenario, implementing a robust change control process would require system administrators to document and communicate any updates to libraries, ensuring that developers are informed and can adjust their work accordingly. This would prevent unexpected conflicts and maintain system integrity.

Question 75

B) Residual Risk (Correct Answer)

Explanation: Residual Risk refers to the risk that remains after security controls have been applied. It is the risk associated with specific threats to assets that management chooses not to safeguard against, often due to cost-benefit analysis or acceptance of a certain level of risk. Residual risk acknowledges that it's often impractical or impossible to eliminate all risks, and some level of risk must be accepted as part of operations. Management's decision not to implement certain safeguards is typically based on a balance between the cost of implementation and the potential impact of the risk. Understanding and managing residual risk is a crucial part of an organization's overall risk management strategy.

Question 76

C) 20% (Correct Answer)

Explanation: The Exposure Factor (EF) is the percentage of asset value that's expected to be lost in a single occurrence of a threat. In this scenario, the data center is valued at $100 million, and the potential damage from a flood is $20 million. To calculate the EF, we divide the potential loss by the total asset value: $20 million / $100 million = 0.20 or 20%. This means that 20% of the data center's value is at risk in the event of a flood.

Question 77

D) Deterrent Access Control (Correct Answer)

Explanation: Deterrent Access Control uses measures designed to discourage potential violators from attempting to breach security policies. This type of control doesn't physically prevent access but rather creates psychological barriers. Examples include locks, security badges, and awareness training, which all serve to make potential violators think twice before attempting unauthorized access. The goal is to reduce the likelihood of security breaches by making them seem more difficult or risky to attempt.

Question 78

B) Assuming control of non-registered BYOD devices (Correct Answer)

Explanation: Mobile Device Management (MDM) solutions typically cannot assume control of non-registered BYOD (Bring Your Own Device) devices. MDM is designed to manage and secure mobile devices that are enrolled in the organization's system. It can enforce device encryption, manage backups, and remotely wipe registered devices. However, it cannot take control of personal devices that haven't been registered with the MDM system. This limitation is crucial for maintaining the privacy of personal devices while still allowing organizations to secure their data on employee-owned devices that are used for work purposes.

Question 79

D) SOC 3 (Correct Answer)

Explanation: SOC 3 reports provide general-use information on controls related to compliance and operations. These reports are designed for a broad audience and do not contain the detailed descriptions found in SOC 1 or SOC 2 reports. SOC 3 reports offer a high-level overview of a service organization's controls, focusing on security, availability, processing integrity, confidentiality, and privacy. They are often used for marketing purposes as they can be freely distributed without the restrictions placed on SOC 1 and SOC 2 reports.

Question 80

D) Flight Time (Correct Answer)

Explanation: In keystroke dynamics biometrics, Flight Time refers to the duration between key presses. It measures the time interval from when one key is released to when the next key is pressed. This metric, along with other timing characteristics like dwell time (how long a key is held down), forms part of an individual's unique typing pattern. Flight time is a crucial component in keystroke dynamics, which is used as a behavioral biometric for user authentication or continuous identity verification in cybersecurity applications.

Question 81

B) Cross-domain SSO (Correct Answer)

Explanation: Cross-domain Single Sign-On (SSO) allows authentication between separate secure domains without relying on a master authentication server. This type of SSO is designed to work across different security domains or organizations that may not share a common centralized authentication infrastructure. It typically uses federated identity protocols like SAML (Security Assertion Markup

Language) or OAuth to enable users to access resources across multiple domains with a single set of credentials. This approach is particularly useful in scenarios involving partnerships between organizations or in cloud-based environments where services may span multiple domains.

Question 82

B) Qualitative Risk Analysis (Correct Answer)

Explanation: Qualitative Risk Analysis uses scenario-oriented analysis for ranking and grading exposure ratings and decisions. This method relies on subjective evaluations and expert judgment to assess the likelihood and impact of potential risks. It often uses scales (like high, medium, low) to rate risks rather than precise numerical values. Qualitative analysis is particularly useful when dealing with intangible factors or when precise data is unavailable. It allows for quick assessments and is often used in the early stages of risk management to prioritize risks for further analysis or immediate action.

Question 83

A) Digital Signature (Correct Answer)

Explanation: A Digital Signature is a method that assures a recipient that a message is authentic and unaltered during transmission. It uses asymmetric cryptography to create a unique mathematical scheme derived from the content of the message and the sender's private key. The recipient can verify the signature using the sender's public key. Digital signatures provide three key security services: authentication (verifying the identity of the sender), integrity (ensuring the message hasn't been altered), and non-repudiation (preventing the sender from denying they sent the message). This makes digital signatures crucial for secure electronic communications and transactions.

Question 84

B) Relational Database (Correct Answer)

Explanation: A Relational Database consists of tables containing sets of related records. This type of database organizes data into one or more tables (or "relations") of columns and rows, with a unique key identifying each row. Relationships can be established between different tables based on these keys. Relational databases use Structured Query Language (SQL) for manipulating and querying data. They are widely used due to their flexibility, scalability, and ability to handle complex queries efficiently. Examples of relational database management systems include MySQL, PostgreSQL, and Oracle.

Question 85

A) Exploratory Testing (Correct Answer)

Explanation: Exploratory Testing is an approach that involves checking systems on the fly without pre-created test cases. In this method, testers simultaneously learn about the system, design tests, and execute them. It relies heavily on the tester's creativity, experience, and intuition. Exploratory testing is particularly useful for discovering unexpected bugs or usability issues that might be missed by more structured testing approaches. It allows testers to adapt their strategies in real-time based on what they discover during the testing process, making it especially valuable for complex systems or when time is limited.

Question 86

C) Jitter (Correct Answer)

Explanation: Jitter refers to the variation in packet delay from source to destination in a network. It's the inconsistency of packet arrival time, which can cause issues in real-time applications like VoIP or video streaming. While latency measures the time it takes for a packet to travel from source to destination, jitter measures the variation in

this travel time among different packets. High jitter can result in choppy audio or video, packet loss, and overall degradation of service quality. Network administrators often monitor and try to minimize jitter to ensure smooth performance of time-sensitive applications.

Question 87

A) Clark-Wilson Model (Correct Answer)

Explanation: The Clark-Wilson Model is a security model that uses limited interfaces or programs to control and maintain object integrity. It focuses on preventing unauthorized modifications to data by enforcing the concept of "well-formed transactions." The model introduces the notion of Constrained Data Items (CDIs) which can only be manipulated by a specific set of Transformation Procedures (TPs). This approach ensures that data integrity is maintained by limiting how data can be accessed and modified. The Clark-Wilson Model is particularly relevant in commercial and industrial settings where data integrity is crucial, such as in financial systems or inventory management.

Question 88

C) Hostile Applet (Correct Answer)

Explanation: A Hostile Applet is a term used to describe mobile code that attempts to perform unwanted or malicious activities. These are typically small programs, often written in Java, that are designed to run within a web browser or another application. Unlike benign applets that enhance user experience, hostile applets exploit vulnerabilities in the host system to perform unauthorized actions. These can include accessing sensitive information, modifying system settings, or serving as a gateway for further attacks. The concept of hostile applets highlights the security risks associated with running untrusted code from

the internet, emphasizing the need for robust security measures in web browsers and runtime environments.

Question 89

D) Children's Online Privacy Protection Act (COPPA) (Correct Answer)

Explanation: The Children's Online Privacy Protection Act (COPPA) is a U.S. law that imposes specific requirements on websites catering to or knowingly collecting information from children under 13 years old. Enacted in 1998 and enforced by the Federal Trade Commission, COPPA aims to protect children's privacy online. It requires websites to obtain verifiable parental consent before collecting, using, or disclosing personal information from children. The law also mandates clear privacy policies, limits on data collection, and provisions for parental access and control over their children's information. COPPA has significant implications for how online services interact with and market to children, affecting everything from social media platforms to educational websites.

Question 90

C) Unpatched web application (Correct Answer)

Explanation: In the context of a potential SQL injection attack, the unpatched web application represents the vulnerability. SQL injection is a code injection technique that exploits vulnerabilities in the way an application interacts with its database. An unpatched web application may contain flaws in its input validation or query construction that allow an attacker to inject malicious SQL statements. These vulnerabilities often arise from outdated or poorly maintained software. By keeping web applications updated and properly patched, many SQL injection vulnerabilities can be mitigated. This scenario underscores the importance of regular security updates and robust coding practices in web application development.

Question 91

B) COPE (Correct Answer)

Explanation: COPE stands for Corporate Owned, Personally Enabled. This mobile device policy involves an organization purchasing and providing devices to employees. Under a COPE policy, the company maintains ownership and control over the devices, but employees are allowed to use them for personal purposes as well. This approach offers several advantages: it ensures standardization of devices, simplifies management and security implementation, and gives the organization greater control over data and applications. At the same time, it provides flexibility to employees by allowing personal use. COPE is often seen as a middle ground between strictly corporate-owned devices and Bring Your Own Device (BYOD) policies.

Question 92

D) Authentication Header (Correct Answer)

Explanation: In IPSec (Internet Protocol Security), the Authentication Header (AH) provides authentication, integrity, and non-repudiation. AH operates by adding a cryptographic checksum to each IP packet, which is calculated using a secret key and the packet's contents. This checksum allows the recipient to verify that the packet hasn't been altered in transit and that it genuinely comes from the claimed sender. While AH doesn't provide confidentiality (encryption), it ensures that the packet's contents haven't been tampered with and verifies the sender's identity. This makes AH crucial for scenarios where data integrity and sender authentication are paramount, but encryption isn't necessary or is handled by other means.

Question 93

C) Secret (Correct Answer)

Explanation: The classification level "Secret" is not typically found in commercial data classification schemes. This term is more commonly associated with government and military classification systems. Commercial organizations usually use a simpler classification scheme that includes levels like Public, Internal Use Only, Confidential, and Restricted. The absence of "Secret" in commercial schemes reflects the different nature of information handled by businesses compared to government agencies. Commercial entities focus more on protecting trade secrets and sensitive business information, while government classifications often deal with national security concerns. This distinction highlights the importance of tailoring classification schemes to the specific needs and risk profiles of different types of organizations.

Question 94

A) Non-Functional Testing (Correct Answer)

Explanation: Non-Functional Testing focuses on the aspects of a software system that are not related to specific behaviors or functions, but rather to its operational qualities. This type of testing evaluates performance, reliability, scalability, usability, security, and other attributes that affect the system's overall quality and user experience. Unlike functional testing, which verifies that the system does what it's supposed to do, non-functional testing ensures that it does it well under various conditions. This includes stress testing to check system behavior under heavy loads, security testing to identify vulnerabilities, and usability testing to assess user-friendliness. Non-functional testing is crucial for ensuring that a system not only works correctly but also meets the necessary quality standards and user expectations.

Question 95

D) Enterprise Extended Mode (Correct Answer)

Explanation: Enterprise Extended Mode refers to the use of multiple wireless access points to support a single network over a larger area. This approach, also known as enterprise Wi-Fi or wireless LAN (WLAN), allows for seamless connectivity across a wide area, such as an office building or campus. In this setup, multiple access points are strategically placed to provide continuous coverage, with users able to move between access points without losing connection (a process called roaming). Enterprise Extended Mode typically involves centralized management of access points, unified security policies, and features like load balancing to optimize network performance. This configuration is essential for large organizations requiring robust, scalable wireless networks that can support a high number of users across extensive areas.

Question 96

C) Programmable Logic Controller (PLC) (Correct Answer)

Explanation: A Programmable Logic Controller (PLC) is a single-purpose digital computer used for managing industrial electromechanical operations. PLCs are ruggedized computer systems designed for controlling manufacturing processes, such as assembly lines, robotic devices, or any activity that requires high-reliability control and ease of programming. They are characterized by their ability to operate in harsh industrial environments, their modular design allowing for easy expansion, and their programming using ladder logic or other specialized languages. PLCs continuously monitor inputs, make decisions based on a custom program, and control outputs to automate a process or machine. Their reliability, flexibility, and ability to withstand industrial conditions make them crucial components in modern industrial control systems.

Question 97

B) Full device encryption and mandatory passcodes (Correct Answer)

Explanation: The combination of full device encryption and mandatory passcodes provides the most assurance that data won't be lost if a mobile device is stolen. Full device encryption ensures that all data stored on the device is converted into an unreadable format, which can only be decrypted with the correct key. Mandatory passcodes add an additional layer of security by preventing unauthorized access to the device itself. Together, these measures create a two-fold protection: even if a thief bypasses the passcode, they still can't access the encrypted data without the encryption key. While GPS tracking and remote wipe are useful features, they don't prevent data access if the device is immediately accessed offline. Encryption and passcodes provide immediate, on-device protection, making them the most effective first line of defense against data loss from stolen devices.

Question 98

A) Type 1 (Correct Answer)

Explanation: Type 1 authentication factor refers to something you know. This category includes knowledge-based authentication methods such as passwords, PINs, security questions, or any other information that a user memorizes and provides to prove their identity. Type 1 factors are widely used due to their simplicity and ease of implementation. However, they are also vulnerable to various attacks like guessing, phishing, or social engineering. To enhance security, Type 1 factors are often combined with other types of authentication factors (like something you have - Type 2, or something you are - Type 3) in multi-factor authentication systems. Understanding the strengths and weaknesses of Type 1 factors is crucial for

designing effective authentication systems in information security.

Question 99

A) IoT (Correct Answer)

Explanation: Based on the image of a network-connected web camera, the type of devices likely composing the botnet are Internet of Things (IoT) devices. IoT refers to everyday objects with computing devices embedded in them, allowing them to send and receive data over the internet. Web cameras, smart home devices, and other connected gadgets fall into this category. IoT devices are often targeted for botnets due to their widespread use, frequent lack of robust security measures, and constant internet connectivity. Attackers can exploit vulnerabilities in these devices to incorporate them into a botnet, using their combined processing power and network access for various malicious activities like DDoS attacks or spam distribution. This scenario highlights the growing security concerns surrounding IoT devices and the need for improved security practices in their design and deployment.

Question 100

B) A Type 1 error (Correct Answer)

Explanation: A Type 1 error, also known as a false rejection or false negative, occurs when a valid subject using biometric authentication is not authenticated. In the context of biometric systems, this means the system incorrectly rejects an authorized user, failing to recognize them as legitimate. Type 1 errors are significant because they can lead to frustration for legitimate users and potentially deny access to authorized individuals. The rate at which these errors occur is often measured by the False Rejection Rate (FRR). Balancing Type 1 errors against Type 2 errors (false acceptances) is a key challenge in biometric system design, as reducing one type of error often increases the other.

Understanding and managing Type 1 errors is crucial for implementing effective and user-friendly biometric authentication systems.

Question 101:

D) CIA Triad (Correct Answer)

Explanation: The CIA Triad is a fundamental concept in Information Systems Security that consists of three essential principles: Confidentiality, Integrity, and Availability. Confidentiality ensures that information is kept secret from unauthorized access. Integrity guarantees that data remains accurate and unaltered throughout its lifecycle. Availability ensures that authorized users can access information when needed. These principles form the cornerstone of information security and are crucial for protecting sensitive data and maintaining system reliability.

Question 102:

B) Granular Object Control (Correct Answer)

Explanation: Granular Object Control refers to the ability to set highly specific and detailed security settings for individual objects within an information system. This level of control allows administrators to fine-tune access permissions, encryption settings, and other security parameters for each object separately. Granular control enhances security by enabling precise management of resources, minimizing the risk of unauthorized access, and ensuring that each object is protected according to its specific security requirements.

Question 103:

B) Document (Correct Answer)

Explanation: In the subject/object model of access control, the subject is the entity requesting access (in this case, Harry), while the object is the resource being accessed (the document). The file server is the system hosting the

resource, and Sally is the owner of the document. The object of the resource request is always the item being accessed, which in this scenario is the document owned by Sally.

Question 104:

A) Pairing (Correct Answer)

Explanation: In Bluetooth technology, "pairing" is the process of establishing a secure connection between two Bluetooth-enabled devices. This process involves the exchange of security keys and the creation of a shared secret that allows the devices to communicate securely. Pairing is essential for ensuring that only authorized devices can connect and share data, thus maintaining the security and privacy of Bluetooth communications.

Question 105:

A) Denial-of-Service (Correct Answer)

Explanation: A Denial-of-Service (DoS) attack is specifically designed to overwhelm a system's resources, preventing it from responding to legitimate service requests. This is typically achieved by flooding the target with an excessive amount of traffic or exploiting vulnerabilities that cause the system to crash or become unresponsive. DoS attacks aim to disrupt normal operations and make services unavailable to intended users, potentially causing significant damage to an organization's operations and reputation.

Question 106:

C) Teardrop Attack (Correct Answer)

Explanation: A Teardrop attack is a specific type of Denial-of-Service (DoS) attack that exploits vulnerabilities in how some operating systems handle fragmented IP packets. The attack sends malformed IP fragments with overlapping, oversized payloads to the target machine. When the victim's operating system attempts to reassemble these fragments,

it can crash, hang, or reboot due to the buffer overflow caused by the malformed packets. This attack is called "Teardrop" because of the "tear" in the packet sequence.

Question 107:

D) System Testing (Correct Answer)

Explanation: System Testing is a comprehensive testing approach that validates the entire software system against specified requirements. It checks both functional and non-functional aspects of the system, ensuring that all components work together as intended. System Testing is typically performed after Integration Testing and before User Acceptance Testing. It can be conducted manually or through automated tools, and it aims to identify any defects in the system's behavior, performance, and compliance with requirements before the software is released to end-users.

Question 108:

A) The employee must comply with the information in this document. (Correct Answer)

Explanation: This statement is incorrect because guidelines, by definition, are not mandatory. While the "Forensic Response Guidelines" document likely contains important information and best practices for handling forensic examinations, it serves as a guide rather than a set of binding rules. Employees are generally encouraged to follow guidelines, but compliance is not strictly required. The other statements are likely true: the document contains information about forensic examinations, should be read thoroughly, and is probably based on industry best practices.

Question 109:

D) Advance and protect the profession. (Correct Answer)

Explanation: By sharing actual exam questions, the individual is directly violating the confidentiality agreement

they agreed to when taking the CISSP exam. This action undermines the integrity of the certification process and potentially gives unfair advantages to future exam takers. Such behavior does not advance or protect the profession; instead, it devalues the certification and potentially compromises its reliability. While this action could be seen as dishonest (option C), the most direct violation is to the principle of advancing and protecting the profession, as it directly impacts the credibility and value of the CISSP certification.

Question 110:

A) PHI (Correct Answer)

Explanation: According to the Health Insurance Portability and Accountability Act (HIPAA), data related to past, present, or future payment for an individual's health care provision is classified as Protected Health Information (PHI). PHI includes any individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage. This classification ensures that such sensitive information is subject to strict privacy and security regulations under HIPAA.

Question 111:

C) A public IP address (Correct Answer)

Explanation: The IP address 201.19.7.45 is a public IP address. Public IP addresses are globally unique and routable on the public internet. They are assigned by Internet Service Providers (ISPs) or regional internet registries. The range 201.0.0.0 to 201.255.255.255 is not reserved for private use (unlike RFC 1918 addresses), not used for loopback (like 127.0.0.1), and not in the Automatic Private IP Addressing (APIPA) range (169.254.0.0 to

169.254.255.255). Therefore, this address is publicly routable on the internet.

Question 112:

A) Face Scan (Correct Answer)

Explanation: A face scan is a biometric factor that uses a physiological characteristic unique to an individual. It analyzes the physical structure of a person's face, including features like the distance between eyes, nose shape, jaw line, and other facial landmarks. This is a physiological biometric as it's based on physical characteristics of the body. In contrast, signature recognition, voice pattern recognition, and typing recognition are behavioral biometrics, as they are based on how a person performs an action rather than their physical traits.

Question 113:

B) Hash Total (Correct Answer)

Explanation: A Hash Total is a type of checksum used to verify the integrity of data transmission in Information Systems Security. It's a mathematical calculation derived from the data being transmitted, which is sent along with the data. The recipient can then perform the same calculation on the received data and compare it to the transmitted hash total. If they match, it indicates that the data has not been altered during transmission. Hash totals are crucial for detecting accidental changes or intentional tampering with data during transfer.

Question 114:

C) Baseline (Correct Answer)

Explanation: In Information Systems Security, a baseline refers to the minimum security level that all systems within an organization must meet. It establishes a standard set of security controls, configurations, and practices that serve as a starting point for securing systems. Baselines help ensure

consistency across an organization's IT infrastructure and provide a reference point for measuring and improving security. They are typically based on industry standards, best practices, and organizational requirements, and are essential for maintaining a uniform level of security across diverse systems and networks.

Question 115:

A) Lessons learned (Correct Answer)

Explanation: The "Lessons Learned" phase is a critical part of the incident response process where the team reviews the incident, analyzes the response, and identifies areas for improvement. During this phase, administrators design new security controls to prevent a recurrence of the incident. This involves evaluating the effectiveness of existing controls, identifying gaps in security measures, and developing strategies to address vulnerabilities exposed by the incident. The lessons learned are then used to update security policies, procedures, and technical controls, enhancing the organization's overall security posture and incident response capabilities.

Question 116:

C) Abstraction (Correct Answer)

Explanation: Abstraction in Information Systems Security refers to the process of grouping similar elements into classes or roles for assigning security controls, restrictions, or permissions collectively. This concept is fundamental in access control models, particularly in Role-Based Access Control (RBAC). By abstracting individual users into roles or groups, administrators can more efficiently manage security policies, reducing complexity and the likelihood of errors. Abstraction allows for scalable and consistent application of security measures across large numbers of users or resources with similar security requirements.

Question 117:

D) Spiral (Correct Answer)

Explanation: The Spiral model is a software development lifecycle characterized by a series of iterative cycles, each consisting of four main phases: Planning, Risk Analysis, Engineering, and Evaluation. What distinguishes the Spiral model is its emphasis on risk assessment and its flexibility to return to previous steps when necessary. Each cycle begins with identifying objectives and constraints, followed by evaluating alternatives and identifying/resolving risks. The development and testing phases come next, followed by planning the next iteration. This model is particularly useful for large, complex projects where risk management is crucial.

Question 118:

D) Spear Phishing Attacks (Correct Answer)

Explanation: Spear Phishing Attacks are a sophisticated form of phishing that targets specific individuals or organizations. Unlike general phishing attempts, spear phishing emails are highly personalized and appear to come from a trusted source known to the recipient. The attackers often conduct extensive research on their targets to make the emails more convincing. The goal is to trick the recipient into revealing sensitive information, such as login credentials, or to influence them to take actions that compromise security, like clicking on malicious links or downloading infected attachments. These attacks are particularly dangerous due to their targeted nature and the high level of social engineering involved.

Question 119:

C) The Transport layer (Correct Answer)

Explanation: In the OSI (Open Systems Interconnection) model, the transition from a datastream to a segment or

datagram occurs at the Transport layer (Layer 4). The Transport layer is responsible for end-to-end communication between hosts, including segmentation of data from the upper layers. It breaks down the datastream received from the Application layer (Layer 7) into smaller units called segments (for TCP) or datagrams (for UDP). This segmentation allows for efficient transmission and flow control. The Transport layer also adds headers to these segments/datagrams, which include information like source and destination port numbers, used for multiplexing and demultiplexing data to and from application-layer processes.

Question 120:

C) It helps decrease the likelihood users will write down their passwords. (Correct Answer)

Explanation: Single Sign-On (SSO) enhances security in an organization primarily by reducing the number of passwords users need to remember. When users only need to remember one set of credentials to access multiple systems, they are less likely to resort to insecure practices like writing down passwords or using simple, easily guessable passwords across multiple accounts. This reduction in password fatigue leads to better password hygiene and reduces the risk of password-related security breaches. Additionally, SSO can centralize authentication, making it easier to implement strong password policies and multi-factor authentication across all connected systems.

Question 121:

C) Out-of-band identity proofing (Correct Answer)

Explanation: When Google sends a text message with a code to a user's cell phone during a login attempt, this is an example of out-of-band identity proofing. Out-of-band authentication uses a separate communication channel (in this case, SMS) to verify the user's identity, rather than relying solely on the channel being used for the primary

interaction (the web browser). This method adds an extra layer of security by requiring access to a physical device (the cell phone) in addition to the password, making it significantly more difficult for an unauthorized person to gain access to the account, even if they have obtained the password.

Question 122:

A) Failover (Correct Answer)

Explanation: Failover is the process of automatically transferring workload or traffic to a backup system when the primary system fails. This is a critical component of high-availability systems and disaster recovery plans. In a failover scenario, the backup system (which is typically a mirror of the primary system) takes over the operations with minimal or no disruption to users. Failover systems are designed to ensure business continuity by maintaining service availability even in the event of hardware failure, network issues, or other problems that could otherwise cause downtime. This approach is commonly used in mission-critical applications where even short periods of unavailability can have significant consequences.

Question 123:

B) Open System Authentication (OSA) (Correct Answer)

Explanation: Open System Authentication (OSA) is a connection scheme in wireless networks that allows communications as long as a radio signal can be transmitted between the client and the Wireless Access Point (WAP), without requiring real authentication. In OSA, any device can connect to the wireless network without providing credentials. While this makes the network easily accessible, it also poses significant security risks as it doesn't provide any form of access control or encryption by default. OSA is often used in public hotspots or for initial connection before implementing more secure authentication

methods. It's important to note that while OSA allows initial connection, it doesn't provide any security for the data transmitted over the network.

Question 124:

B) Waterfall (Correct Answer)

Explanation: For a mission-critical application with a direct impact on human safety, where time and cost are less important than correctly functioning software, the Waterfall methodology is most appropriate. The Waterfall model is a linear sequential approach to software development that emphasizes thorough planning, documentation, and testing at each phase before moving to the next. This rigorous, step-by-step approach is well-suited for projects where requirements are well-understood and unlikely to change, and where the highest level of reliability and safety is required. Each phase (requirements, design, implementation, verification, and maintenance) is completed and perfected before the next begins, allowing for extensive review and testing. This methodical approach, while potentially slower and less flexible than other methodologies, ensures that all requirements are met and thoroughly tested, which is crucial for applications where human safety is at stake.

Question 125:

D) Accountability (Correct Answer)

Explanation: The CIA Triad consists of three essential security principles: Confidentiality, Integrity, and Availability. Accountability, while an important concept in information security, is not part of the CIA Triad. Confidentiality ensures that data is kept secret and only accessible to authorized parties. Integrity guarantees that data remains accurate and unaltered throughout its lifecycle. Availability ensures that information is accessible to authorized users when needed. Accountability, which refers to the ability to trace actions

and changes to specific users, is often considered a separate principle that supports the CIA Triad but is not one of its core components.

Question 126:

C) Closed-Circuit Television (CCTV) (Correct Answer)

Explanation: Closed-Circuit Television (CCTV) is a security system that uses video cameras to transmit a signal to a specific place on a limited set of monitors. It's widely used for surveillance in areas that need monitoring, such as banks, casinos, airports, military installations, and stores. CCTV systems can record footage continuously, be motion-activated, or use other triggers. Unlike broadcast television, CCTV signals are not openly transmitted, which is why it's called "closed-circuit."

Question 127:

D) Baseband (Correct Answer)

Explanation: Baseband is a type of communication medium that can only support one signal at a time. It uses the entire bandwidth of the cable to transmit a single signal. This is in contrast to broadband, which can carry multiple signals simultaneously. Baseband is typically used in Ethernet networks and requires less complex hardware, but it's limited in its capacity to carry multiple signals concurrently.

Question 128:

D) Encrypt (Correct Answer)

Explanation: Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data) using an algorithm and a key. This process is fundamental to information security, ensuring confidentiality by making the data unreadable to unauthorized parties. Decryption is the reverse process, while hashing is a one-way process, and salting is used to add randomness to hashed passwords.

Question 129:

A) One-Time Password (OTP) (Correct Answer)

Explanation: A One-Time Password (OTP) is a dynamic password that changes with each use. It's typically valid for only one login session or transaction. OTPs are more secure than static passwords because they're not vulnerable to replay attacks. They can be generated by hardware tokens, mobile apps, or sent via SMS. OTPs are often used as a second factor in multi-factor authentication systems.

Question 130:

A) Deterrence (Correct Answer)

Explanation: In the sequence of physical security controls, deterrence is typically addressed first. The goal of deterrence is to discourage potential intruders from attempting to breach security in the first place. This can include visible security measures like warning signs, security cameras, or guards. After deterrence, the sequence usually follows: delay (slowing down an intruder), detection (identifying a breach), and finally denial (preventing access to assets).

Question 131:

A) Implement a SIEM (Correct Answer)

Explanation: A Security Information and Event Management (SIEM) system is the most comprehensive solution for addressing log management challenges outlined in NIST SP 800-92. SIEM tools collect, analyze, and correlate log data from various sources across an organization's IT infrastructure. They provide real-time analysis of security alerts, automate log analysis, and offer advanced reporting capabilities. This holistic approach helps organizations effectively manage large volumes of log data, detect security incidents, and comply with regulatory requirements.

Question 132:

D) Username (Correct Answer)

Explanation: A username is an identification tool commonly used in computer systems, but it's not suitable as an authenticator. Usernames are typically public or easily guessable, and their primary purpose is to identify a user, not to prove their identity. Authentication requires something the user knows (like a password), has (like a token), or is (like a biometric). Usernames fall into the category of identification, which is separate from authentication in the AAA (Authentication, Authorization, and Accounting) model.

Question 133:

A) Content-Aware Authentication (Correct Answer)

Explanation: Content-Aware Authentication, also known as Context-Aware Authentication, is an advanced method that considers various contextual factors when authenticating a user. These factors can include user location, time of day, device type, IP address, and behavioral patterns. This approach is particularly useful in mobile device management systems as it can adapt security measures based on the current context, providing a balance between security and user convenience. It allows for more flexible and intelligent access control decisions.

Question 134:

D) SPNEGO-based SSO (Correct Answer)

Explanation: SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) is used in Single Sign-On (SSO) systems when the client and server are unsure of each other's supported authentication types. It allows for negotiation of an authentication mechanism between the client and server. SPNEGO can work with various authentication protocols like Kerberos or NTLM, making it

versatile in heterogeneous environments. This flexibility is particularly useful in enterprise settings where different systems may support different authentication methods.

Question 135:

D) Physical (Correct Answer)

Explanation: In the OSI (Open Systems Interconnection) model, the Physical layer (Layer 1) is responsible for transmitting raw bitstream over the physical medium. This layer defines the electrical and physical specifications for devices, focusing on the physical interface between devices and the transmission medium. It deals with characteristics such as voltage levels, data rates, maximum transmission distances, and physical connectors. The Physical layer ensures that raw bits can be sent over a physical medium, whether it's a copper wire, optical fiber, or wireless signal.

Question 136:

B) RAID 0 (Correct Answer)

Explanation: RAID 0, also known as disk striping, is a RAID (Redundant Array of Independent Disks) configuration that focuses on performance improvement rather than data redundancy. In RAID 0, data is split evenly across two or more disks, allowing for parallel read/write operations, which significantly improves performance. However, it offers no fault tolerance; if one drive fails, all data is lost. RAID 0 is often used in applications where high performance is crucial and data loss is not critical, such as in temporary data storage or video editing workstations.

Question 137:

C) ICMP echo request (Correct Answer)

Explanation: In a Ping Flood Attack, the attacker overwhelms the target system with ICMP echo request packets (pings). These packets are typically associated with the standard "ping" utility used to test network connectivity. In a flood

attack, the target is inundated with these requests faster than it can process them, potentially leading to a denial of service. The ICMP echo request is the outbound packet in a normal ping operation, with the target responding with an ICMP echo reply. In an attack scenario, the volume of requests is the key factor, not the replies.

Question 138:

C) Virtual Private Network (VPN) (Correct Answer)

Explanation: A Virtual Private Network (VPN) is a technology that creates a secure, encrypted connection over a less secure network, typically the public internet. VPNs provide confidentiality by encrypting data in transit, ensuring that even if intercepted, the data remains unreadable. They also maintain data integrity through encryption and authentication mechanisms. VPNs are widely used for secure remote access to corporate networks, protecting sensitive data when using public Wi-Fi, and bypassing geographical restrictions. They work by creating a "tunnel" between two points, encapsulating and encrypting data packets.

Question 139:

D) Access Control (Correct Answer)

Explanation: Access Control is the overarching category that encompasses preventative, detective, corrective, recovery, deterrent, and compensation controls. These are all types of security controls aimed at managing access to resources and protecting assets. Preventative controls stop unwanted events, detective controls identify when a breach occurs, corrective controls mitigate the impact of an incident, recovery controls restore systems to normal, deterrent controls discourage potential threats, and compensation controls provide alternatives when primary controls are unavailable. Together, these form a comprehensive access control strategy.

Question 140:

B) Federation (Correct Answer)

Explanation: Federation should be investigated when needing to share identity information with a business partner in an identity management implementation. Federation allows for the sharing of identity attributes across otherwise autonomous security domains. It enables single sign-on and access control between organizations without the need to replicate user accounts. In a federated system, each organization maintains control over its own user identities, but can securely share authentication and authorization information. This approach is particularly useful for B2B scenarios, cloud services, and large, distributed organizations.

Question 141:

C) RPO (Correct Answer)

Explanation: RPO (Recovery Point Objective) is the metric that determines the acceptable amount of data loss following an outage in a disaster recovery plan. It represents the maximum tolerable period during which data might be lost due to a major incident. RPO is essentially answering the question, "To what point in time do we need to recover data?" For example, an RPO of 1 hour means the system should be restored to a state no older than 1 hour before the disaster. RPO helps organizations determine the frequency of data backups and the technologies needed to meet these objectives.

Question 142:

A) Warm site (Correct Answer)

Explanation: A warm site is a type of alternate processing site that has the necessary hardware and infrastructure for restoring operations but lacks current data copies. It's a middle ground between a hot site (fully equipped and ready

to take over operations immediately) and a cold site (basic infrastructure only). A warm site typically includes servers, network equipment, and possibly some software installations, but requires data to be restored and some configuration before it can take over operations. This balance makes warm sites a cost-effective option for many organizations, providing faster recovery than a cold site without the high costs of maintaining a hot site.

Question 143:

C) RSA (Correct Answer)

Explanation: RSA (Rivest-Shamir-Adleman) would be the most efficient encryption algorithm for key management in a large organization with 10,000 employees. RSA is an asymmetric encryption algorithm, which means it uses a pair of keys: a public key for encryption and a private key for decryption. In a large organization, asymmetric encryption is more manageable because each user only needs to securely store their own private key, while public keys can be freely distributed. With symmetric algorithms like 3DES, IDEA, or Skipjack, each pair of users would need a unique shared key, resulting in millions of keys to manage for 10,000 employees. RSA simplifies this by requiring only 10,000 key pairs.

Question 144:

B) Attenuation (Correct Answer)

Explanation: Attenuation refers to the decrease in signal strength and integrity in a cable due to its length. As an electrical or optical signal travels along a cable, it naturally loses strength over distance due to factors like resistance, capacitance, and in the case of optical signals, light scattering. This weakening of the signal can lead to data errors or loss if the cable is too long. Attenuation is an important consideration in network design, particularly for long cable runs, and often necessitates the use of signal

amplifiers or repeaters to maintain signal quality over extended distances.

Question 145:

B) Registration Authority (RA) (Correct Answer)

Explanation: While the question describes a functionality that is not typically associated with a Registration Authority (RA), the closest match among the given options is RA. A Registration Authority is typically responsible for verifying the identity of entities requesting their digital certificates before a Certificate Authority (CA) issues them. It doesn't usually handle CRL distribution or certificate verification directly. These functions are more commonly associated with a Certificate Authority (CA) or sometimes a dedicated component called a Validation Authority (VA). However, in some PKI implementations, an RA might be configured to perform these read-only operations to offload work from the main CA.

Question 146:

B) Pseudo Flaw (Correct Answer)

Explanation: A Pseudo Flaw is a technique used on honeypot systems and critical resources to simulate known operating system vulnerabilities. This approach involves creating the appearance of a vulnerability without actually exposing the system to real risk. The purpose is to attract and detect potential attackers, allowing security teams to study their methods and motivations. By presenting what appears to be an exploitable flaw, organizations can lure attackers away from genuine vulnerabilities while gathering intelligence on attack techniques. This deception technique is a key component of many honeypot strategies, providing valuable insights for improving overall security posture.

Question 147:

A) Fail-Closed (Correct Answer)

Explanation: Fail-Closed describes a system's response to failure that results in a default "deny" posture. In a fail-closed system, when a failure occurs, the system automatically restricts access or shuts down to prevent potential security breaches. This approach prioritizes security over availability. It's commonly used in high-security environments where preventing unauthorized access is more critical than maintaining continuous operation. For example, an electronic door lock might default to a locked state if it loses power, ensuring that security is maintained even during system failures. While fail-closed systems offer strong security, they can impact business continuity, so their implementation requires careful consideration of the balance between security and operational needs.

Question 148:

C) Business logic errors (Correct Answer)

Explanation: After conducting automated functional testing with 100% coverage, business logic errors are most likely to persist. Automated functional testing primarily focuses on verifying that individual functions of the software work as expected based on defined inputs and outputs. However, it may not capture errors in the overall business logic or workflow of the application. Business logic errors relate to incorrect implementation of business rules or processes, which often require human understanding of the intended functionality. These errors can include issues like incorrect calculations, improper handling of edge cases, or misinterpretation of business requirements. Automated tests might not detect these unless specifically programmed to do so, making manual testing and code reviews crucial for identifying such errors.

Question 149:

C) Recipient's public key (Correct Answer)

Explanation: In an asymmetric cryptosystem, to encrypt a private message when communicating with another party, you should use the recipient's public key. Asymmetric encryption, also known as public-key cryptography, uses a pair of keys for each party: a public key that can be freely distributed, and a private key that is kept secret. To send an encrypted message, the sender uses the recipient's public key to encrypt the data. Only the recipient, who possesses the corresponding private key, can decrypt and read the message. This system ensures confidentiality and is the foundation of secure communication in many protocols, including SSL/TLS for secure web browsing and PGP for email encryption.

Question 150:

C) Machine Language (Correct Answer)

Explanation: Machine Language is the only programming language that can be directly executed by a computer without further translation. It consists of binary code - sequences of 1s and 0s - that directly correspond to specific processor instructions. Each type of CPU has its own machine language, which it can execute directly. All other programming languages, including Assembly, high-level languages, and scripting languages, require some form of translation or interpretation before the computer can execute them. Assembly language, while very close to machine code, still requires an assembler to convert it into machine language. Machine language is the lowest-level programming language and represents the actual operations performed by the computer's processor.

Practice Tests 2

Question 1

In the context of network security, what is the term for software that monitors user actions and transmits important details to a remote system for surveillance purposes?

A) Pharming

B) Spoofing

C) Spyware

D) Spear Phishing

Question 2

Which of the following is not a valid key length for the Advanced Encryption Standard?

A) 384 bits

B) 256 bits

C) 192 bits

D) 128 bits

Question 3

What type of access control system allows the owner to determine who can access the objects they possess?

A) Role-Based Access Control

B) Discretionary Access Control

C) Task-Based Access Control

D) Rule-Based Access Control

Question 4

In the OSI model, which layer is primarily responsible for preparing data for use by the application layer?

A) Human-Computer Interaction

B) Circuit Level Gateway Firewall

C) Presentation

D) Transport

Question 5

What is the term for a storage scenario where database backups are transferred to a remote location in bulk?

A) Electronic Vaulting

B) Hot Storage

C) Cold Storage

D) Data Archiving

Question 6

Which protocol should be monitored when capturing traffic from a TACACS+ server, and what data can be expected to be readable?

A) TCP; none - TACACS+ encrypts the full session

B) UDP; all but the username and password, which are encrypted

C) UDP; none – TACACS+ encrypts the full session

D) TCP; all but the username and password, which are encrypted

Question 7

What is the highest classification level in the military classification scheme?

A) Confidential

B) Secret

C) SBU

D) Top Secret

Question 8

Which of the following is a biometric identification method that uses a mathematical pattern-recognition technique on a video image of part of the eye?

A) Iris Recognition

B) Retinal Scanning

C) Iris Scanning

D) Eye Recognition

Question 9

What is Microsoft's standard for using components within a process or between processes running on the same system?

A) Component Object Model (COM)

B) Microsoft Interface Definition Language (MIDL)

C) Microsoft Transaction Server (MTS)

D) OLE Automation

Question 10

Which cipher applies the encryption algorithm to an entire message block simultaneously?

A) Block Cipher

B) Transformation Cipher

C) Transmutation Cipher

D) Array Cipher

Question 11

What type of authenticator is a "something that you have" factor that typically includes a microprocessor and one or more certificates?

A) Type III Authenticator

B) Type I Validator

C) A Token

D) A Smart Card

Question 12

In which situation does an individual not have a reasonable expectation of privacy?

A) Sending a letter through the US Mail

B) Placing a telephone call on your cell phone

C) Sending an email at work

D) Retrieving your personal voicemail

Question 13

What algorithm is useful for key exchange when two parties need to communicate but have no physical means to exchange key material and no public key infrastructure?

A) Asymmetric

B) Blockchain

C) Symmetric

D) Diffie-Hellman

Question 14

What role in an organization typically involves maintaining system security plans and ensuring system users and support staff receive necessary security training?

A) Data owner

B) Custodian

C) User

D) System owner

Question 15

When preparing for a trial related to a contract dispute where a vendor claims a verbal agreement amended a written contract, what rule of evidence should be raised in defense?

A) Best Evidence Rule

B) Real Evidence Rule

C) Parol Evidence Rule

D) Testimonial Evidence Rule

Question 16

What is the XML-based convention for communicating authentication and authorization details between security domains over web protocols?

A) SPNEGO

B) Kerberos

C) NTLM

D) SAML

Question 17

What digital end-to-end communications mechanism was developed by telephone companies to support digital communications over voice infrastructure?

A) Wide Area Network (WAN)

B) Integrated Services Digital Network (ISDN)

C) Local Area Network (LAN)

D) Twisted-Pair COAX Network

Question 18

Which practices help prevent spear phishing attacks?

A) SQL injection prevention

B) Critical thinking, hovering over links, analyzing headers, and sandboxing

C) Birthday attack mitigation

D) Password complexity enforcement

Question 19

What type of memory is readable and writable, contains information the computer uses during processing, and only retains its contents when power is continuously supplied?

A) DVR

B) CDRW

C) RAM

D) ROM

Question 20

What type of network is designed for small physical areas such as an office or group of buildings, where personal computers and workstations are connected to each other?

A) LAN

B) MAN

C) CAN

D) DAN

Question 21

What U.S. law places specific demands on websites that cater to children or knowingly collect information from children?

A) Global Internet Protection Act (GIPA)

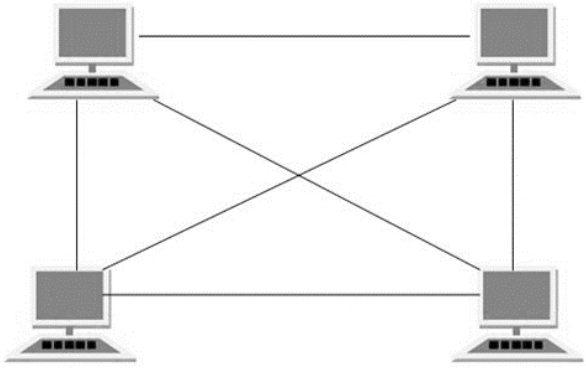
B) Online Privacy Protection Act (OPPA)

C) Children's Online Privacy Protection Act (COPPA)

D) Minor's Protection on Internet Activity (MPIA)

Question 22

What network topology is characterized by all computers being connected to a single hub through a cable?



A) Mesh

B) Ring

C) Bus

D) Star

Question 23

What is the term for an activity used to test the strength and effectiveness of deployed security measures with an authorized attempted intrusion attack?

A) Penetration Testing

B) Remote File Inclusion Detection (RFI)

C) SQL Injection Detection (SQLI)

D) Unvalidated Redirect Detection

Question 24

What process adds a header and footer to data received at each layer of the OSI model?

A) TCP wrapping

B) Attribution

C) Data hiding

D) Encapsulation

Question 25

What is a contracted minimum guaranteed bandwidth allocation for a virtual circuit called?

A) Data Flow Assurance (DFA)

B) Pledged Rate of Velocity (PRV)

C) Guaranteed Data Feed (GDF)

D) Committed Information Rate (CIR)

Question 26

Which authentication factor is something you know, such as a password, PIN, or combination lock?

A) Type 4

B) Type 3

C) Type 2

D) Type 1

Question 27

What European Union law provides a single, harmonized regulation covering data security and privacy?

A) General Data Protection Regulation (GDPR)

B) European Personal Data Protection (EPDP)

C) European Union Data Protection Regulation (EUDPR)

D) European Commission Data Protection Regulation (ECDPR)

Question 28

What type of network topology provides each system with a direct physical link to every other system in the network?

A) Star

B) Bus

C) Ring

D) Mesh

Question 29

If a company wants to ensure the integrity of email messages sent via their central email servers without prioritizing confidentiality, what solution should be suggested?

A) Digitally sign but don't encrypt all messages

B) Use TLS to protect messages, ensuring their integrity

C) Use a hashing algorithm to provide a hash in each message to prove that it hasn't changed

D) Digitally sign and encrypt all messages to ensure integrity

Question 30

What is the term for unwanted software installed in your system without your consent?

A) Man-in-the-Middle attack

B) Malware attack

C) Cross-site scripting attack

D) SQL injection attack

Question 31

What is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all of the necessary supporting elements?

A) Essential Element Analysis

B) Critical Path Analysis

C) Straight-Line Analysis

D) Kill Chain Analysis

Question 32

What form of cryptography does not use like keys and either uses complex formulas to solve problems or uses key pair sets to provide digital signatures and digital envelopes?

A) Asymmetric key

B) Symmetric key

C) Private key

D) Ciphertext

Question 33

What process ensures that data cannot be recovered by any means from destroyed or discarded media?

A) Atheization

B) Sanitization

C) Purification

D) Euthanization

Question 34

When an intruder is detected by an IDS, to what simulated environment are they transferred that has the look and layout of the actual network but prevents malicious activities?

A) Isolation Chamber

B) Prison Camp

C) Padded Cell

D) Monitoring Room

Question 35

What type of audit report should be requested to ensure input from an external auditor?

A) SOC 3, Type 2

B) SOC 3, Type 1

C) SOC 2, Type 1

D) SOC 2, Type 2

Question 36

What change management process provides an organized framework for company employees to suggest new features for development?

A) Request control

B) Configurational control

C) Release control

D) Change control

Question 37

What is an SMTP server configured to accept email messages from any source and forward them to their destination called?

A) Open Relays

B) Public Use Mail Relays (PUMR)

C) Open System Authentication (OSA)

D) Open Source Mail Services (OSMS)

Question 38

What stage of the incident response process is being conducted when an analyst performs an initial triage of a potential brute-force password attack alert?

A) Mitigation

B) Recovery

C) Detection

D) Response

Question 39

When an attacker calls an organization's helpdesk and persuades them to reset a password due to the employee's trust and willingness to help, what type of attack has succeeded?

A) Social Engineering

B) Whaling

C) A Human Trojan

D) Fishing

Question 40

Who are the people trained in responsible network security methodology with a philosophy towards non-destructive and non-intrusive testing?

A) UAT Managers

B) Ethical Hackers

C) SIT Leaders

D) Network Administrators

Question 41

What network protocol conceptual model was derived from TCP/IP and has four layers: Link, Internet, Host-to-Host, and Process?

A) TCP Model

B) XML Model

C) OSI Model

D) SDLC Model

Question 42

What is the length of time a key on the keyboard is pressed called in the context of keystroke dynamics biometric factor?

A) Transient Time

B) Rest Time

C) Flight Time

D) Dwell Time

Question 43

What is any system activity that does not normally occur on your system referred to as?

A) Substandard activity

B) Unrecognized activity

C) Questionable activity

D) Abnormal activity

Question 44

What technology is likely to be involved when an organization needs to provide authentication and authorization assertions to their e-commerce cloud partner?

A) SAML

B) Active Directory

C) SPML

D) RADIUS

Question 45

What is the Gramm-Lilly-Bliley Act (GLBA)?

A) A law that erased strict government barriers between financial institutions

B) An act regulating the use of personal data in healthcare

C) Legislation governing internet service providers

D) A regulation for cybersecurity in government agencies

Question 46

What type of attack involves recording traffic between a client and server, then playing back or retransmitting the packets with slight variations?

A) Malware Attack

B) Replay Attack

C) Drive-by Attack

D) Broadcast Attack

Question 47

What is the Component Object Model (COM) used for?

A) Database management

B) Network security

C) Use of components within or between processes on the same system

D) Web application development

Question 48

What is the purpose of the presentation layer in the OSI model?

A) Establish network connections

B) Route data between networks

C) Prepare data for use by the application layer

D) Manage physical transmission of data

Question 49

What is electronic vaulting in the context of data storage?

A) A method of encrypting data at rest

B) A process of transferring database backups to a remote site in bulk

C) A technique for compressing large data files

D) A system for real-time data replication

Question 50

What is the primary function of the Children's Online Privacy Protection Act (COPPA)?

A) Regulate adult content on the internet

B) Protect children's personal information collected online

C) Establish guidelines for educational websites

D) Monitor internet usage in schools

Question 51: In the context of Information Systems Security, what term describes a deceptive technique that attempts to manipulate users into divulging sensitive information, often through email?

A) Phreaking

B) VVishing

C) Pharming

D) Phishing

Question 52: Which protocol provides real-time certificate status verification, replacing certificate revocation lists?

A) RTVP

B) RTCP

C) OCSP

D) CSTP

Question 53: What are the three primary types of interfaces typically evaluated during software testing procedures?

A) Network interfaces, APIs, and UIs

B) Network, physical, and application interfaces

C) Application, programmatic, and user interfaces

D) APIs, UIs, and physical interfaces

Question 54: What term describes a cyber attack that exploits vulnerabilities unknown to the software vendor or recently discovered?

A) Zero-Day Exploit

B) Trojan Exploit

C) Bot Exploit

D) Worm Exploit

Question 55: In information security, what collective term encompasses files, databases, computers, programs, processes, devices, and media?

A) Objects

B) Users

C) Subjects

D) File sources

Question 56: When a process requires access to a file currently in use, what state does the process scheduler assign to it?

A) Waiting

B) Stopped

C) Ready

D) Running

Question 57: Which access control method is implemented to detect unauthorized or unwanted activities, including the use of security personnel and intrusion detection systems?

A) Mandatory Access Control

B) Discretionary Access Control

C) Role-Based Access Control

D) Detective Access Control

Question 58: What term describes a cyber attack involving the transmission of excessive traffic to overwhelm a target system?

A) Flooding

B) Swamping

C) Bursting

D) Inundation

Question 59: What type of access control system utilizes information such as user identity, department, working hours, job category, and location to make authorization decisions?

A) Role-Based access control

B) Attribute-Based access control

C) Administrative Access control

D) System Discretionary Access Control

Question 60: What component of an operating system remains constantly present in memory to facilitate immediate execution when needed?

A) SWAP

B) RAM

C) ROM

D) Kernel

Question 61: Which 1996 legislation introduced significant changes to health insurance regulations and mandated strict privacy measures for medical information?

A) Health Insurance Portability and Accountability Act (HIPAA)

B) Rights and Protections for Participants and Healthcare Beneficiaries Act (RPPHB)

C) Health Insurance Privacy Rule (HIPR)

D) Health Information Technology for Economic and Clinical Health Act (HITECH)

Question 62: What is the minimum number of disk drives required to implement RAID level 0?

A) 1

B) 2

C) 3

D) 5

Question 63: Which testing approach validates the entire software system, including interconnected subsystems, and examines the complete process flow?

A) Functional Testing

B) System Testing

C) Start-To-End Testing

D) End-To-End Testing

Question 64: What term best describes characteristics such as fingerprints, iris scans, signature dynamics, voice patterns, and keystroke patterns when used for identification or authentication?

A) Physiological Characteristics

B) Biometric Factors

C) Possession Authenticators

D) Behavioural Tendencies

Question 65: When Aldebron requests a SOC 2 report and receives a SAS70 report instead, what concern should they raise?

A) SAS 70 only uses a three month period for testing

B) SAS 70 has been replaced

C) SAS 70 is a financial reporting standard and does not cover data centres

D) SAS 70 does not include Type 2 reports, so control evaluation is only point in time

Question 66: In asymmetric encryption, what key should Richard use to decrypt a message received from Sanil?

A) Richard's public key

B) Sanil's public key

C) Sanil's private key

D) Richard's private key

Question 67: What project management tool is used to estimate software size and calculate standard deviation for risk assessment?

A) Bounding Distributions

B) Network Reduction

C) Monte Carlo Simulation

D) Program Evaluation Review Technique (PERT)

Question 68: What encryption method secures entire communication circuits by creating a protected tunnel between two points?

A) Link Encryption

B) IDEA Encryption

C) Blowfish Encryption

D) RSA Encryption

Question 69: What security solution should Colin implement to reduce zero-day attacks and enforce security policies on systems before network connection?

A) An NAC system

B) An intrusion detection system

C) A firewall

D) Port security

Question 70: Which statement is not one of the four canons of the (ISC)2 code of ethics?

A) Avoid conflicts of interest that may jeopardize impartiality

B) Protect society, the common good, necessary public trust and confidence, and the infrastructure

C) Act honourably, honestly, justly, responsibly, and legally

D) Provide diligent and competent service to principles

Question 71: What term describes passwords that change regularly or with each use, rather than remaining static?

A) Random

B) Evolving

C) Dynamic

D) Altering

Question 72: Which technique can an attacker use to exploit a TOC/TOU vulnerability?

A) File locking

B) Concurrency control

C) Exception handling

D) Algorithmic complexity

Question 73: What term describes a violation or imminent threat to an organization's security policy, often resulting from attacks, malware, or inappropriate employee actions?

A) Perimeter Breach Incident

B) Computer Security Incident

C) Cross-Border Incident

D) Hostile Incursion Incident

Question 74: What type of software testing involves executing predefined test steps and comparing results, often suitable for automation?

A) Exploratory Testing

B) Start-To-End Testing

C) Scripted Testing

D) End-To-End Testing

Question 75: For a project with clearly defined requirements and emphasis on comprehensive documentation, which

software development model is most appropriate?

A) Agile

B) Spiral

C) Waterfall

D) DevOps

Question 76: What type of testing evaluates how well modules perform against interface specifications to ensure proper integration?

A) Beta Testing

B) UAT Testing

C) Interface Testing

D) Requirements Testing

Question 77: Which of the following exemplifies risk transference in information security?

A) Building a guard shack

B) Relocating facilities

C) Purchasing insurance

D) Erecting fences

Question 78: In Baxter Industries' backup scenario, how long is the period where data changes may be irretrievably lost?

A) 5 hours

B) 3 hours

C) No data will be lost

D) 8 hours

Question 79: What cryptographic analysis technique examines letter repetition in encrypted messages and compares it to language-specific letter frequency statistics?

A) Weak Password Analysis

B) Common Word Analysis

C) Frequency Analysis

D) Dictionary Analysis

Question 80: Which access control method applies labels to subjects and objects, allowing access when labels match?

A) Rule BAC

B) DAC

C) Roll BAC

D) MAC

Question 81: What term describes the method by which a processor references various memory locations?

A) Polling

B) Association

C) Addressing

D) Mem-line

Question 82: What cryptographic method encrypts messages using letter-by-letter conversion and multiple alphabets from different languages or countries?

A) Pigpen Cipher

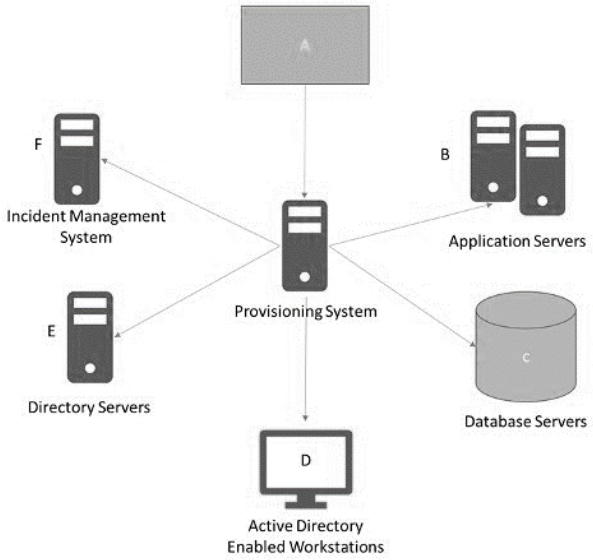
B) Monoalphabetic Substitution

C) Vigenère Cipher

D) Polyalphabetic Substitution

Question 83: Bill Hollister has been with the University he works at for over 10 years. During that time, he has been assistant administrator, database administrator, and he has worked in the university’s help desk. He is now a manager for the team that runs the university's web applications.

When Bill changes roles, what should occur?



A) Rights should be set to match those of the person they're replacing

B) New rights should be added to their existing account

C) They should be de-provisioned and a new account created

D) They should be provisioned only for rights matching the new role

Question 84: What role is Olivia likely playing in her organization if she's concerned about the conflict between profit and security requirements?

A) Data processor

B) Mission owner

C) Information security analyst

D) Business manager

Question 85: What type of code analysis uses techniques like control flow graphs and lexical analysis to assess code without execution?

A) Dynamic

B) Fuzzing

C) Manual

D) Static

Question 86: In a database table, which column type is typically the best candidate for a primary key?

Company ID	Company Name	Address	City	State/Province	Postal Code	Telephone	Sales Rep
1	Stark Industries	1 Stark Avenue	New York	New York	10001	(212) 989-2654	12
2	Daily Bugle	203 39th Street	New York	New York	10028	(312) 302-5689	18
3	Mel's Diner	140 University Avenue W	Waterloo	Ontario	N2L 6J3	(519) 579-6357	33

A) Company ID

B) Postal Code

C) Company Name

D) Sales Rep

Question 87: What term describes a momentary loss of power in a facility?

A) Brownout

B) Fault

C) Sag

D) Blackout

Question 88: Why might a company require Patsy Walker to sign an NDA when starting a new job?

A) To protect the confidentiality of their data

B) To prevent Patsy from directly competing with them in the future

C) To require Patsy to ensure the availability of their data as part of her job

D) To ensure that Patsy did not delete their data

Question 89: What category of testing includes unit testing, smoke testing, sanity testing, integration testing, white box

testing, black box testing, user acceptance testing, and regression testing?

A) Functional Testing

B) Non-Functional Testing

C) Focused Testing

D) Generic Testing

Question 90: What process generates a unique output value from a full message, commonly referred to as a message digest?

A) Private Address

B) Hash Function

C) Key Function

D) Public Address

Question 91: What term describes a section of an organization's network that functions as an intranet for the private network while also serving information to specific external parties?

A) Internet

B) LAN

C) Intranet

D) Extranet

Question 92: During which phase of the Electronic Discovery Reference Model is potentially discoverable information protected against alteration or deletion?

A) Production

B) Preservation

C) Collection

D) Identification

Question 93: In the take-grant protection model, which rule would allow Pavel Chekov to obtain read permissions on an object if James Kirk already has those rights?

A) Remote Rule

B) Take Rule

C) Grant Rule

D) Create Rule

Question 94: What regulatory framework aims to give EU citizens more control over their personal data and simplify the business environment in the European Union?

A) OPPA

B) COPPA

C) CalOPPA

D) GDPR

Question 95: What mechanism allows users to authenticate once and then access multiple resources without repeated authentication challenges?

A) JSON

B) ISO

C) XML

D) SSO

Question 96: In database terminology, what term describes a column or attribute of a table?

A) Element

B) Field

C) Range

D) Expression

Question 97: During which phase of penetration testing is application banner information typically recorded?

A) Attack

B) Discovery

C) Reporting

D) Planning

Question 98: What type of access control is typically controlled by the owner of the objects?

A) Mandatory Access Control (MAC)

B) Discretionary Access Control (DAC)

C) Role-Based Access Control (RBAC)

D) Rule-Based Access Control (RBAC)

Question 99: What term describes the process of identifying and addressing potential security vulnerabilities in software before it is released or deployed?

A) Penetration Testing

B) Vulnerability Assessment

C) Security Auditing

D) Threat Modeling

Question 100: Which cryptographic protocol is designed to provide secure communication over a computer network, commonly used for internet connections?

A) SSL

B) TLS

C) SSH

D) IPsec

Correct Answers & Explanations

Question 1

C) Spyware (Correct Answer)

Explanation: Spyware is a type of malicious software that secretly monitors and collects information about a user's activities on a computer or network without their knowledge or consent. It operates covertly, gathering sensitive data such as keystrokes, browsing habits, and personal information, which is then transmitted to a remote system for surveillance purposes. Unlike pharming (which redirects users to fake websites), spoofing (which involves impersonation), or spear phishing (a targeted email scam), spyware specifically focuses on continuous monitoring and data collection.

Question 2

A) 384 bits (Correct Answer)

Explanation: The Advanced Encryption Standard (AES) is a symmetric block cipher adopted by the U.S. government to protect classified information. AES supports three key lengths: 128 bits, 192 bits, and 256 bits. The 384-bit key length is not a valid option for AES. This standardization ensures compatibility and security across various implementations of AES. The longer the key length, the more secure the encryption, with 256-bit keys providing the highest level of security among the valid options.

Question 3

B) Discretionary Access Control (Correct Answer)

Explanation: Discretionary Access Control (DAC) is an access control model where the owner of a resource determines who can access it and what privileges they have. In DAC, the owner has full control over the access rights and can grant or revoke permissions at their discretion. This is in contrast to other access control models like Role-Based Access Control (RBAC), which assigns permissions based on predefined roles, or Mandatory Access Control (MAC), where

access is determined by system-wide policies. DAC provides flexibility but requires careful management to prevent security risks.

Question 4

C) Presentation (Correct Answer)

Explanation: In the OSI (Open Systems Interconnection) model, the Presentation layer (Layer 6) is primarily responsible for preparing data for use by the Application layer. This layer handles data formatting, encryption, compression, and translation between different data formats. It ensures that data from the application layer of one system can be read by the application layer of another system. The Presentation layer acts as a translator, converting data from a format used by the application layer into a standardized format for transmission and vice versa.

Question 5

A) Electronic Vaulting (Correct Answer)

Explanation: Electronic vaulting refers to the process of transferring database backups or other critical data to a remote location in bulk, typically over a network connection. This method is used for off-site data storage and disaster recovery purposes. Unlike hot storage (which provides immediate access to data) or cold storage (used for long-term, infrequently accessed data), electronic vaulting focuses on the regular, scheduled transfer of large amounts of backup data to a secure, off-site location. This ensures that a copy of critical data is always available at a separate location in case of a disaster at the primary site.

Question 6

A) TCP; none - TACACS+ encrypts the full session (Correct Answer)

Explanation: TACACS+ (Terminal Access Controller Access-Control System Plus) is a network protocol that provides

centralized authentication, authorization, and accounting (AAA) services. It uses TCP (Transmission Control Protocol) as its transport protocol, which ensures reliable, ordered delivery of data. TACACS+ encrypts the entire session, including the username and password, providing a high level of security. This full encryption means that when capturing traffic from a TACACS+ server, no readable data should be visible, as the entire payload is encrypted. This is in contrast to some other protocols that might only encrypt sensitive fields like passwords.

Question 7

D) Top Secret (Correct Answer)

Explanation: In the U.S. military classification scheme, Top Secret is the highest level of classification for information. The classification levels, from lowest to highest, are: Unclassified, Confidential, Secret, and Top Secret. Top Secret information is defined as information that, if disclosed unauthorized, could cause "exceptionally grave damage" to national security. This classification requires the most stringent security measures and clearance levels for access. SBU (Sensitive But Unclassified) is not part of the formal classification system but is used for information requiring protection but not rising to the level of classified information.

Question 8

A) Iris Recognition (Correct Answer)

Explanation: Iris recognition is a biometric identification method that uses mathematical pattern-recognition techniques on video images of the iris, which is the colored part of the eye surrounding the pupil. This method captures high-resolution images of the iris's intricate structures, which are unique to each individual and remain stable throughout life. Iris recognition is different from retinal scanning, which examines the pattern of blood vessels at

the back of the eye. Iris recognition is considered one of the most accurate biometric identification methods due to the complexity and uniqueness of iris patterns.

Question 9

A) Component Object Model (COM) (Correct Answer)

Explanation: The Component Object Model (COM) is Microsoft's standard for using components within a process or between processes running on the same system. It's a binary-interface standard that allows for inter-process communication and dynamic object creation in a large range of programming languages. COM is the foundation for other Microsoft technologies like OLE (Object Linking and Embedding), ActiveX, COM+, and DCOM (Distributed COM). It enables software components to communicate with each other regardless of the language they were developed in, providing a way for different software components to interact and share data efficiently within Windows environments.

Question 10

A) Block Cipher (Correct Answer)

Explanation: A block cipher is a method of encrypting text in which the algorithm operates on a fixed-length group of bits, called a block, rather than on a single bit at a time. It applies the encryption algorithm to an entire message block simultaneously. This is in contrast to stream ciphers, which encrypt data one bit or byte at a time. Block ciphers divide the plaintext into fixed-size blocks (typically 64 or 128 bits) and encrypt each block using the same key. Examples of block ciphers include AES (Advanced Encryption Standard) and DES (Data Encryption Standard). Block ciphers are widely used due to their security and efficiency in processing large amounts of data.

Question 11

D) A Smart Card (Correct Answer)

Explanation: A smart card is a "something you have" factor in multi-factor authentication. It typically includes a microprocessor and one or more certificates, making it a secure and portable device for storing sensitive information and performing cryptographic operations. Smart cards can store digital certificates, encryption keys, and other security credentials. They often require a PIN (something you know) to activate, combining two authentication factors. Smart cards are widely used in secure access systems, financial transactions, and identity verification due to their ability to securely store and process data, making them more sophisticated than simple tokens or magnetic stripe cards.

Question 12

C) Sending an email at work (Correct Answer)

Explanation: When sending an email at work, an individual typically does not have a reasonable expectation of privacy. This is because work email accounts are generally considered the property of the employer, and many organizations have policies that allow them to monitor, access, and review employee emails sent through company systems. Courts have consistently ruled that employers have the right to monitor work-related communications on company-owned devices and networks. In contrast, personal communications through private channels (like personal mail, personal cell phones, or personal voicemail) generally do have a reasonable expectation of privacy, unless explicitly stated otherwise in employment agreements or policies.

Question 13

D) Diffie-Hellman (Correct Answer)

Explanation: The Diffie-Hellman key exchange algorithm is a method for securely exchanging cryptographic keys over a

public channel. It allows two parties who have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This is particularly useful when the parties need to communicate securely but have no physical means to exchange key material and no existing public key infrastructure. The algorithm's security is based on the difficulty of the discrete logarithm problem. While it doesn't provide authentication, Diffie-Hellman is fundamental in many secure communication protocols, including HTTPS, SSH, and VPNs, often used in combination with other cryptographic techniques to ensure both confidentiality and authentication.

Question 14

D) System owner (Correct Answer)

Explanation: The system owner is typically responsible for maintaining system security plans and ensuring that system users and support staff receive necessary security training. This role is crucial in the overall information security governance of an organization. The system owner is accountable for the overall production, development, maintenance, and security of an information system. Their responsibilities include:

1. Developing and maintaining system security plans
2. Ensuring compliance with security policies and regulations
3. Coordinating security-related activities
4. Overseeing user access and privileges
5. Ensuring that system users and support staff are properly trained in security procedures

This role is distinct from data owners (who are responsible for the data itself), custodians (who manage the data), and users (who utilize the system).

Question 15

C) Parol Evidence Rule (Correct Answer)

Explanation: The Parol Evidence Rule is a legal principle that prevents a party to a written contract from presenting extrinsic evidence that contradicts or adds to the written terms of the contract that appears to be whole. This rule is particularly relevant in contract disputes where one party claims that a verbal agreement amended a written contract. The rule generally holds that once a written contract is signed, it supersedes all prior negotiations or agreements, and evidence of these prior or contemporaneous agreements cannot be admitted to alter the terms of the written contract. There are exceptions, such as cases of fraud, mistake, or ambiguity, but generally, the Parol Evidence Rule helps to ensure the integrity and finality of written agreements.

Question 16

D) SAML (Correct Answer)

Explanation: SAML (Security Assertion Markup Language) is an XML-based open standard for exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider. It is specifically designed for communicating authentication and authorization details between security domains over web protocols. SAML allows for single sign-on (SSO) across different systems and organizations, enhancing user experience and security. Key features of SAML include:

- Platform-neutral, XML-based protocol
- Supports web browser SSO and attribute exchange
- Enables federated identity management
- Provides a standardized way to assert user identity and attributes

SAML is widely used in enterprise and cloud environments to enable secure, seamless access to multiple applications with a single set of credentials.

Question 17

B) Integrated Services Digital Network (ISDN) (Correct Answer)

Explanation: Integrated Services Digital Network (ISDN) is a set of communication standards for digital transmission over ordinary telephone copper wire as well as over other media. It was developed by telephone companies to provide a digital, end-to-end network for delivering a wide range of services, including voice and non-voice services. Key aspects of ISDN include:

1. Supports digital transmission of voice, video, data, and other network services over traditional circuits
2. Provides end-to-end digital connectivity for delivering various services
3. Offers circuit-switched connections for voice and data services
4. Delivers packet-switched connections for data communications
5. Provides significantly faster data transmission compared to analog modems

While largely superseded by broadband technologies in many areas, ISDN played a crucial role in the transition from analog to digital communications and is still used in some specific applications.

Question 18

B) Critical thinking, hovering over links, analyzing headers, and sandboxing (Correct Answer)

Explanation: Preventing spear phishing attacks involves a combination of technical measures and user awareness. The

correct practices include:

- Critical thinking: Training users to be skeptical of unsolicited emails and to verify the sender's identity.
- Hovering over links: Encouraging users to check the actual URL destination before clicking on links in emails.
- Analyzing headers: Examining email headers can reveal discrepancies in the sender's information.
- Sandboxing: Using isolated environments to open suspicious attachments or links safely.

These practices are specifically tailored to combat spear phishing, which involves highly targeted and personalized attacks. Unlike SQL injection prevention or password complexity enforcement, which are important for other aspects of security, these practices directly address the human element that spear phishing exploits. By combining technical analysis (like header examination) with behavioral practices (like critical thinking), organizations can significantly reduce the risk of falling victim to these sophisticated social engineering attacks.

Question 19

C) RAM (Correct Answer)

Explanation: RAM (Random Access Memory) is the type of memory that fits the description given. Key characteristics of RAM include:

Readable and writable: Data can be both read from and written to RAM.

Volatile: RAM only retains its contents when power is continuously supplied. When the power is cut off, all data in RAM is lost.

Used for active processing: RAM contains the information that the computer is actively using during processing.

Fast access: Provides quick read and write access for the CPU.

Temporary storage: Used for short-term data storage while a computer is running.

This is in contrast to ROM (Read-Only Memory), which retains data without power but is not typically writable during normal operation, or storage devices like DVRs or CDRWs, which provide non-volatile storage but are not used for active processing by the CPU. RAM's ability to quickly store and access data makes it crucial for a computer's performance in running applications and processing tasks.

Question 20

A) LAN (Correct Answer)

Explanation: A Local Area Network (LAN) is the type of network designed for small physical areas such as an office or group of buildings. Key characteristics of a LAN include:

- Limited geographical area: Typically covers a small area like an office, home, or campus.
- High-speed connectivity: Offers faster data transfer rates compared to wide area networks.
- Shared resources: Enables sharing of resources like printers, files, and internet connections.
- Direct connections: Computers and devices are directly connected to each other.
- Private ownership: Usually owned, controlled, and managed by a single organization.

LANs are distinct from other network types like MANs (Metropolitan Area Networks), which cover larger areas like a city, or WANs (Wide Area Networks), which span even broader geographical areas. LANs provide the advantage of

high-speed, low-latency communication between devices in close proximity, making them ideal for local collaborative work environments and resource sharing within an organization.

Question 21

C) Children's Online Privacy Protection Act (COPPA) (Correct Answer)

Explanation: The Children's Online Privacy Protection Act (COPPA) is a United States federal law enacted in 1998 that specifically addresses the online privacy of children under 13 years of age. Key aspects of COPPA include:

1. Applies to websites and online services directed to children under 13 or those that knowingly collect information from children under 13.
2. Requires parental consent for the collection or use of any personal information of young website users.
3. Mandates clear privacy policies on websites collecting data from children.
4. Prohibits requiring children to provide more information than necessary to participate in activities.
5. Gives parents the ability to review their child's information, revoke consent, and request deletion of information.

COPPA aims to protect children's privacy online by giving parents control over what information is collected from their children. It places significant responsibilities on website operators to ensure compliance, including obtaining verifiable parental consent before collecting, using, or disclosing personal information from children.

Question 22

D) Star (Correct Answer)

Explanation: A star network topology is characterized by all computers being connected to a single central hub through individual cables. Key features of a star topology include:

1. Central hub: All devices connect to a central device (hub, switch, or router).
2. Point-to-point connections: Each device has its own dedicated connection to the central hub.
3. Easy to install and manage: Adding or removing devices is simple and doesn't disrupt the network.
4. Fault tolerance: If one connection fails, it doesn't affect the rest of the network.
5. Centralized management: Network management is simplified due to the centralized structure.

This is different from other topologies like:

1. Bus: All devices connect to a single cable.
2. Ring: Devices are connected in a circular chain.
3. Mesh: Devices are interconnected with multiple redundant connections.

The star topology is widely used in modern networks due to its reliability, ease of management, and scalability, especially in Ethernet networks using switches or routers as the central device.

Question 23

A) Penetration Testing (Correct Answer)

Explanation: Penetration Testing, often referred to as "pen testing," is a authorized simulated cyberattack on a computer system, network, or web application to evaluate the security of the system. Key aspects of penetration testing include:

1. Authorized attempt: Conducted with the knowledge and permission of the organization.

2. Simulates real attacks: Uses techniques and tools that actual attackers might use.
3. Identifies vulnerabilities: Uncovers weaknesses in the system's defenses.
4. Tests deployed security measures: Evaluates the effectiveness of existing security controls.
5. Provides actionable insights: Offers detailed reports on vulnerabilities and recommendations for improvement.

Penetration testing goes beyond simple vulnerability scanning by actively exploiting vulnerabilities to demonstrate the potential impact of security weaknesses. It's a proactive approach to security, allowing organizations to identify and address vulnerabilities

Question 24

D) Encapsulation (Correct Answer)

Explanation: Encapsulation is the process that adds a header and footer to data as it moves through each layer of the OSI (Open Systems Interconnection) model. This process wraps the data from higher layers with additional information needed for transmission at lower layers. As data moves down the OSI stack, each layer adds its own header (and sometimes a trailer) to the data received from the layer above. This additional information is used by the corresponding layer on the receiving end to properly handle and route the data. Encapsulation is crucial for maintaining the independence of each layer while allowing them to work together seamlessly.

Question 25

D) Committed Information Rate (CIR) (Correct Answer)

Explanation: The Committed Information Rate (CIR) is a contracted minimum guaranteed bandwidth allocation for a virtual circuit in a network. It represents the amount of

bandwidth that a service provider guarantees to deliver under normal conditions. CIR is typically used in frame relay and other packet-switched networks to ensure a minimum level of service quality. It's important in Service Level Agreements (SLAs) between network providers and customers, as it defines the baseline performance expectations for data transmission. The CIR helps in managing network congestion and ensuring that critical applications receive the necessary bandwidth.

Question 26

D) Type 1 (Correct Answer)

Explanation: In multi-factor authentication, Type 1 refers to "something you know," which includes passwords, PINs, or combination locks. This is one of the three main categories of authentication factors:

- Type 1 (Something you know): Passwords, PINs, security questions
- Type 2 (Something you have): Smart cards, tokens, mobile devices
- Type 3 (Something you are): Biometrics like fingerprints, retinal scans

Type 1 factors are widely used due to their simplicity and ease of implementation, but they can be vulnerable to various attacks if not properly managed. Combining Type 1 with other factor types strengthens overall security.

Question 27

A) General Data Protection Regulation (GDPR) (Correct Answer)

Explanation: The General Data Protection Regulation (GDPR) is a comprehensive data protection law in the European Union (EU) that came into effect in May 2018. It provides a single, harmonized regulation covering data security and

privacy across all EU member states. Key aspects of GDPR include:

1. Enhanced personal data protection rights for EU citizens
2. Strict rules for obtaining consent for data collection and processing
3. Mandatory breach notifications
4. Significant fines for non-compliance
5. Applies to any organization handling EU citizens' data, regardless of the organization's location

GDPR has had a global impact, influencing data protection laws and practices worldwide.

Question 28

D) Mesh (Correct Answer)

Explanation: A mesh network topology provides each system with a direct physical link to every other system in the network. Key characteristics of a mesh topology include:

- High redundancy: Multiple paths between nodes increase reliability
- Decentralized structure: No central point of failure
- Scalability: Easy to add new nodes without disrupting the network
- Efficient data routing: Data can take the shortest path between nodes
- Fault tolerance: Network continues to function if one or more connections fail

While a full mesh topology (where every node connects to every other node) can be complex and expensive for large networks, partial mesh topologies are often used to balance redundancy and cost.

Question 29

A) Digitally sign but don't encrypt all messages (Correct Answer)

Explanation: To ensure the integrity of email messages without prioritizing confidentiality, the best solution is to digitally sign but not encrypt all messages. Digital signatures provide:

1. Integrity: Ensures the message hasn't been altered in transit
2. Authentication: Verifies the sender's identity
3. Non-repudiation: Sender cannot deny sending the message

By not encrypting, the company allows for easier content inspection and archiving while still maintaining message integrity. This approach balances security needs with operational requirements, especially when confidentiality is not the primary concern.

Question 30

B) Malware attack (Correct Answer)

Explanation: Malware, short for malicious software, refers to any software intentionally designed to cause damage to a computer, server, client, or computer network. Characteristics of malware include:

1. Installed without user consent
2. Performs unwanted actions on the system
3. Can include viruses, trojans, worms, ransomware, spyware, etc.
4. Often disguised as legitimate software
5. Can lead to data theft, system damage, or unauthorized access

Malware is distinct from other types of attacks like Man-in-the-Middle (which intercepts communications) or SQL

injection (which targets databases), as it specifically involves unwanted software installation.

Question 31

A) Essential Element Analysis (Correct Answer)

Explanation: Essential Element Analysis is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all of the necessary supporting elements. This analysis is crucial for:

- Business continuity planning
- Disaster recovery strategies
- Risk assessment and management
- Resource allocation and prioritization
- Identifying dependencies and vulnerabilities in critical systems

By mapping out these relationships, organizations can better understand their operational vulnerabilities and develop more effective strategies for maintaining essential functions during disruptions or crises.

Question 32

A) Asymmetric key (Correct Answer)

Explanation: Asymmetric key cryptography, also known as public-key cryptography, is a form of encryption that uses two mathematically related, but not identical, keys – a public key and a private key. Key features include:

- Different keys for encryption and decryption
- Public key can be freely distributed
- Private key must be kept secret
- Used for digital signatures and secure key exchange

Typically slower than symmetric key cryptography, but more secure for key distribution

Asymmetric cryptography solves the key distribution problem inherent in symmetric key systems and is fundamental to many secure communication protocols on the internet.

Question 33

B) Sanitization (Correct Answer)

Explanation: Sanitization is the process that ensures data cannot be recovered by any means from destroyed or discarded media. This process is crucial for protecting sensitive information when disposing of or repurposing storage devices. Key aspects of sanitization include:

1. Overwriting data multiple times with random patterns
2. Degaussing (for magnetic media)
3. Physical destruction of the storage medium
4. Cryptographic erasure for certain types of storage
5. Verification to ensure complete data removal

Proper sanitization is essential for compliance with data protection regulations and preventing data breaches from discarded or repurposed hardware.

Question 34

C) Padded Cell (Correct Answer)

Explanation: A Padded Cell, in the context of network security, is a simulated environment to which an intruder is transferred when detected by an Intrusion Detection System (IDS). Characteristics of a Padded Cell include:

1. Mimics the look and layout of the actual network
2. Prevents malicious activities from affecting the real system
3. Allows for observation and analysis of the intruder's actions
4. Contains non-critical or fake data to appear genuine

5. Helps in gathering intelligence about attack methods and motivations

This approach allows security teams to study attack patterns while protecting the actual network infrastructure from harm.

Question 35

D) SOC 2, Type 2 (Correct Answer)

Explanation: A SOC 2, Type 2 report is the most comprehensive type of Service Organization Control (SOC) report and ensures input from an external auditor. Key features include:

- Evaluates the design and operating effectiveness of controls
- Covers a specified period (usually 6-12 months)
- Provides detailed testing of controls over time
- Includes the auditor's opinion on the effectiveness of controls
- Often required for compliance and vendor management purposes

This report is particularly valuable for service organizations that handle sensitive client data, as it demonstrates the organization's commitment to security, availability, processing integrity, confidentiality, and privacy.

Question 36

D) Change control (Correct Answer)

Explanation: Change control is the change management process that provides an organized framework for company employees to suggest new features for development. Key aspects of change control include:

1. Formal process for submitting and evaluating change requests

2. Assessment of potential impacts on existing systems and processes
3. Prioritization of proposed changes
4. Documentation of approved changes
5. Implementation planning and execution
6. Post-implementation review

This process ensures that changes are implemented in a controlled and systematic manner, reducing risks and maintaining system integrity while allowing for innovation and improvement.

Question 37

A) Open Relays (Correct Answer)

Explanation: An Open Relay is an SMTP server configured to accept and forward email messages from any source to any destination. Characteristics of open relays include:

- Accept email from unknown or untrusted sources
- Forward emails to any destination, not just local users
- Often exploited by spammers to send bulk unsolicited emails
- Can lead to an organization's IP addresses being blacklisted
- Considered a security risk in modern email systems

Due to their potential for abuse, open relays are generally considered a poor practice in email server configuration and are often blocked or restricted by network administrators.

Question 38

C) Detection (Correct Answer)

Explanation: When an analyst performs an initial triage of a potential brute-force password attack alert, they are in the Detection stage of the incident response process. The incident response lifecycle typically includes:

1. Preparation: Establishing policies and procedures
2. Detection: Identifying potential security incidents
3. Analysis: Investigating the nature and scope of the incident
4. Containment: Limiting the damage and preventing further spread
5. Eradication: Removing the threat from the environment
6. Recovery: Restoring systems to normal operation
7. Post-Incident Activity: Learning and improving from the incident

The detection stage is crucial as it initiates the response process and determines the need for further action.

Question 39

A) Social Engineering (Correct Answer)

Explanation: Social Engineering is a type of attack that exploits human psychology to gain unauthorized access to systems or information. In this scenario, the attacker uses psychological manipulation to trick the helpdesk employee into resetting a password. Key aspects of social engineering include:

1. Exploits trust, fear, or desire to help
2. Often involves impersonation or pretexting
3. Bypasses technical security measures by targeting human vulnerabilities
4. Can be conducted via phone, email, in-person, or other communication channels
5. Highly effective due to the human element in security

Social engineering attacks are particularly dangerous because they can circumvent even the most sophisticated technical security measures by exploiting human behavior.

Question 40

B) Ethical Hackers (Correct Answer)

Explanation: Ethical Hackers, also known as White Hat Hackers, are security professionals trained in responsible network security methodology with a philosophy towards non-destructive and non-intrusive testing. Key characteristics of ethical hackers include:

1. Use hacking techniques for defensive purposes
2. Operate with explicit permission from the target organization
3. Follow a strict code of ethics and legal guidelines
4. Aim to identify and report vulnerabilities to improve security
5. Often hold certifications like CEH (Certified Ethical Hacker)
6. Employ the same tools and techniques as malicious hackers, but for beneficial purposes

Ethical hackers play a crucial role in proactive cybersecurity, helping organizations identify and address vulnerabilities before they can be exploited by malicious actors.

Question 41

A) TCP Model (Correct Answer)

Explanation: The TCP Model, also known as the TCP/IP Model or the Department of Defense (DoD) Model, is a network protocol conceptual model derived from TCP/IP. It has four layers:

1. Link Layer (Network Interface Layer)
2. Internet Layer
3. Transport Layer (Host-to-Host Layer)
4. Application Layer (Process Layer)

This model is simpler than the OSI model but closely reflects the structure of the internet. It's widely used in practical

networking and forms the basis of most modern network communications.

Question 42

D) Dwell Time (Correct Answer)

Explanation: In the context of keystroke dynamics as a biometric factor, Dwell Time refers to the length of time a key on the keyboard is pressed. Key aspects of dwell time in keystroke dynamics include:

- Measures how long each key is held down
- Part of an individual's unique typing pattern
- Used along with flight time (time between keystrokes) to create a biometric profile
- Can vary based on factors like typing speed, keyboard type, and user's physical condition
- One of several metrics used in keystroke dynamics for user authentication

This biometric factor is based on the premise that each person has a unique typing rhythm, which can be used as an additional layer of security in authentication systems.

Question 43

D) Abnormal activity (Correct Answer)

Explanation: Abnormal activity refers to any system activity that does not normally occur on your system. In the context of cybersecurity, identifying abnormal activity is crucial for detecting potential security threats. Characteristics of abnormal activity include:

- Deviations from established baselines of normal system behavior
- Unexpected processes or services running
- Unusual network traffic patterns
- Atypical user behaviors or login attempts
- Unexpected system resource usage

Monitoring for abnormal activity is a key component of many intrusion detection and prevention systems, helping to identify potential security incidents early in their lifecycle.

Question 44

A) SAML (Correct Answer)

Explanation: Security Assertion Markup Language (SAML) is likely to be involved when an organization needs to provide authentication and authorization assertions to their e-commerce cloud partner. SAML is an XML-based open standard for exchanging authentication and authorization data between parties. Key features of SAML include:

1. Enables single sign-on (SSO) across different domains
2. Provides a standardized way to communicate identity information
3. Supports federated identity management
4. Allows for secure transfer of user credentials across security domains
5. Widely used in enterprise and cloud environments

SAML is particularly useful in scenarios where an organization needs to securely share identity information with external partners or cloud services, making it ideal for e-commerce integrations.

Question 45

A) A law that erased strict government barriers between financial institutions (Correct Answer)

Explanation: The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, is a United States federal law that erased strict government barriers between financial institutions. Key aspects of GLBA include:

Allowed commercial banks, investment banks, securities firms, and insurance companies to consolidate

1. Repealed part of the Glass-Steagall Act of 1933
2. Introduced new privacy rules for financial institutions
3. Required financial institutions to explain their information-sharing practices to customers
4. Gave consumers the right to opt-out of having their information shared with third parties

While primarily known for its impact on the structure of the financial industry, GLBA also has significant implications for data privacy and security in financial services.

Question 46

B) Replay Attack (Correct Answer)

Explanation: A Replay Attack involves recording traffic between a client and server, then playing back or retransmitting the packets with slight variations. Key characteristics of a replay attack include:

- Intercepts valid data transmission
- Stores captured data for later use
- Retransmits the data to trick the receiving system
- Can be used to gain unauthorized access or perform fraudulent transactions
- Often targets authentication protocols

Replay attacks can be particularly dangerous because they use valid data, making them difficult to detect. Countermeasures include using session tokens, timestamps, or nonces (numbers used once) to ensure each transmission is unique and cannot be replayed.

Question 47

C) Use of components within or between processes on the same system (Correct Answer)

Explanation: The Component Object Model (COM) is Microsoft's standard for using components within a process or between processes running on the same system. Key features of COM include:

1. Enables inter-process communication
2. Allows for creation and use of reusable software components
3. Language-independent, allowing components written in different languages to interact
4. Forms the basis for other Microsoft technologies like OLE, ActiveX, and COM+
5. Supports both in-process and out-of-process components

COM is fundamental to many Windows applications and services, providing a standardized way for software components to communicate regardless of the language they were developed in.

Question 48

C) Prepare data for use by the application layer (Correct Answer)

Explanation: The primary purpose of the presentation layer in the OSI model is to prepare data for use by the application layer. Key functions of the presentation layer include:

1. Data formatting and conversion between different formats
2. Data compression to reduce transmission time
3. Data encryption and decryption for security
4. Character code translation (e.g., ASCII to EBCDIC)
5. Ensuring that data from the application layer of one system can be read by the application layer of another

This layer acts as a translator between the application layer and the lower layers, ensuring that data is in a usable format for the receiving application

Question 49

B) A process of transferring database backups to a remote site in bulk (Correct Answer)

Explanation: Electronic vaulting is a data protection strategy where large volumes of backup data are transferred to a remote location, typically over a network connection. This method ensures off-site data storage for disaster recovery purposes. It differs from real-time replication as it involves periodic, bulk transfers rather than continuous synchronization. Electronic vaulting provides a balance between data protection and cost-effectiveness, allowing organizations to secure their data off-site without the need for constant high-bandwidth connections.

Question 50

B) Protect children's personal information collected online (Correct Answer)

Explanation: The Children's Online Privacy Protection Act (COPPA) is a U.S. federal law enacted in 1998 to safeguard the online privacy of children under 13. Its primary function is to regulate the collection and use of personal information from children by websites and online services. COPPA requires parental consent for collecting data from children, mandates clear privacy policies, and gives parents control over their children's information. The act applies to websites specifically targeting children or knowingly collecting data from users under 13, aiming to create a safer online environment for young users.

Question 51

D) Phishing (Correct Answer)

Explanation: Phishing is a deceptive technique used in information systems security where attackers attempt to manipulate users into divulging sensitive information, often through email. It typically involves creating fraudulent messages that appear to be from legitimate sources, tricking recipients into revealing personal data, login credentials, or financial information.

Question 52

C) OCSP (Correct Answer)

Explanation: OCSP (Online Certificate Status Protocol) provides real-time certificate status verification, replacing traditional certificate revocation lists (CRLs). It allows clients to determine the current status of a digital certificate without downloading entire CRLs, offering more up-to-date information and reducing network traffic.

Question 53

C) Application, programmatic, and user interfaces (Correct Answer)

Explanation: The three primary types of interfaces typically evaluated during software testing procedures are application interfaces, programmatic interfaces (APIs), and user interfaces (UIs). These cover the main ways in which software components interact with each other and with users, ensuring comprehensive testing of the system's functionality and usability.

Question 54

A) Zero-Day Exploit (Correct Answer)

Explanation: A Zero-Day Exploit refers to a cyber attack that exploits vulnerabilities unknown to the software vendor or recently discovered. These attacks take advantage of security flaws before developers have had the opportunity to create and distribute patches, making them particularly dangerous and difficult to defend against.

Question 55

A) Objects (Correct Answer)

Explanation: In information security, "objects" is the collective term that encompasses files, databases, computers, programs, processes, devices, and media. Objects are the resources that subjects (users or processes) interact with and that require protection through various security measures.

Question 56

A) Waiting (Correct Answer)

Explanation: When a process requires access to a file currently in use, the process scheduler assigns it to the "Waiting" state. This state indicates that the process is temporarily unable to execute because it's waiting for a resource (in this case, the file) to become available.

Question 57

D) Detective Access Control (Correct Answer)

Explanation: Detective Access Control is implemented to detect unauthorized or unwanted activities, including the use of security personnel and intrusion detection systems. Unlike preventive controls, detective controls aim to identify and alert about security breaches after they have occurred, allowing for rapid response and mitigation.

Question 58

A) Flooding (Correct Answer)

Explanation: Flooding is a term that describes a cyber attack involving the transmission of excessive traffic to overwhelm a target system. This type of attack, often seen in Distributed Denial of Service (DDoS) attacks, aims to exhaust the target's resources, making it unable to respond to legitimate requests.

Question 59

B) Attribute-Based access control (Correct Answer)

Explanation: Attribute-Based Access Control (ABAC) utilizes information such as user identity, department, working hours, job category, and location to make authorization decisions. This flexible approach allows for fine-grained access control based on a wide range of attributes, providing more dynamic and context-aware security.

Question 60

D) Kernel (Correct Answer)

Explanation: The kernel is the component of an operating system that remains constantly present in memory to facilitate immediate execution when needed. It manages critical tasks such as memory allocation, process scheduling, and hardware communication, forming the core of the operating system.

Question 61

A) Health Insurance Portability and Accountability Act (HIPAA) (Correct Answer)

Explanation: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 introduced significant changes to health insurance regulations and mandated strict privacy measures for medical information. HIPAA established national standards for electronic health care transactions and addressed the security and privacy of health data.

Question 62

B) 2 (Correct Answer)

Explanation: The minimum number of disk drives required to implement RAID level 0 is 2. RAID 0 uses striping to distribute data across multiple disks for improved performance, but it requires at least two disks to function.

This configuration offers increased speed but no redundancy.

Question 63

D) End-To-End Testing (Correct Answer)

Explanation: End-To-End Testing is the testing approach that validates the entire software system, including interconnected subsystems, and examines the complete process flow. This comprehensive testing method ensures that the system functions correctly as a whole, simulating real-world scenarios and user workflows.

Question 64

B) Biometric Factors (Correct Answer)

Explanation: Biometric Factors best describes characteristics such as fingerprints, iris scans, signature dynamics, voice patterns, and keystroke patterns when used for identification or authentication. These unique physical or behavioral traits provide a high level of security by verifying an individual's identity based on who they are, rather than what they know or possess.

Question 65

B) SAS 70 has been replaced (Correct Answer)

Explanation: The concern Aldebron should raise when receiving a SAS70 report instead of a SOC 2 report is that SAS 70 has been replaced. SAS 70 was superseded by SSAE 16 and later by SSAE 18, which introduced SOC reports. SOC 2 reports specifically address controls relevant to security, availability, processing integrity, confidentiality, and privacy.

Question 66

D) Richard's private key (Correct Answer)

Explanation: In asymmetric encryption, Richard should use his private key to decrypt a message received from Sanil. Asymmetric encryption uses a pair of keys: a public key for

encryption and a private key for decryption. The sender (Sanil) would have used Richard's public key to encrypt the message, so only Richard's corresponding private key can decrypt it.

Question 67

D) Program Evaluation Review Technique (PERT) (Correct Answer)

Explanation: The Program Evaluation Review Technique (PERT) is a project management tool used to estimate software size and calculate standard deviation for risk assessment. PERT uses three time estimates (optimistic, most likely, and pessimistic) to calculate expected duration and variance, providing a probabilistic approach to project scheduling and risk analysis.

Question 68

A) Link Encryption (Correct Answer)

Explanation: Link Encryption is the encryption method that secures entire communication circuits by creating a protected tunnel between two points. This approach encrypts all data transmitted over a specific communication link, providing security for the entire communication path rather than just the data itself.

Question 69

A) An NAC system (Correct Answer)

Explanation: Colin should implement a Network Access Control (NAC) system to reduce zero-day attacks and enforce security policies on systems before network connection. NAC systems verify the security posture of devices attempting to connect to the network, ensuring they meet specific security requirements before granting access, thus mitigating risks from unknown vulnerabilities.

Question 70

D) Provide diligent and competent service to principles (Correct Answer)

Explanation: The statement "Provide diligent and competent service to principles" is not one of the four canons of the (ISC)² Code of Ethics. The correct canon is "Provide diligent and competent service to principals." The word "principles" in the given option is incorrect, as the canon refers to serving clients or employers (principals), not abstract principles.

Question 71

C) Dynamic (Correct Answer)

Explanation: Dynamic passwords are those that change regularly or with each use, rather than remaining static. This approach enhances security by ensuring that even if a password is compromised, it will only be valid for a limited time or a single use, significantly reducing the risk of unauthorized access.

Question 72

B) Concurrency control (Correct Answer)

Explanation: An attacker can use concurrency control techniques to exploit a Time-of-Check/Time-of-Use (TOC/TOU) vulnerability. TOC/TOU vulnerabilities occur when there's a time gap between checking a condition and using the results of that check. By manipulating the system during this gap, an attacker can cause the program to make incorrect decisions based on outdated information.

Question 73

B) Computer Security Incident (Correct Answer)

Explanation: A Computer Security Incident describes a violation or imminent threat to an organization's security policy, often resulting from attacks, malware, or inappropriate employee actions. This term encompasses a

wide range of security-related events that could potentially compromise the confidentiality, integrity, or availability of an organization's information assets.

Question 74

C) Scripted Testing (Correct Answer)

Explanation: Scripted Testing involves executing predefined test steps and comparing results, making it often suitable for automation. This approach follows a structured set of instructions (scripts) to test specific functionalities, allowing for consistent, repeatable testing processes that can be easily automated to improve efficiency and coverage.

Question 75

C) Waterfall (Correct Answer)

Explanation: For a project with clearly defined requirements and emphasis on comprehensive documentation, the Waterfall software development model is most appropriate. This linear sequential approach progresses through distinct phases (requirements, design, implementation, verification, maintenance) with extensive documentation at each stage, making it suitable for projects with well-understood, stable requirements.

Question 76

C) Interface Testing (Correct Answer)

Explanation: Interface Testing evaluates how well modules perform against interface specifications to ensure proper integration. This type of testing focuses on the communication between different components or systems, verifying that data is correctly passed and received according to defined interfaces.

Question 77

C) Purchasing insurance (Correct Answer)

Explanation: Purchasing insurance exemplifies risk transference in information security. This strategy involves shifting the potential financial impact of a risk to a third party (the insurance company) in exchange for a premium. It doesn't reduce the likelihood of an incident but mitigates its financial consequences.

Question 78

B) 3 hours (Correct Answer)

Explanation: In Baxter Industries' backup scenario, the period where data changes may be irretrievably lost is 3 hours. This represents the maximum time between backups, during which any changes made to the data could be lost if a system failure occurs before the next backup is performed.

Question 79

C) Frequency Analysis (Correct Answer)

Explanation: Frequency Analysis is a cryptographic analysis technique that examines letter repetition in encrypted messages and compares it to language-specific letter frequency statistics. This method exploits the fact that certain letters appear more frequently in a given language, helping to decipher substitution ciphers.

Question 80

D) MAC (Correct Answer)

Explanation: Mandatory Access Control (MAC) applies labels to subjects and objects, allowing access when labels match. This method enforces access control based on security clearance and sensitivity levels, ensuring that users can only access information for which they have the appropriate clearance.

Question 81

C) Addressing (Correct Answer)

Explanation: Addressing describes the method by which a processor references various memory locations. It involves assigning unique identifiers (addresses) to memory locations, allowing the processor to store and retrieve data efficiently from specific points in memory.

Question 82

D) Polyalphabetic Substitution (Correct Answer)

Explanation: Polyalphabetic Substitution is a cryptographic method that encrypts messages using letter-by-letter conversion and multiple alphabets from different languages or countries. This technique enhances security by using multiple substitution alphabets, making it more resistant to frequency analysis attacks than simple substitution ciphers.

Question 83

D) They should be provisioned only for rights matching the new role (Correct Answer)

Explanation: When an employee changes roles within an organization, they should be provisioned only for rights matching the new role. This approach, known as the principle of least privilege, ensures that employees have access only to the resources necessary for their current position, reducing security risks.

Question 84

D) Business manager (Correct Answer)

Explanation: Olivia is likely playing the role of a business manager if she's concerned about the conflict between profit and security requirements. Business managers often need to balance security measures with business objectives, considering both the cost of security implementations and potential risks to the organization.

Question 85

D) Static (Correct Answer)

Explanation: Static code analysis uses techniques like control flow graphs and lexical analysis to assess code without execution. This method examines the source code or compiled version of the code without running the program, allowing for early detection of potential vulnerabilities and coding errors.

Question 86

A) Company ID (Correct Answer)

Explanation: In a database table, the Company ID is typically the best candidate for a primary key. It's likely to be a unique identifier for each company record, ensuring that each row in the table can be uniquely identified. Unlike other options, it's less likely to change and is more efficient for indexing and joining tables.

Question 87

C) Sag (Correct Answer)

Explanation: A sag describes a momentary loss of power in a facility. It's characterized by a brief reduction in voltage, typically lasting from a few cycles to a few seconds. Sags are common power quality issues that can affect sensitive electronic equipment.

Question 88

A) To protect the confidentiality of their data (Correct Answer)

Explanation: A company might require Patsy Walker to sign a Non-Disclosure Agreement (NDA) when starting a new job to protect the confidentiality of their data. NDAs legally bind employees to keep sensitive company information confidential, preventing unauthorized disclosure of proprietary or confidential information.

Question 89

A) Functional Testing (Correct Answer)

Explanation: Functional Testing is the category that includes unit testing, smoke testing, sanity testing, integration testing, white box testing, black box testing, user acceptance testing, and regression testing. These testing types focus on verifying that the software functions according to specified requirements and behaves as expected.

Question 90

B) Hash Function (Correct Answer)

Explanation: A Hash Function generates a unique output value from a full message, commonly referred to as a message digest. This cryptographic process takes an input of any length and produces a fixed-size output, useful for data integrity checks and digital signatures.

Question 91

D) Extranet (Correct Answer)

Explanation: An Extranet describes a section of an organization's network that functions as an intranet for the private network while also serving information to specific external parties. It provides controlled access to authorized external users, such as suppliers or customers, to specific internal resources.

Question 92

B) Preservation (Correct Answer)

Explanation: During the Preservation phase of the Electronic Discovery Reference Model, potentially discoverable information is protected against alteration or deletion. This phase ensures that relevant data is safeguarded from intentional or accidental modification, maintaining its integrity for legal proceedings.

Question 93

C) Grant Rule (Correct Answer)

Explanation: In the take-grant protection model, the Grant Rule would allow Pavel Chekov to obtain read permissions on an object if James Kirk already has those rights. This rule allows a subject with both 'read' and 'grant' rights to an object to grant 'read' rights to another subject.

Question 94

D) GDPR (Correct Answer)

Explanation: The General Data Protection Regulation (GDPR) is the regulatory framework that aims to give EU citizens more control over their personal data and simplify the business environment in the European Union. It establishes strict data protection requirements for organizations handling EU residents' personal data.

Question 95

D) SSO (Correct Answer)

Explanation: Single Sign-On (SSO) is the mechanism that allows users to authenticate once and then access multiple resources without repeated authentication challenges. This approach enhances user experience and security by reducing the number of credentials a user needs to remember and manage.

Question 96

B) Field (Correct Answer)

Explanation: In database terminology, a Field describes a column or attribute of a table. It represents a specific piece of data within each record of the table, such as a name, date, or numerical value.

Question 97

B) Discovery (Correct Answer)

Explanation: Application banner information is typically recorded during the Discovery phase of penetration testing. This phase involves gathering information about the target

system, including identifying running services, software versions, and other potentially useful details for planning the actual penetration attempt.

Question 98

B) Discretionary Access Control (DAC) (Correct Answer)

Explanation: Discretionary Access Control (DAC) is typically controlled by the owner of the objects. In this model, the owner of a resource has the ability to grant or restrict access to that resource, allowing for flexible and decentralized access management.

Question 99

D) Threat Modeling (Correct Answer)

Explanation: Threat Modeling describes the process of identifying and addressing potential security vulnerabilities in software before it is released or deployed. This proactive approach involves analyzing the application design, identifying potential threats, and developing strategies to mitigate these risks early in the development lifecycle.

Question 100

B) TLS (Correct Answer)

Explanation: Transport Layer Security (TLS) is the cryptographic protocol designed to provide secure communication over a computer network, commonly used for internet connections. It's the successor to SSL, offering improved security and is widely used to encrypt data transmitted between web browsers and servers.

Practice Tests 3

Question 1

In the context of information systems security, what type of controls are described as the policies and procedures defined by an organization's security policy to implement and enforce overall access control?

A) High-level Access Controls

B) Top-level Access Management

C) Administrative Access Controls

D) Administrative Access Management

Question 2

How is a monetary value assigned to an asset based on actual cost and non-monetary expenses, such as development, maintenance, administration, advertising, support, repair, and replacement costs referred to in information systems security?

A) Equity Valuation

B) Market Valuation

C) Asset Valuation

D) Liquidation Valuation

Question 3

In an organization where users can log into any workstation, even those assigned to different departments, which information security principle is most directly violated?

A) Separation of duties

B) Need to know

C) Two-person control

D) Least privilege

Question 4

Which RAID level is commonly referred to as a "disk stripe of mirrors"?

A) RAID 5

B) RAID 1

C) RAID 10

D) RAID 0

Question 5

In the context of authentication factors, what type is a Smart Card classified as?

A) Type 2

B) Type 1

C) Type 4

D) Type 3

Question 6

What logical operation, represented by the ∨ symbol, evaluates whether at least one input value is true?

A) OR

B) OMNIUS

C) DELTA

D) SUM

Question 7

What term describes the computational rules for bits and bytes used by computers?

A) Cryptography Hashing

B) Binate Manipulation

C) Binary Mathematics

D) Order of Operations

Question 8

At which layer of the OSI model are datagrams associated?

A) Network

B) Datalink

C) Transport

D) Session

Question 9

For a gigabit Ethernet network aiming to provide 1000 Mbps to users, which combination of cable categories is most appropriate?

A) Cat 4e and Cat 5e

B) Cat 5e and Cat 6

C) Cat 5 and Cat 6

D) Cat 6 and Cat 7

Question 10

What component of the Kerberos Key Distribution Centre (KDC) is responsible for verifying or rejecting the authenticity and timeliness of tickets?

A) Ingestion Port

B) Authenticator Device (AD)

C) Authentication Service (AS)

D) Permission Gateway (PG)

Question 11

What type of communication relies on start and stop flags or bits to manage data transmission?

A) Synchronous

B) Analog

C) Asynchronous

D) Digital

Question 12

Which authentication mechanism employs a trusted third party for identification and is based on tickets?

A) Screen Scraping SSO

B) Smart Card-based SSO

C) Cookie-based SSO

D) Kerberos-based SSO

Question 13

For integration with a cloud identity provider using OAuth 2.0, which authentication framework is most suitable?

A) OpenID Connect

B) RADIUS

C) SAML

D) Kerberos

Question 14

What type of Single Sign-On (SSO) creates an encrypted cookie on the user's machine containing credentials, allowing automatic login on subsequent visits?

A) Form-filling SSO

B) Enrollment-based SSO

C) Kerberos-based SSO

D) Cross-domain SSO

Question 15

Which protocol provides real-time verification of a digital certificate's validity and confirms it hasn't been revoked by the issuing authority?

A) Hypertext Transfer Protocol Secure (HTTPS)

B) Secure Sockets Layer (SSL)

C) Online Certificate Status Protocol (OCSP)

D) Transport Layer Security (TLS)

Question 16

What type of attack involves intercepting network traffic to obtain sensitive information like passwords and credit card numbers?

A) SQL injection attack

B) Drive-by attack

C) Password attack

D) Eavesdropping attack

Question 17

When developing an input validation routine to protect a web application's database from SQL injection attacks, where should the validation code be placed?

A) JavaScript embedded in the web pages

B) Code on the user's web browser

C) Backend code on the web server

D) Stored procedure on the database

Question 18

Which ITU-T standard is typically used when a Smart Card provides a certificate to an upstream authentication service?

A) X.500

B) X.509

C) SPML

D) SAML

Question 19

What authentication protocol for Point-to-Point Protocol (PPP) transmits usernames and passwords in clear text, offering no encryption?

A) Credential Transmission Portal (CTP)

B) Password Authentication Protocol (PAP)

C) Microsoft Challenge Handshake Authentication Protocol (CHAPv2)

D) Challenge Handshake Authentication Protocol (CHAP)

Question 20

Which penetration testing tool is capable of performing port scans, ping sweeps, banner grabbing, and network discovery?

A) Nmap

B) Netsparker

C) Acunetix

D) Indusface

Question 21

In a Linux system, what do the letters "rwx" in file attributes indicate?

A) Accountability

B) Authentication

C) Identification

D) Authorization

Question 22

For a Windows 10 system processing credit cards, which security standard is most appropriate?

A) The NSA Windows 10 baseline

B) The CIS Windows 10 baseline

C) PCI DSS

D) Microsoft's Windows 10 security baseline

Question 23

In NIST Special Publication 800-53, which measure of developmental assurance refers to the rigor, detail, and formality of artifacts produced during system component design and development?

A) Depth

B) Suitability

C) Affirmation

D) Coverage

Question 24

Which intellectual property protection mechanism typically has the shortest duration?

A) Trade secret

B) Copyright

C) Patent

D) Trademark

Question 25

What term describes the ability of virtualization and cloud solutions to expand or contract based on need?

A) Pertinacity

B) Elasticity

C) Contumacy

D) Rigor

Question 26

What is the term for the automated process that moves transaction records from a primary site to a backup site on an hourly basis in database recovery?

A) Remote journaling

B) Transaction logging

C) Remote mirroring

D) Electronic vaulting

Question 27

When determining the time it should take to restore an IT service after an outage in a disaster recovery plan, what variable is being calculated?

A) RPO

B) MTD

C) RTO

D) SLA

Question 28

For uniquely identifying BYOD devices not joined to a central management system, which method is most reliable?

A) Requiring users to fill out a registration form

B) Recording the MAC address of each system

C) Using device fingerprinting via a web-based registration system

D) Scanning each system using a port scanner

Question 29

What term describes an electronic filing system for organizing collections of information, typically structured with files, records, and fields?

A) CPU

B) Hash

C) Database

D) Blockchain

Question 30

Which component is not typically considered one of the three main elements of the DevOps model?

A) Change Management

B) Quality Assurance

C) Software Development

D) Operations

Question 31

What process involves assessing various risks to organizational processes and creating policies, plans, and procedures to minimize their potential impact?

A) Business Continuity Planning (BCP)

B) Risk Response Register (RRR)

C) Executive Rescue Response (ERR)

D) Disaster Contingency Planning (DCP)

Question 32

Which capability is not typically associated with Mobile Device Management (MDM) solutions?

A) Enforcing device encryption

B) Managing device backups

C) Remotely wiping device contents

D) Assuming control of non-registered BYOD devices

Question 33

What characteristic is true of heuristic-based anti-malware software?

A) It monitors systems for files with known virus content

B) It has a higher chance of detecting zero-day exploits than signature-based methods

C) It has a lower false positive rate than signature detection

D) It requires frequent definition updates to detect new malware

Question 34

In information systems security, what term describes a passive entity that provides information or data to subjects, such as files, databases, or programs?

A) Item

B) Object

C) Solution

D) Script

Question 35

What type of testing involves relocating personnel to an alternate recovery site and implementing site activation procedures?

A) Compatibility Testing

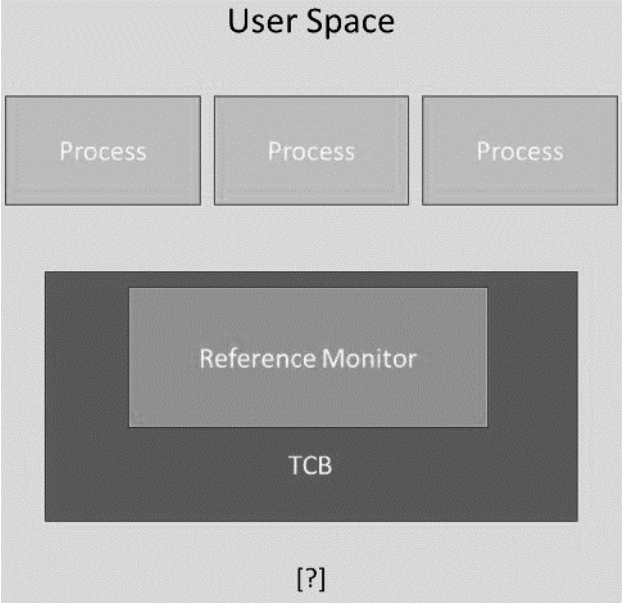
B) Black box Testing

C) Parallel Testing

D) Alpha Testing

Question 36

In a diagram of security boundaries within a computer system, what term typically refers to the central component that implements a secure, reliable operating system?



A) Privilege core

B) Kernel

C) Security perimeter

D) User monitor

Question 37

In Kerberos authentication, what does a Service Ticket (ST) provide?

A) Proof of authentication through a KDC and ability to request tickets

B) Authentication host services

C) Proof of authorization to access an object

D) Ticket granting services

Question 38

What type of software testing validates a system against its functional requirements by providing input and verifying output?

A) Beta Testing

B) Functional Testing

C) Alpha Testing

D) Non-Functional Testing

Question 39

What term describes a collection of computers across the internet under an attacker's control?

A) Darknet

B) Botuniverse

C) Botworld

D) Botnet

Question 40

When a web server experiences unusually high traffic volume from a botnet, causing it to reject requests, what type of attack has occurred?

A) Reconnaissance

B) Denial of Service

C) Malicious insider

D) Compromise

Question 41

What term describes a private network designed to host the same information services found on the Internet?

A) LAN

B) WAN

C) Intranet

D) VPN

Question 42

Which markup language uses concepts like Requesting Authority, Provisioning Service Point, and Provisioning Service Target for handling core functionality?

A) SAMP

B) SPML

C) XACML

D) SAMPL

Question 43

What deployment uses FDDI with twisted-pair copper wires, reducing maximum segment length to 100 meters and increasing susceptibility to interference?

A) ETH-NET

B) COAX

C) CDDI

D) FDDA

Question 44

When concerned about third-party developers embedding backdoors in code, which programming language would be least susceptible due to its human-readable final form?

A) JavaScript

B) C++

C) C

D) Java

Question 45

What decision-making process takes into account non-numerical factors such as emotions, investor/customer confidence, and workforce stability?

A) Rational Decision-Making

B) Qualitative Decision-Making

C) Quantitative Decision-Making

D) Intuitive Decision-Making

Question 46

What type of attack targets the most commonly used mechanism for authenticating users to information systems?

A) Password attack

B) Denial-of-Service

C) Malware attack

D) Phishing attack

Question 47

What is a computer or network designed to appear vulnerable and attract attackers, diverting them from legitimate systems?

A) Beehive

B) Honeynet/Honeypot

C) Wasp Nest

D) Jackpot

Question 48

What term describes a message that has been encrypted for transmission?

A) A Public Message

B) A Hash

C) A Private Message

D) Ciphertext

Question 49

What process involves reviewing and selecting security controls based on the specific IT system they will be applied to?

A) Standardizing

B) Scoping

C) Baselining

D) Tailoring

Question 50

Which type of background check is not typically performed during normal pre-hire activities?

A) Criminal records check

B) Credit check

C) Reference verification

D) Medical records check

Question 51

Countermeasures are actions taken to address vulnerabilities or protect systems from attacks. These can involve adjusting security configurations, implementing new protective mechanisms, modifying services, and other similar steps.

What term best describes these protective actions?

A) Responses

B) Retaliations

C) Countermeasures

D) Mitigations

Question 52

Which engineering discipline focuses on designing computing systems at the logical level?

A) SAML Architecture

B) LAN Architecture

C) WAN Architecture

D) Computer Architecture

Question 53

What Windows feature automatically assigns an IP address in the 169.254.0.0-169.254.255.255 range if DHCP assignment fails?

A) Windows Automated IP Allocation (WAIPA)

B) Automatic Private IP Addressing (APIPA)

C) Active Directory IP Assignment (ADIPA)

D) ActiveX IP Assignment (AXIPA)

Question 54

Which type of software testing is performed by internal employees to identify potential issues before releasing a product to end users?

A) Omega Testing

B) Alpha Testing

C) Delta Testing

D) Beta Testing

Question 55

When evaluating software for both security flaws and usability from an end-user perspective while referencing the source code, what type of testing is being conducted?

A) Black box

B) Blue box

C) White box

D) Gray box

Question 56

What term describes the body of knowledge defined by (ISC)2 as the source material for the CISSP exam?

A) CBK

B) CFBOK

C) ABK

D) PMBOK

Question 57

In database design, what term refers to a primary key from another table used to establish relationships between tables?

A) Outside Key

B) Index Key

C) Foreign Key

D) Principal Key

Question 58

Which type of data transmission relies on timing mechanisms like independent clocks or embedded timestamps?

A) Analog

B) Asynchronous

C) Synchronous

D) Digital

Question 59

What concept describes the process of holding individuals responsible for their actions?

A) Immunity

B) Accountability

C) Justification

D) Culpability

Question 60

Which of these is not a key principle in the COBIT framework for IT security control objectives?

A) Performing exhaust analysis

B) Meeting stakeholder needs

C) Separating governance from management

D) Covering the enterprise end-to-end

Question 61

When recording data and replaying it against a test website to evaluate performance based on real production workload, what type of monitoring is being conducted?

A) Proactive

B) Passive

C) Replay

D) Reactive

Question 62

Which principle is not included in the EU-US privacy shield provisions?

A) Nonrepudiation

B) Security

C) Access

D) Enforcement

Question 63

To prevent session hijacking via cookies in a web application, which technique is most effective?

A) Set the Domain cookie attribute to example.com

B) Set the Expires cookie attribute to less than a week

C) Set the Secure attribute for the cookies

D) Set the HTTPOnly attribute

Question 64

Who is responsible for implementing the protection measures defined by security policies and management?

A) Data Analyst

B) Data Custodian

C) Content Guardian

D) Security Controls & Access Analyst

Question 65

In the ring protection model, which ring operates in non-privileged mode?

A) Ring 0

B) Ring 2

C) Ring 1

D) Ring 3

Question 66

Which block cipher operates on 64-bit text blocks and uses variable-length keys ranging from 32 to 448 bits?

A) Blowfish

B) Rubber-band

C) Mutant

D) Titan

Question 67

What is the standard language used for interacting with relational databases?

A) NoSQL

B) SQL

C) NRXQL

D) XML

Question 68

When an organization has limited public IP addresses but needs to connect many internal devices to the internet,

which technology is typically used?

A) SDN

B) IPX

C) IPSec

D) PAT

Question 69

What term describes evidence that includes copies made from original documents?

A) Opinion evidence

B) Clone Evidence

C) Indirect Evidence

D) Secondary Evidence

Question 70

To monitor production servers using actual traffic for testing, which type of monitoring should be employed?

A) Active

B) Passive

C) Replay

D) Real-time

Question 71

What device generates in-band signaling tones to control telephone switches, historically used for bypassing toll collection?

A) Blue Box

B) Black Box

C) Orange Box

D) Green Box

Question 72

Which type of computer memory can be read but not written to?

A) RAM

B) ROM

C) CDRW

D) DVR

Question 73

Which type of forensic investigation typically has the most stringent standards for evidence?

A) Administrative

B) Industry

C) Civil

D) Criminal

Question 74

What SCAP component provides a standardized naming system for operating systems, applications, and devices?

A) Random Name Generator (RNG)

B) Arbitrary Platform Register Tool (APRT)

C) Security Content Random Name Generator (SCRNG)

D) Common Platform Enumeration (CPE)

Question 75

In asymmetric cryptography, what key is typically contained within a digital certificate issued by a Certificate Authority?

A) Subject's private key

B) CA's public key

C) Subject's public key

D) CA's private key

Question 76

Which biometric factor uses the shape of a person's hand for authentication or identification?

A) Palm Geography

B) Mani-Graph

C) Mani-Printing

D) Hand-Scan

Question 77

Which statement about SSAE-18 is incorrect?

A) It mandates a specific control set

B) It uses a framework including SOC 1, SOC 2, and SOC 3 reports

C) It is used for external audits

D) It is an attestation standard

Question 78

What approach aims to integrate software development, quality assurance, and technology operations into a single operational model?

A) Jira

B) Full Stack

C) DevOps

D) Github

Question 79

What file contains DNS entries that are preloaded into a cache when a system boots, predating query-based DNS?

A) HOSTS File

B) DOS File

C) IOS File

D) BOOT File

Question 80

Which fire suppression system contains compressed air that, when triggered, releases to open a water valve and fill pipes?

A) Air Pipe

B) Relay Pipe

C) Wet Pipe

D) Dry Pipe

Question 81

What term describes cloud computing services offered by third-party providers over the public internet, often with on-demand pricing?

A) Hybrid Cloud

B) Platform-as-a-Service (PaaS)

C) Private Cloud

D) Public Cloud

Question 82

Which of these is not an object-oriented programming language?

A) C++

B) Fortran

C) C#

D) Java

Question 83

In object-oriented programming, what term describes the output or result from an object after processing a message using a method?

A) Behaviour

B) Release

C) Deliverable

D) Reaction

Question 84

What component should be included in an organization's emergency response guidelines?

A) Activation procedures for cold sites

B) Secondary response procedures for first responders

C) Long-term business continuity protocols

D) Contact information for equipment ordering

Question 85

In which single sign-on (SSO) method does a user insert a smart card into a reader to access multiple applications?

A) Kerberos-based SSO

B) Smart Card-based SSO

C) Claims-based SSO

D) Cookie-based SSO

Question 86

Which protocol at layer 4 of the OSI model is connection-oriented?

A) Session Connection Protocol (SCP)

B) Network Flow Protocol (NFP)

C) Transmission Control Protocol (TCP)

D) Datalink Format Protocol (DFP)

Question 87

In which type of software testing does the tester have full knowledge of the system's implementation before beginning?

A) White Box

B) Blue Box

C) Black Box

D) Grey Box

Question 88

What networking approach separates the infrastructure layer from the control layer to increase flexibility and reduce vendor lock-in?

A) VPN

B) ISDNs

C) SPN

D) SDNs

Question 89

Which service is used to centralize authentication for VPN connections, including legacy dial-up and broadband internet connections?

A) JUPITER

B) ATOM

C) PHANTOM

D) RADIUS

Question 90

When limiting users to installing only approved software, which application control approach is most appropriate?

A) Blacklisting

B) Greylisting

C) Whitelisting

D) Blue listing

Question 91

On a modern, security-conscious Linux system, where are password hashes typically stored?

A) /etc/passwd

B) /etc/shadow

C) /etc/hash

D) /etc/secure

Question 92

Which authentication factor refers to biometric characteristics like fingerprints, voice prints, or retina patterns?

A) Type 1

B) Type 3

C) Type 2

D) Type 4

Question 93

In object-oriented programming, what term describes a collection of common methods that define the behavior of a set of objects?

A) Class

B) Set

C) Group

D) Field

Question 94

In which type of trusted recovery does a system automatically recover from failures while protecting against data loss, without administrator intervention?

A) Functional recovery

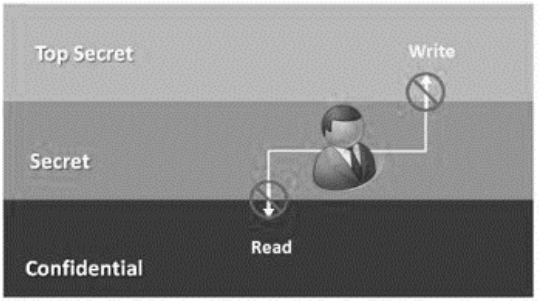
B) Manual recovery

C) Automated recovery without undue data loss

D) Automated recovery

Question 95

Which security model includes an axiom stating that a subject at a specific classification level cannot write data to a higher classification level?



A) Bell-LaPadula

B) Diba

C) Biba

D) DAC

Question 96

What type of password system requires users to answer predefined personal questions for authentication?

A) Multifactor passwords

B) Passphrase

C) Cognitive passwords

D) Password reset questions

Question 97

What term describes a workstation with minimal local processing or storage capacity, used primarily to connect to and operate a remote system?

A) Thin Client

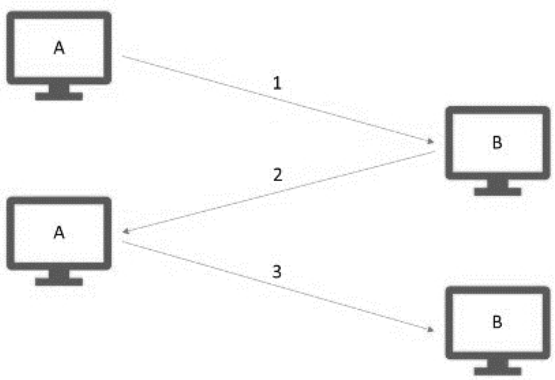
B) Shallow Client

C) Skinny Client

D) Mini Client

Question 98

In a TCP three-way handshake, what does the responding system send in the second step?



A) SYN

B) SYN/ACK

C) ACK

D) FIN/ACK

Question 99

The Low Orbit Ion Cannon (LOIC) attack tool, which uses multiple home PCs to target systems, is an example of what type of network attack?

A) DDoS

B) Zombie Horde

C) Ionization

D) Teardrop

Question 100

In the US legal system, what term describes evidence consisting of expert opinions and facts?

A) Expert Advice

B) Expert Evidence

C) Expert Witness

D) Expert Opinion

Question 101: In the realm of Information Systems Security, what term describes a set of rules or procedures applied to input data, often associated with cryptographic functions that dictate encryption and decryption permutations?

A) Private Key Routine (PKR)

B) Script

C) Algorithm

D) Hash

Question 102: Within the context of Information Systems Security, what term refers to a numerical code assigned to an individual for identification purposes, which should be kept confidential?

A) MFA

B) OTP

C) 2FA

D) PIN

Question 103: In Information Systems Security, which email encryption mechanism provides authentication, integrity, confidentiality, and non-repudiation, operates at layer 7, and utilizes RSA, DES, and X.509?

A) Privacy Enhanced Mail (PEM)

B) Pretty Good Privacy (PGP)

C) GNUPGK

D) GPG4Win

Question 104: The Open Shortest Path First (OSPF) protocol maintains a map of all connected remote networks and uses it to determine the shortest path to a remote destination. What category of routing protocol does OSPF belong to?

A) Critical path protocol

B) Link state protocol

C) Distance vector protocol

D) Link mapping protocol

Question 105: Which RAID configuration is commonly referred to as disk mirroring?

A) RAID 2

B) RAID 1

C) RAID 5

D) RAID 0

Question 106: Which encryption/decryption algorithm possesses the following attributes:

Classified as a cryptosystem algorithm

Employed for secure data transmission

Developed in 1977

Created by Adi Shamir, Leonard Adleman, and Ron Rives

Utilizes the mathematical concept of factorization of two large prime numbers' product

Particularly suitable for verification and encryption purposes

A) ARS

B) RSA

C) DSA

D) SAR

Question 107: In the field of Information Systems Security, what term describes code objects encompassing a wide range of programmed computer security threats that exploit various network, operating system, software, and physical security vulnerabilities to propagate malicious payloads to computer systems?

A) Phishing and Spear Phishing Attack

B) Malware Attack

C) Drive-By Attack

D) Malicious Code

Question 108: Baxter Industries, a mid-sized company specializing in building automation systems, maintains local file servers in their on-premise data center for storing critical business data. Tarra, an IT department employee responsible for backup strategy, performs full backups every Sunday at 8:00 PM and differential backups Monday through Friday at noon. If a server failure occurs at 3:00 PM on Wednesday, how many backups must Tarra apply to restore the system to its most current state possible?

A) 1

B) 3

C) 2

D) 4

Question 109: Which type of investigation consistently employs the "beyond a reasonable doubt" standard for evidence?

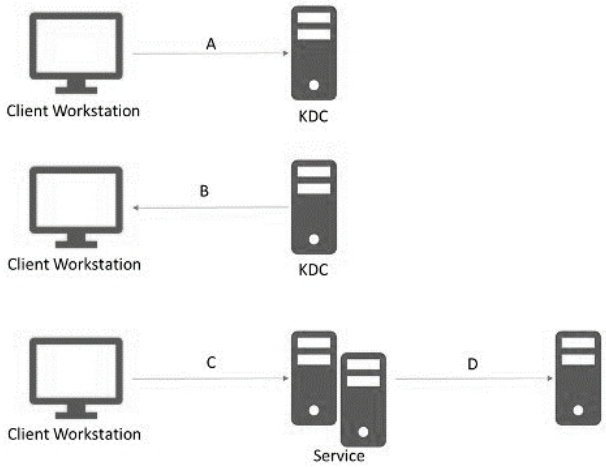
A) Civil investigation

B) Operational investigation

C) Regulatory investigation

D) Criminal investigation

Question 110: In a Kerberos authentication and authorization scenario, if a client has already authenticated to the KDC and wishes to access a resource, what does the client workstation transmit to the KDC at point A?



A) It re-sends the password

B) A service ticket

C) A TGR

D) Its TGT

Question 111: In Information Systems Security, what term describes an attack that exploits vulnerabilities in the fragment reassembly functionality of the TCP/IP protocol stack?

A) Augmentation

B) Virtualization

C) Re-Genesys

D) Fragmentation

Question 112: The EU-US Privacy Shield Framework is built upon seven fundamental principles. Which of the following lists accurately identifies all seven?

A) Notice, choice, onward transfer, security, data integrity, access, enforcement

B) Awareness, selection, control, security, data integrity, access, enforcement

C) Privacy, security, control, notification, data integrity, access, enforcement

D) Submission, editing, updates, confidential, integrity, security, access

Question 113: In Information Systems Security, what concept ensures that any behavior will only affect the memory and resources associated with the process?

A) Admittance

B) Isolation

C) Inclusion

D) Interlinking

Question 114: Which type of malware utilizes built-in propagation mechanisms that exploit system vulnerabilities to spread?

A) Trojan horse

B) Worm

C) Logic bomb

D) Virus

Question 115: What form of twisted-pair cable supports 1 Gbps throughput at distances up to 100 meters?

A) 1000BaseTX

B) 10000BaseT

C) 1BaseTX

D) 1000BaseT

Question 116: In Information Systems Security, what term refers to an unused portion of network space used to monitor network-based attacks and traffic?

A) Trapdoor

B) Boobytrap

C) Darknet

D) Void

Question 117: Sanil and Richard, friends in different physical locations, wish to begin communicating using cryptography to protect the confidentiality of their messages. They exchange digital certificates and plan to use an asymmetric encryption algorithm for secure email exchange. When Sanil adds a digital signature to the message, which encryption key does he use to create it?

A) Richard's public key

B) Sanil's private key

C) Richard's private key

D) Sanil's public key

Question 118: Which of the following is an example of a hardening measure that could strengthen an organization's existing physical facilities and potentially avoid implementing a business continuity plan?

A) Upgrading operating systems

B) Patching a leaky roof

C) Deploying network intrusion detection system

D) Reviewing and updating firewall access control lists

Question 119: What RADIUS alternative is frequently used with Cisco network equipment and supports two-factor authentication?

A) XTACACS

B) RADUIS+

C) TACACS+

D) Kerberos

Question 120: In Information Systems Security, what term describes a type of biometric control that recognizes the physical dimensions of a hand?

A) Hand-Scan

B) Hand Geometry

C) Digit Biometrics

D) Mani-Graph

Question 121: In Information Systems Security, what term refers to an application that analyzes business data and presents it in a way designed to facilitate decision-making for users?

A) User Decision Platform (UDP)

B) Programed Decision Logic (PDL)

C) Business Logic Application (BLA)

D) Decision Support System (DSS)

Question 122: What key assumption made by EAP can be addressed by implementing PEAP?

A) EAP does not allow additional authentication methods, and PEAP adds additional methods

B) There are no TLS implementations available using EAP

C) EAP originally assumed the use of physically isolated channels and did not include encryption

D) EAP assumes that LEAP will replace TKIP, ensuring authentication will occur

Question 123: In which type of matrix would you encounter the following items: Accountable, Consulted, Informed, Responsible?

A) Stakeholder Engagement Assessment Matrix

B) Responsibility Assignment Matrix

C) Power-Interest Matrix

D) Stakeholder Analysis Matrix

Question 124: In Information Systems Security, what term describes the wire in an electrical circuit that is connected to the earth?

A) Negative Pole

B) Positive Pole

C) Ground

D) Neutral Pole

Question 125: In Information Systems Security, what term describes an attack based on a human statistical anomaly where the malicious individual attempts to substitute a digitally signed communication with a different message that produces the same message digest, thereby maintaining the validity of the original digital signature?

A) Birthday Attack

B) Brute Force Attack

C) Calendar Attack

D) Lottery Attack

Question 126: The company Dane works for has notifications posted at each door reminding employees to be cautious about allowing people to enter. Which type of control best describes this measure?

A) Physical

B) Detective

C) Preventative

D) Directive

Question 127: In Information Systems Security, what term describes a set of rules or procedures to be performed on input data, commonly related to cryptographic functions that dictate the permutations of encryption and decryption?

A) Private Key Routine (PKR)

B) Script

C) Algorithm

D) Hash

Question 128: Within the context of Information Systems Security, what term refers to a number or code assigned to an individual for identification purposes, which should be kept confidential?

A) MFA

B) OTP

C) 2FA

D) PIN

Question 129: Which email encryption mechanism provides authentication, integrity, confidentiality, and non-repudiation, operates at layer 7, and utilizes RSA, DES, and X.509?

A) Privacy Enhanced Mail (PEM)

B) Pretty Good Privacy (PGP)

C) GNUPGK

D) GPG4Win

Question 130: The Open Shortest Path First (OSPF) protocol is a routing protocol that maintains a map of all connected remote networks and uses this map to select the shortest path to a remote destination. What type of routing protocol is OSPF classified as?

A) Critical path protocol

B) Link state protocol

C) Distance vector protocol

D) Link mapping protocol

Question 131: Which RAID level is also known as disk mirroring?

A) RAID 2

B) RAID 1

C) RAID 5

D) RAID 0

Question 132: Which encryption/decryption algorithm possesses the following characteristics:

Classified as a cryptosystem algorithm

Used for secure data transmission

Developed in 1977

Created by Adi Shamir, Leonard Adleman, and Ron Rives

Utilizes the mathematical concept of factorization of two large prime numbers' product

Particularly suitable for verification and encryption purposes

A) ARS

B) RSA

C) DSA

D) SAR

Question 133: In Information Systems Security, what term describes code objects that encompass a wide range of programmed computer security threats exploiting various network, operating system, software, and physical security vulnerabilities to propagate malicious payloads to computer systems?

A) Phishing and Spear Phishing Attack

B) Malware Attack

C) Drive-By Attack

D) Malicious Code

Question 134: Baxter Industries, a mid-sized company focusing on building automation systems, hosts local file servers in their on-premise data center storing critical business data. Tarra, an IT department employee responsible for backup strategy, performs full backups every Sunday at 8:00 PM and differential backups Monday through

Friday at noon. If a server failure occurs at 3:00 PM on Wednesday, how many backups must Tarra apply to restore the system to its most current state possible?

A) 1

B) 3

C) 2

D) 4

Question 135: Which type of investigation consistently employs the "beyond a reasonable doubt" standard for evidence?

A) Civil investigation

B) Operational investigation

C) Regulatory investigation

D) Criminal investigation

Question 136: In a Kerberos authentication and authorization scenario, if a client has already authenticated to the KDC and wishes to access a resource, what does the client workstation transmit to the KDC at point A?

A) It re-sends the password

B) A service ticket

C) A TGR

D) Its TGT

Question 137: In Information Systems Security, what term describes an attack that exploits vulnerabilities in the fragment reassembly functionality of the TCP/IP protocol stack?

A) Augmentation

B) Virtualization

C) Re-Genesys

D) Fragmentation

Question 138: The EU-US Privacy Shield Framework is built upon seven fundamental principles. Which of the following lists accurately identifies all seven?

A) Notice, choice, onward transfer, security, data integrity, access, enforcement

B) Awareness, selection, control, security, data integrity, access, enforcement

C) Privacy, security, control, notification, data integrity, access, enforcement

D) Submission, editing, updates, confidential, integrity, security, access

Question 139: In Information Systems Security, what concept ensures that any behavior will only affect the memory and resources associated with the process?

A) Admittance

B) Isolation

C) Inclusion

D) Interlinking

Question 140: Which type of malware utilizes built-in propagation mechanisms that exploit system vulnerabilities to spread?

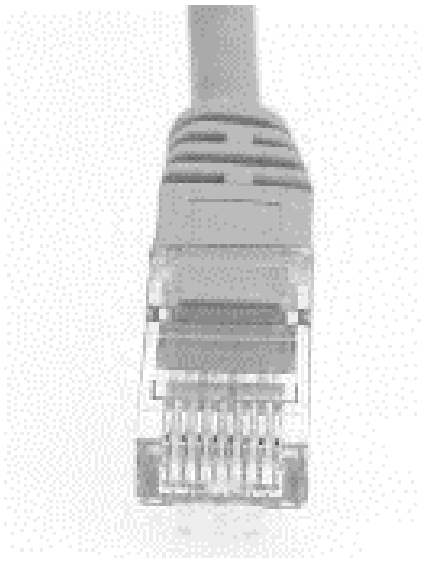
A) Trojan horse

B) Worm

C) Logic bomb

D) Virus

Question 141: What form of twisted-pair cable supports 1 Gbps throughput at distances up to 100 meters?



A) 1000BaseTX

B) 10000BaseT

C) 1BaseTX

D) 1000BaseT

Question 142: In Information Systems Security, what term refers to an unused portion of network space used to monitor network-based attacks and traffic?

A) Trapdoor

B) Boobytrap

C) Darknet

D) Void

Question 143: Sanil and Richard, friends in different physical locations, wish to begin communicating using cryptography to protect the confidentiality of their messages. They exchange digital certificates and plan to use an asymmetric encryption algorithm for secure email exchange. When Sanil adds a digital signature to the message, which encryption key does he use to create it?

A) Richard's public key

B) Sanil's private key

C) Richard's private key

D) Sanil's public key

Question 144: Which of the following is an example of a hardening measure that could strengthen an organization's existing physical facilities and potentially avoid implementing a business continuity plan?

A) Upgrading operating systems

B) Patching a leaky roof

C) Deploying network intrusion detection system

D) Reviewing and updating firewall access control lists

Question 145: What RADIUS alternative is frequently used with Cisco network equipment and supports two-factor authentication?

A) XTACACS

B) RADUIS+

C) TACACS+

D) Kerberos

Question 146: In Information Systems Security, what term describes a type of biometric control that recognizes the physical dimensions of a hand?

A) Hand-Scan

B) Hand Geometry

C) Digit Biometrics

D) Mani-Graph

Question 147: In Information Systems Security, what term refers to an application that analyzes business data and presents it in a way designed to facilitate decision-making for users?

A) User Decision Platform (UDP)

B) Programed Decision Logic (PDL)

C) Business Logic Application (BLA)

D) Decision Support System (DSS)

Question 148: What key assumption made by EAP can be addressed by implementing PEAP?

A) EAP does not allow additional authentication methods, and PEAP adds additional methods

B) There are no TLS implementations available using EAP

C) EAP originally assumed the use of physically isolated channels and did not include encryption

D) EAP assumes that LEAP will replace TKIP, ensuring authentication will occur

Question 149: In which type of matrix would you encounter the following items: Accountable, Consulted, Informed, Responsible?

A) Stakeholder Engagement Assessment Matrix

B) Responsibility Assignment Matrix

C) Power-Interest Matrix

D) Stakeholder Analysis Matrix

Question 150: In Information Systems Security, what term describes the wire in an electrical circuit that is connected to the earth?

A) Negative Pole

B) Positive Pole

C) Ground

D) Neutral Pole

Question 151

A security professional is tasked with implementing a system that combines hierarchical and compartmentalized

concepts, where each level can contain isolated sub-compartments. What type of mandatory access control environment is this?

A) Discretionary MAC

B) Attribute-Based MAC

C) Hybrid MAC

D) Role-Based MAC

Question 152

In the realm of computer security, what term describes an undocumented command sequence that allows individuals with specific knowledge to bypass standard access controls?

A) Mirage

B) Mirror

C) Trapdoor

D) Backdoor

Question 153

What is the term for an attack that enables hackers to covertly connect to Bluetooth devices and extract data, potentially accessing contact lists and conversations?

A) Blueprinting

B) Bluesnarfing

C) Bludgeoning

D) Bluefishing

Question 154

Which category of testing encompasses performance testing, load testing, volume testing, stress testing, security testing, installation testing, penetration testing, compatibility testing, and migration testing?

A) Functional Testing

B) Non-Functional Testing

C) Generic Testing

D) Focused Testing

Question 155

In cryptography, what provides the confidential component of the algorithm used for data encryption and decryption?

A) Authentic Key

B) Cryptographic Key

C) Master Key

D) Signature Keys

Question 156

A network administrator wants to implement a system that requires users to authenticate with an email address and agree to an acceptable use policy before accessing the network. What technology should be used?

A) A wireless gateway

B) A captive portal

C) NAC

D) 802.11

Question 157

In the context of cybercrime investigations, what term refers to any hardware, software, or data that can be used to prove an attacker's identity and actions in a legal setting?

A) A Witness

B) Impartial Testimony

C) Evidence

D) Expert Commentary

Question 158

What technology allows an automated tool to interact with a human interface to parse results and extract relevant information?

A) Vacuuming

B) Content Threading

C) Data Mining

D) Screen Scraping

Question 159

When configuring a wireless network, which three factors are most crucial for controlling signal strength and accessibility?

A) Antenna design, power levels, use of a captive portal

B) Power levels, antenna placement, FCC minimum strength requirements

C) Antenna placement, antenna type, and antenna power levels

D) Antenna placement, antenna design, use of a captive portal

Question 160

According to EU data protection law, what term describes a natural or legal person who processes personal data on behalf of the data controller?

A) Data Delegate

B) Data Programmer

C) Data Analyst

D) Data Processor

Question 161

What term describes the computing concept where processing and storage occur remotely over a network connection instead of locally?

A) Server Farm

B) Cloud Computing

C) WAN

D) VPN

Question 162

Which UDP port is commonly associated with the syslog service?

A) 515

B) 443

C) 445

D) 514

Question 163

What authentication method involves asking a series of questions about facts or predefined responses that only the subject should know?

A) Cognitive Password

B) Passphrase

C) One-Time Password

D) Multifactor Authentication

Question 164

In the modern project management waterfall model, what feature allows development to return to a previous phase to address defects discovered in a subsequent phase?

A) Rinse and Repeat Process

B) Recycle Phase

C) Feedback Loop Characteristic

D) Revisit Ability

Question 165

When a vendor prepares a product for Common Criteria evaluation, what document do they complete to describe the security claims of their product?

A) ITSEC

B) PP

C) ST

D) TCSEC

Question 166

What term describes a number generated from a text string that is substantially smaller than the original text and is extremely unlikely to be produced by any other text?

A) Validator Sum

B) Reverse Lookup

C) Hash Value

D) Key-Sum Value

Question 167

Which category of programming languages are not machine or assembly languages, are hardware-independent, more human-readable, and require conversion to machine language before or during execution?

A) High-Level Languages

B) Low-Level Languages

C) Hybrid-Level Languages

D) Middle-Level Languages

Question 168

During which disaster recovery test do team members discuss their response to a scenario without activating any disaster recovery controls?

A) Parallel Test

B) Full Interruption Test

C) Tabletop Exercise

D) Checklist Review

Question 169

What is the primary identifier associated with an 802.11 Wireless Local Area Network (WLAN) that client devices use to identify and join wireless networks?

A) MCS Index

B) Service Set Identifier (SSID)

C) Guard Interval

D) Wireless Mode

Question 170

What term describes the practice of recording keystrokes performed on a physical keyboard, either visually or through hardware/software means?

A) Clavicle Tapping

B) Genkey Recording

C) Keystroke Monitoring

D) Keystroke Patterns

Question 171

In legal contexts, what type of evidence is based on personal knowledge or observation and, if true, proves a fact without inference or presumption?

A) Direct Evidence

B) Real Evidence

C) Best Evidence

D) Primary Evidence

Question 172

To track and prevent abuse of an API by third-party users, what should be implemented?

A) An API firewall

B) An API buffer

C) Session IDs

D) API keys

Question 173

Which user category typically performs actions such as purging log entries, restoring systems from backups, and managing user accounts?

A) Manager user actions

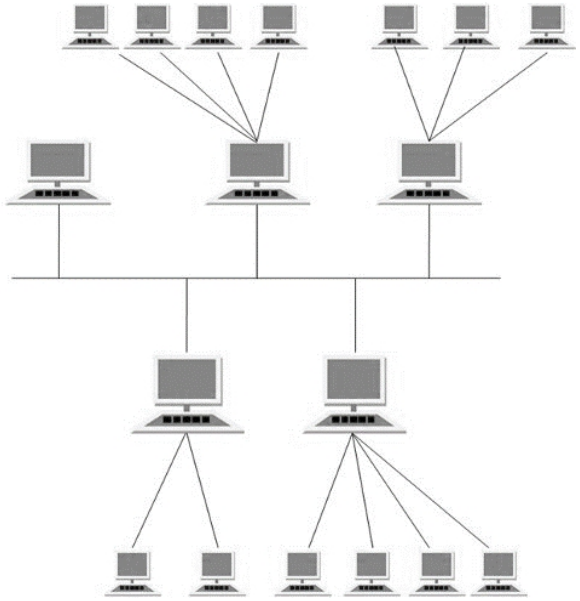
B) Level 1 user actions

C) Super user actions

D) Default user actions

Question 174

What type of network topology combines two or more different topologies, such as ring and star topologies in different departments of an office?



A) A tree

B) A bus

C) A hybrid

D) A mesh

Question 175

What concept involves separating network infrastructure from the control layer and allowing centralized, vendor-neutral network programming?

A) SDN, a converged protocol for network virtualization

B) MPLS, a method to replace long network addresses with shorter labels

C) FCoE, a converged protocol for common applications over Ethernet

D) CDN, a protocol for accessible network designs

Question 176

The United States government's Common Access Card (CAC) is an example of which Type 2 authentication factor?

A) A PIP

B) A token

C) A biometric identifier

D) A smart card

Question 177

What term describes temporary data stored on a client for future reuse, such as ARP cache, DNS cache, and Internet files cache?

A) Local Cache

B) Virtual Cache

C) Remote Cache

D) Swap Cache

Question 178

What type of attack involves compromising multiple systems to launch attacks against one or more victims, often using "slave" or "zombie" systems?

A) Cross-Site Scripting (XSS)

B) Distributed Denial of Service (DDoS)

C) OS Command Injection (OSCI)

D) Lightweight Directory Access Protocol (LDAP)

Question 179

What practice involves generating traffic on a network or system and monitoring the response or flow of the environment?

A) UAT Testing

B) Release Testing

C) Active Monitoring

D) Deployment Monitoring

Question 180

Which type of Denial of Service attack uses an amplifying server or network to flood a victim with useless data?

A) Popeye Attack

B) Smurf Attack

C) Rumpelstiltskin Attack

D) Micky Attack

Question 181

Which of the following is typically part of the business continuity planning process rather than disaster recovery?

A) Activation of cold sites

B) Alternate facility selection

C) Restoration of data from backup

D) Business impact assessment

Question 182

What process involves extracting specific elements from a large dataset to create a meaningful representation or summary?

A) Data Mining

B) Data Extraction

C) Data Abstraction

D) Data Tapping

Question 183

Which penetration testing technique is most effective for evaluating the effectiveness of security training and awareness programs?

A) Vulnerability scanning

B) Discovery

C) Social Engineering

D) Port scanning

Question 184

What legislation provides protection for Internet service providers against liability for copyrighted content illegally transmitted by their customers?

A) Wiretap Act

B) Copyright Code

C) Digital Millennium Copyright Act

D) Computer Fraud and Abuse Act

Question 185

What security design organizes code, components, and operating system elements into concentric rings with

varying levels of capabilities and access?

A) Protection Ring

B) Kernel Defence

C) Kill Chain Defense

D) Protection Core

Question 186

Which tool is most appropriate for testing known exploits against a system?

A) Metasploit

B) Nikto

C) Ettercap

D) THC Hydra

Question 187

What legislation criminalizes the invasion of individual electronic privacy and protects against unauthorized monitoring and disclosure of email and voicemail communications?

A) Radiocommunications Act of 1985

B) Communication and Speech Act (CSA)

C) Telecommunications Act of 2001

D) Electronic Communications Privacy Act (ECPA)

Question 188

What term describes the act of assuming someone's identity or online account, typically through spoofing and session replay, and is considered more active than masquerading?

A) ID Spoofing

B) Identity generation

C) Portrayal

D) Impersonation

Question 189

In the context of Information Systems Security, what type of attack uses a combination of non-sensitive information pieces to gain access to higher-classified information?

A) Attack Eavesdropping

B) Birthday Attack

C) Phishing Attack

D) Inference Attack

Question 190

In a mandatory access control system using Top Secret, Secret, Confidential, and Unclassified labels, what data can a user with secret clearance access?

A) Secret data only

B) Secret and Unclassified

C) Top Secret and Secret

D) Secret, Confidential, and Unclassified

Question 191

What type of Denial of Service attack uses oversized ping packets to potentially freeze, crash, or reboot the victim's system?

A) Smurf Attack

B) R.U.D.Y. attack

C) Ping-of-Death-Attack

D) Low and Slow Attack

Question 192

Which block cipher was developed to address concerns about the DES algorithm's key length, operating on 64-bit blocks with a 128-bit key?

A) Blockchain Data Encryption Algorithm (BDEA)

B) International Data Encryption Algorithm (IDEA)

C) Asymmetric Key Algorithm (AKA)

D) Symmetric Key Algorithm (SKA)

Question 193

What technique involves hiding individual data items in a database to prevent aggregation or inference attacks?

A) Cell Suppression

B) Data Cloaking

C) Dimensional Hiding

D) Content Phasing

Question 194

To ensure accountability in a centralized logging environment, what combination of practices is most effective?

A) Require authentication for all actions and centrally capture logs

B) Log administrative credentials and encrypt log data in transit

C) Require authorization and capture logs essentially

D) Review logs and require digital signatures for each log

Question 195

What biometric authentication factor uses speech, tone, modulation, and pitch patterns to establish identity?

A) Voice Pattern

B) Audio Pitch Variance

C) Oratory Fluctuation

D) Vocal Swing

Question 196

Which network protocol ensures that data is received correctly, completely, and in order?

A) IBM Protocol

B) UDP Protocol

C) AWS Protocol

D) TCP Protocol

Question 197

What testing technique provides various inputs to software to stress its limits and uncover previously undetected flaws?

A) Spoof Testing

B) Switch'em-Up Testing

C) Fuzz Testing

D) Albatross Testing

Question 198

Which computing model allows multiple processes to run on a single processor by having the operating system switch between them without modifying the applications?

A) Multiprocessing

B) Multitasking

C) Multiprogramming

D) Multithreading

Question 199

What is an undocumented command sequence that allows individuals with specific knowledge to bypass normal access restrictions?

A) Backdoor

B) Mirage

C) Mirror

D) Trapdoor

Question 200

Which of the following is an example of a biometric factor that uses unique behavioral or physiological characteristics for authentication?

A) Voice Pattern

B) Audio Pitch Variance

C) Oratory Fluctuation

D) Vocal Swing

Question 201

Bruce Banner would like to ask all of his staff to sign an agreement that they will not share his organization's intellectual property with unauthorized individuals.

What type of agreement should Bruce ask employees to sign?

A. NDA

B. DLP

C. OLA

D. SLA

Question 202

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] is the encryption standard selected in October 2000 by the National Institute of Standards and Technology (NIST) that is based on the Rijndael cypher.

A. Quantum Encryption Standard

B. Asymmetric Cryptographic Encryption Standard

C. Advanced Encryption Standard

D. Blockchain Encryption Standard

Question 203

What US law mandates the protection of protected health information?

A. HIPAA

B. FERPA

C. GLBA

D. SAFE Act

Question 204

Sally's organization needs to be able to prove that certain staff members sent emails, and she wants to adopt a technology that will provide that capability without changing their existing email system.

What is the technical term for the capability Sally needs to implement as the owner of the email system, and what tool could she use to do it?

A. Nonrepudiation; Digital signatures

B. Integrity; IMAP

C. Authentication; DKIM

D. Repudiation; Encryption

Question 205

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is the address that all devices within a given network grouping or container receive data on.

A. Intranet

B. Broadcast Address

C. Inbound Frequency

D. Very-High Frequency (FHF)

Question 206

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] is done on mobile devices with GPS support to enable the embedding of geographical locations in the form of latitude and longitude as well as date/time information on photos taken with these devices.

A. Geopositioning

B. Geomarking

C. Geolocating

D. Geotagging

Question 207

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] is a data classification label used for data that is for internal use or office use only. Often [?] is used to protect information that could violate the privacy rights of individuals.

A. Sensitive But Unclassified

B. Unclassified (General)

C. Prohibited

D. Level 10

Question 208

Cornelius would like to implement a control that protects his organization from the momentary loss of power to the data centre.

Which control was most appropriate for her needs?

A. Redundant servers

B. Generator

C. UPS

D. RAID

Question 209

Which one of the following backup types does not alter the status of the archive bit on a file?

A. Incremental backup

B. Differential backup

C. Full backup

D. Partial backup

Question 210

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] is evidence consisting of statements made to a witness by someone else outside of court. Computer log files that are not authenticated by a System Administrator can also be considered [?].

A. Demonstrative Evidence

B. Digital Evidence

C. Anecdotal Evidence

D. Hearsay Evidence

Question 211

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] is a type of authentication that uses two or more factors of authentication. [?] requires different factors (something-you-know, something-you-have, and something-you-are).

A. Real-Time Monitoring & Authentication

B. SSO Authentication

C. Active Directory Authentication

D. Multifactor Authentication

Question 212

What type of policy describes how long data is kept before destruction?

A. Classification

B. Record retention

C. Audit

D. Availability

Question 213

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is a specific key from the set of candidate keys that is used as the main differentiator between records. Every record must have a unique value in its [?] field.

A. Candidate Key

B. Unique Key

C. Primary Key

D. Foreign Key

Question 214

Aleta wants to monitor traffic between systems in a VMWare environment.

What solution would be her best option to monitor that traffic?

A. Install Wireshark on each virtual system.

B. Use netcat to capture all traffic sent between VMS.

C. Use a traditional hardware based IPS.

D. Set up a virtual span port and capture data using a VM IDs.

Question 215

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is an example of a biometric factor, which is behavioural or physical logical characteristic that is unique to a subject. The blood vessel pattern at the back of the eyeball is used to establish identity are provide authentication.

A. Octreotide Scan

B. Retina Scan

C. SPECT Scan

D. Gallium Scan

Question 216

Sanil, Richard, and Ravi would like to exchange messages with each other using symmetric cryptography. They want to ensure that each individual can privately send a message to the other without the third person being able to read the message.

How many keys do they need?

A. 6

B. 2

C. 3

D. 1

Question 217

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] refers to the combination of cryptography and cryptanalysis.

A. Cryptocurrency

B. Cryptographic Compliance

C. Cryptology

D. Blockchain

Question 218

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is a combination dry pipe/wet pipe system. The system exists as a dry pipe until the initial stages of a fire (smoke, heat, and so on) are detected and then the pipes are filled with water. The water is released only after the sprinkler head activation triggers are melted by sufficient heat.

A. PrePaK Systems

B. Preaction System

C. Conditional System Valves

D. Deluge System Valves

Question 219

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

The [?] system is another form of dry pipe (fire suppression) system that uses larger pipes and therefore a significantly larger volume of water.

A. Argonite

B. FM-200

C. Deluge

D. Pre-action

Question 220

Blade has been with the University he works at for over 10 years. During that time, he has been assistant administrator, a database administrator, and he has worked in the university’s help desk. He is now a manager for the team that runs the university's web applications.

Blade has access to B, C, and D. What concern should he raise to the university's identity management team.

A. Logging is not properly enabled.

B. Privilege creep may be taking place.

C. He has excessive privilege.

D. The provisioning process did not give him rights he needs.

Question 221

What problem drives the recommendation to physically destroy SSD drives to prevent data leaks when they are retired?

A. The built-in erase commands are not completely effective on SSDs.

B. SSDs don't have data remnants.

C. Degaussing only partially wipes the data on SSDs.

D. SSDs Are unable to perform a zero fill.

Question 222

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is a complete copy of data contained on the protected device on the backup media.

A. Incremental Backup

B. Virtual Backup

C. Full Backup

D. Cold Backup

Question 223

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is a firewall used to manage communication sessions between trusted partners in the OSI Model.

A. Transport

B. Human-Computer Interaction

C. Circuit Level Gateway Firewall

D. Presentation

Question 224

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] is a mechanism that allows devices to exchange data directly with real memory (RAM) without requiring assistance from the CPU.

A. SSD

B. HDD

C. SWAP

D. DMA

Question 225

Which one of the following metrics specifies the amount of time that business continuity planners believe it will take to restore a service when it goes down?

A. MTD

B. RTO

C. MTO

D. RPO

Question 226

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is a real barrier deployed to prevent direct contact with systems. Examples of [?] include guards, fences,

motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, swipe cards, dogs, CCTV, mantraps, and alarms.

A. Real Access Control

B. Logical Access Control

C. Physical Access Control

D. Tactual Access Control

Question 227

An accounting clerk for Dorian Gray’s Cheesecakes does not have access to the salary information for individual employees but wanted to know the salary of the new hire.

He pulled the total payroll expenses for the pay period before the new person was hired and then pulled the same expenses for the following pay period. He then computed the difference between those two amounts to determine the individual’s salary.

What type of attack occurred?

A. Aggregation Attack

B. Social Engineering Attack

C. Inference Attack

D. Data diddling Attack

Question 228

What law prevents the removal of protection mechanisms placed on a copyrighted work by the Copyright Holder?

A. DMCA

B. ECPA

C. HIPAA

D. GLBA

Question 229

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

The [?] is a law that states that anyone found guilty of stealing trade secrets from a US Corporation with the intention of benefiting a foreign government or agent may be fined up to $500,000 and imprisoned for up to 15 years and that anyone found guilty of stealing trade secrets under other circumstances may be fined up to $250,000 and imprisoned for up to 10 years.

A. The Economic Espionage Act of 1996

B. International Trade Secret Protection Act of 1987

C. Trade Secrets and Intellectual Property Protection Act of 1995

D. North American Free Trade Act of 1994

Question 230

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] refers to evidence of the highest quality available as measured by the nature of the case rather than the thing being offered as evidence.

A. Best Evidence

B. Presidential Evidence

C. Supreme Evidence

D. Crown Evidence

Question 231

In the diagram of the TCP three-way handshake here, what should system A send to system B in step three?

A. RST

B. FIN

C. ACK

D. SYN

Question 232

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is an enclosure that absorbs or blocks EM signals from entering or leaving the contained space.

A. Faraday Cage

B. SAML Block

C. Firewall

D. Gatekeeper

Question 233

In which cloud computing model does the customer build a cloud computing environment in his or her own data centre or build an environment in another data centre that is for the customers exclusive use?

A. Private Cloud

B. Public Cloud

C. Hybrid Cloud

D. Shared Cloud

Question 234

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] is a fire suppression system that is always full of water. Water discharges immediately when triggered by a fire or smoke.

A. Relay Pipe System

B. Triggered Pipe System

C. Wet Pipe System

D. Hybrid Pipe System

Question 235

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

A(n) [?] uses a set of rules, restrictions, or filters to determine what can and cannot occur on the system, such as granting subject access, performing an action on an object, or accessing a resource.

A. Discretionary Access Control

B. Role Based Access Control

C. Mandatory Access Control

D. Rule-Based Access Control

Question 236

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] refers to a risk management technique in which risk is assumed by a third party.

A. Risk acceptance

B. Risk mitigation

C. Risk Transfer

D. Risk avoidance

Question 237

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

The [?] is an extension of the state machine concept and serves as the basis of design for both the Biba and Bell-LaPadula models. This model consists of objects, state transitions, and lattice (flow policy) states. The real goal of this model is to prevent unauthorized, insecure information flow in any direction. This model and others can make use of

guards. Guards allow the exchange of data between various systems.

A. Information Flow Model

B. State Machine Model

C. Non-interference Model

D. Bell-LaPadula Model

Question 238

Using the following table and your knowledge of the auditing process, answer the below question.

As they prepare to migrate their data centre to an Infrastructure as a Service (IaaS) provider, Alflyse’s company wants to understand the effectiveness of their new provider security, integrity, and availability controls .

What SOC report would provide them with the most detail?

A. None of the SOC reports are suited to this and they should request another form of report.

B. SOC 3

C. SOC 1

D. SOC 2

Question 239

Jennifer needs to measure the effectiveness of her information security program as she works toward her organization's long term goals.

What type of measures should she select?

A. Metrics

B. KPIs

C. SLAs

D. OKRs

Question 240

What type of log file is shown in this figure?

A. Web server

B. Firewall

C. Application

D. System

Question 241

Which of the following multi factor authentication technologies provides both low management overhead and flexibility?

A. Biometrics

B. Asynchronous hardware tokens

C. Software tokens

D. Synchronous hardware tokens

Question 242

Alejandro is an incident response analyst for a large corporation. He is on the midnight shift when an intrusion detection system alerts him to a potential brute-force password attack against one of the company's critical information systems. He performs an initial triage of the event before taking any additional action.

As the incident response progress is, during which stage should the team conduct a root cause analysis?

A. Remediation

B. Response

C. Reporting

D. Lessons learned

Question 243

NIST Special Publication 800-115, the Technical Guide to Information Security Testing and Assessment, provides

NIST’s process for penetration testing.

Which of the following is not a typical part of a penetration test report?

A. Mitigation guidance for issues identified.

B. All sensitive data that was gathered during the test.

C. Risk ratings for each issue discovered.

D. A list of identified vulnerabilities.

Question 244

The large businesses Jack works for has been using noncentralized logging for years. They have recently started to implement centralized logging, however, as they have received logs they have discovered that a breach appeared to have involved a malicious insider.

How can Jack detect issues like this using his organization's new centralized logging?

A. Deploy and use IDS

B. Use syslog

C. Deploy and use a SIEM

D. Send logs to a central logging server

Question 245

The following are examples of what type of testing?

Vulnerability Scanning

Security Scanning

Penetration testing

Risk Assessment

Security Auditing

Ethical hacking

Posture Assessment

A. QAQC Testing

B. Beta Testing

C. Security Testing

D. Functional Testing

Question 246

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

An ISDN [?] uses your existing telephone line as a low-cost way to send voice and data at the same time, with digital clarity, speed, and reliability, over our digital network. A (n) [?] is an ISDN service type that provides two B (or data) channels and one D (or management) channel. Each B channel offers 64 Kbps, and the D channel offers 16 Kbps.

A. Basic Rate Interface (BRI)

B. Root Level Concatenation (RLC)

C. Primary Coupling Junction (PCJ)

D. Elemental Terminal Splice (ETS)

Question 247

Identify the missing word(s) in the following sentence within the context of Information Systems Security.

[?] is the act of gathering information from a system by observing the monitor or the use of the keyboard by the operator.

A. Form Copying

B. Social engineering

C. Screen Scraping

D. Shoulder Surfing

Question 248

Which type attack do the following fall under?

- Macro viruses
- File infectors
- System or boot-record infectors
- Polymorphic viruses
- Stealth viruses
- Trojans
- Logic bombs
- Worms
- Droppers
- Ransomware
- Adware
- Spyware

A. Malware attack

B. SQL injection attack

C. Man-in-the-Middle attack

D. Cross-site scripting attack

Question 249

CDMA, GSM, and IDEN are all examples of what generation of cellular technology?

A. 3G

B. 4G

C. 2G

D. 1G

Correct Answers & Explanations

Question 1

C) Administrative Access Controls (Correct Answer)

Explanation: Administrative Access Controls are the policies and procedures defined by an organization's security policy

to implement and enforce overall access control. These controls include policies, procedures, and guidelines that dictate how security measures should be implemented and managed within an organization.

Question 2

C) Asset Valuation (Correct Answer)

Explanation: Asset Valuation is the process of assigning a monetary value to an asset based on its actual cost and non-monetary expenses. This includes development, maintenance, administration, advertising, support, repair, and replacement costs. It's crucial for determining the true value of an asset in information systems security.

Question 3

B) Need to know (Correct Answer)

Explanation: The "need to know" principle is violated in this scenario. This principle states that users should only have access to the information and resources necessary for their specific job functions. When users can log into any workstation, even those assigned to different departments, they potentially gain access to information they don't need for their roles.

Question 4

C) RAID 10 (Correct Answer)

Explanation: RAID 10, also known as RAID 1+0, is often referred to as a "disk stripe of mirrors." It combines the mirroring of RAID 1 with the striping of RAID 0, providing both improved performance and fault tolerance.

Question 5

D) Type 3 (Correct Answer)

Explanation: In the context of authentication factors, a Smart Card is classified as Type 3, or "something you have." The three main types are: Type 1 (something you know, like

a password), Type 2 (something you are, like biometrics), and Type 3 (something you have, like a smart card or token).

Question 6

A) OR (Correct Answer)

Explanation: The logical OR operation, represented by the ∨ symbol, evaluates whether at least one input value is true. In Boolean algebra, the OR operation returns true if any of its operands are true.

Question 7

C) Binary Mathematics (Correct Answer)

Explanation: Binary Mathematics refers to the computational rules for bits and bytes used by computers. It's the foundation of all digital computing, involving operations on binary numbers (0s and 1s) that computers use to process and store data.

Question 8

A) Network (Correct Answer)

Explanation: Datagrams are associated with the Network layer (Layer 3) of the OSI model. This layer is responsible for packet forwarding, including routing through intermediate routers, and datagrams are the fundamental unit of information transfer in the IP protocol at this layer.

Question 9

B) Cat 5e and Cat 6 (Correct Answer)

Explanation: For a gigabit Ethernet network aiming to provide 1000 Mbps to users, the combination of Cat 5e and Cat 6 cables is most appropriate. Cat 5e can support gigabit speeds up to 100 meters, while Cat 6 offers even better performance and is more future-proof.

Question 10

C) Authentication Service (AS) (Correct Answer)

Explanation: In the Kerberos Key Distribution Centre (KDC), the Authentication Service (AS) is responsible for verifying or rejecting the authenticity and timeliness of tickets. It issues tickets to users who want to use services requiring authentication.

Question 11

C) Asynchronous (Correct Answer)

Explanation: Asynchronous communication relies on start and stop flags or bits to manage data transmission. This method doesn't require a continuous stream of data and allows for variable time intervals between transmissions, using start and stop indicators to signal the beginning and end of each data unit.

Question 12

D) Kerberos-based SSO (Correct Answer)

Explanation: Kerberos-based Single Sign-On (SSO) employs a trusted third party for identification and is based on tickets. It uses a ticket-granting system to authenticate users and provide access to various services without requiring multiple logins.

Question 13

A) OpenID Connect (Correct Answer)

Explanation: OpenID Connect is the most suitable authentication framework for integration with a cloud identity provider using OAuth 2.0. It's an identity layer built on top of OAuth 2.0, providing a standardized way to verify the identity of users and obtain basic profile information.

Question 14

D) Cross-domain SSO (Correct Answer)

Explanation: Cross-domain SSO creates an encrypted cookie on the user's machine containing credentials, allowing automatic login on subsequent visits. This type of SSO enables users to access multiple applications or domains with a single set of credentials, improving user experience and security.

Question 15

C) Online Certificate Status Protocol (OCSP) (Correct Answer)

Explanation: The Online Certificate Status Protocol (OCSP) provides real-time verification of a digital certificate's validity and confirms it hasn't been revoked by the issuing authority. It offers a more efficient and timely method of checking certificate status compared to Certificate Revocation Lists (CRLs).

Question 16

D) Eavesdropping attack (Correct Answer)

Explanation: An eavesdropping attack involves intercepting network traffic to obtain sensitive information like passwords and credit card numbers. This type of attack is passive, where the attacker secretly listens to the communication between two parties without their knowledge.

Question 17

C) Backend code on the web server (Correct Answer)

Explanation: To protect a web application's database from SQL injection attacks, the input validation routine should be placed in the backend code on the web server. This ensures that all input is validated before it reaches the database, regardless of the client-side environment or potential tampering with client-side code.

Question 18

B) X.509 (Correct Answer)

Explanation: X.509 is the ITU-T standard typically used when a Smart Card provides a certificate to an upstream authentication service. It defines the format of public key certificates and is widely used in various internet protocols, including TLS/SSL, which is the basis for HTTPS.

Question 19

B) Password Authentication Protocol (PAP) (Correct Answer)

Explanation: The Password Authentication Protocol (PAP) is an authentication protocol for Point-to-Point Protocol (PPP) that transmits usernames and passwords in clear text, offering no encryption. It's considered insecure due to this lack of encryption, making it vulnerable to interception.

Question 20

A) Nmap (Correct Answer)

Explanation: Nmap (Network Mapper) is a powerful and versatile penetration testing tool capable of performing port scans, ping sweeps, banner grabbing, and network discovery. It's widely used for network exploration, security auditing, and discovering open ports and services on a network.

Question 21

D) Authorization (Correct Answer)

Explanation: In a Linux system, the letters "rwx" in file attributes indicate Authorization. They represent Read (r), Write (w), and Execute (x) permissions, which determine what actions users are authorized to perform on the file or directory.

Question 22

C) PCI DSS (Correct Answer)

Explanation: For a Windows 10 system processing credit cards, the Payment Card Industry Data Security Standard (PCI DSS) is the most appropriate security standard. PCI DSS provides a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

Question 23

A) Depth (Correct Answer)

Explanation: In NIST Special Publication 800-53, "Depth" is the measure of developmental assurance that refers to the rigor, detail, and formality of artifacts produced during system component design and development. It indicates the level of scrutiny and thoroughness applied during the development process.

Question 24

C) Patent (Correct Answer)

Explanation: Among intellectual property protection mechanisms, patents typically have the shortest duration. In most countries, patents are granted for a fixed period, usually 20 years from the filing date, after which the invention enters the public domain. This is shorter than copyright protection and potentially shorter than trademark or trade secret protection.

Question 25

B) Elasticity (Correct Answer)

Explanation: Elasticity describes the ability of virtualization and cloud solutions to expand or contract based on need. This characteristic allows systems to automatically scale resources up or down to match demand, ensuring efficient resource utilization and cost-effectiveness in cloud computing environments.

Question 26

A) Remote journaling (Correct Answer)

Explanation: Remote journaling is the automated process that moves transaction records from a primary site to a backup site on an hourly basis in database recovery. This method ensures that the backup site has a near-real-time copy of the transaction logs, minimizing data loss in case of a disaster.

Question 27

C) RTO (Correct Answer)

Explanation: RTO (Recovery Time Objective) is the variable being calculated when determining the time it should take to restore an IT service after an outage in a disaster recovery plan. It represents the maximum tolerable length of time a computer, system, network, or application can be down after a failure or disaster occurs.

Question 28

C) Using device fingerprinting via a web-based registration system (Correct Answer)

Explanation: Device fingerprinting via a web-based registration system is the most reliable method for uniquely identifying BYOD devices not joined to a central management system. This technique collects a combination of device characteristics to create a unique identifier, making it more difficult to spoof than other methods.

Question 29

C) Database (Correct Answer)

Explanation: A database is an electronic filing system for organizing collections of information, typically structured with files, records, and fields. It allows for efficient storage, retrieval, and management of large amounts of structured data.

Question 30

A) Change Management (Correct Answer)

Explanation: Change Management is not typically considered one of the three main elements of the DevOps model. The three main elements are usually Development, Operations, and Quality Assurance. Change Management, while important, is a separate process that supports DevOps practices.

Question 31

A) Business Continuity Planning (BCP) (Correct Answer)

Explanation: Business Continuity Planning (BCP) is the process that involves assessing various risks to organizational processes and creating policies, plans, and procedures to minimize their potential impact. It aims to ensure that critical business functions can continue during and after a crisis.

Question 32

D) Assuming control of non-registered BYOD devices (Correct Answer)

Explanation: Assuming control of non-registered BYOD devices is not typically associated with Mobile Device Management (MDM) solutions. MDM solutions generally manage only devices that are enrolled in the system, and cannot take control of devices that are not registered or managed by the organization.

Question 33

B) It has a higher chance of detecting zero-day exploits than signature-based methods (Correct Answer)

Explanation: Heuristic-based anti-malware software has a higher chance of detecting zero-day exploits than signature-based methods. It uses behavioral analysis and pattern recognition to identify potentially malicious activity, even if the specific malware signature is unknown.

Question 34

B) Object (Correct Answer)

Explanation: In information systems security, an object is a passive entity that provides information or data to subjects, such as files, databases, or programs. Objects are resources that subjects (users or processes) act upon or interact with.

Question 35

C) Parallel Testing (Correct Answer)

Explanation: Parallel Testing involves relocating personnel to an alternate recovery site and implementing site activation procedures. This type of testing simulates a disaster scenario to evaluate the effectiveness of the recovery plan and the readiness of the alternate site.

Question 36

B) Kernel (Correct Answer)

Explanation: In a diagram of security boundaries within a computer system, the kernel typically refers to the central component that implements a secure, reliable operating system. It manages system resources and provides the most basic level of control over all hardware and software operations.

Question 37

C) Proof of authorization to access an object (Correct Answer)

Explanation: In Kerberos authentication, a Service Ticket (ST) provides proof of authorization to access an object. It is issued by the Ticket Granting Service (TGS) and allows a client to authenticate itself to a specific service.

Question 38

B) Functional Testing (Correct Answer)

Explanation: Functional Testing is the type of software testing that validates a system against its functional requirements by providing input and verifying output. It focuses on testing the functionality of the software system, ensuring that it behaves according to the specified requirements.

Question 39

D) Botnet (Correct Answer)

Explanation: A botnet is a collection of computers across the internet under an attacker's control. These compromised computers, often called "zombies," can be used to perform distributed attacks, send spam, or steal data without the knowledge of their owners.

Question 40

B) Denial of Service (Correct Answer)

Explanation: When a web server experiences unusually high traffic volume from a botnet, causing it to reject requests, it is classified as a Denial of Service (DoS) attack. This type of attack aims to overwhelm the server's resources, making it unavailable to legitimate users.

Question 41

C) Intranet (Correct Answer)

Explanation: An intranet is a private network designed to host the same information services found on the Internet, but accessible only within an organization. It uses Internet protocols and technologies to share information and resources internally.

Question 42

B) SPML (Correct Answer)

Explanation: SPML (Service Provisioning Markup Language) uses concepts like Requesting Authority, Provisioning Service Point, and Provisioning Service Target for handling

core functionality. It is an XML-based framework for managing the provisioning and allocation of identity information and system resources within and between organizations.

Question 43

C) CDDI (Correct Answer)

Explanation: CDDI (Copper Distributed Data Interface) is the deployment that uses FDDI with twisted-pair copper wires, reducing maximum segment length to 100 meters and increasing susceptibility to interference. It's a copper-based alternative to fiber optic FDDI, trading some performance for lower cost.

Question 44

A) JavaScript (Correct Answer)

Explanation: JavaScript would be least susceptible to third-party developers embedding backdoors due to its human-readable final form. As an interpreted language, JavaScript code is typically delivered in its source form, making it easier to inspect and audit compared to compiled languages.

Question 45

B) Qualitative Decision-Making (Correct Answer)

Explanation: Qualitative Decision-Making is the process that takes into account non-numerical factors such as emotions, investor/customer confidence, and workforce stability. It focuses on subjective, non-quantifiable information to make decisions.

Question 46

A) Password attack (Correct Answer)

Explanation: A password attack targets the most commonly used mechanism for authenticating users to information

systems. This type of attack attempts to gain unauthorized access by guessing or cracking user passwords.

Question 47

B) Honeynet/Honeypot (Correct Answer)

Explanation: A honeynet or honeypot is a computer or network designed to appear vulnerable and attract attackers, diverting them from legitimate systems. It's used as a security measure to detect, deflect, or study attempts at unauthorized use of information systems.

Question 48

D) Ciphertext (Correct Answer)

Explanation: Ciphertext is the term that describes a message that has been encrypted for transmission. It's the result of applying an encryption algorithm to plaintext, making the original message unreadable without the proper decryption key.

Question 49

D) Tailoring (Correct Answer)

Explanation: Tailoring is the process that involves reviewing and selecting security controls based on the specific IT system they will be applied to. It ensures that the chosen security controls are appropriate and effective for the particular system and its operating environment.

Question 50

D) Medical records check (Correct Answer)

Explanation: A medical records check is not typically performed during normal pre-hire activities. Such checks are generally considered invasive and are subject to strict privacy laws. The other options (criminal records check, credit check, and reference verification) are more common and legally permissible pre-employment screening methods.

Question 51

C) Countermeasures (Correct Answer)

Explanation: Countermeasures are specific actions taken to address vulnerabilities or protect systems from attacks. This term accurately describes the protective actions mentioned in the question, including adjusting security configurations, implementing new protective mechanisms, and modifying services.

Question 52

D) Computer Architecture (Correct Answer)

Explanation: Computer Architecture is the engineering discipline that focuses on designing computing systems at the logical level. It deals with the organization and structure of computer systems, including the design of processors, memory systems, and other hardware components.

Question 53

B) Automatic Private IP Addressing (APIPA) (Correct Answer)

Explanation: APIPA is a Windows feature that automatically assigns an IP address in the 169.254.0.0-169.254.255.255 range when DHCP assignment fails. This allows devices to communicate on a local network even without a DHCP server.

Question 54

B) Alpha Testing (Correct Answer)

Explanation: Alpha testing is performed by internal employees to identify potential issues before releasing a product to end users. It is typically conducted in a controlled environment by the development team or a dedicated testing team within the organization.

Question 55

D) Gray box (Correct Answer)

Explanation: Gray box testing combines elements of both black box and white box testing. In this approach, the tester has partial knowledge of the system's internal workings (source code) while also evaluating it from an end-user perspective for security flaws and usability.

Question 56

A) CBK (Correct Answer)

Explanation: CBK stands for Common Body of Knowledge, which is the term used by (ISC)2 to describe the comprehensive body of information that serves as the source material for the CISSP (Certified Information Systems Security Professional) exam.

Question 57

C) Foreign Key (Correct Answer)

Explanation: In database design, a foreign key is a field in one table that refers to the primary key in another table. It is used to establish and maintain relationships between tables in a relational database.

Question 58

C) Synchronous (Correct Answer)

Explanation: Synchronous data transmission relies on timing mechanisms like independent clocks or embedded timestamps to coordinate the sending and receiving of data. This ensures that data is transmitted and received in a coordinated manner.

Question 59

B) Accountability (Correct Answer)

Explanation: Accountability is the concept of holding individuals responsible for their actions. It involves assigning responsibility, tracking actions, and ensuring that individuals are answerable for the consequences of their decisions and behaviors.

Question 60

A) Performing exhaust analysis (Correct Answer)

Explanation: Performing exhaust analysis is not a key principle in the COBIT framework. The other options (meeting stakeholder needs, separating governance from management, and covering the enterprise end-to-end) are all fundamental principles of COBIT.

Question 61

C) Replay (Correct Answer)

Explanation: Replay monitoring involves recording data from real production workloads and then replaying it against a test environment to evaluate performance. This method allows for realistic testing without impacting the live production environment.

Question 62

A) Nonrepudiation (Correct Answer)

Explanation: Nonrepudiation is not explicitly included in the EU-US Privacy Shield provisions. The other options (Security, Access, and Enforcement) are key principles covered by the Privacy Shield framework to ensure data protection and privacy.

Question 63

C) Set the Secure attribute for the cookies (Correct Answer)

Explanation: Setting the Secure attribute for cookies is the most effective technique to prevent session hijacking. This ensures that cookies are only transmitted over HTTPS, encrypting the data and making it much harder for attackers to intercept or manipulate.

Question 64

B) Data Custodian (Correct Answer)

Explanation: Data Custodians are responsible for implementing the protection measures defined by security policies and management. They handle the day-to-day tasks of securing and maintaining data and systems according to established guidelines.

Question 65

D) Ring 3 (Correct Answer)

Explanation: In the ring protection model, Ring 3 operates in non-privileged mode. This is the outermost ring where user applications run, with the least privileges and access to system resources. Rings 0-2 have progressively higher privileges.

Question 66

A) Blowfish (Correct Answer)

Explanation: Blowfish is a block cipher that operates on 64-bit text blocks and uses variable-length keys ranging from 32 to 448 bits. It was designed as a fast, free alternative to existing encryption algorithms and is known for its flexibility in key size.

Question 67

B) SQL (Correct Answer)

Explanation: SQL (Structured Query Language) is the standard language used for interacting with relational databases. It allows users to create, read, update, and delete data in relational database management systems.

Question 68

D) PAT (Correct Answer)

Explanation: PAT (Port Address Translation) is typically used when an organization has limited public IP addresses but needs to connect many internal devices to the internet. It allows multiple devices to share a single public IP address

by mapping internal IP addresses and port numbers to the public IP.

Question 69

D) Secondary Evidence (Correct Answer)

Explanation: Secondary Evidence refers to evidence that includes copies made from original documents. This type of evidence is not the original source but is derived from it, such as photocopies, transcripts, or reproductions of original documents.

Question 70

B) Passive (Correct Answer)

Explanation: Passive monitoring is used to observe production servers using actual traffic for testing. This method involves capturing and analyzing real-time data without interfering with the normal operation of the system, allowing for accurate performance evaluation under real-world conditions.

Question 71

A) Blue Box (Correct Answer)

Explanation: A Blue Box is a device that generates in-band signaling tones to control telephone switches. Historically, it was used for bypassing toll collection by mimicking the tones used by telephone company equipment to route calls.

Question 72

B) ROM (Correct Answer)

Explanation: ROM (Read-Only Memory) is a type of computer memory that can be read but not written to under normal operating conditions. It is used to store firmware or software that rarely needs to be updated.

Question 73

D) Criminal (Correct Answer)

Explanation: Criminal forensic investigations typically have the most stringent standards for evidence. This is due to the higher burden of proof required in criminal cases and the potential consequences for the accused, necessitating rigorous evidence collection and handling procedures.

Question 74

D) Common Platform Enumeration (CPE) (Correct Answer)

Explanation: Common Platform Enumeration (CPE) is an SCAP component that provides a standardized naming system for operating systems, applications, and devices. It helps in identifying and categorizing IT products and platforms in a consistent manner.

Question 75

C) Subject's public key (Correct Answer)

Explanation: In asymmetric cryptography, a digital certificate issued by a Certificate Authority typically contains the subject's public key. This allows others to verify the authenticity of the certificate holder and encrypt messages intended for them using their public key.

Question 51

C) Countermeasures (Correct Answer)

Explanation: Countermeasures are specific actions taken to address vulnerabilities or protect systems from attacks. This term accurately describes the protective actions mentioned in the question, including adjusting security configurations, implementing new protective mechanisms, and modifying services.

Question 52

D) Computer Architecture (Correct Answer)

Explanation: Computer Architecture is the engineering discipline that focuses on designing computing systems at the logical level. It deals with the organization and structure

of computer systems, including the design of processors, memory systems, and other hardware components.

Question 53

B) Automatic Private IP Addressing (APIPA) (Correct Answer)

Explanation: APIPA is a Windows feature that automatically assigns an IP address in the 169.254.0.0-169.254.255.255 range when DHCP assignment fails. This allows devices to communicate on a local network even without a DHCP server.

Question 54

B) Alpha Testing (Correct Answer)

Explanation: Alpha testing is performed by internal employees to identify potential issues before releasing a product to end users. It is typically conducted in a controlled environment by the development team or a dedicated testing team within the organization.

Question 55

D) Gray box (Correct Answer)

Explanation: Gray box testing combines elements of both black box and white box testing. In this approach, the tester has partial knowledge of the system's internal workings (source code) while also evaluating it from an end-user perspective for security flaws and usability.

Question 56

A) CBK (Correct Answer)

Explanation: CBK stands for Common Body of Knowledge, which is the term used by (ISC)2 to describe the comprehensive body of information that serves as the source material for the CISSP (Certified Information Systems Security Professional) exam.

Question 57

C) Foreign Key (Correct Answer)

Explanation: In database design, a foreign key is a field in one table that refers to the primary key in another table. It is used to establish and maintain relationships between tables in a relational database.

Question 58

C) Synchronous (Correct Answer)

Explanation: Synchronous data transmission relies on timing mechanisms like independent clocks or embedded timestamps to coordinate the sending and receiving of data. This ensures that data is transmitted and received in a coordinated manner.

Question 59

B) Accountability (Correct Answer)

Explanation: Accountability is the concept of holding individuals responsible for their actions. It involves assigning responsibility, tracking actions, and ensuring that individuals are answerable for the consequences of their decisions and behaviors.

Question 60

A) Performing exhaust analysis (Correct Answer)

Explanation: Performing exhaust analysis is not a key principle in the COBIT framework. The other options (meeting stakeholder needs, separating governance from management, and covering the enterprise end-to-end) are all fundamental principles of COBIT.

Question 61

C) Replay (Correct Answer)

Explanation: Replay monitoring involves recording data from real production workloads and then replaying it against a test environment to evaluate performance. This method

allows for realistic testing without impacting the live production environment.

Question 62

A) Nonrepudiation (Correct Answer)

Explanation: Nonrepudiation is not explicitly included in the EU-US Privacy Shield provisions. The other options (Security, Access, and Enforcement) are key principles covered by the Privacy Shield framework to ensure data protection and privacy.

Question 63

C) Set the Secure attribute for the cookies (Correct Answer)

Explanation: Setting the Secure attribute for cookies is the most effective technique to prevent session hijacking. This ensures that cookies are only transmitted over HTTPS, encrypting the data and making it much harder for attackers to intercept or manipulate.

Question 64

B) Data Custodian (Correct Answer)

Explanation: Data Custodians are responsible for implementing the protection measures defined by security policies and management. They handle the day-to-day tasks of securing and maintaining data and systems according to established guidelines.

Question 65

D) Ring 3 (Correct Answer)

Explanation: In the ring protection model, Ring 3 operates in non-privileged mode. This is the outermost ring where user applications run, with the least privileges and access to system resources. Rings 0-2 have progressively higher privileges.

Question 66

A) Blowfish (Correct Answer)

Explanation: Blowfish is a block cipher that operates on 64-bit text blocks and uses variable-length keys ranging from 32 to 448 bits. It was designed as a fast, free alternative to existing encryption algorithms and is known for its flexibility in key size.

Question 67

B) SQL (Correct Answer)

Explanation: SQL (Structured Query Language) is the standard language used for interacting with relational databases. It allows users to create, read, update, and delete data in relational database management systems.

Question 68

D) PAT (Correct Answer)

Explanation: PAT (Port Address Translation) is typically used when an organization has limited public IP addresses but needs to connect many internal devices to the internet. It allows multiple devices to share a single public IP address by mapping internal IP addresses and port numbers to the public IP.

Question 69

D) Secondary Evidence (Correct Answer)

Explanation: Secondary Evidence refers to evidence that includes copies made from original documents. This type of evidence is not the original source but is derived from it, such as photocopies, transcripts, or reproductions of original documents.

Question 70

B) Passive (Correct Answer)

Explanation: Passive monitoring is used to observe production servers using actual traffic for testing. This

method involves capturing and analyzing real-time data without interfering with the normal operation of the system, allowing for accurate performance evaluation under real-world conditions.

Question 71

A) Blue Box (Correct Answer)

Explanation: A Blue Box is a device that generates in-band signaling tones to control telephone switches. Historically, it was used for bypassing toll collection by mimicking the tones used by telephone company equipment to route calls.

Question 72

B) ROM (Correct Answer)

Explanation: ROM (Read-Only Memory) is a type of computer memory that can be read but not written to under normal operating conditions. It is used to store firmware or software that rarely needs to be updated.

Question 73

D) Criminal (Correct Answer)

Explanation: Criminal forensic investigations typically have the most stringent standards for evidence. This is due to the higher burden of proof required in criminal cases and the potential consequences for the accused, necessitating rigorous evidence collection and handling procedures.

Question 74

D) Common Platform Enumeration (CPE) (Correct Answer)

Explanation: Common Platform Enumeration (CPE) is an SCAP component that provides a standardized naming system for operating systems, applications, and devices. It helps in identifying and categorizing IT products and platforms in a consistent manner.

Question 75

C) Subject's public key (Correct Answer)

Explanation: In asymmetric cryptography, a digital certificate issued by a Certificate Authority typically contains the subject's public key. This allows others to verify the authenticity of the certificate holder and encrypt messages intended for them using their public key.

Question 76

D) Hand-Scan (Correct Answer)

Explanation: Hand-scan is a biometric authentication method that uses the unique characteristics of a person's hand, including shape, size, and geometry, for identification or verification purposes. This technology captures a three-dimensional image of the hand and analyzes various measurements to create a unique template for each individual.

Question 77

A) It mandates a specific control set (Correct Answer)

Explanation: SSAE-18 (Statement on Standards for Attestation Engagements No. 18) does not mandate a specific control set. Instead, it provides a framework for conducting and reporting on various types of attestation engagements, including SOC 1, SOC 2, and SOC 3 reports. The standard allows organizations to define their own control objectives and related controls based on their specific needs and risks.

Question 78

C) DevOps (Correct Answer)

Explanation: DevOps is an approach that aims to integrate software development (Dev), quality assurance (QA), and technology operations (Ops) into a single, cohesive operational model. This methodology promotes collaboration, automation, and continuous improvement

throughout the software development lifecycle, leading to faster delivery, improved quality, and increased efficiency.

Question 79

A) HOSTS File (Correct Answer)

Explanation: The HOSTS file is a local system file that contains DNS entries preloaded into a cache when a system boots. It predates query-based DNS and allows for local name resolution without relying on external DNS servers. The HOSTS file can be used to override DNS settings or block access to specific websites by mapping hostnames to IP addresses.

Question 80

D) Dry Pipe (Correct Answer)

Explanation: A dry pipe fire suppression system contains compressed air in the pipes instead of water. When triggered, the air is released, opening a water valve and allowing water to fill the pipes and be discharged through sprinklers. This system is particularly useful in areas where freezing temperatures might cause water in the pipes to freeze and potentially damage the system.

Question 81

D) Public Cloud (Correct Answer)

Explanation: Public cloud refers to cloud computing services offered by third-party providers over the public internet, typically with on-demand pricing. These services are available to the general public and offer scalable, flexible resources that can be quickly provisioned and released with minimal management effort. Examples include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Question 82

B) Fortran (Correct Answer)

Explanation: Fortran (Formula Translation) is not an object-oriented programming language. It is a procedural programming language primarily used for scientific and engineering applications. The other options (C++, C#, and Java) are all object-oriented programming languages that support concepts such as classes, objects, inheritance, and polymorphism.

Question 83

A) Behaviour (Correct Answer)

Explanation: In object-oriented programming, the term "behaviour" describes the output or result from an object after processing a message using a method. Behaviour refers to the actions or operations that an object can perform in response to a message or method call. It encapsulates the functionality of an object and defines how it interacts with other objects in the system.

Question 84

A) Activation procedures for cold sites (Correct Answer)

Explanation: An organization's emergency response guidelines should include activation procedures for cold sites. Cold sites are backup facilities that contain the necessary infrastructure to resume operations but lack equipment and data. Including activation procedures for cold sites ensures that the organization can quickly establish operations at an alternate location during an emergency, supporting business continuity efforts.

Question 85

B) Smart Card-based SSO (Correct Answer)

Explanation: Smart Card-based Single Sign-On (SSO) is a method where a user inserts a smart card into a reader to access multiple applications. The smart card contains the user's credentials and cryptographic keys, providing a secure and convenient way to authenticate across various

systems and applications without the need to enter multiple passwords.

Question 86

C) Transmission Control Protocol (TCP) (Correct Answer)

Explanation: TCP (Transmission Control Protocol) is a connection-oriented protocol that operates at layer 4 (Transport layer) of the OSI model. TCP establishes a reliable, ordered, and error-checked connection between two hosts before data transmission begins. It ensures that data packets are delivered in the correct order and without errors, making it suitable for applications that require guaranteed delivery of data.

Question 87

A) White Box (Correct Answer)

Explanation: White Box testing is a software testing method where the tester has full knowledge of the system's internal structure, design, and implementation before beginning the testing process. This approach allows testers to examine the code, logic, and data flow of the application, enabling them to create more targeted and comprehensive test cases based on the system's internal workings.

Question 88

D) SDNs (Correct Answer)

Explanation: SDNs (Software-Defined Networks) is a networking approach that separates the infrastructure layer from the control layer to increase flexibility and reduce vendor lock-in. SDN centralizes network intelligence and control, allowing for more dynamic and programmable network configurations. This separation enables network administrators to manage network services through abstraction, making it easier to adapt to changing requirements and implement new technologies.

Question 89

D) RADIUS (Correct Answer)

Explanation: RADIUS (Remote Authentication Dial-In User Service) is used to centralize authentication for VPN connections, including legacy dial-up and broadband internet connections. RADIUS provides authentication, authorization, and accounting (AAA) services for network access, allowing organizations to manage user access to various network resources from a central server.

Question 90

C) Whitelisting (Correct Answer)

Explanation: Whitelisting is the most appropriate application control approach when limiting users to installing only approved software. This method involves creating a list of authorized applications that are allowed to run on a system, while blocking all other software by default. Whitelisting provides a higher level of security compared to blacklisting, as it prevents the execution of any unauthorized or potentially malicious applications.

Question 91

B) /etc/shadow (Correct Answer)

Explanation: On modern, security-conscious Linux systems, password hashes are typically stored in the /etc/shadow file. This file is only readable by the root user, providing an additional layer of security compared to the older method of storing hashes in the world-readable /etc/passwd file.

Question 92

B) Type 3 (Correct Answer)

Explanation: Type 3 authentication factors, also known as "something you are" or inherence factors, refer to biometric characteristics such as fingerprints, voice prints, or retina

patterns. These are unique physical attributes of an individual used for authentication purposes.

Question 93

A) Class (Correct Answer)

Explanation: In object-oriented programming, a class is a blueprint or template that defines the common attributes and behaviors (methods) of a set of objects. It encapsulates data for the object and defines how the object will behave.

Question 94

C) Automated recovery without undue data loss (Correct Answer)

Explanation: In trusted recovery, automated recovery without undue data loss refers to a system's ability to automatically recover from failures while protecting against data loss, without requiring administrator intervention. This type of recovery includes additional mechanisms to protect specific objects on the system.

Question 95

A) Bell-LaPadula (Correct Answer)

Explanation: The Bell-LaPadula model includes the *-property (star property) which states that a subject at a given security level cannot write data to a higher security level. This is often referred to as "no write up" and is a key component of the model's focus on maintaining confidentiality.

Question 96

C) Cognitive passwords (Correct Answer)

Explanation: Cognitive passwords, also known as security questions or knowledge-based authentication, require users to answer predefined personal questions for authentication. These questions are based on information that should be known only to the user.

Question 97

A) Thin Client (Correct Answer)

Explanation: A thin client is a lightweight computer that is purpose-built for remoting into a server. It depends heavily on another computer (its server) to fulfill its computational roles and has minimal local processing or storage capacity.

Question 98

B) SYN/ACK (Correct Answer)

Explanation: In a TCP three-way handshake, the responding system (usually the server) sends a SYN/ACK (Synchronization/Acknowledgement) packet in the second step. This acknowledges the initial SYN packet from the client and continues the process of establishing the connection.

Question 99

A) DDoS (Correct Answer)

Explanation: The Low Orbit Ion Cannon (LOIC) is a tool often used in Distributed Denial of Service (DDoS) attacks. In a DDoS attack, multiple compromised systems (often home PCs acting as "zombies") are used to target a single system, overwhelming it with traffic or requests.

Question 100

C) Expert Witness (Correct Answer)

Explanation: In the US legal system, an expert witness is a person with specialized knowledge or experience who can provide testimony consisting of expert opinions and facts. Their role is to assist the court in understanding complex technical or scientific matters relevant to the case

Question 101:

C) Algorithm (Correct Answer)

Explanation: An algorithm is a set of step-by-step procedures or rules designed to perform a specific task or solve a particular problem. In cryptography, algorithms are used to define the precise steps for encrypting and decrypting data, ensuring the security and confidentiality of information.

Question 102:

D) PIN (Correct Answer)

Explanation: A Personal Identification Number (PIN) is a numeric code assigned to an individual for identification and authentication purposes. It is typically used in conjunction with a card or device to access secure systems or accounts, and it should be kept confidential to maintain security.

Question 103:

B) Pretty Good Privacy (PGP) (Correct Answer)

Explanation: Pretty Good Privacy (PGP) is an email encryption protocol that provides authentication, integrity, confidentiality, and non-repudiation. It operates at the application layer (Layer 7) of the OSI model and utilizes various cryptographic algorithms, including RSA for key exchange, DES for symmetric encryption, and X.509 for digital certificates.

Question 104:

B) Link state protocol (Correct Answer)

Explanation: OSPF (Open Shortest Path First) is a link state routing protocol. It maintains a complete map of the network topology and uses this information to calculate the shortest path to each destination. Link state protocols are more efficient and scalable than distance vector protocols for large networks.

Question 105:

B) RAID 1 (Correct Answer)

Explanation: RAID 1, also known as disk mirroring, is a configuration where data is written identically to two or more drives. This provides redundancy and improves read performance, as data can be read from multiple disks simultaneously. In case of a drive failure, the mirrored copy ensures data availability.

Question 106:

B) RSA (Correct Answer)

Explanation: RSA (Rivest-Shamir-Adleman) is a widely used public-key cryptosystem that meets all the described criteria. Developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, it uses the factorization of large prime numbers for its security. RSA is particularly suitable for both encryption and digital signatures, providing confidentiality and authentication.

Question 107:

D) Malicious Code (Correct Answer)

Explanation: Malicious code refers to a broad category of software designed to infiltrate, damage, or disrupt computer systems without the user's consent. This includes viruses, worms, trojans, and other types of malware that exploit various vulnerabilities in networks, operating systems, and software to propagate and execute harmful actions.

Question 108:

C) 2 (Correct Answer)

Explanation: To restore the system to its most current state, Tarra needs to apply two backups: the last full backup (from Sunday) and the most recent differential backup (from Wednesday noon). Differential backups contain all changes since the last full backup, so only the latest differential backup is needed along with the full backup.

Question 109:

D) Criminal investigation (Correct Answer)

Explanation: Criminal investigations consistently use the "beyond a reasonable doubt" standard of evidence. This high standard is required in criminal cases to protect the rights of the accused and ensure that a conviction is based on overwhelming evidence of guilt, minimizing the risk of wrongful convictions.

Question 110:

D) Its TGT (Correct Answer)

Explanation: In a Kerberos authentication scenario, when a client wants to access a resource after initial authentication, it sends its Ticket Granting Ticket (TGT) to the Key Distribution Center (KDC). The TGT, obtained during initial authentication, proves the client's identity and is used to request service tickets for specific resources without re-entering credentials.

Question 111:

D) Fragmentation (Correct Answer)

Explanation: Fragmentation attacks exploit vulnerabilities in the way TCP/IP protocols handle the reassembly of fragmented packets. Attackers can manipulate packet fragments to bypass security measures or cause system crashes. This type of attack takes advantage of the complexity involved in properly reassembling fragmented data.

Question 112:

A) Notice, choice, onward transfer, security, data integrity, access, enforcement (Correct Answer)

Explanation: The EU-US Privacy Shield Framework is built on seven principles that ensure adequate protection for personal data transferred from the EU to the US. These principles cover the entire data lifecycle, from collection to

use and transfer, and include mechanisms for individual rights and enforcement.

Question 113:

B) Isolation (Correct Answer)

Explanation: Isolation in Information Systems Security refers to the principle of containing processes and their associated resources within defined boundaries. This ensures that the behavior or failure of one process does not affect others, enhancing system stability and security by preventing unauthorized access or interference between different processes.

Question 114:

B) Worm (Correct Answer)

Explanation: A worm is a type of malware that can replicate and spread across networks without human intervention. Unlike viruses, which require a host file to propagate, worms contain built-in propagation mechanisms that exploit system vulnerabilities to spread autonomously, making them particularly dangerous in networked environments.

Question 115:

D) 1000BaseT (Correct Answer)

Explanation: 1000BaseT, also known as Gigabit Ethernet, is a standard for twisted-pair Ethernet cables that supports 1 Gbps (Gigabit per second) data transmission speeds over distances up to 100 meters. It uses all four pairs of wires in a Cat5e or Cat6 cable to achieve this high-speed performance.

Question 116:

C) Darknet (Correct Answer)

Explanation: A darknet is an intentionally unused portion of IP address space within a network. It is often used as a security measure to monitor for unauthorized network

activity, detect potential attacks, or analyze malware behavior. Traffic directed to these unused addresses is likely to be malicious, making darknets valuable for network security monitoring.

Question 117:

B) Sanil's private key (Correct Answer)

Explanation: When creating a digital signature, the sender (Sanil) uses their private key to encrypt a hash of the message. This ensures that only Sanil could have created the signature (non-repudiation) and allows the recipient (Richard) to verify the signature using Sanil's public key, thus authenticating the message's origin and integrity.

Question 118:

B) Patching a leaky roof (Correct Answer)

Explanation: Patching a leaky roof is a physical hardening measure that directly addresses a vulnerability in the facility's infrastructure. This type of improvement can prevent water damage to equipment and data, potentially avoiding the need to implement a business continuity plan due to environmental damage. The other options are IT security measures, not physical facility improvements.

Question 119:

C) TACACS+ (Correct Answer)

Explanation: TACACS+ (Terminal Access Controller Access-Control System Plus) is a proprietary Cisco protocol that provides authentication, authorization, and accounting (AAA) services. It is widely used in Cisco environments and supports two-factor authentication, making it a popular alternative to RADIUS for network device administration and access control.

Question 120:

B) Hand Geometry (Correct Answer)

Explanation: Hand Geometry is a biometric authentication method that measures and analyzes the shape and size of an individual's hand, including finger length, width, and thickness. This technique provides a unique identifier for each person and is used in various access control systems for its reliability and user acceptance.

Question 121:

D) Decision Support System (DSS) (Correct Answer)

Explanation: A Decision Support System (DSS) is an information system that analyzes business data and presents it in a way that helps users make informed decisions. DSS typically combines data from various sources, provides analytical tools, and offers interactive interfaces to support complex decision-making processes in organizations.

Question 122:

C) EAP originally assumed the use of physically isolated channels and did not include encryption (Correct Answer)

Explanation: The original Extensible Authentication Protocol (EAP) was designed for point-to-point connections and assumed a secure, isolated channel. PEAP (Protected EAP) addresses this limitation by encapsulating EAP within a TLS tunnel, providing encryption and protecting the authentication process from eavesdropping and man-in-the-middle attacks in less secure network environments.

Question 123:

B) Responsibility Assignment Matrix (Correct Answer)

Explanation: The Responsibility Assignment Matrix, often referred to as a RACI matrix (Responsible, Accountable, Consulted, Informed), is a project management tool used to clarify roles and responsibilities in projects or processes. It defines who is responsible for tasks, who is accountable for

decisions, who should be consulted, and who needs to be kept informed throughout the project lifecycle.

Question 124:

C) Ground (Correct Answer)

Explanation: In electrical systems, the ground wire is connected to the earth, providing a reference point for voltage measurements and a path for excess electrical current to dissipate safely. Proper grounding is crucial for electrical safety, protecting equipment and people from electrical faults and reducing electromagnetic interference.

Question 125:

A) Birthday Attack (Correct Answer)

Explanation: A Birthday Attack is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. In the context of digital signatures, an attacker attempts to find two different messages that produce the same hash value (collision), potentially allowing the substitution of a fraudulent message while maintaining a valid signature. This attack is named after the surprising probability of shared birthdays in a small group of people.

Question 126:

D) Directive (Correct Answer)

Explanation: Directive controls are policies, procedures, or guidelines that direct employees on proper behavior. The notifications reminding employees to be cautious about allowing people to enter are a form of directive control, as they provide instructions on how to behave in a specific security-related situation.

Question 127:

C) Algorithm (Correct Answer)

Explanation: An algorithm is a set of step-by-step procedures or rules designed to perform a specific task. In cryptography, algorithms define the precise steps for encrypting and decrypting data, ensuring the security and confidentiality of information through mathematical operations.

Question 128:

D) PIN (Correct Answer)

Explanation: A Personal Identification Number (PIN) is a numeric code assigned to an individual for identification and authentication purposes. It is typically used in conjunction with a card or device to access secure systems or accounts and should be kept confidential to maintain security.

Question 129:

B) Pretty Good Privacy (PGP) (Correct Answer)

Explanation: Pretty Good Privacy (PGP) is an email encryption protocol that provides authentication, integrity, confidentiality, and non-repudiation. It operates at the application layer (Layer 7) of the OSI model and utilizes various cryptographic algorithms, including RSA for key exchange, DES for symmetric encryption, and X.509 for digital certificates.

Question 130:

B) Link state protocol (Correct Answer)

Explanation: OSPF (Open Shortest Path First) is a link state routing protocol. It maintains a complete map of the network topology and uses this information to calculate the shortest path to each destination. Link state protocols are more efficient and scalable than distance vector protocols for large networks.

Question 131:

B) RAID 1 (Correct Answer)

Explanation: RAID 1, also known as disk mirroring, is a configuration where data is written identically to two or more drives. This provides redundancy and improves read performance, as data can be read from multiple disks simultaneously. In case of a drive failure, the mirrored copy ensures data availability.

Question 132:

B) RSA (Correct Answer)

Explanation: RSA (Rivest-Shamir-Adleman) is a widely used public-key cryptosystem that meets all the described criteria. Developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, it uses the factorization of large prime numbers for its security. RSA is particularly suitable for both encryption and digital signatures, providing confidentiality and authentication.

Question 133:

D) Malicious Code (Correct Answer)

Explanation: Malicious code refers to a broad category of software designed to infiltrate, damage, or disrupt computer systems without the user's consent. This includes viruses, worms, trojans, and other types of malware that exploit various vulnerabilities in networks, operating systems, and software to propagate and execute harmful actions.

Question 134:

C) 2 (Correct Answer)

Explanation: To restore the system to its most current state, Tarra needs to apply two backups: the last full backup (from Sunday) and the most recent differential backup (from Wednesday noon). Differential backups contain all changes since the last full backup, so only the latest differential backup is needed along with the full backup.

Question 135:

D) Criminal investigation (Correct Answer)

Explanation: Criminal investigations consistently use the "beyond a reasonable doubt" standard of evidence. This high standard is required in criminal cases to protect the rights of the accused and ensure that a conviction is based on overwhelming evidence of guilt, minimizing the risk of wrongful convictions.

Question 136:

D) Its TGT (Correct Answer)

Explanation: In a Kerberos authentication scenario, when a client wants to access a resource after initial authentication, it sends its Ticket Granting Ticket (TGT) to the Key Distribution Center (KDC). The TGT, obtained during initial authentication, proves the client's identity and is used to request service tickets for specific resources without re-entering credentials.

Question 137:

D) Fragmentation (Correct Answer)

Explanation: Fragmentation attacks exploit vulnerabilities in the way TCP/IP protocols handle the reassembly of fragmented packets. Attackers can manipulate packet fragments to bypass security measures or cause system crashes. This type of attack takes advantage of the complexity involved in properly reassembling fragmented data.

Question 138:

A) Notice, choice, onward transfer, security, data integrity, access, enforcement (Correct Answer)

Explanation: The EU-US Privacy Shield Framework is built on seven principles that ensure adequate protection for personal data transferred from the EU to the US. These principles cover the entire data lifecycle, from collection to

use and transfer, and include mechanisms for individual rights and enforcement.

Question 139:

B) Isolation (Correct Answer)

Explanation: Isolation in Information Systems Security refers to the principle of containing processes and their associated resources within defined boundaries. This ensures that the behavior or failure of one process does not affect others, enhancing system stability and security by preventing unauthorized access or interference between different processes.

Question 140:

B) Worm (Correct Answer)

Explanation: A worm is a type of malware that can replicate and spread across networks without human intervention. Unlike viruses, which require a host file to propagate, worms contain built-in propagation mechanisms that exploit system vulnerabilities to spread autonomously, making them particularly dangerous in networked environments.

Question 141:

D) 1000BaseT (Correct Answer)

Explanation: 1000BaseT, also known as Gigabit Ethernet, is a standard for twisted-pair Ethernet cables that supports 1 Gbps (Gigabit per second) data transmission speeds over distances up to 100 meters. It uses all four pairs of wires in a Cat5e or Cat6 cable to achieve this high-speed performance.

Question 142:

C) Darknet (Correct Answer)

Explanation: A darknet is an intentionally unused portion of IP address space within a network. It is often used as a security measure to monitor for unauthorized network

activity, detect potential attacks, or analyze malware behavior. Traffic directed to these unused addresses is likely to be malicious, making darknets valuable for network security monitoring.

Question 143:

B) Sanil's private key (Correct Answer)

Explanation: When creating a digital signature, the sender (Sanil) uses their private key to encrypt a hash of the message. This ensures that only Sanil could have created the signature (non-repudiation) and allows the recipient (Richard) to verify the signature using Sanil's public key, thus authenticating the message's origin and integrity.

Question 144:

B) Patching a leaky roof (Correct Answer)

Explanation: Patching a leaky roof is a physical hardening measure that directly addresses a vulnerability in the facility's infrastructure. This type of improvement can prevent water damage to equipment and data, potentially avoiding the need to implement a business continuity plan due to environmental damage. The other options are IT security measures, not physical facility improvements.

Question 145:

C) TACACS+ (Correct Answer)

Explanation: TACACS+ (Terminal Access Controller Access-Control System Plus) is a proprietary Cisco protocol that provides authentication, authorization, and accounting (AAA) services. It is widely used in Cisco environments and supports two-factor authentication, making it a popular alternative to RADIUS for network device administration and access control.

Question 146:

B) Hand Geometry (Correct Answer)

Explanation: Hand Geometry is a biometric authentication method that measures and analyzes the shape and size of an individual's hand, including finger length, width, and thickness. This technique provides a unique identifier for each person and is used in various access control systems for its reliability and user acceptance.

Question 147:

D) Decision Support System (DSS) (Correct Answer)

Explanation: A Decision Support System (DSS) is an information system that analyzes business data and presents it in a way that helps users make informed decisions. DSS typically combines data from various sources, provides analytical tools, and offers interactive interfaces to support complex decision-making processes in organizations.

Question 148:

C) EAP originally assumed the use of physically isolated channels and did not include encryption (Correct Answer)

Explanation: The original Extensible Authentication Protocol (EAP) was designed for point-to-point connections and assumed a secure, isolated channel. PEAP (Protected EAP) addresses this limitation by encapsulating EAP within a TLS tunnel, providing encryption and protecting the authentication process from eavesdropping and man-in-the-middle attacks in less secure network environments.

Question 149:

B) Responsibility Assignment Matrix (Correct Answer)

Explanation: The Responsibility Assignment Matrix, often referred to as a RACI matrix (Responsible, Accountable, Consulted, Informed), is a project management tool used to clarify roles and responsibilities in projects or processes. It defines who is responsible for tasks, who is accountable for

decisions, who should be consulted, and who needs to be kept informed throughout the project lifecycle.

Question 150:

C) Ground (Correct Answer)

Explanation: In electrical systems, the ground wire is connected to the earth, providing a reference point for voltage measurements and a path for excess electrical current to dissipate safely. Proper grounding is crucial for electrical safety, protecting equipment and people from electrical faults and reducing electromagnetic interference.

Question 151

C) Hybrid MAC (Correct Answer)

Explanation: A Hybrid Mandatory Access Control (MAC) environment combines hierarchical and compartmentalized concepts. This type of system allows for both vertical (hierarchical) and horizontal (compartmentalized) segregation of information, where each level can contain isolated sub-compartments. It provides a more flexible and granular approach to access control, allowing for complex security structures that can accommodate various organizational needs.

Question 152

D) Backdoor (Correct Answer)

Explanation: A backdoor in computer security refers to an undocumented command sequence or method that allows individuals with specific knowledge to bypass standard access controls. It's often created by system designers or hackers for gaining unauthorized access. Unlike a trapdoor, which is typically a legitimate debugging tool, a backdoor is generally considered a security vulnerability.

Question 153

B) Bluesnarfing (Correct Answer)

Explanation: Bluesnarfing is a specific type of attack targeting Bluetooth-enabled devices. It allows hackers to covertly connect to these devices and extract data without the owner's knowledge or consent. This can include accessing contact lists, calendars, emails, and even eavesdropping on conversations. The term combines "Blue" from Bluetooth and "snarfing," which in hacker jargon means to steal or copy data.

Question 154

B) Non-Functional Testing (Correct Answer)

Explanation: Non-Functional Testing encompasses a wide range of tests that evaluate the operational aspects of a software application, rather than its specific behaviors. This includes performance testing, load testing, volume testing, stress testing, security testing, installation testing, penetration testing, compatibility testing, and migration testing. These tests focus on how well the system performs under various conditions, its reliability, scalability, and overall quality attributes.

Question 155

B) Cryptographic Key (Correct Answer)

Explanation: In cryptography, a Cryptographic Key is the confidential component of the algorithm used for data encryption and decryption. It's a piece of information that determines the functional output of a cryptographic algorithm. The security of encrypted data is directly tied to the protection of this key. Without the correct key, even if an attacker knows the algorithm, they cannot decrypt the data.

Question 156

B) A captive portal (Correct Answer)

Explanation: A captive portal is the technology that should be used when a network administrator wants to implement a system requiring users to authenticate with an email

address and agree to an acceptable use policy before accessing the network. It's a web page that is displayed to newly connected users before they are granted broader access to network resources. Captive portals are commonly used in public Wi-Fi hotspots and can enforce authentication, payment, or agreement to terms of service.

Question 157

C) Evidence (Correct Answer)

Explanation: In the context of cybercrime investigations, Evidence refers to any hardware, software, or data that can be used to prove an attacker's identity and actions in a legal setting. This can include log files, network traffic captures, hard drives, mobile devices, or any other digital artifacts that can be presented in court to support the case. Proper handling and preservation of digital evidence is crucial for maintaining its admissibility in legal proceedings.

Question 158

D) Screen Scraping (Correct Answer)

Explanation: Screen Scraping is a technology that allows an automated tool to interact with a human interface to parse results and extract relevant information. It's used to programmatically gather data from web pages or applications that don't offer more convenient data access methods like APIs. Screen scraping tools simulate human web browsing, interpreting the displayed output and extracting the desired data, often when no other automated access is available.

Question 159

C) Antenna placement, antenna type, and antenna power levels (Correct Answer)

Explanation: When configuring a wireless network, the three most crucial factors for controlling signal strength and accessibility are antenna placement, antenna type, and

antenna power levels. Antenna placement affects the coverage area and signal penetration through obstacles. Antenna type determines the radiation pattern and gain. Power levels directly impact the signal strength and range. Together, these factors allow network administrators to optimize wireless coverage while minimizing interference and unauthorized access.

Question 160

D) Data Processor (Correct Answer)

Explanation: According to EU data protection law, specifically the General Data Protection Regulation (GDPR), a Data Processor is a natural or legal person who processes personal data on behalf of the data controller. The data processor acts on the instructions of the data controller and doesn't have decision-making power over the purposes and means of processing. This role is crucial in ensuring compliance with data protection regulations and maintaining the privacy and security of personal data.

Question 161

B) Cloud Computing (Correct Answer)

Explanation: Cloud Computing describes the computing concept where processing and storage occur remotely over a network connection instead of locally. It allows users to access computing resources (like servers, storage, databases, networking, software) over the internet, on-demand, without direct active management by the user. This model offers benefits such as scalability, flexibility, and cost-effectiveness, as resources can be rapidly provisioned and released with minimal management effort.

Question 162

D) 514 (Correct Answer)

Explanation: UDP port 514 is commonly associated with the syslog service. Syslog is a standard protocol used for

computer message logging, allowing separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. It's widely used for system management and security auditing. While some implementations may use TCP, traditionally syslog uses UDP port 514 for log message transmission.

Question 163

A) Cognitive Password (Correct Answer)

Explanation: A Cognitive Password is an authentication method that involves asking a series of questions about facts or predefined responses that only the subject should know. This method relies on the user's personal knowledge or experiences, which are difficult for an attacker to guess or obtain. Examples might include questions about childhood memories, favorite books, or significant life events. It's a form of knowledge-based authentication that adds an extra layer of security beyond traditional passwords.

Question 164

C) Feedback Loop Characteristic (Correct Answer)

Explanation: In the modern project management waterfall model, the Feedback Loop Characteristic allows development to return to a previous phase to address defects discovered in a subsequent phase. This feature adds flexibility to the traditional linear waterfall model, enabling teams to iterate and improve based on findings in later stages. It helps in catching and fixing issues earlier in the development process, potentially saving time and resources in the long run.

Question 165

C) ST (Correct Answer)

Explanation: When a vendor prepares a product for Common Criteria evaluation, they complete a Security Target (ST)

document to describe the security claims of their product. The ST defines the security problem, security objectives, security requirements, and summary specification for the product being evaluated. It's a key document in the Common Criteria evaluation process, providing a detailed description of the security functionality claimed by the product and the assurance measures used to test those claims.

Question 166

C) Hash Value (Correct Answer)

Explanation: A Hash Value is a number generated from a text string that is substantially smaller than the original text and is extremely unlikely to be produced by any other text. Hash functions are designed to be one-way, meaning it's computationally infeasible to reverse the process and obtain the original input from the hash value. They are widely used in cryptography, data integrity checks, and efficient data storage and retrieval. The uniqueness and fixed size of hash values make them ideal for tasks like digital signatures and password storage.

Question 167

A) High-Level Languages (Correct Answer)

Explanation: High-Level Languages are programming languages that are not machine or assembly languages, are hardware-independent, more human-readable, and require conversion to machine language before or during execution. These languages use abstractions to make programming easier and more intuitive for humans. Examples include Python, Java, and C++. They offer features like automatic memory management and complex data structures, allowing programmers to focus on problem-solving rather than low-level hardware details. High-level languages typically need to be compiled or interpreted to run on a computer.

Question 168

C) Tabletop Exercise (Correct Answer)

Explanation: A Tabletop Exercise is a disaster recovery test where team members discuss their response to a scenario without activating any disaster recovery controls. It's a low-stress, discussion-based session where team members meet in an informal setting to review their roles during an emergency and their responses to a particular emergency situation. This type of exercise helps in identifying gaps in plans and procedures, improving team coordination, and familiarizing staff with their responsibilities in a crisis, all without the cost and disruption of a full-scale simulation.

Question 169

B) Service Set Identifier (SSID) (Correct Answer)

Explanation: The Service Set Identifier (SSID) is the primary identifier associated with an 802.11 Wireless Local Area Network (WLAN) that client devices use to identify and join wireless networks. It's essentially the name of the wireless network that is broadcast by the access point. When a device scans for available networks, it sees a list of SSIDs. Users can then select the desired network to connect to. The SSID plays a crucial role in network identification and is a fundamental component of Wi-Fi network configuration and management.

Question 170

C) Keystroke Monitoring (Correct Answer)

Explanation: Keystroke Monitoring describes the practice of recording keystrokes performed on a physical keyboard, either visually or through hardware/software means. This can be done for various purposes, including security monitoring, productivity tracking, or malicious intent (keylogging malware). In a security context, it can be used to detect unauthorized access attempts or to monitor

employee activities. However, it also raises significant privacy concerns and may be subject to legal restrictions in many jurisdictions.

Question 171

A) Direct Evidence (Correct Answer)

Explanation: In legal contexts, Direct Evidence is evidence based on personal knowledge or observation and, if true, proves a fact without inference or presumption. This type of evidence directly establishes a fact in question without the need for additional reasoning. Examples include eyewitness testimony, video recordings of an event, or a confession. Direct evidence is contrasted with circumstantial evidence, which requires inference to connect it to a conclusion of fact. In legal proceedings, direct evidence is often considered stronger and more persuasive than circumstantial evidence.

Question 172

D) API keys (Correct Answer)

Explanation: API keys should be implemented to track and prevent abuse of an API by third-party users. An API key is a unique identifier used to authenticate a user, developer, or calling program to an API. It helps in monitoring and controlling how the API is being used, allowing the API provider to track usage, enforce rate limits, and revoke access if necessary. API keys also add a layer of security by ensuring that only authorized parties can access the API. They're essential for managing access, preventing abuse, and maintaining the integrity and performance of the API service.

Question 173

C) Super user actions (Correct Answer)

Explanation: Super user actions typically include tasks such as purging log entries, restoring systems from backups, and

managing user accounts. A super user, often referred to as the root user in Unix-like systems or an administrator in Windows, has the highest level of access and control over a system. These privileged users can perform critical system operations, modify system configurations, and access all files and resources. Due to the extensive power of super user accounts, their use is typically restricted and carefully monitored to maintain system security and integrity.

Question 174

C) A hybrid (Correct Answer)

Explanation: A hybrid network topology combines two or more different topologies, such as ring and star topologies in different departments of an office. This approach allows organizations to leverage the strengths of multiple topologies to meet specific needs in different parts of the network. For example, a company might use a star topology for its main office for centralized management, while using a ring topology in a manufacturing plant for reliability. Hybrid topologies offer flexibility and can be optimized for performance, reliability, and scalability based on the requirements of different network segments.

Question 175

A) SDN, a converged protocol for network virtualization (Correct Answer)

Explanation: Software-Defined Networking (SDN) is the concept that involves separating network infrastructure from the control layer and allowing centralized, vendor-neutral network programming. SDN decouples the network control and forwarding functions, enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. This approach allows for more flexible and efficient network management, enabling administrators to respond quickly to changing business requirements. SDN

facilitates network virtualization and allows for more dynamic, automated, and programmable network configurations.

Question 176

D) A smart card (Correct Answer)

Explanation: The United States government's Common Access Card (CAC) is an example of a smart card, which is a Type 2 authentication factor. Smart cards are physical devices that contain embedded integrated circuits for storing and processing data. They provide a higher level of security than traditional magnetic stripe cards by requiring a PIN for access and using cryptographic protocols for data protection. CACs are used for both physical access to facilities and logical access to computer networks, combining identification, authentication, and digital signature capabilities in a single device.

Question 177

A) Local Cache (Correct Answer)

Explanation: Local Cache refers to temporary data stored on a client device for future reuse. This includes various types of caches such as ARP cache (for mapping IP addresses to MAC addresses), DNS cache (for storing recently resolved domain names), and Internet files cache (for storing web content). Local caching improves system performance by reducing the need to repeatedly fetch the same data from external sources. It speeds up operations by providing quick access to frequently used information, but it also requires proper management to ensure data consistency and security.

Question 178

B) Distributed Denial of Service (DDoS) (Correct Answer)

Explanation: A Distributed Denial of Service (DDoS) attack involves compromising multiple systems to launch attacks

against one or more victims, often using "slave" or "zombie" systems. In a DDoS attack, the attacker uses numerous compromised computers (often referred to as a botnet) to flood the target system or network with traffic, overwhelming its resources and making it unavailable to legitimate users. This distributed nature makes DDoS attacks particularly challenging to mitigate, as the traffic comes from many different sources simultaneously.

Question 179

C) Active Monitoring (Correct Answer)

Explanation: Active Monitoring is the practice of generating traffic on a network or system and monitoring the response or flow of the environment. This approach involves proactively sending requests or stimuli to network components and analyzing their responses. It allows administrators to measure performance, detect issues, and assess the health of network services in real-time. Unlike passive monitoring, which only observes existing traffic, active monitoring can provide more detailed insights into specific aspects of network or system behavior, helping to identify potential problems before they impact users.

Question 180

B) Smurf Attack (Correct Answer)

Explanation: A Smurf Attack is a type of Denial of Service attack that uses an amplifying server or network to flood a victim with useless data. In this attack, the attacker sends ICMP echo request packets (pings) to a network broadcast address, spoofing the source IP address to be that of the intended victim. All hosts on the network then respond to these requests, sending a flood of ICMP echo reply packets to the victim's IP address. This amplifies the attack, as a single packet sent by the attacker results in numerous packets being sent to the victim, potentially overwhelming their network resources.

Question 181

D) Business impact assessment (Correct Answer)

Explanation: A Business Impact Assessment (BIA) is typically part of the business continuity planning process rather than disaster recovery. The BIA is a crucial step in developing a comprehensive business continuity plan. It involves analyzing business functions and the effect that a business disruption might have upon them. This assessment helps identify critical business processes, potential losses in case of a disruption, and the resources required to recover essential operations. Unlike disaster recovery, which focuses on restoring IT systems and infrastructure, the BIA takes a broader view of the entire business operation and its dependencies.

Question 182

C) Data Abstraction (Correct Answer)

Explanation: Data Abstraction is the process of extracting specific elements from a large dataset to create a meaningful representation or summary. This technique involves identifying the essential features or patterns within complex data and presenting them in a simplified form. Data abstraction is crucial in data analysis and visualization, as it allows for the creation of models or representations that capture the essence of the data without overwhelming details. It helps in making large datasets more manageable and understandable, facilitating better decision-making and insight generation.

Question 183

C) Social Engineering (Correct Answer)

Explanation: Social Engineering is the most effective penetration testing technique for evaluating the effectiveness of security training and awareness programs. This approach involves attempting to manipulate individuals

into divulging confidential information or performing actions that may compromise security. By simulating real-world social engineering attacks (such as phishing emails, pretexting calls, or impersonation attempts), organizations can assess how well their employees apply security training in practice. This method directly tests human behavior and decision-making, which are often the weakest links in an organization's security posture.

Question 184

C) Digital Millennium Copyright Act (Correct Answer)

Explanation: The Digital Millennium Copyright Act (DMCA) provides protection for Internet service providers against liability for copyrighted content illegally transmitted by their customers. Enacted in 1998, the DMCA implements two 1996 World Intellectual Property Organization (WIPO) treaties and addresses a number of copyright-related issues. It includes "safe harbor" provisions that protect service providers from copyright infringement liability for simply transmitting information over the Internet or storing it on behalf of customers. However, this protection is contingent on the service providers meeting certain conditions, such as promptly removing infringing material when notified.

Question 185

A) Protection Ring (Correct Answer)

Explanation: A Protection Ring is a security design that organizes code, components, and operating system elements into concentric rings with varying levels of capabilities and access. This concept, also known as hierarchical protection domains, is used in computer security to isolate different levels of system access. Typically, a system might have multiple rings, with the innermost ring (Ring 0) having the highest privileges and direct access to hardware, while outer rings have progressively fewer privileges. This design helps to protect

critical system components from less trusted code, enhancing overall system security and stability.

Question 186

A) Metasploit (Correct Answer)

Explanation: Metasploit is the most appropriate tool for testing known exploits against a system. It is an open-source penetration testing framework that provides a comprehensive platform for developing, testing, and executing exploit code. Metasploit contains a large database of known vulnerabilities and corresponding exploit modules, allowing security professionals to simulate real-world attacks on their systems. It can be used to test the effectiveness of security controls, identify vulnerabilities, and demonstrate the potential impact of successful exploits. This makes it an invaluable tool for both offensive security testing and defensive security validation.

Question 187

D) Electronic Communications Privacy Act (ECPA) (Correct Answer)

Explanation: The Electronic Communications Privacy Act (ECPA) criminalizes the invasion of individual electronic privacy and protects against unauthorized monitoring and disclosure of email and voicemail communications. Enacted in 1986 and amended several times since, the ECPA extends government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. It prohibits unauthorized access to stored electronic communications and regulates the use of pen registers and trap and trace devices. The Act aims to balance the government's legitimate law enforcement needs with protecting the privacy of citizens in the digital age.

Question 188

D) Impersonation (Correct Answer)

Explanation: Impersonation describes the act of assuming someone's identity or online account, typically through spoofing and session replay, and is considered more active than masquerading. In cybersecurity, impersonation attacks involve an attacker actively pretending to be a legitimate user or system to gain unauthorized access or privileges. This can include using stolen credentials, creating fake profiles, or manipulating communication protocols to appear as a trusted entity. Impersonation is more sophisticated than simple masquerading, as it often involves real-time interaction and may require detailed knowledge of the impersonated entity's characteristics or behaviors.

Question 189

D) Inference Attack (Correct Answer)

Explanation: An Inference Attack, in the context of Information Systems Security, uses a combination of non-sensitive information pieces to gain access to higher-classified information. This type of attack exploits the ability to deduce sensitive information from a collection of less sensitive data points. Attackers use logical reasoning, statistical analysis, or data correlation to infer protected information without directly accessing it. For example, an attacker might combine publicly available information with seemingly innocuous data from a database to deduce confidential details. Inference attacks are particularly challenging to defend against as they often involve data that is not inherently sensitive when viewed in isolation.

Question 190

D) Secret, Confidential, and Unclassified (Correct Answer)

Explanation: In a mandatory access control system using Top Secret, Secret, Confidential, and Unclassified labels, a user with secret clearance can access Secret, Confidential, and Unclassified data. This follows the principle of hierarchical access in mandatory access control systems,

where users can access information at their clearance level and all lower levels. The hierarchy from highest to lowest is typically: Top Secret > Secret > Confidential > Unclassified. Therefore, a user with Secret clearance has access to Secret and all lower classifications but cannot access Top Secret information. This structure ensures that sensitive information is only accessible to those with appropriate clearance levels.

Question 191

C) Ping-of-Death-Attack (Correct Answer)

Explanation: A Ping-of-Death Attack is a type of Denial of Service attack that uses oversized ping packets to potentially freeze, crash, or reboot the victim's system. In this attack, the attacker sends ping packets that exceed the maximum IP packet size of 65,535 bytes. When these oversized packets are reassembled at the receiving end, they can overflow memory buffers, causing system crashes or reboots. While modern systems are generally patched against this specific vulnerability, variations of this attack can still be effective against improperly configured or outdated systems. The Ping-of-Death Attack exploits vulnerabilities in how systems handle fragmented IP packets.

Question 192

B) International Data Encryption Algorithm (IDEA) (Correct Answer)

Explanation: The International Data Encryption Algorithm (IDEA) is a block cipher developed to address concerns about the DES algorithm's key length, operating on 64-bit blocks with a 128-bit key. IDEA was designed as a replacement for DES and was first described in 1991. It uses a series of eight identical transformations and a complex key-schedule to encrypt data. The 128-bit key length provides significantly stronger security compared to DES's

56-bit key. IDEA's design principles influenced later encryption standards and it was widely used in PGP (Pretty Good Privacy) for email encryption.

Question 193

A) Cell Suppression (Correct Answer)

Explanation: Cell Suppression is a technique that involves hiding individual data items in a database to prevent aggregation or inference attacks. This method is commonly used in statistical databases and data publishing to protect sensitive information while still allowing useful analysis. In cell suppression, specific cells or data points are removed or replaced with a placeholder (like an asterisk) to prevent the disclosure of sensitive information. This technique is particularly useful when the combination of multiple non-sensitive data points could lead to the inference of sensitive information. Cell suppression requires careful implementation to balance data utility with privacy protection.

Question 194

A) Require authentication for all actions and centrally capture logs (Correct Answer)

Explanation: To ensure accountability in a centralized logging environment, the most effective combination of practices is to require authentication for all actions and centrally capture logs. This approach ensures that every action is tied to a specific, authenticated user, creating a clear audit trail. Authentication helps prevent unauthorized access and ensures that each log entry can be attributed to a specific individual. Centralized log capture allows for comprehensive monitoring and analysis of all system activities across the organization. This combination provides a robust framework for detecting suspicious activities, investigating incidents, and maintaining compliance with security policies and regulations.

Question 195

A) Voice Pattern (Correct Answer)

Explanation: Voice Pattern is a biometric authentication factor that uses speech, tone, modulation, and pitch patterns to establish identity. This method analyzes the unique characteristics of an individual's voice, including factors like accent, speaking style, and vocal tract shape. Voice pattern recognition systems typically create a voiceprint or voice model for each user, which is then compared to live samples for authentication. This biometric factor is particularly useful for remote authentication scenarios, such as telephone banking or voice-activated security systems. Voice pattern authentication can be more user-friendly than other biometric methods but may be affected by factors like background noise or changes in the user's voice due to illness.

Question 196

D) TCP Protocol (Correct Answer)

Explanation: The Transmission Control Protocol (TCP) is the network protocol that ensures data is received correctly, completely, and in order. TCP is a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data between applications running on hosts communicating over an IP network. It achieves this through mechanisms such as sequence numbers for ordering packets, acknowledgments for confirming receipt, and retransmission of lost packets. TCP also includes flow control and congestion control features to prevent overwhelming the receiver or the network. These characteristics make TCP ideal for applications requiring high reliability, such as web browsing, email, and file transfers.

Question 197

C) Fuzz Testing (Correct Answer)

Explanation: Fuzz Testing is a testing technique that provides various inputs to software to stress its limits and uncover previously undetected flaws. This method involves inputting massive amounts of random data, called fuzz, into the system in an attempt to make it crash. Fuzz testing is particularly effective at finding security vulnerabilities, such as buffer overflows, memory leaks, and input validation errors. It can uncover edge cases and unexpected behaviors that might not be detected through conventional testing methods. Fuzz testing tools can generate a wide range of inputs, including valid, invalid, and malformed data, to thoroughly test the robustness and security of software applications.

Question 198

B) Multitasking (Correct Answer)

Explanation: Multitasking is the computing model that allows multiple processes to run on a single processor by having the operating system switch between them without modifying the applications. In a multitasking environment, the CPU rapidly switches between different tasks or processes, giving the illusion that multiple programs are running simultaneously. This is achieved through time-sharing, where each process is allocated a certain amount of CPU time before being paused to allow another process to run. Multitasking improves overall system efficiency and responsiveness by allowing the CPU to work on other tasks while waiting for I/O operations to complete. It's a fundamental feature of modern operating systems, enabling users to run multiple applications concurrently on a single-processor system.

Question 199

A) Backdoor (Correct Answer)

Explanation: A Backdoor is an undocumented command sequence that allows individuals with specific knowledge to

bypass normal access restrictions. Backdoors are often created by system developers for troubleshooting or maintenance purposes but can also be maliciously inserted by attackers. They provide a way to access a system or application while circumventing normal authentication procedures. Backdoors can take various forms, such as hidden user accounts, specific keystroke combinations, or specially crafted network packets that trigger unauthorized access. While sometimes used legitimately, backdoors are generally considered a significant security risk as they can be exploited by malicious actors to gain unauthorized access to systems.

Question 200

A) Voice Pattern (Correct Answer)

Explanation: Voice Pattern is an example of a biometric factor that uses unique behavioral or physiological characteristics for authentication. Voice pattern recognition analyzes the unique aspects of an individual's voice, including pitch, tone, and speech patterns. This biometric method falls under both behavioral (how a person speaks) and physiological (the physical structure of the vocal tract) categories. Voice pattern authentication systems create a voiceprint of the user, which is then compared to live samples during the authentication process. This method is non-invasive and can be used for remote authentication, making it suitable for various applications like telephone banking or voice-activated security systems.

Question 201

A) NDA (Correct Answer)

Explanation: An NDA (Non-Disclosure Agreement) is the appropriate type of agreement for Bruce Banner to use in this situation. NDAs are legal contracts that bind employees to keep confidential information, trade secrets, and intellectual property private. This agreement protects the

organization's sensitive information from being shared with unauthorized individuals, which is exactly what Bruce wants to achieve.

Question 202

C) Advanced Encryption Standard (Correct Answer)

Explanation: The Advanced Encryption Standard (AES) is the encryption standard selected by NIST in October 2000. It is based on the Rijndael cipher, which was chosen for its combination of security, performance, efficiency, and flexibility. AES has become the de facto standard for symmetric encryption in many applications and is widely used in government and commercial systems.

Question 203

A) HIPAA (Correct Answer)

Explanation: HIPAA (Health Insurance Portability and Accountability Act) is the US law that mandates the protection of protected health information (PHI). Enacted in 1996, HIPAA sets national standards for the security and privacy of electronic protected health information, including requirements for how healthcare providers, health plans, and healthcare clearinghouses must handle and safeguard patients' medical information.

Question 204

A) Nonrepudiation; Digital signatures (Correct Answer)

Explanation: Nonrepudiation is the technical term for the capability Sally needs to implement. It ensures that a party cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Digital signatures are the tool that can provide this capability without changing the existing email system. They use cryptographic techniques to create a unique, verifiable "signature" for each email, ensuring the sender cannot later deny sending it.

Question 205

B) Broadcast Address (Correct Answer)

Explanation: A broadcast address is the network address at which all devices connected to a multiple-access communications network are enabled to receive datagrams. It's a special address in IPv4 networks that allows information to be sent to all devices on a network simultaneously. When a packet is sent to the broadcast address, it is delivered to all hosts on that network segment.

Question 206

D) Geotagging (Correct Answer)

Explanation: Geotagging is the process of adding geographical identification metadata to various media such as photographs, video, websites, or SMS messages. In the context of mobile devices with GPS support, geotagging involves embedding the latitude and longitude coordinates, as well as time and date information, into the metadata of photos taken with these devices. This allows for easy organization, searching, and sharing of location-specific information.

Question 207

A) Sensitive But Unclassified (Correct Answer)

Explanation: "Sensitive But Unclassified" (SBU) is a data classification label used for information that is not classified but is still sensitive and requires protection. This designation is often used in government and corporate settings for data that is intended for internal use only and could potentially violate individual privacy rights if disclosed. It's a way to ensure that information is handled with care without requiring the stringent controls associated with classified information.

Question 208

C) UPS (Correct Answer)

Explanation: A UPS (Uninterruptible Power Supply) is the most appropriate control for protecting against momentary loss of power to the data center. A UPS is a device that provides emergency power to a load when the main power source fails. It provides near-instantaneous protection from input power interruptions by supplying energy stored in batteries. This makes it ideal for protecting against brief power outages or fluctuations, giving time for systems to properly shut down or for backup generators to start up in case of longer outages.

Question 209

B) Differential backup (Correct Answer)

Explanation: A differential backup does not alter the status of the archive bit on a file. In a differential backup, all files that have changed since the last full backup are copied, but the archive bit is not reset. This means that subsequent differential backups will continue to include all files that have changed since the last full backup, regardless of whether they were included in previous differential backups. This is in contrast to incremental backups, which do reset the archive bit, and full backups, which back up all files and reset all archive bits.

Question 210

D) Hearsay Evidence (Correct Answer)

Explanation: Hearsay evidence refers to testimony from a witness under oath who is reciting an out-of-court statement that is being offered to prove the truth of the matter asserted. In the context of information systems security, computer log files that are not authenticated by a System Administrator can be considered hearsay evidence because they are essentially out-of-court statements that haven't been verified by a competent witness. This type of evidence

is often considered less reliable and may be inadmissible in court unless it falls under specific exceptions to the hearsay rule.

Question 211

D) Multifactor Authentication (Correct Answer)

Explanation: Multifactor Authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. It combines two or more independent credentials: what the user knows (password), what the user has (security token), and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network, or database.

Question 212

B) Record retention (Correct Answer)

Explanation: A record retention policy describes how long data is kept before destruction. This type of policy is crucial for organizations to manage their information lifecycle, comply with legal and regulatory requirements, and minimize both storage costs and legal risks. Record retention policies typically specify the types of records to be retained, the duration of retention for each type of record, the method of storage, and the proper procedures for destruction when the retention period expires.

Question 213

C) Primary Key (Correct Answer)

Explanation: A Primary Key is a specific key from the set of candidate keys that is used as the main differentiator between records in a database table. It is a unique identifier for each record in a table, ensuring that every record can be uniquely identified and accessed. The primary key must

contain unique values and cannot contain null values. It is used to establish relationships between tables in a relational database and to enforce the integrity and consistency of the data.

Question 214

D) Set up a virtual span port and capture data using a VM IDs (Correct Answer)

Explanation: In a VMWare environment, setting up a virtual span port and capturing data using VM IDs is the best option for monitoring traffic between systems. This method allows for comprehensive traffic monitoring without the need to install additional software on each virtual machine or use physical hardware. A virtual span port can mirror traffic from multiple virtual machines to a single monitoring point, allowing Aleta to capture and analyze all inter-VM traffic efficiently. This approach is less intrusive, more scalable, and provides a more complete view of the virtual network traffic compared to the other options.

Question 215

B) Retina Scan (Correct Answer)

Explanation: A retina scan is an example of a biometric factor used for authentication. It involves analyzing the unique patterns of blood vessels in the retina, which is the light-sensitive tissue at the back of the eye. Retina scans are considered one of the most accurate and secure forms of biometric authentication because the retinal vascular pattern is unique to each individual and remains stable throughout a person's lifetime. This method is highly resistant to forgery and provides a high level of security for access control systems.

Question 216

A) 6 (Correct Answer)

Explanation: In this scenario, Sanil, Richard, and Ravi need 6 keys to exchange messages privately using symmetric cryptography. With symmetric cryptography, the same key is used for both encryption and decryption. To ensure that each person can send a message to either of the other two without the third person being able to read it, each pair of individuals needs a unique shared key. The number of keys needed can be calculated using the formula n(n-1)/2, where n is the number of people. In this case, with 3 people, the calculation is 3(3-1)/2 = 3, which equals 6 keys.

Question 217

C) Cryptology (Correct Answer)

Explanation: Cryptology refers to the combination of cryptography and cryptanalysis. It is the scientific study of codes, ciphers, and related algorithms. Cryptography is the practice and study of techniques for secure communication in the presence of adversaries, focusing on creating and analyzing protocols that prevent third parties from reading private messages. Cryptanalysis, on the other hand, is the study of methods for obtaining the meaning of encrypted information without access to the secret information normally required to do so. Together, these two disciplines form the field of cryptology.

Question 218

B) Preaction System (Correct Answer)

Explanation: A preaction system is a type of fire suppression system that combines features of both dry pipe and wet pipe systems. In normal conditions, the pipes are filled with air or nitrogen, similar to a dry pipe system. However, when the initial stages of a fire are detected (through smoke detectors, heat sensors, etc.), the pipes are filled with water. The water is only released when the heat from the fire melts the sprinkler head activation triggers. This two-stage process helps prevent accidental discharge and water

damage in sensitive areas while still providing rapid fire suppression when needed.

Question 219

C) Deluge (Correct Answer)

Explanation: A deluge system is a type of fire suppression system that uses larger pipes and therefore holds a significantly larger volume of water compared to standard sprinkler systems. In a deluge system, all sprinkler heads are open, and there are no fusible links or glass bulbs to be melted or broken. When activated, water flows through all sprinklers simultaneously, providing rapid and extensive coverage. This type of system is typically used in high-hazard areas where fast-spreading fires are a concern, such as in aircraft hangars, power plants, or chemical storage facilities.

Question 220

B) Privilege creep may be taking place (Correct Answer)

Explanation: Privilege creep is the gradual accumulation of access rights beyond what an individual needs to perform their current job responsibilities. In Blade's case, having worked in various roles over 10 years, he has likely accumulated access rights from his previous positions (assistant administrator, database administrator, help desk) in addition to his current role as a web applications team manager. This accumulation of unnecessary privileges poses a security risk as it violates the principle of least privilege. Blade should raise this concern to the identity management team so they can review and adjust his access rights to match his current job requirements, reducing potential security vulnerabilities.

Question 221

A) The built-in erase commands are not completely effective on SSDs. (Correct Answer)

Explanation: SSDs use a different technology than traditional hard drives, making conventional data erasure methods less effective. The built-in erase commands may not completely remove all data due to wear-leveling algorithms and over-provisioning in SSDs. These features can leave remnants of data in areas not accessible through normal operations, potentially leading to data recovery. Physical destruction ensures that no data can be recovered, making it the most secure method for retiring SSDs.

Question 222

C) Full Backup (Correct Answer)

Explanation: A full backup is a complete copy of all data contained on the protected device, stored on backup media. This type of backup includes all files and folders, regardless of whether they have changed since the last backup. Full backups provide the most comprehensive protection but also require the most storage space and time to complete. They serve as a baseline for incremental and differential backups and are crucial for complete system recovery.

Question 223

C) Circuit Level Gateway Firewall (Correct Answer)

Explanation: A Circuit Level Gateway Firewall operates at the session layer (Layer 5) of the OSI Model. It manages communication sessions between trusted partners by monitoring TCP handshaking between packets to determine whether a requested session is legitimate. This type of firewall doesn't inspect the contents of packets but instead focuses on the session establishment process, making it faster than application-level gateways but less secure than stateful inspection firewalls.

Question 224

D) DMA (Correct Answer)

Explanation: DMA stands for Direct Memory Access. It is a feature of computer systems that allows certain hardware subsystems to access main system memory (RAM) independently of the central processing unit (CPU). DMA enables data transfer between devices and memory to occur without constant CPU oversight, significantly improving system performance by freeing up the CPU to perform other tasks while data transfer is in progress.

Question 225

B) RTO (Correct Answer)

Explanation: RTO stands for Recovery Time Objective. It is a metric used in business continuity planning that represents the maximum tolerable length of time a computer, system, network, or application can be down after a failure or disaster occurs. RTO defines the time frame within which a business process must be restored to avoid unacceptable consequences associated with a break in business continuity. It's crucial for determining appropriate recovery strategies, technologies, and processes.

Question 226

C) Physical Access Control (Correct Answer)

Explanation: Physical Access Control refers to tangible barriers and measures implemented to prevent unauthorized direct contact with systems and sensitive areas. This includes guards, fences, locked doors, and other physical security measures that create a real, physical obstacle to access. Unlike logical access controls which are implemented through software, physical access controls are tangible and visible deterrents and barriers.

Question 227

C) Inference Attack (Correct Answer)

Explanation: An inference attack occurs when an individual or system uses deduction or inference to gain knowledge

about protected or sensitive information without directly accessing it. In this case, the accounting clerk used available information (total payroll expenses before and after the new hire) to deduce the new employee's salary. This type of attack exploits indirect information to derive protected data, circumventing access controls without directly breaching them.

Question 228

A) DMCA (Correct Answer)

Explanation: The Digital Millennium Copyright Act (DMCA) is the law that prevents the removal of protection mechanisms placed on copyrighted works. Enacted in 1998, the DMCA criminalizes the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works. It also heightens the penalties for copyright infringement on the Internet, protecting digital rights management (DRM) systems.

Question 229

A) The Economic Espionage Act of 1996 (Correct Answer)

Explanation: The Economic Espionage Act of 1996 is the U.S. federal law that criminalizes the theft of trade secrets. It provides severe penalties for individuals and organizations engaged in economic espionage, particularly when benefiting foreign entities. The act aims to protect U.S. companies from industrial espionage and safeguard valuable intellectual property and trade secrets.

Question 230

A) Best Evidence (Correct Answer)

Explanation: "Best Evidence" refers to the most reliable form of evidence available in a legal proceeding. This principle, also known as the "original document rule," requires that the original version of a document be

presented in court rather than a copy, unless a satisfactory explanation is provided for its absence. In the context of information security, this could apply to presenting original log files or digital artifacts rather than copies or summaries.

Question 231

C) ACK (Correct Answer)

Explanation: In the TCP three-way handshake, system A should send an ACK (Acknowledgment) to system B in step three. The three steps are: 1) SYN from client to server, 2) SYN-ACK from server to client, and 3) ACK from client to server. This final ACK confirms that the connection has been established and both sides are ready to begin data transfer.

Question 232

A) Faraday Cage (Correct Answer)

Explanation: A Faraday Cage is an enclosure that blocks electromagnetic fields from entering or exiting. It's named after physicist Michael Faraday and is constructed using conductive materials. Faraday cages are used in various applications in information security, such as protecting sensitive electronic equipment from electromagnetic interference or preventing unauthorized access to wireless communications.

Question 233

A) Private Cloud (Correct Answer)

Explanation: A Private Cloud is a cloud computing model where the infrastructure is dedicated to a single organization. It can be built and managed by the organization in its own data center or hosted by a third-party provider exclusively for that organization. Private clouds offer greater control, security, and customization compared to public clouds, making them suitable for organizations with strict data privacy and compliance requirements.

Question 234

C) Wet Pipe System (Correct Answer)

Explanation: A Wet Pipe System is a type of fire suppression system where the pipes are always filled with water under pressure. When a fire is detected and the sprinkler head is activated by heat, water is immediately discharged. This system provides rapid response to fires but can be susceptible to freezing in cold environments and may cause water damage if accidentally triggered.

Question 235

D) Rule-Based Access Control (Correct Answer)

Explanation: Rule-Based Access Control (RBAC) is an access control mechanism that uses predefined rules to determine user permissions. These rules can be based on various factors such as user attributes, resource properties, or environmental conditions. RBAC allows for flexible and granular control over system access, enabling administrators to define complex access policies that can adapt to changing security requirements.

Question 236

C) Risk Transfer (Correct Answer)

Explanation: Risk transfer is a risk management technique where the potential for a loss is shifted from one entity to another. This is typically done through insurance policies, contracts, or other agreements. In this approach, the organization pays a third party to assume some or all of the potential financial impact of a risk. For example, purchasing cyber insurance transfers some of the financial risk of a data breach to the insurance company.

Question 237

A) Information Flow Model (Correct Answer)

Explanation: The Information Flow Model is an extension of the state machine concept and forms the basis for both the Biba and Bell-LaPadula models. It focuses on controlling the flow of information within a system to prevent unauthorized or insecure information transfers. The model uses objects, state transitions, and lattice (flow policy) states to define and enforce security policies. Guards are used to regulate the exchange of data between different security levels or systems, ensuring that information only flows in authorized directions.

Question 238

D) SOC 2 (Correct Answer)

Explanation: SOC 2 (Service Organization Control 2) report would provide Alflyse's company with the most detailed information about their IaaS provider's security, integrity, and availability controls. SOC 2 reports are specifically designed to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy. This report is ideal for technology and cloud computing service providers, making it the most suitable for assessing an IaaS provider. It offers in-depth insights into the provider's controls and their effectiveness, which is crucial for Alflyse's company as they prepare to migrate their data center.

Question 239

B) KPIs (Correct Answer)

Explanation: Key Performance Indicators (KPIs) are the most appropriate measures for Jennifer to select to gauge the effectiveness of her information security program in relation to long-term organizational goals. KPIs are quantifiable measurements that reflect the critical success factors of an organization. In the context of information security, KPIs can include metrics such as number of security incidents, time to detect and respond to threats, compliance rates, and

employee security awareness levels. Unlike simple metrics, KPIs are directly tied to strategic objectives, making them ideal for tracking progress towards long-term goals.

Question 240

A) Web server (Correct Answer)

Explanation: Without seeing the actual figure, it's impossible to provide a definitive answer. However, web server logs typically contain information such as client IP addresses, requested resources, HTTP status codes, and timestamps of requests. They are crucial for analyzing website traffic, troubleshooting issues, and monitoring security events related to web applications.

Question 241

C) Software tokens (Correct Answer)

Explanation: Software tokens provide both low management overhead and flexibility in multi-factor authentication. They are typically implemented as mobile apps, eliminating the need for physical hardware distribution and management. Software tokens can be easily deployed, updated, and revoked remotely, offering flexibility in user management. They also allow for integration with various systems and can support multiple accounts on a single device, making them a cost-effective and user-friendly MFA solution.

Question 242

D) Lessons learned (Correct Answer)

Explanation: Root cause analysis should be conducted during the "Lessons learned" stage of incident response. This stage occurs after the incident has been contained, eradicated, and systems have been recovered. During this phase, the team reviews the entire incident, from detection to resolution, to understand what happened, why it happened, and how to prevent similar incidents in the

future. This analysis helps improve the organization's overall security posture and incident response processes.

Question 243

B) All sensitive data that was gathered during the test (Correct Answer)

Explanation: Including all sensitive data gathered during the test is not a typical part of a penetration test report. While the report should include findings and evidence, it should not contain raw sensitive data that was accessed during the test. This protects the confidentiality of the organization's data and limits potential exposure. The report typically includes a list of vulnerabilities, risk ratings, and mitigation guidance, but sensitive data should be securely destroyed or returned to the client after the test.

Question 244

C) Deploy and use a SIEM (Correct Answer)

Explanation: A Security Information and Event Management (SIEM) system is the best solution for detecting issues like insider threats using centralized logging. SIEM tools collect, aggregate, and analyze log data from various sources across the organization. They can correlate events, identify patterns, and generate alerts for suspicious activities. SIEM systems often include user and entity behavior analytics (UEBA) capabilities, which are particularly useful for detecting insider threats by identifying anomalous user behaviors.

Question 245

C) Security Testing (Correct Answer)

Explanation: The listed activities (Vulnerability Scanning, Security Scanning, Penetration Testing, Risk Assessment, Security Auditing, Ethical Hacking, and Posture Assessment) are all examples of security testing. These methods are used to evaluate the security posture of an organization's

systems, networks, and applications. They aim to identify vulnerabilities, assess risks, and verify the effectiveness of security controls. Security testing is a comprehensive approach to ensuring the confidentiality, integrity, and availability of information assets.

Question 246

A) Basic Rate Interface (BRI) (Correct Answer)

Explanation: An ISDN Basic Rate Interface (BRI) uses existing telephone lines to send voice and data simultaneously with digital clarity. BRI is an ISDN service type that provides two B (Bearer) channels for data transmission, each offering 64 Kbps, and one D (Delta) channel for signaling and control, offering 16 Kbps. This configuration allows for simultaneous voice and data transmission over a single line, making it a cost-effective solution for small businesses and home offices.

Question 247

D) Shoulder Surfing (Correct Answer)

Explanation: Shoulder surfing is the act of gathering information from a system by observing the monitor or the use of the keyboard by the operator. This is a type of social engineering attack where the attacker physically observes the user's screen or keyboard inputs to obtain sensitive information such as passwords, PINs, or other confidential data. It can occur in public spaces, offices, or any environment where screens are visible to others. To prevent shoulder surfing, organizations often implement privacy screens and train employees on awareness of their surroundings.

Question 248

A) Malware attack (Correct Answer)

Explanation: The listed items (Macro viruses, File infectors, System or boot-record infectors, Polymorphic viruses,

Stealth viruses, Trojans, Logic bombs, Worms, Droppers, Ransomware, Adware, Spyware) are all examples of malware (malicious software). Malware attacks involve the use of software designed to disrupt, damage, or gain unauthorized access to a computer system. These various types of malware have different methods of infection, propagation, and payloads, but they all fall under the broader category of malware attacks.

Question 249

C) 2G (Correct Answer)

Explanation: CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications), and iDEN (Integrated Digital Enhanced Network) are all examples of second-generation (2G) cellular technology. 2G systems were the first to use digital encryption of conversations, and they introduced data services for mobile, starting with SMS text messages. These technologies marked a significant improvement over 1G analog systems, offering better sound quality and increased capacity. 2G was widely adopted in the 1990s and early 2000s before the advent of 3G and subsequent generations.

Practice Tests 4

Question 1

A company's identity management team creates a new user object and ensures it is available in the necessary directories and systems when onboarding a new employee. What is this process called?

A) Population

B) Authenticator loading

C) Registration

D) Provisioning

Question 2

An organization is adopting biometric authentication for their high-security building access control system. If the False Acceptance Rate (FAR) and False Rejection Rate (FRR) do not provide acceptable performance, what action should be taken?

A) Adjust the sensitivity of the biometric devices

B) Evaluate alternative biometric systems for comparison

C) Modify the FRR settings in the software

D) Shift the Crossover Error Rate (CER)

Question 3

In the OSI model, which layer is responsible for transmitting data using protocols such as TCP and UDP?

A) Transport

B) Human-Computer Interaction

C) Network

D) Presentation

Question 4

What type of testing is performed by end users or clients to verify and accept a software system before it is moved to the production environment?

A) User Acceptance Testing

B) Functional Testing

C) Focused Testing

D) Non-Functional Testing

Question 5

What term describes electrical interference that can cause issues with equipment functionality and impact the quality of communications, transmissions, and playback?

A) Transformer Obstruction

B) Electrical Spikes

C) Commutator Hindrance

D) Electromagnetic Interference

Question 6

How is a weakness or flaw in an organization's IT infrastructure or other aspects, which may result from the absence of safeguards or protection measures, referred to?

A) Vulnerability

B) Invulnerability

C) Immunity

D) Robustness

Question 7

What legal protection guarantees creators of "original works of authorship" against unauthorized duplication of their work?

A) Copyright

B) Trademark

C) Patent

D) Guarantee

Question 8

An employee suspects that confidential information is being smuggled out of the company despite data loss prevention systems. They discover suspicious photos posted on public message boards. What technique might be used to hide messages within these images?

A) Steganography

B) VPN

C) Watermarking

D) Covert timing channel

Question 9

According to NIST SP 800-18, what action should a system owner take when a significant change occurs in their system?

A) Select custodians for daily operational tasks

B) Develop a data confidentiality plan

C) Classify the system's data

D) Update the system security plan

Question 10

What term describes an attack where a malicious user obtains information about network traffic, often using a packet-capturing program to duplicate packet contents?

A) Sniffer Attack

B) Popeye Attack

C) Smurf Attack

D) Rumpelstiltskin Attack

Question 11

Which biometric factor uses near-infrared light to measure unique vein patterns in the palm for authentication purposes?

A) Palm Scan

B) Hand-Scan

C) Mani-Printing

D) Mani-Graph

Question 12

An organization implements an access control system with the following permissions:

Reviewers: update files, delete files

Submitters: upload files

Editors: upload files, update files

Archivists: delete files

What type of access control has been implemented?

A) Discretionary Access Control

B) Rule-Based Access Control

C) Task-Based Access Control

D) Role-Based Access Control

Question 13

Which cybersecurity model includes the following stages: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives?

A) Cyber Defence Planning Model

B) Defence in Depth

C) Cybersecurity Maturity Model

D) Kill Chain Model

Question 14

What authentication protocol, commonly used over PPP links, involves a server sending a challenge to the client after establishing a network connection?

A) Challenge Handshake Authentication Protocol (CHAP)

B) Decentralized Acceptance Protocol (DAP)

C) Centralized Control Protocol

D) One-Time Password Model

Question 15

If an organization suspects employees are storing sensitive information on laptops in an unsafe manner that violates security policy, what control can be used to identify the presence of those files?

A) Network DLP

B) Endpoint DLP

C) Network IPS

D) Endpoint IPS

Question 16

What term describes the traditional deployment concept where an organization owns the hardware, licenses the

software, and operates and maintains systems within their own facilities?

A) Off-Premise Solution

B) Data Centre

C) Server Farm

D) On-Premise Solution

Question 17

Which tool can be used to directly compromise the confidentiality of communications on an unencrypted VoIP network?

A) Nmap

B) Nikto

C) Nessus

D) Wireshark

Question 18

During a security audit, it's discovered that hand geometry scanners are used for data center access control. What recommendation should be made regarding their use?

A) Replace them due to high False Rejection Rate

B) Consider alternate biometrics due to accessibility concerns

C) Expand their use to other high-security areas

D) Add a second authentication factor for more reliable identification

Question 19

Which control would be most effective in detecting zero-day attack attempts?

A) Full-disk encryption

B) Signature-based intrusion detection

C) Strong patch management

D) Anomaly-based intrusion detection

Question 20

What term describes the act of sending large amounts of unwanted bulk messages to a system to cause denial of service, consume resources, or create general irritation?

A) Pharming

B) Spamming

C) Whaling

D) Phishing

Question 21

In software design, what term refers to the level of interaction between objects, where lower levels indicate better design due to increased independence?

A) Compatibility

B) Synergy

C) Ostracization

D) Coupling

Question 22

Which tool is specifically designed for network vulnerability scanning?

A) Nikto

B) Nmap

C) QualysGuard

D) Aircrack-ng

Question 23

Who has the authority to add a compromised digital certificate to a Certificate Revocation List (CRL)?

A) The Certificate Authority that issued the certificate

B) The root authority for the top-level domain

C) The certificate owner

D) The relocation authority for the top-level domain

Question 24

What network device is used to connect networks with different speeds, cable types, or topologies that use the same protocol?

A) Train

B) Tunnel

C) Bridge

D) Wormhole

Question 25

In risk assessment, what metric represents the amount of damage expected from a single occurrence of a specific risk event?

A) AV

B) ALE

C) ARO

D) SLE

Question 26

When examining the /etc/passwd file on a system configured to use shadowed passwords, what should be seen in the password field?

A) Hashed passwords

B) *

C) Plaintext passwords

D) Encrypted passwords

Question 27

What term describes the process of decompiling code to understand its functionality, often considered unethical when used to create competing or compatible products?

A) Reverse Engineering

B) Back-to-Front Engineering

C) Forward Engineering

D) Stealth Engineering

Question 28

What describes an event that triggers an alarm in a security scanner when there isn't enough information to conclusively determine a vulnerability, resulting in a false report?

A) True Negative

B) False Positive

C) True Positive

D) False Negative

Question 29

Which disaster recovery test type involves activating the disaster recovery facility while the primary site remains operational?

A) Tabletop Exercise

B) Checklist Review

C) Simulation Test

D) Parallel Test

Question 30

What two logical network topologies can be physically implemented as a star topology?

A) A ring and a mesh

B) A bus and a ring

C) A bus and a mesh

D) It is not possible to implement other topologies as a star

Question 31

What process involves developing options and actions to enhance opportunities and reduce threats to project objectives in the context of risk management?

A) Risk avoidance

B) Risk transfer

C) Risk mitigation

D) Risk acceptance

Question 32

In the context of Mandatory Access Control (MAC), what term describes environments where classification labels are structured in an ordered hierarchy from low to high security?

A) Flat Environments

B) Holacratic Environments

C) Flatarchy Environments

D) Hierarchical Environments

Question 33

What type of credit card fraud involves establishing a normal usage pattern and solid repayment history before maxing out the card with no intention of paying?

A) Fraud-Recovery-Duping

B) Loss-Automation

C) Bust-Out

D) Positive-Pay

Question 34

Which protocol makes TCP a connection-oriented protocol?

A) It works via network connections

B) It monitors for dropped connections

C) It uses a complex header

D) It uses a handshake

Question 35

What form of access control involves authorization verification performed by various entities distributed throughout a system?

A) Discretionary Access Control

B) Distributed Access Control

C) Directive Access Control

D) Direct Memory Access

Question 36

In asymmetric-key encryption, what term describes the publicly available value used to encrypt or decrypt messages?

A) Private Key

B) Index Key

C) Primary Key

D) Public Key

Question 37

Which rule in the Take-Grant Protection model allows a subject to create new objects and establish rights to those objects?

A) Remove rule

B) Grant rule

C) Take rule

D) Create rule

Question 38

What term can refer to both a momentary loss of power and a failure or problem within a system, device, or process?

A) Dead Zone

B) Surge

C) Fault

D) Spike

Question 39

What describes the unauthorized alteration of a domain name's registration without the valid owner's permission?

A) DNS Tunneling

B) Domain Hijacking

C) Phantom Domain Attack

D) DNS Spoofing

Question 40

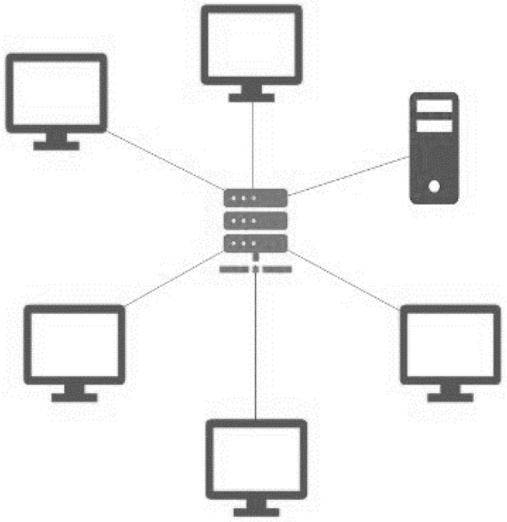
What network topology uses a central connected device to which all nodes are directly linked?

A) Ring Topology

B) Mesh Topology

C) Bus Topology

D) Star Topology



Question 41

Which encryption protocol is used exclusively for securing data in transit over a network and cannot be applied to data at rest?

A) TKIP

B) 3DES

C) AES

D) RSA

Question 42

What allows application developers to interact directly with underlying services through function calls, bypassing traditional web pages?

A) Core Programming Interfaces

B) Application Programming Interfaces

C) Java-Core Programming Interfaces

D) Flash Programming Interfaces

Question 43

In legal proceedings, what type of evidence is considered inadmissible when a witness provides their personal

interpretation or sentiment regarding facts, rather than direct observations?

A) Opinion Evidence

B) Circumstantial Evidence

C) Secondary Evidence

D) Hearsay Evidence

Question 44

Who holds the ultimate corporate responsibility for data protection and storage, and may be liable for negligence in establishing and enforcing security policies?

A) Responsible Project Manager

B) Owner

C) Data Analyst

D) Sponsor

Question 45

What type of Single Sign-On (SSO) combines existing authentication methods with biometric factors such as fingerprints, retinal scans, or facial recognition?

A) Kerberos-based SSO

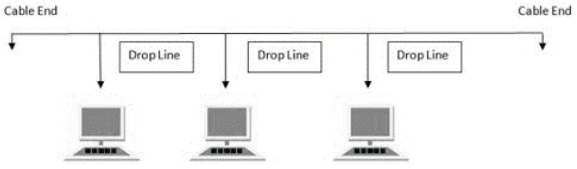
B) Biometric-based SSO

C) NTLM-based SSO

D) SPNEGO-based SSO

Question 46

What network topology is depicted when all devices are connected to a single cable, forming a single line of communication?



A) Mesh

B) Star

C) Bus

D) Ring

Question 47

What term describes data that persists on storage media after it has supposedly been removed?

A) Data Partitions

B) Data Remanence

C) Data Shadows

D) Data Sectors

Question 48

When conducting a disaster recovery test, which type is considered the most thorough but also potentially the most disruptive?

A) Parallel Test

B) Full Interruption Test

C) Tabletop Exercise

D) Checklist Review

Question 49

What type of attack occurs when a malicious actor positions themselves between the communications of a client and a server?

A) Malware

B) SQL injection

C) Eavesdropping

D) Man-in-the-Middle

Question 50

What physical security measure is used to clearly define and differentiate areas under specific levels of security protection?

A) Fence

B) Bridge

C) Firewall

D) Gateway

Question 51

Jasper Diamonds, a jewelry manufacturer, sells custom jewelry online. Bethany, the software development manager, is implementing industry-standard practices. She's creating a new change management process and wants to enable multiple developers to work on code simultaneously.

Which change management process supports this goal?

A) Request control

B) Release control

C) Change control

D) Configuration control

Question 52

Which category of attack do the following methods fall under?

- Brute-force
- Dictionary attack

A) Denial-of-Service

B) Malware attack

C) Password attack

D) Phishing attack

Question 53

In developing a medical software application for body mass index calculation, Monica wants to implement a control on the weight input field to ensure it falls within an expected range.

What type of control should Monica implement?

A) Fail secure

B) Buffer sound

C) Fall open

D) Limit check

Question 54

Eduard has been assigned to find a service that provides low latency, high performance, and high availability for hosting his employer's content.

What solution should he seek to ensure global customers can access content quickly, easily, and reliably?

A) Redundant servers

B) A CDN

C) A P2P CDN

D) A hot site

Question 55

Which technology is an example of key stretching that adds a salt to a password, making it more challenging for attackers to discover passwords using rainbow tables?

A) Keylength

B) Keybloc

C) KST

D) Bcrypt

Question 56

Barry White, a software tester, is evaluating a new gaming application on a smartphone to simulate a normal end-user experience while referencing the source code during his test.

What type of testing is Barry conducting?

A) Gray box

B) Blue box

C) Black box

D) White box

Question 57

Stark Industries is worried about hackers stealing sensitive information from their file server and decides to pursue a risk mitigation strategy.

Which action aligns with this strategy?

A) Taking no action

B) Deleting the files

C) Encrypting the files

D) Purchasing cyber liability insurance

Question 58

Alan's Wrenches has developed a new manufacturing process for its product. They plan to use this technology internally without sharing it and want it to remain protected for as long as possible.

What type of intellectual property protection is most suitable for this situation?

A) Copyright

B) Patent

C) Trademark

D) Trade secret

Question 59

Which public/private key system employs the IDEA algorithm to encrypt files and email messages, and is not a standard but rather an independently developed product with widespread Internet grassroots support?

A) GPG4Win

B) GNUPGK

C) Paubox

D) PGP

Question 60

Which of the following is not a valid application for Key Risk Indicators?

A) Providing historical views of past risks

B) Offering real-time incident response information

C) Providing insight into organizational risk tolerance

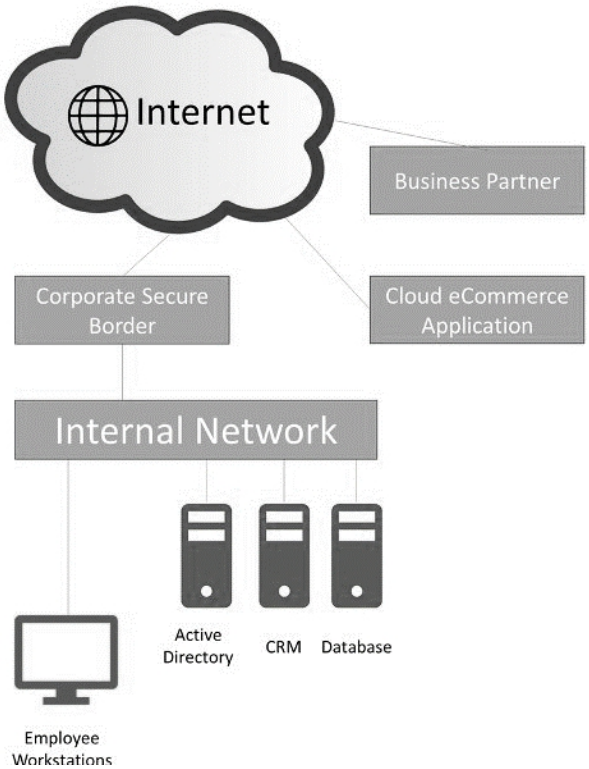
D) Giving warnings before issues occur

Question 61

Cap'n Oz's organization has a traditional on-site Active Directory environment with manual provisioning for each addition to their 35-employee company. As they adopt new technologies, they're increasingly using software-as-a-service applications to replace their internally developed software stack.

Cap'n must design an identity management implementation that allows his company to use cloud services while supporting their existing systems.

Which model should be employed to provide the required services?



A) Outsourced

B) On-Site

C) Cloud Based

D) Hybrid

Question 62

What term describes a label applied to a resource to indicate its sensitivity or value to an organization and therefore designate the level of security necessary to protect that resource?

A) Set

B) Genre

C) Classification

D) Group

Question 63

Which regulatory mechanism includes a set of principles aimed at preventing unauthorized disclosure of information handled by data processors and transmitted between data processors and the data controller?

The seven principles are:

- Notice
- Choice
- Onward transfer
- Security
- Data integrity
- Access
- Enforcement

A) Safe Harbor

B) Access to Information Act

C) Privacy and Information Act

D) Freedom of Information Act

Question 64

What term describes a malicious code object that appears to be a benign program, such as a game or simple utility that performs the "cover" functions as advertised but also carries an unknown payload?

A) Trojan Horse

B) Virus

C) Hyde-Jekyll Attack

D) Wild Cat Attack

Question 65

What is the term for a methodical examination or review of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or outright crimes?

A) Research

B) Investigation

C) Probe

D) Audit

Question 66

What type of virus is a self-contained executable file that evades detection by using a file name similar to, but slightly different from, a legitimate operating system file?

A) Hitchhiker Virus

B) Parasite Virus

C) Companion Virus

D) Steward Virus

Question 67

What is the correct chronological order for the following software testing phases?

1. Alpha
2. Beta
3. Pre-Alpha
4. Release
5. Release Candidate

A) 3, 1, 2, 5, 4

B) 1, 3, 2, 5, 4

C) 4, 5, 3, 1, 2

D) 2, 3, 1, 4, 5

Question 68

What is the name for the portion of a hard drive or floppy disk that the computer uses to load the operating system during the boot process?

A) Removable Boot Area

B) Master Boot Record (MBR)

C) Optical Boot Sector (OBS)

D) Immovable Boot Partition (IBP)

Question 69

What principle requires having access to, knowledge about, or possession of data or resources in order to perform specific work tasks, with users needing a legitimate requirement to gain access to data or resources?

A) Resource-based policies

B) Need-to-know

C) Minimum Permission Boundaries

D) Identity-based policies

Question 70

Fred needs to transfer files between two servers on an untrusted network. He needs to select an encrypted protocol to ensure his data remains secure.

Which protocol should Fred choose?

A) TCP

B) IPSec

C) SFTP

D) SSH

Question 71

What type of data is maintained by Lauren's healthcare provider, including details about her health, treatments, and medical billing?

A) Individual Protected Data

B) Protected Health Information

C) Protected Health Insurance

D) Personally Identifiable Information

Question 72

In an organization with a formal data governance program, who is responsible for assigning the classification level to a new class of data?

A) Data owner

B) Data creator

C) Data custodian

D) CISO

Question 73

What is the term for the act of following someone through a secure gate or doorway without being personally identified or authorized?

A) Hijacking

B) Piggybacking

C) Trojaning

D) Sandwiching

Question 74

Which model, as defined by Goguen and Meseguer, was designed to ensure that objects and subjects of different levels don't interfere with those of other levels, using inputs and outputs of either low or high sensitivity?

A) Information Flow Model

B) Non-interference Model

C) State Machine Model

D) Bell-LaPadula Model

Question 75

Which amendment to the US Constitution prohibits government agents from searching private property without a warrant and probable cause?

A) Fourth Amendment

B) Third Amendment

C) Second Amendment

D) Fifth Amendment

Question 76

Which protocol provides mutual authentication between a client and a server, where the client authenticates against the server and the server authenticates itself against the client?

A) File Transfer Function (FTF)

B) Blockchain

C) Hypertext Transfer Permission (HTTP)

D) Kerberos

Question 77

What feature of a security control or application prevents the sender of a message or the subject of an activity or event from denying that the event occurred?

A) Nonrepudiation

B) Espousal

C) Condemnation

D) Repudiation

Question 78

What analysis identifies the resources critical to an organization's ongoing viability, the threats posed to those resources, and assesses the likelihood and impact of each threat occurring?

A) Business Continuity Planning (BCP)

B) Risk Response Appraisal (RRA)

C) Disaster Contingency Reckoning (DCR)

D) Business Impact Assessment (BIA)

Question 79

What concept states that each individual must maintain local security whether or not its network or telecommunications channels provide or offer security?

A) Enduser Protection

B) Endpoint Security

C) Finaluser Responsibility

D) Customer Diligence

Question 80

During a business impact assessment, what metric provides crucial information about the amount of time an organization can be without a service before irreparable harm occurs?

A) RTO

B) RPO

C) MTD

D) ALE

Question 81

What two critical factors does accountability for access control rely on?

A) Accountability and authentication

B) Identification and authorization

C) Identification and authentication

D) Authentication and authorization

Question 82

Which of the following is not a key process area for the repeatable phase of the Software Capability Maturity Model (SW-CMM)?

A) Software Project Planning

B) Software Quality Management

C) Software Subcontract Management

D) Software Project Tracking

Question 83

What type of web application attack occurs when a site contains some form of reflected input, often exploited using script injection?

A) Browser-to-Browser Hijacking (BBHJ)

B) Guerrilla Website Attack (GWA)

C) Blunt-Force Attack (BFA)

D) Cross-Site Scripting (XSS)

Question 84

Bell-LaPadula is an example of which type of Access Control Model?

A) RBAC

B) ABAC

C) DAC

D) MAC

Question 85

What term describes electromagnetic interference (EMI) noise generated by the difference in power between the hot and ground wires of a power source or operating electrical equipment?

A) Dips and Surges

B) Common Mode Noise

C) Electrical Spikes

D) Electromagnetic Pulse

Question 86

What is the name for an attack that grants hackers remote control over the features and functions of a Bluetooth device, potentially including the ability to turn on the microphone to use the telephone as an audio bug?

A) Bluebugging

B) Blueprinted

C) Bluetooth hacking

D) Bluegeoning

Question 87

What does a constrained user interface do?

A) It limits what users can do or see based on privileges

B) It prevents users from logging in

C) It limits the access a user is provided based on what activity they are performing

D) It limits the data visible in an interface based on the content

Question 88

Which IPSec protocol performs authentication for the sender and also encrypts the data being sent?

A) Authentication Header

B) Authentication Digest

C) Sequence Number

D) Encapsulating Security Payload

Question 89

In the context of transaction processing, what does the "C" in the acronym ACID stand for?

A) Circumpolar

B) Complete

C) Consistency

D) Censorial

Question 90

What process provides the CPU with the actual address of the memory location to be accessed?

A) Fixed Address Allocation

B) Static URL Allocation

C) Dynamic URL Allocation

D) Direct Addressing

Question 91

What is the act of altering or falsifying DNS information using a rogue DNS server to send false DNS replies in order to route or misdirect legitimate traffic?

A) DNS Spoofing

B) DNS Tunneling

C) Phantom Domain Attack

D) DNS Poisoning

Question 92

In computer science, what data type has one of two possible values (usually denoted true and false) which is intended to represent the two truth values of logic?

A) Floating-Point

B) Primitive

C) Boolean

D) Integer

Question 93

Ed is constructing a network that supports IPv6 but needs to connect it to an IPv4 network.

What type of device should Ed place between the networks?

A) A gateway

B) A router

C) A bridge

D) A switch

Question 94

Jasper Diamonds, a jewelry manufacturer, markets and sells custom jewelry through their website. Bethany, the software development manager, is implementing industry-standard practices and developing a new change management process.

Bethany is collaborating with her colleagues to conduct user acceptance testing.

Which change management process encompasses this task?

A) Configuration control

B) Release control

C) Change control

D) Request control

Question 95

What is the term for the 3-way process utilized by the TCP/IP protocol stack to establish connections between two hosts?

A) Meet & Greet

B) Handshake

C) Triparty Authentication

D) No-Trust Authentication

Question 96

What computational technique is designed to more closely approximate human thought patterns rather than a rigid set

of mathematical theory or algebraic approaches that utilize binary categorizations of data?

A) Fuzzy Logic

B) Logic Simulation

C) Real-Data Inputs

D) DNA Logic

Question 97

Monica is developing a medical software application for body mass index calculation. She wants to implement a control on the weight input field to ensure it falls within an expected range.

What type of control should Monica use?

A) Fail secure

B) Buffer sound

C) Fall open

D) Limit check

Question 98

Eduard has been tasked with identifying a service that will provide low latency, high performance, and high availability for hosting his employer's content.

What solution should he seek to ensure global customers can access content quickly, easily, and reliably?

A) Redundant servers

B) A CDN

C) A P2P CDN

D) A hot site

Question 99

Barry White, a software tester, is evaluating a new gaming application on a smartphone to simulate a normal end-user

experience while referencing the source code during his test.

What type of testing is Barry conducting?

A) Gray box

B) Blue box

C) Black box

D) White box

Question 100

Stark Industries is concerned about the risk of hackers stealing sensitive information from their file server and decides to pursue a risk mitigation strategy.

Which action supports this strategy?

A) Taking no action

B) Deleting the files

C) Encrypting the files

D) Purchasing cyber liability insurance

Question 101

Donald Blake has implemented an access control list that enumerates the objects users are permitted to access. When users try to access an object they don't have rights to, they are denied access, even though there isn't an explicit rule prohibiting it.

Which access control principle is fundamental to this behavior?

A) Exploit deny

B) Implicit deny

C) Final rule fall-through

D) Least privilege

Question 102

In the context of Information Systems Security, how would you describe a situation where IT personnel make security decisions independently without consulting senior management?

A) Mutiny

B) Bottom-up approach

C) Vigilante methodology

D) Inside attack

Question 103

In the realm of Information Systems Security, what term describes the concept where, when an organization utilizes a cloud solution, there is a division of security and stability responsibilities between the provider and the customer?

A) Fair-Use Cloud Model

B) Responsible-Use Cloud Community Model

C) Shared Cloud Obligation Model

D) Cloud Shared-Responsibility Model

Question 104

Which LDAP operation incorporates authentication to the LDAP server?

A) StartLDAP

B) Auth

C) Bind

D) AuthDN

Question 105

Elaine is formulating a business continuity plan for her organization.

Which metric should she aim to minimize?

A) RTO

B) MTO

C) SSL

D) AV

Question 106

Quan Yaozu is evaluating tax software, and part of the testing procedure involves inputting data into various actual tax forms to verify that the software generates accurate results.

What type of testing is Quan conducting?

A) Dynamic Testing

B) Fuzzing

C) Misuse Testing

D) Use Case Testing

Question 107

In the context of Information Systems Security, what term describes a system where communicating parties use a shared secret key or pairs of public and private keys to facilitate secure communication?

A) Private Line System

B) Cryptosystem

C) Secure Line System

D) Dedicated Line System

Question 108

In the field of Information Systems Security, what term refers to the practice of maintaining an active database server at the backup location, which is considered the most advanced database backup solution?

A) Secondary Drive

B) Remote Desktop Access

C) Remote Mirroring

D) Tape Backup

Question 109

Which form of twisted-pair cable is capable of supporting network traffic at a nominal rate of 100 Mbit/s?

A) 1BaseTX

B) 100BaseTX

C) 10000BaseT

D) 1000BaseTX

Question 110

Which protocol is connectionless, meaning no connection is established prior to communication, and does not guarantee the delivery of data packets?

A) AWS Protocol

B) TCP Protocol

C) IBM Protocol

D) UDP Protocol

Question 111

In the realm of Information Systems Security, what term describes an attack against a system designed to uncover

the password associated with a known identity (i.e., a username), where a script of common passwords and dictionary words is employed to attempt to discover an account's password?

A) Malware Attack

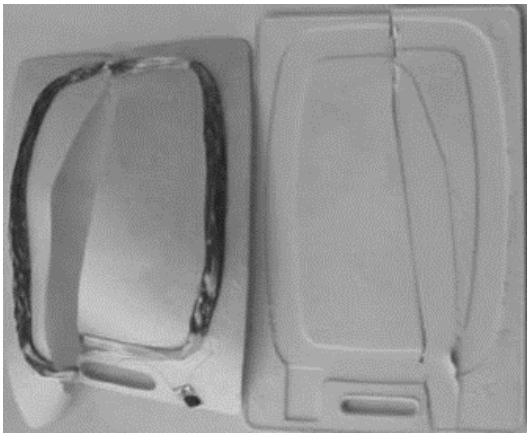
B) Man-in-the-Middle (MitM) Attack

C) Drive-by Attack

D) Dictionary Attack

Question 112

Allen is evaluating new identification cards for his organization to be used for physical access control. He encounters a sample card and is uncertain about the technology. Upon opening it, he observes the following internal structure:



What type of card is this?

A) Proximity card

B) Smart card

C) Phase-two card

D) Magnetic stripe

Question 113

Which legislative act, implemented following the September 11, 2001 terrorist attacks, significantly expanded the

powers of law enforcement organizations and intelligence agencies across various areas, including the monitoring of electronic communications?

A) Foreign & Domestic Intelligence Surveillance Act

B) National Security Act

C) USA Patriot Act

D) USA Freedom Act

Question 114

LexCorp Industries, an Irish company handling personal information, exchanges data with numerous other countries.

Which of the following nations would activate the onward transfer provisions of the International Safe Harbour Privacy Principles?

A) United States

B) Germany

C) United Kingdom

D) Italy

Question 115

In the context of Information Systems Security, what term describes a disaster recovery test that involves ceasing operations at the primary site and transferring them to the recovery site?

A) Stress Test

B) Fail-Safe Test

C) Full-Interruption Test

D) End-to-End Test

Question 116

In the field of Information Systems Security, what term refers to a thorough and systematic form of monitoring

where logged information is analyzed in detail to identify trends, patterns, and abnormal, unauthorized, illegal, or policy-violating activities?

A) CSI Observation

B) UI Monitoring

C) Log Analysis

D) Activity Protocol Surveillance

Question 117

Saria needs to draft a request for proposal for code review and wants to ensure that the reviewers consider the business logic behind her organization's applications.

What type of code review should she specify in the RFP?

A) Static

B) Dynamic

C) Manual

D) Fuzzing

Question 118

Which of the following is not a principle in the Agile approach to software development?

A) The most efficient method of conveying information is electronic.

B) Simplicity is essential.

C) Working software is the primary measure of progress.

D) Business people and developers must work together daily.

Question 119

Lily aims to secure her organization's VoIP systems.

Which of the following attacks is one she shouldn't need to be concerned about?

A) Caller ID spoofing

B) Blackboxing

C) Denial of Service

D) Eavesdropping

Question 120

Which encryption/decryption algorithm possesses the following characteristics?

Used for digital signature and its verification

Developed in 1991

Created by National Institute of Standards and Technology (NIST)

Employs modular exponentiation and discrete logarithm

Best suited for signing in and decryption

Classified as a digital signature algorithm

A) DSA

B) ARS

C) RSA

D) SAR

Question 121

In the context of Information Systems Security, what term describes a connection address within a protocol?

A) Plug

B) Port

C) Jack

D) Connector

Question 122

What term refers to malicious software in a script or program that performs an unwanted, unauthorized, or

unknown activity on a computer system?

A) Malware

B) Guerillaware

C) Terrorware

D) Third-Party Software

Question 123

Megan needs to create a forensic copy of a hard drive for use in an investigation.

Which of the following tools is most appropriate for her task?

A) xcopy

B) DBAN

C) dd

D) ImageMagik

Question 124

In the realm of Information Systems Security, what term describes the act of using a magnet to destroy data stored on magnetic media to prevent data leakage attacks or events?

A) Reformatting

B) Data Erasure

C) Wiping

D) Degaussing

Question 125

In the context of Information Systems Security, which operation (represented by the ^ symbol) verifies whether two values are both true?

A) HAVING

B) IF

C) WHERE

D) AND

Question 126

Which of the following memory types is classified as volatile memory?

A) EEPROM

B) EPROM

C) RAM

D) Flash

Question 127

Bei Bang-Wen needs to install a network cable spanning over a kilometer.

Which wiring option should he select to avoid potential issues?

A) 10Base5

B) Fiber optic

C) STP

D) 10BaseT

Question 128

Alice wants to send James Kirk a message with the assurance that James will know the message was not altered during transmission.

Which goal of cryptography is Alice trying to achieve?

A) Confidentiality

B) Integrity

C) Authentication

D) Nonrepudiation

Question 129

In which type of trusted recovery process can the system recover without administrator intervention, but may experience some data loss?

A) Automated recovery

B) Manual Recovery

C) Functional Recovery without Undue Data Loss

D) Automated Recovery without Undue Data Loss

Question 130

In the context of Information Systems Security, what term describes a biometric factor, which is a behavioral or psychological characteristic unique to an individual, where the pattern and speed of a person manually entering a passphrase is used to establish identity or provide authentication?

A) Keystroke Patterns

B) Clavicle Tapping

C) Genkey Recording

D) Keystroke Monitoring

Question 131

In the field of Information Systems Security, what term describes an attack typically motivated by a sense of resentment and carried out to harm an organization or individual?

A) Malware Attack

B) Grudge Attack

C) Man-in-the-Middle (MitM) Attack

D) Drive-by Attack

Question 132

In the realm of Information Systems Security, which integrity model is based on predetermining the set or

domain of objects that a subject can access?

A) Clark-Wilson Model

B) Harrison–Ruzzo–Ullman Model

C) Bell-LaPadula Model

D) Goguen-Meseguer Model

Question 133

In the context of Information Systems Security, what term describes a product that automates the inspection of audit logs and real-time system events, generally used to detect intrusion attempts but also capable of identifying system failures or assessing overall performance?

A) DDoS Attack Monitoring Protocol

B) Intrusion Detection System

C) Botnet Surveillance

D) Illegal File Transfer Protection

Question 134

In the field of Information Systems Security, what term refers to a form of physical identification and/or electronic access control devices?

A) Voice patterns

B) Wedges

C) Badges

D) Jumpkins

Question 135

In the context of Information Systems Security, what term describes the database programming language that enables the creation and modification of a database's structure (known as the schema)?

A) Data Manipulation Language (DML)

B) Transaction Control Language (TCL)

C) Data Definition Language (DDL)

D) Data Control Language (DCL)

Question 136

Hawal is preparing to send backup tapes offsite to a secure third-party storage facility.

What measures should Hawal take before dispatching the tapes to the facility?

A) Increase the classification level of the tapes because they are leaving the company's possession.

B) Decrypt the tapes in case they are lost in transit.

C) Ensure that the tapes are handled in the same manner as the original media would be, based on their classification.

D) Purge the tapes to prevent the loss of classified data.

Question 137

Lucky has developed the password hashing system for the web application he is building. His hashing code function for passwords results in the following process for a series of passwords:

[Image of password hashing process]

What flaw has been introduced in this hashing implementation?

A) Salt reuse

B) Poor salt algorithm selection

C) Plaintext salting

D) Use of short salt

Question 138

Lauren wants to implement a software review process for the application she is developing.

Which of the following processes would be most suitable if she is a remote worker operating on a different schedule from the rest of the team?

A) Team review

B) Fagan inspection

C) Pass around

D) Pair programming

Question 139

Which of the following categories encompasses first generation programming languages?

A) Assembly languages

B) Natural languages

C) Machine languages

D) Compiled languages

Question 140

In the context of Information Systems Security, what term describes a network device that is considered an intelligent hub because it knows the addresses of the systems connected to each outbound port, and instead of repeating traffic on every outbound port, it only repeats traffic out of the port where the destination is known to exist?

A) Switch

B) Modem

C) Amplifier

D) Router

Question 141

In the realm of Information Systems Security, what term describes an attack used to redirect traffic to a rogue or impostor system, or to divert traffic away from its intended destination, often through the malicious alteration of

hyperlink URLs in the HTML code of documents sent to clients?

A) Link Imposter

B) Domain Diversion

C) URL Hijacking

D) Hyperlink Spoofing

Question 142

In the context of Information Systems Security, what rule states that when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements may modify the written agreement?

A) Default Evidence Judgment

B) Binding Terms Assumption

C) Contract Law

D) Parol Evidence Rule

Question 143

Timothy, a forensic analyst, is attempting to retrieve information from a hard drive. It appears that the user tried to erase the data, and Tim is working to reconstruct it.

What type of forensic analysis is Timothy performing?

A) Network analysis

B) Embedded device analysis

C) Software analysis

D) Media analysis

Question 144

Fran, a web developer for an online retailer, has been tasked by her boss to create a way for customers to easily integrate with the company's site. They need to be able to

check inventory in real-time, place orders, and check order status programmatically without accessing the web page.

What can Fran develop to most directly facilitate this interaction?

A) Data dictionary

B) API

C) Web scraper

D) Call centre

Question 145

In the context of Information Systems Security, what type of error refers to a False Rejection Rate (FRR)?

A) Type 4 Error

B) Type 1 Error

C) Type 3 Error

D) Type 2 Error

Question 146

What type of information do both CVE and NVD provide?

A) Penetration testing methodologies

B) Vulnerabilities

C) Vulnerability assessment tools

D) Markup languages

Question 147

In which software development methodology is software developed in incremental, rapid cycles, with emphasis on interactions among customers, developers, and clients rather than processes and tools, and a focus on responding to change rather than extensive planning?

A) Six-Sigma Methodology

B) Kanban Methodology

C) Agile Methodology

D) Waterfall Methodology

Question 148

In the context of Information Systems Security, what term is often used in reference to documents, specifically the original document itself produced for the court's inspection?

A) Direct Evidence

B) Primary Evidence

C) Subject Evidence

D) Real evidence

Question 149

In the field of Information Systems Security, what term describes the process of moving a resource into a lower classification level once its value no longer justifies the security protections provided by a higher level of classification?

A) Taxonomy

B) Declassification

C) Departmentalization

D) Designation

Question 150

What type of motion detector employs high microwave frequency signal transmissions to identify potential intruders?

A) Capacitance

B) Wave pattern

C) Heat-based

D) Infrared

Question 151

Microsoft's STRIDE threat assessment framework categorizes threats into six types:

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

If a security tester manages to alter audit logs, which STRIDE categories most accurately describe this issue?

A) Repudiation and Tampering

B) Tampering and Information Disclosure

C) Repudiation and Denial of Service

D) Elevation-of-Privilege and Tampering

Question 152

An IT professional discovers a software application running under a service account with full administrative privileges on a web server. Which information security principle does this situation violate?

A) Job rotation

B) Separation of duties

C) Least privilege

D) Need to know

Question 153

Who ultimately bears the responsibility for data protection tasks within an organization?

A) Data custodian

B) Auditor

C) Data owner

D) User

Question 154

A company is exploring the use of an object-based storage system where data is stored in a vendor-managed environment through API calls. What category of cloud computing service does this represent?

A) SaaS

B) CaaS

C) PaaS

D) IaaS

Question 155

What term describes the practice of concealing messages within other messages, often using image or audio files?

A) Stenography

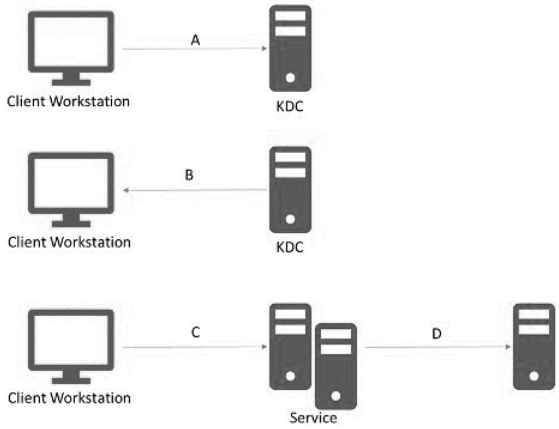
B) Hidden-in-Plain-Site (HiPS)

C) Encryption

D) Sublimination

Question 156

In the context of Kerberos authentication and authorization, what occurs between the client's request for a service ticket and the Key Distribution Center (KDC) issuing that ticket?



A) The KDC reviews its service listing and prepares an updated Ticket Granting Ticket based on the service request.

B) The KDC updates its access control list based on the data in the Ticket Granting Ticket.

C) The KDC confirms the validity of the Ticket Granting Ticket and verifies the user's privileges for the requested resource.

D) The KDC creates a service ticket to be issued to the client.

Question 157

During a system review, an administrator finds that a crucial system has its log settings configured to a maximum size of 20 megabytes with overwrite as needed. What potential issue might this configuration cause?

A) The logs will only retain the most recent 20 megabytes of data.

B) An excessive amount of log data will be stored on the system.

C) The logs will lack necessary information.

D) The system is automatically deleting archived logs.

Question 158

What term is typically used to describe the initial creation of a user account in the provisioning process?

A) Background checks

B) Clearance verification

C) Enrollment

D) Initialization

Question 159

An IT manager wants to establish a service to provide information about the organization's users and services using a centralized, open, vendor-neutral, standards-based system that can be easily queried. Which technology best meets these requirements?

A) Active Directory

B) Radius

C) LDAP

D) Kerberos

Question 160

What type of application enables the storage, modification, and retrieval of information from a database?

A) SQL application

B) SAML application

C) DBMS application

D) SSD application

Question 161

Which single sign-on (SSO) method uses web-based HTTP cookies to transmit user credentials from browser to server without user input, gathering and encrypting existing credentials on the client machine before storing and sending them to the destination server?

A) Screen Scraping SSO

B) Kerberos-based SSO

C) Cookie-based SSO

D) Smart Card-based SSO

Question 162

What term describes a message that has not been encrypted?

A) Ciphertext

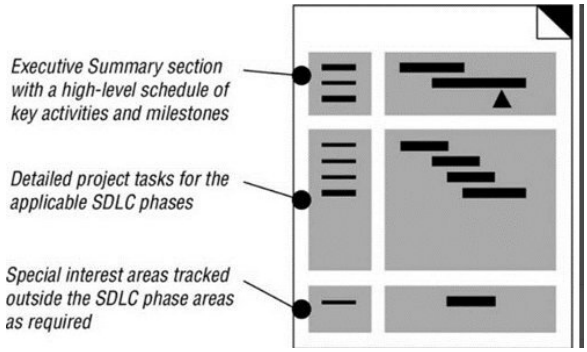
B) Originaltext

C) Deciphertext

D) Plaintext

Question 163

A project manager receives a document outlining tasks, subtasks, and work packages for a new software development project. What type of planning document is this?



A) Project plan

B) Work Breakdown Structure

C) Functional requirements

D) Test analysis report

Question 164

A team of system administrators is struggling to manage numerous usernames and passwords for systems with varying security requirements. What solution should be recommended to ensure proper password handling, logging, and rotation?

A) Separation of duties

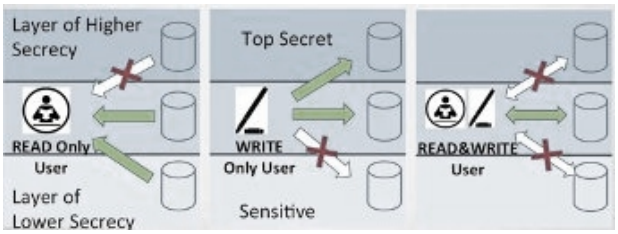
B) A credential management system

C) A strong password policy

D) Single sign-on

Question 165

Which security model property states that a subject at a specific classification level cannot write data to a lower classification level?



A) Diba

B) Bell-LaPadula

C) Biba

D) DAC

Question 166

What term describes the process of monitoring outgoing network traffic to detect and prevent unauthorized data transfer outside an organization?

A) Data Exploitation Monitoring

B) Embezzlement Monitoring

C) Data Vent Monitoring

D) Egress Monitoring

Question 167

Which government-standard hash function was developed by the National Institute of Standards and Technology and specified in an official publication?

A) SAML

B) SSH

C) SHA

D) SSL

Question 168

A facilities manager is evaluating the installation of a flood prevention system at a data center valued at $100 million. The system would cost $10 million to install. Flood experts determined the facility is in a 200-year flood plain, and a flood would likely cause $20 million in damage. What is the annualized loss expectancy for a flood at this data center?

A) $100,000

B) $1,000,000

C) $40,000

D) $400,000

Question 169

Which type of attack would be best prevented by requiring proof of identity, callback authorizations for voice-only requests, and prohibiting password changes via voice communications?

A) Social Engineering

B) Worms

C) Shoulder Surfing

D) DoS Attacks

Question 170

Which of the following is not considered a type of structural coverage in software testing?

A) Statement

B) Data flow

C) Trace

D) Loop

Question 171

What term describes the process of removing restrictions on iOS devices to allow root-level access to the underlying operating system?

A) Jailbreaking

B) Rootbreaking

C) Unlocking a Bootloader

D) Bricking

Question 172

What technology uses systems designed to detect and block attempts to exfiltrate data from an organization?

A) Data Loss Prevention (DLP)

B) Data Violation Blocking (DVB)

C) Data Vector Machine (DVM)

D) Blocking Input/Output (BIO)

Question 173

A network administrator at an industrial facility needs to ensure the network is not susceptible to electromagnetic interference from large motors and other equipment. Which type of network cabling should be chosen if this concern outweighs cost and installation difficulty?

A) 100 BaseT

B) Fiber-optic

C) 10Base2

D) 1000BaseT

Question 174

What term describes the act of changing a single bit to its opposite value, a technique commonly used in fuzzing to slightly modify input data?

A) Bit Flipping

B) Boolean Reversing

C) Binary Exchange

D) Digi-Swap

Question 175

Which software testing method involves partial knowledge of an application's internal workings and aims to identify defects due to improper code structure or functionality?

A) Gray-Box Testing

B) White-Box Testing

C) Blue-Box Testing

D) Black-Box Testing

Question 176

What is the final stage of the Software Capability Maturity Model (SW-CMM)?

A) Repeatable

B) Managed

C) Defined

D) Optimizing

Question 177

In risk assessment, what term describes the percentage of loss an organization would experience if a specific asset were compromised by a realized risk?

A) Risk Rating (RR)

B) Exposure Factor (EF)

C) Estimated Loss (EL)

D) Likelihood of Occurrence

Question 178

What type of electrical disturbance can be caused by atmospheric lightning?

A) Common Mode Noise

B) Electromagnetic Pulse

C) Dips and Surges

D) Electrical Spikes

Question 179

What term describes the system that provides connections between a telecommunication room and work areas, including cabling, cross-connection blocks, patch panels, and supporting hardware infrastructure?

A) Variable Distribution System

B) Vertical Distribution System

C) Parallel Distribution System

D) Horizontal Distribution System

Question 180

Which organization is an independent oversight body that defines and maintains computer, networking, and technology standards, along with thousands of other international standards for business, government, and society?

A) International Organization for Standardization (ISO)

B) International Standardization Protocols (ISP)

C) International Data Management Standards (IDMS)

D) International Organization for Standardization (IOS)

Question 181

Purchasing insurance is an example of which type of risk response?

A) Transfer

B) Avoid

C) Mitigate

D) Accept

Question 182

Which confidentiality-focused security model is based on the state machine model and employs mandatory access controls and the lattice model?

A) Information Flow Model

B) Bell-LaPadula Model

C) Non-interference Model

D) State Machine Model

Question 183

In the subject/object model of access control, when a user attempts to log into a VPN to access a remote file server, who or what is considered the subject of this login attempt?

A) Remote file server

B) VPN

C) User

D) Files contained on the remote server

Question 184

Which of the following is not typically a classification level found in commercial data classification schemes?

A) Public

B) Sensitive

C) Confidential

D) Secret

Question 185

Which of the following is not a principle of the agile approach to software development?

A) Welcome changing requirements, even late in the development process.

B) The best architecture, requirements, and designs emerge from self-organizing teams.

C) Simplicity is essential.

D) Deliver working software infrequently, with an emphasis on creating accurate code over longer timelines.

Question 186

What programming method uses encapsulated code sets called objects and is particularly suited for modeling real-world scenarios and tracking error propagation?

A) Authoring Programming

B) Object-Oriented Programming

C) Machine Programming

D) Compiled Programming

Question 187

Which Layer 1 protocol is used to connect routers and multiplexers to ATM or frame relay connection devices?

A) Synchronous Data Encryption (SDE)

B) Asynchronous Data Encryption (ADE)

C) High-Speed Serial Interface (HSSI)

D) High-Level Data Link Control (HDLC)

Question 188

Which type of code review is most effective for identifying flaws in business logic?

A) Interface testing

B) Manual

C) Generalization fuzzing

D) Mutational fuzzing

Question 189

What term describes the high-performance storage resource available to a system, typically consisting of volatile Random Access Memory (RAM)?

A) Flash Memory

B) Dynamic Memory

C) Swap Memory

D) Primary Memory

Question 190

What term describes the practice of auditing, logging, and monitoring the attempted access and activities of a subject in an information system?

A) Access Tracking

B) Access Accounting

C) Subject Monitoring

D) Activity Matrix

Question 191

What category of security controls includes facility construction and selection, site management, personnel controls, awareness training, and emergency response procedures?

A) Procedural Security Policy Controls

B) Federal Policy & Procedure Controls

C) Administrative Physical Security Controls

D) Executive-order Control Policies

Question 192

What field of study involves examining raw data to extract useful information from large datasets?

A) Data Analytics

B) Data Engineering

C) Machine Learning Engineering

D) Machine Learning Analytics

Question 193

In a backup strategy using incremental backups, assuming the same amount of data changes each day, how would the size of Monday's, Tuesday's, and Wednesday's incremental backups compare?

A) Wednesday's incremental backup would be largest

B) Monday's incremental backup would be largest

C) Tuesday's incremental backup would be largest

D) All three would be the same size

Question 194

Which of the following activities should not automatically be logged as a privileged administrative action?

A) Logging into a workstation

B) Restoring a system from backup

C) Purging log entries

D) Managing user accounts

Question 195

What term describes the various strategies and testing types used to ensure that an application under test meets

client expectations, including unit testing, integration testing, system testing, and performance testing?

A) Testing Methodology

B) Vulnerability Testing

C) QAQC Testing

D) UAT Testing

Question 196

In which single sign-on (SSO) method does a user's initial login to an HTTP server through a web browser result in a session token being generated on the server and returned to the user as an in-memory cookie for subsequent authentication?

A) Form-filling SSO

B) Kerberos-based SSO

C) Enrollment-based SSO

D) Session-based SSO

Question 197

Which type of attack relies on precise timing to exploit the gap between when a system checks authorization and when it uses that authorization to perform an action?

A) SQL Injection

B) Cross-site scripting

C) TOCTOU

D) Pass the hash

Question 198

An information security professional notices a door to a secure area left ajar and takes immediate action to close it, despite physical security not being their responsibility. What principle does this action demonstrate?

A) Informed consent

B) Due care

C) Due diligence

D) Separation of duties

Question 199

What term describes the process of slightly modifying input data by changing individual bits, commonly used in software testing and security analysis?

A) Bit Flipping

B) Boolean Reversing

C) Binary Exchange

D) Digi-Swap

Question 200

Which of the following is not a privileged administrative activity that should be automatically logged for superuser actions?

A) Logging into a workstation

B) Restoring a system from backup

C) Purging log entries

D) Managing user accounts

Question 201: What security measure can be implemented to enforce the concept of two-person control?

A) Least privilege

B) Defense in depth

C) Separation of duties

D) Mandatory vacation

Question 202: How would you describe a type of attack where an adversary attempts to connect to all 65,536 TCP ports on a single system within a brief timeframe?

A) Reconnaissance

B) Denial-of-Service

C) Compromise

D) Malicious insider

Question 203: Which methodology for threat modeling consists of seven steps, including defining objectives, technical scope, application decomposition, threat analysis, vulnerability assessment, attack modeling, and risk impact analysis?

A) DREAD

B) STRIDE

C) VAST

D) PASTA

Question 204: What term is used to describe software that is stored in a Read-Only Memory (ROM) chip?

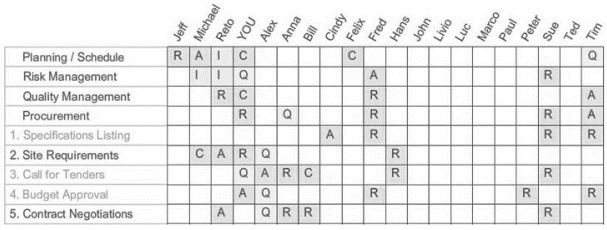
A) Gateway

B) Firmware

C) Proxy

D) Firewall

Question 205: What is the name given to a matrix that clearly outlines roles and responsibilities for various activities or groups of tasks?



	Jeff	Michael	Reto	YOU	Alex	Anna	Bill	Cindy	Felix	Fred	Hans	John	Livio	Luc	Marco	Paul	Peter	Sue	Ted	Tim
Planning / Schedule	R	A	I	C					C											Q
Risk Management		I	I	Q						A								R		
Quality Management			R	C						R										A
Procurement				R		Q				R								R		A
1. Specifications Listing								A		R								R		R
2. Site Requirements		C	A	R	Q						R									
3. Call for Tenders				Q	A	R	C				R							R		
4. Budget Approval				A	Q					R							R			R
5. Contract Negotiations			A		Q	R	R											R		

A) Stakeholder Engagement Assessment Matrix

B) Responsibility Assignment Matrix

C) Power-Interest Matrix

D) Stakeholder Analysis Matrix

Question 206: Which category does the IP address 10.11.45.170 fall under?

A) A loopback address

B) A public IP address

C) An APIPA address

D) An RFC 1918 address

Question 207: What is the term for a smart card used by US government personnel that includes a photograph and other identifying information, serving as both a badge and a smart card?

A) Personal Identity Verification (PIV)

B) Personal Identity Number (PIN)

C) Personal Identity Card (PIC)

D) Government Identity Badge (GIB)

Question 208: Which type of firewall has the capability to inspect traffic at the application layer (Layer 7) and perform protocol-specific analysis for malicious content?

A) Bastion host

B) Application firewall

C) Packet filtering firewall

D) Stateful inspection firewall

Question 209: How would you describe an approach to risk analysis that involves scenario-based evaluation using ranking and grading for exposure ratings and decision-making?

A) Qualitative Risk Analysis

B) Intuitive Risk Analysis

C) Rational Risk Analysis

D) Quantitative Risk Analysis

Question 210: What is the term for a timing vulnerability that occurs when a program verifies access permissions too far in advance of a resource request?

A) TOCTOU

B) GKLX

C) WWWH

D) IOCD

Question 211: Which cryptographic technique provides a partial digital signature, ensuring message integrity during transmission but not offering non-repudiation?

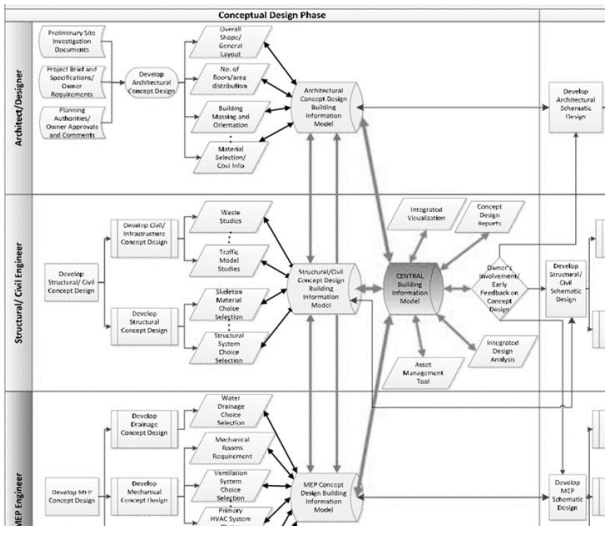
A) Encrypted Message Code Verifier (EMCV)

B) Hashed Message Authentication Code (HMAC)

C) Asymmetric Checksum Verifier (ACV)

D) Encoded Value Verification Code (EVVC)

Question 212: What security model focuses on information flow to maintain and enforce security regardless of how information moves, and is based on a State Machine Model?



A) Noninterference Model

B) Confidentiality Model

C) Information Flow Model

D) Discretionary Model

Question 213: What is the name of the programming tool that converts high-level language code into an executable file designed for a specific operating system?

A) WYSIWYG

B) Interchanger

C) Compiler

D) Transposer

Question 214: In the context of web application security, what potential issue arises when attempting to prevent cross-site scripting attacks by filtering out only the <SCRIPT> tag on the server side?

A) There is no problem with this approach

B) Server-side validation requires removing all HTML tags, not just the <SCRIPT> tag

C) Attackers may use XSS filter evasion techniques against this approach

D) Validation should always be performed on the client side

Question 215: What term describes the process of verifying or testing the validity of an identity claimed by a subject?

A) Verification

B) Confirmation

C) Certification

D) Authentication

Question 216: What type of protocol relies on encapsulation as its core concept?

A) Hashing

B) Bridging

C) Storage

D) Multilayer

Question 217: How would you describe actions that occur on a computer or over IT infrastructure that may not be criminal but often result in internal disciplinary measures or termination?

A) Condoned Activities

B) Appropriate Activities

C) Inappropriate Activities

D) Countenanced Activities

Question 218: When a certificate authority creates a digital signature for a certificate, which key is used to sign the completed certificate?

A) The subject's public key

B) The subject's private key

C) The CA's public key

D) The CA's private key

Question 219: Which type of fuzzing is also known as intelligent fuzzing?

A) Mutation

B) ZZUF

C) Code based

D) Generational

Question 220: What term is used to describe anything within an environment that should be protected?

A) Core Code

B) Trade Secret

C) Master-Object

D) Asset

Question 221: What contractual obligation requires implementation of sound Business Continuity Planning practices for clients?

A) NHL

B) SLA

C) WFL

D) WHO

Question 222: What is the term for a human-readable only card ID typically featuring a photo and written information about the authorized bearer, used in environments where automated controls are impractical but security guards are available?

A) Dumb Card

B) Visual Card

C) Manual Card

D) Key Card

Question 223: What is the comprehensive process of identifying potential threats, evaluating their impact, and implementing cost-effective solutions to mitigate or reduce risk?

A) Risk Management

B) Risk Avoidance

C) Risk Deterrence

D) Risk Prevention

Question 224: What term describes a backup facility maintained in constant working order, with a full complement of servers, workstations, and communication links ready to assume primary operations responsibilities?

A) Warm Site

B) Hot Site

C) Parallel Site

D) Cold Site

Question 225: Which type of SQL functions accumulate values and return a single result?

A) Mathematical Functions

B) Scalar Functions

C) Table-Valued Functions

D) Aggregate Functions

Question 226: Which type of investigation typically has the most relaxed standards for information collection and preservation?

A) Operational investigation

B) Civil investigation

C) Regulatory investigation

D) Criminal investigation

Question 227: What additional function can be added to local or centralized alarm systems to notify police or fire services when an alarm is triggered?

A) Notification Plugin

B) Alert Protocol

C) Escalation Path Matrix

D) Auxiliary Alarm System

Question 228: What type of testing involves diagramming potential hacker approaches to an application and determining how the system would respond to likely attacker behavior?

A) Static code analysis

B) Use case testing

C) Misuse case testing

D) Hacker use case testing

Question 229: In a backup strategy involving full backups on Sundays and differential backups Monday through Friday, what should be applied first when restoring data after a server failure?

A) Tuesday's differential backup

B) Monday's differential backup

C) Sunday's full backup

D) Wednesday's differential backup

Question 230: What is the term for an attack where a hacker operates a false access point that automatically clones the identity of another access point based on a client device's automatic reconnection request?

A) Evil Twin

B) Drive-by Attack

C) Dictionary Attack

D) Man-in-the-Middle Attack

Question 231: What is the combination of the Data Link Layer header, payload, and footer called?

A) On-Page portion

B) <Body>

C) Physical Construct

D) Frame

Question 232: Which security control would be most effective for tracing the source of sensitive documents if they appear in a public forum?

A) Hashing

B) Watermarking

C) Digital signature

D) Document staining

Question 233: What category of technology do cable modems, ISDN, and DSL fall under?

A) Broadband

B) Digital

C) Baseband

D) Broadcast

Question 234: Which of the following is not a recognized design in Mandatory Access Control systems?

A) Hybrid

B) Compartmentalized

C) Bracketed

D) Hierarchical

Question 235: What methods are commonly employed to protect data in transit?

A) Encrypted storage media

B) TLS, VPN, IPsec

C) Telnet, ISDN, UDP

D) AES, Serpent, IDEA

Question 236: What term describes a sophisticated local telephone exchange often used by organizations for inbound call support, extension-to-extension calling, conference calling, and voicemail?

A) Cloud Phones (VoIP)

B) Private Branch Exchange (PBX)

C) Computer Telephony Integration (CTI)

D) Unified Voicemail Desktop Telephony (UVDT)

Question 237: What is typically the largest RAM storage resource available to a computer, composed of dynamic

RAM chips that require periodic refreshing by the CPU?

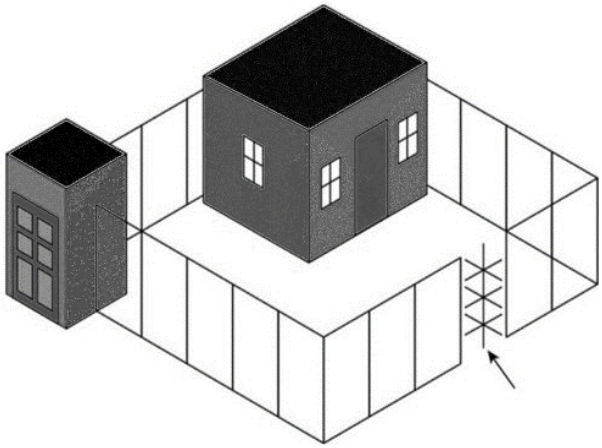
A) Shared Memory

B) Private Memory

C) Virtual Memory

D) Real Memory

Question 238: What security control is indicated by an arrow pointing to a unidirectional gate that prevents more than one person from entering a facility at a time?



A) Turnstile

B) Mantrap

C) Portal

D) Intrusion prevention system

Question 239: Which protocol is primarily used for moving email messages from clients to servers and between servers?

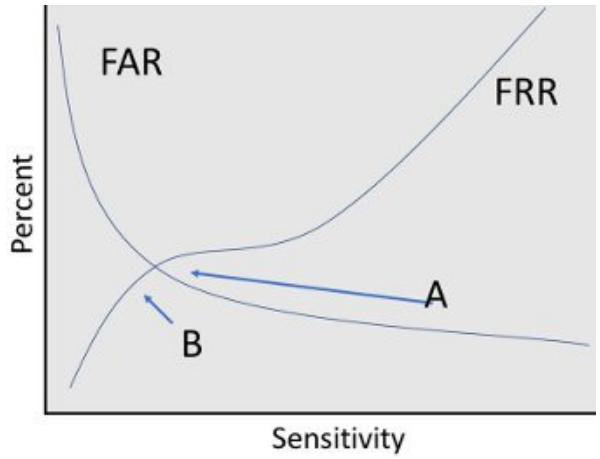
A) HTML

B) IMAP

C) POP3

D) SMTP

Question 240: At what point on a biometric authentication curve would false acceptance rates be very high?



A) False acceptance will be very low

B) False rejection will be very high

C) False projection will be very low

D) False acceptance will be very high

Question 241: How many symmetric encryption keys are needed for a system with 6 users where any 2 users should be able to communicate securely?

A) 15

B) 6

C) 12

D) 30

Question 242: How would you describe an object that can perform a task with minimal assistance from other objects?

A) Highly cohesive

B) Pliable

C) Serviceable

D) Durable

Question 243: What is the term for the portion of a storage device used to load the operating system and the types of viruses that target this process?

A) SSD

B) Genesis Partition

C) Core Drive

D) Boot Sector

Question 244: What vulnerability allows users in an open wireless network to potentially capture other customers' web traffic, including usernames and passwords?

A) A user has ARP spoofed the router, making all traffic broadcast to all users

B) Open networks are unencrypted, making traffic easily sniffable

C) The password is shared by all users, making traffic vulnerable

D) A malicious user has installed a Trojan on the router

Question 245: What two controls would be most effective in preventing password cracking attacks against a system?

A) Salting and use of MD5

B) Over-the-wire encryption and use of SHA1 instead of MD5

C) Longer passwords and salting

D) Using shadow passwords and salting

Question 246: When configuring egress monitoring on a network, which type of packets should be allowed to leave the network headed for the Internet?

A) Packets with source address from the private address block

B) Packets with the destination address from the public IP address block

C) Packets with the source address from the public IP address block

D) Packets with the source address outside of the address block

Question 247: What risk metric is reduced when using encryption to protect sensitive business information during transmission over the Internet?

A) Likelihood

B) Impact

C) MTO

D) RTO

Question 248: Which type of intellectual property protection is most suitable for a company wanting to license a newly developed manufacturing process to other companies while preventing unauthorized use?

A) Trade secret

B) Copyright

C) Trademark

D) Patent

Question 249: What is the set of rules and restrictions that define how data is transmitted over a network medium, enabling computer-to-computer communications?

A) Program

B) Protocol

C) Router

D) Port

Question 250: Which type of SQL functions, such as COUNT(), MIN(), MAX(), SUM(), and AVG(), can be run against a database to produce an information set?

A) Mathematical Functions

B) Scalar Functions

C) Table-Valued Functions

D) Aggregate Functions

Correct Answers & Explanations

Question 1

D) Provisioning (Correct Answer)

Explanation: Provisioning is the process of creating and managing user accounts, including setting up access rights and ensuring the account is available across all necessary systems. This is a crucial part of identity management, especially when onboarding new employees.

Question 2

A) Adjust the sensitivity of the biometric devices (Correct Answer)

Explanation: When FAR and FRR are not providing acceptable performance, adjusting the sensitivity of biometric devices can help balance these rates. This allows fine-tuning of the system to achieve optimal performance without replacing the entire system.

Question 3

A) Transport (Correct Answer)

Explanation: The Transport layer (Layer 4) in the OSI model is responsible for end-to-end communication between hosts, using protocols like TCP and UDP. It ensures reliable data transfer, error recovery, and flow control.

Question 4

A) User Acceptance Testing (Correct Answer)

Explanation: User Acceptance Testing (UAT) is the final phase of software testing where end users or clients test the software to verify that it can handle required tasks in real-world scenarios, ensuring it meets the business requirements before moving to production.

Question 5

D) Electromagnetic Interference (Correct Answer)

Explanation: Electromagnetic Interference (EMI) refers to unwanted electrical or electromagnetic disturbances that can affect the performance of electronic equipment, causing issues with functionality and impacting the quality of communications and transmissions.

Question 6

A) Vulnerability (Correct Answer)

Explanation: A vulnerability is a weakness or flaw in an organization's IT infrastructure, systems, or processes that can be exploited by threats. It often results from inadequate security measures or the absence of proper safeguards.

Question 7

A) Copyright (Correct Answer)

Explanation: Copyright is a form of intellectual property protection that grants creators exclusive rights to their original works, including the right to reproduce, distribute, and adapt the work. It protects against unauthorized duplication or use of the copyrighted material.

Question 8

A) Steganography (Correct Answer)

Explanation: Steganography is the practice of concealing information within other non-secret data or media, such as images. In this scenario, sensitive information could be hidden within the suspicious photos, making it difficult for standard data loss prevention systems to detect.

Question 9

D) Update the system security plan (Correct Answer)

Explanation: According to NIST SP 800-18, when a significant change occurs in a system, the system owner

should update the system security plan. This ensures that the security plan remains current and accurately reflects the system's security posture.

Question 10

A) Sniffer Attack (Correct Answer)

Explanation: A sniffer attack involves intercepting and logging network traffic using packet-capturing software. This allows attackers to view and analyze data passing through a network, potentially exposing sensitive information.

Question 11

A) Palm Scan (Correct Answer)

Explanation: Palm scan biometrics use near-infrared light to capture the unique vein patterns in a person's palm. This method is highly accurate and difficult to forge, making it suitable for high-security authentication purposes.

Question 12

D) Role-Based Access Control (Correct Answer)

Explanation: The described system is an example of Role-Based Access Control (RBAC). In RBAC, access permissions are associated with roles (e.g., Reviewers, Submitters), and users are assigned to appropriate roles, simplifying access management.

Question 13

D) Kill Chain Model (Correct Answer)

Explanation: The Kill Chain Model, developed by Lockheed Martin, describes the stages of a cyber attack: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives. It helps in understanding and defending against advanced persistent threats.

Question 14

A) Challenge Handshake Authentication Protocol (CHAP) (Correct Answer)

Explanation: CHAP is an authentication protocol that uses a challenge-response mechanism. After establishing a connection, the server sends a challenge to the client, which must be correctly responded to for authentication to succeed. It's commonly used in Point-to-Point Protocol (PPP) connections.

Question 15

B) Endpoint DLP (Correct Answer)

Explanation: Endpoint Data Loss Prevention (DLP) is the most appropriate solution for identifying sensitive files stored on individual laptops. It can monitor, detect, and prevent unauthorized use or transfer of sensitive data on endpoint devices.

Question 16

D) On-Premise Solution (Correct Answer)

Explanation: An on-premise solution refers to the traditional IT deployment model where an organization purchases, owns, and maintains its hardware and software within its own facilities. This contrasts with cloud-based or off-premise solutions.

Question 17

D) Wireshark (Correct Answer)

Explanation: Wireshark is a powerful network protocol analyzer that can capture and inspect network traffic in real-time. For unencrypted VoIP communications, Wireshark can be used to intercept and analyze voice data, compromising confidentiality.

Question 18

D) Add a second authentication factor for more reliable identification (Correct Answer)

Explanation: While hand geometry scanners can be effective, adding a second authentication factor (multi-factor authentication) significantly enhances security. This approach combines something you are (biometrics) with something you know (e.g., PIN) or have (e.g., smart card), providing more reliable identification.

Question 19

D) Anomaly-based intrusion detection (Correct Answer)

Explanation: Anomaly-based intrusion detection is most effective against zero-day attacks because it can identify unusual patterns or behaviors that deviate from the norm, even if the specific attack signature is unknown. This makes it capable of detecting novel threats.

Question 20

B) Spamming (Correct Answer)

Explanation: Spamming refers to the practice of sending unsolicited bulk messages, often for advertising purposes but also as a form of attack. It can overwhelm systems, consume resources, and cause general annoyance to users.

Question 21

D) Coupling (Correct Answer)

Explanation: In software design, coupling refers to the degree of interdependence between software modules. Lower coupling indicates a better design as it means modules are more independent, making the system easier to maintain, modify, and understand.

Question 22

C) QualysGuard (Correct Answer)

Explanation: QualysGuard is a comprehensive vulnerability management solution specifically designed for network vulnerability scanning. It can identify, track, and manage vulnerabilities in an organization's IT infrastructure.

Question 23

A) The Certificate Authority that issued the certificate (Correct Answer)

Explanation: The Certificate Authority (CA) that issued the digital certificate has the authority to add it to a Certificate Revocation List (CRL). This ensures that only the entity that vouched for the certificate's validity can declare it compromised or invalid.

Question 24

C) Bridge (Correct Answer)

Explanation: A bridge is a network device that connects multiple network segments, potentially with different speeds or topologies, but using the same protocol. It operates at the data link layer of the OSI model and can filter traffic between network segments.

Question 25

D) SLE (Correct Answer)

Explanation: SLE stands for Single Loss Expectancy, which represents the monetary value expected to be lost from a single occurrence of a risk event. It's a crucial metric in risk assessment for understanding the potential impact of individual risk events.

Question 26

B) * (Correct Answer)

Explanation: In systems using shadowed passwords, the /etc/passwd file contains an asterisk (*) or an 'x' in the password field. This indicates that the actual password hash is stored in a separate, more secure file (usually /etc/shadow) that is only accessible by privileged users.

Question 27

A) Reverse Engineering (Correct Answer)

Explanation: Reverse engineering is the process of analyzing a finished product to understand its design, architecture, and functionality. In software, it often involves decompiling or disassembling code to understand how it works. This practice can be controversial when used to create competing products.

Question 28

B) False Positive (Correct Answer)

Explanation: A false positive in security scanning occurs when a scanner incorrectly identifies a vulnerability that doesn't actually exist. This happens when there's insufficient information to conclusively determine if a vulnerability is present, leading to an erroneous alert.

Question 29

D) Parallel Test (Correct Answer)

Explanation: A parallel test in disaster recovery involves activating the disaster recovery site and running it simultaneously with the primary site. This allows for testing the disaster recovery capabilities without disrupting normal operations, ensuring the backup site can handle the workload if needed.

Question 30

B) A bus and a ring (Correct Answer)

Explanation: Both bus and ring logical topologies can be physically implemented as a star topology. In a star-wired bus, all nodes connect to a central hub, but logically operate as if on a single cable. Similarly, a star-wired ring connects all nodes to a central device but maintains a logical ring structure for data flow.

Question 31

C) Risk mitigation (Correct Answer)

Explanation: Risk mitigation involves developing and implementing strategies to reduce the likelihood or impact of identified risks. This process includes creating action plans to enhance opportunities and minimize threats to project objectives, making it a crucial part of risk management.

Question 32

D) Hierarchical Environments (Correct Answer)

Explanation: In Mandatory Access Control (MAC), hierarchical environments refer to systems where security classifications are organized in a structured hierarchy from lowest to highest security levels. This allows for clear delineation of access rights based on security clearance levels.

Question 33

C) Bust-Out (Correct Answer)

Explanation: A bust-out scheme is a type of credit card fraud where the perpetrator builds a good credit history through normal usage and timely payments, then maxes out the credit limit with no intention of repaying. This sudden change in behavior often occurs just before the fraudster disappears.

Question 34

D) It uses a handshake (Correct Answer)

Explanation: TCP (Transmission Control Protocol) is connection-oriented because it uses a three-way handshake to establish a connection before data transfer begins. This handshake ensures both parties are ready to communicate and sets up the parameters for the connection.

Question 35

B) Distributed Access Control (Correct Answer)

Explanation: Distributed Access Control involves spreading the responsibility for access control decisions across multiple entities within a system. This approach enhances security by not relying on a single point of control and allows for more flexible and scalable access management in complex environments.

Question 36

D) Public Key (Correct Answer)

Explanation: In asymmetric-key encryption, the public key is the value that is freely distributed and used by anyone to encrypt messages or verify digital signatures. The corresponding private key, kept secret by the owner, is used to decrypt messages or create digital signatures.

Question 37

D) Create rule (Correct Answer)

Explanation: In the Take-Grant Protection model, the Create rule allows a subject to create new objects and establish initial rights to those objects. This rule is fundamental in defining how new entities are introduced into the system and how initial access permissions are set.

Question 38

C) Fault (Correct Answer)

Explanation: A fault can refer to both a temporary power loss and a malfunction within a system or device. In electrical systems, it can mean a short-term power interruption, while in computing and engineering, it describes any abnormal condition or defect that causes a component to fail to perform its required function.

Question 39

B) Domain Hijacking (Correct Answer)

Explanation: Domain hijacking refers to the unauthorized alteration or takeover of a domain name's registration

without the legitimate owner's consent. This can involve changing the domain's registration information, transferring it to another registrar, or redirecting it to different name servers.

Question 40

D) Star Topology (Correct Answer)

Explanation: In a star topology, all nodes (computers or other network devices) are connected directly to a central device, typically a hub or switch. This central device acts as a conduit to transmit messages, providing a centralized network structure with individual point-to-point connections for each node.

Question 41

A) TKIP (Correct Answer)

Explanation: Temporal Key Integrity Protocol (TKIP) is a security protocol used in wireless networks, specifically designed to secure data in transit. Unlike other protocols mentioned, TKIP is exclusively used for protecting data as it travels over a network and is not applicable to data at rest.

Question 42

B) Application Programming Interfaces (Correct Answer)

Explanation: Application Programming Interfaces (APIs) allow developers to interact directly with underlying services and functionalities through predefined function calls. They provide a way to access features and data of an application or service programmatically, often bypassing traditional user interfaces.

Question 43

A) Opinion Evidence (Correct Answer)

Explanation: Opinion evidence refers to a witness's personal interpretation or sentiment about facts, rather than direct observations. In legal proceedings, this type of evidence is

generally considered inadmissible unless the witness is qualified as an expert in the relevant field.

Question 44

B) Owner (Correct Answer)

Explanation: The owner, typically referring to the business owner or top-level executive, holds ultimate corporate responsibility for data protection and storage. They are accountable for establishing and enforcing security policies and can be held liable for negligence in these areas.

Question 45

B) Biometric-based SSO (Correct Answer)

Explanation: Biometric-based Single Sign-On (SSO) integrates traditional authentication methods with biometric factors like fingerprints, retinal scans, or facial recognition. This approach enhances security by combining something you know or have with something you are (biometric data).

Question 46

C) Bus (Correct Answer)

Explanation: In a bus topology, all devices are connected to a single cable, known as the bus or backbone. This forms a single line of communication where data transmitted by any device is received by all others on the network, though only the intended recipient processes the data.

Question 47

B) Data Remanence (Correct Answer)

Explanation: Data remanence refers to the residual representation of data that remains on storage media even after attempts have been made to remove or erase it. This persistence of data can pose security risks if sensitive information is recoverable from discarded or repurposed storage devices.

Question 48

B) Full Interruption Test (Correct Answer)

Explanation: A full interruption test, also known as a full-scale test, is the most comprehensive and potentially disruptive type of disaster recovery test. It involves completely shutting down the primary site and fully activating the disaster recovery site, simulating a real disaster scenario.

Question 49

D) Man-in-the-Middle (Correct Answer)

Explanation: A Man-in-the-Middle (MitM) attack occurs when an attacker secretly intercepts and potentially alters the communication between two parties who believe they are directly communicating with each other. This allows the attacker to eavesdrop on or manipulate the exchanged data.

Question 50

A) Fence (Correct Answer)

Explanation: In physical security, a fence is used to clearly define and differentiate areas under specific levels of security protection. It serves as a visible boundary, deterrent, and first line of defense, helping to control access and delineate secure zones from public or less secure areas.

Question 51

D) Configuration control (Correct Answer)

Explanation: Configuration control is the process that supports multiple developers working on code simultaneously. It allows for version control, tracking changes, and managing different versions of code, which is essential for collaborative software development.

Question 52

C) Password attack (Correct Answer)

Explanation: Brute-force and dictionary attacks are methods used specifically to crack passwords. They involve systematically attempting various combinations (brute-force) or using a list of common words (dictionary attack) to guess passwords, making them types of password attacks.

Question 53

D) Limit check (Correct Answer)

Explanation: A limit check is a control that ensures input falls within a predefined range. For a BMI calculator, it would prevent unrealistic weight values from being entered, improving data accuracy and application reliability.

Question 54

B) A CDN (Correct Answer)

Explanation: A Content Delivery Network (CDN) is the best solution for providing low latency, high performance, and high availability for global content delivery. CDNs use distributed servers worldwide to cache and serve content closer to end-users, reducing load times and improving reliability.

Question 55

D) Bcrypt (Correct Answer)

Explanation: Bcrypt is a password-hashing function that incorporates a salt to protect against rainbow table attacks. It's designed for password storage and uses key stretching techniques to make it computationally intensive, increasing security against brute-force attacks.

Question 56

A) Gray box (Correct Answer)

Explanation: Gray box testing combines elements of both black box and white box testing. The tester has partial knowledge of the internal workings (source code in this

case) while also testing from an end-user perspective, which matches Barry's approach.

Question 57

C) Encrypting the files (Correct Answer)

Explanation: Encrypting the files is a risk mitigation strategy that directly addresses the concern of hackers stealing sensitive information. It ensures that even if unauthorized access occurs, the data remains unreadable without the decryption key.

Question 58

D) Trade secret (Correct Answer)

Explanation: A trade secret is the most appropriate form of intellectual property protection for a manufacturing process that a company wants to keep confidential indefinitely. Unlike patents, which require public disclosure and have a limited lifespan, trade secrets can be protected indefinitely as long as they remain secret.

Question 59

D) PGP (Correct Answer)

Explanation: Pretty Good Privacy (PGP) is a widely used encryption program that employs the IDEA algorithm for file and email encryption. It's known for its grassroots support and is not a formal standard but an independently developed product.

Question 60

B) Offering real-time incident response information (Correct Answer)

Explanation: Key Risk Indicators (KRIs) are typically used for proactive risk management and monitoring. They provide insights into potential future risks rather than real-time incident response information, which is more aligned with

Security Information and Event Management (SIEM) systems.

Question 61

D) Hybrid (Correct Answer)

Explanation: A hybrid identity management model is the most suitable for Cap'n Oz's situation. It allows the organization to maintain its existing on-premises Active Directory while integrating with cloud-based services, providing a seamless experience across both environments.

Question 62

C) Classification (Correct Answer)

Explanation: Classification is the process of categorizing information or resources based on their sensitivity or value to an organization. This label determines the level of security measures required to protect the resource.

Question 63

A) Safe Harbor (Correct Answer)

Explanation: The Safe Harbor principles were designed to prevent unauthorized disclosure of information in data transfers between the EU and the US. These seven principles align with the description provided in the question.

Question 64

A) Trojan Horse (Correct Answer)

Explanation: A Trojan Horse is malicious software that appears legitimate but contains hidden malicious code. It performs the advertised functions while also executing unauthorized actions, matching the description in the question.

Question 65

D) Audit (Correct Answer)

Explanation: An audit is a systematic examination or review of an environment to ensure compliance with regulations and to detect abnormalities or unauthorized activities. It's a methodical process used in various contexts, including financial, operational, and security reviews.

Question 66

C) Companion Virus (Correct Answer)

Explanation: A companion virus is a type of virus that creates a file with a similar name to a legitimate system file but with a different extension. When executed, it runs instead of the legitimate file, allowing it to evade detection while carrying out malicious activities.

Question 67

A) 3, 1, 2, 5, 4 (Correct Answer)

Explanation: The correct chronological order for software testing phases is: Pre-Alpha (3), Alpha (1), Beta (2), Release Candidate (5), and finally Release (4). This sequence represents the typical progression of software from initial development to public release.

Question 68

B) Master Boot Record (MBR) (Correct Answer)

Explanation: The Master Boot Record (MBR) is the first sector of a hard drive or floppy disk that contains information on how to load the operating system. It's crucial for the boot process and is read by the computer when starting up.

Question 69

B) Need-to-know (Correct Answer)

Explanation: The need-to-know principle is a fundamental concept in information security that restricts access to information or resources based on what is necessary for an

individual to perform their job duties. It ensures that users only have access to what they legitimately require.

Question 70

C) SFTP (Correct Answer)

Explanation: SFTP (Secure File Transfer Protocol) is the most appropriate choice for secure file transfer over an untrusted network. It provides encryption and secure authentication, ensuring data confidentiality and integrity during transfer.

Question 71

B) Protected Health Information (Correct Answer)

Explanation: Protected Health Information (PHI) refers to health data that is created, received, stored, or transmitted by HIPAA-covered entities. It includes medical records, billing information, and other health-related data that is individually identifiable.

Question 72

A) Data owner (Correct Answer)

Explanation: In a formal data governance program, the data owner is typically responsible for assigning classification levels to data. They have the authority and knowledge to determine the sensitivity and value of the data to the organization.

Question 73

B) Piggybacking (Correct Answer)

Explanation: Piggybacking refers to the unauthorized act of following an authorized person through a secure entrance without proper authentication. It's a common physical security breach where an unauthorized individual gains access by closely following someone with legitimate access.

Question 74

B) Non-interference Model (Correct Answer)

Explanation: The Non-interference Model, developed by Goguen and Meseguer, is designed to prevent information flow between different security levels. It ensures that actions at a higher security level do not affect or interfere with observations at a lower security level.

Question 75

A) Fourth Amendment (Correct Answer)

Explanation: The Fourth Amendment to the US Constitution protects against unreasonable searches and seizures. It requires law enforcement to obtain a warrant based on probable cause before searching private property, thus safeguarding citizens' privacy rights.

Question 76

D) Kerberos (Correct Answer)

Explanation: Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography. It offers mutual authentication, where both the client and server verify each other's identity, making it ideal for secure network communications.

Question 77

A) Nonrepudiation (Correct Answer)

Explanation: Nonrepudiation is a security service that prevents an individual or entity from denying that they performed a particular action related to data. It ensures that a party in a dispute cannot repudiate, or refute, the validity of a statement or contract.

Question 78

D) Business Impact Assessment (BIA) (Correct Answer)

Explanation: A Business Impact Assessment (BIA) is a crucial component of business continuity planning. It identifies critical business functions, assesses potential impacts of

disruptions, and helps determine recovery priorities and strategies.

Question 79

B) Endpoint Security (Correct Answer)

Explanation: Endpoint Security refers to the practice of securing end-user devices such as desktops, laptops, and mobile devices. It emphasizes that each device must maintain its own security, regardless of network protections, to create a comprehensive security posture.

Question 80

C) MTD (Correct Answer)

Explanation: Maximum Tolerable Downtime (MTD) is the longest period a business can survive without its critical systems before suffering irrevocable damage. It's a crucial metric in business continuity planning, helping prioritize recovery efforts.

Question 81

C) Identification and authentication (Correct Answer)

Explanation: Accountability in access control relies on identification (claiming an identity) and authentication (proving that identity). These two factors ensure that users are who they claim to be before granting access, enabling traceability of actions.

Question 82

B) Software Quality Management (Correct Answer)

Explanation: Software Quality Management is not a key process area for the repeatable phase of SW-CMM. The repeatable phase focuses on project management processes, including planning, tracking, and subcontract management, but not specifically on quality management.

Question 83

D) Cross-Site Scripting (XSS) (Correct Answer)

Explanation: Cross-Site Scripting (XSS) is a web application vulnerability where attackers inject malicious scripts into web pages viewed by other users. It often exploits inadequate input validation, allowing attackers to execute scripts in the victim's browser.

Question 84

D) MAC (Correct Answer)

Explanation: Bell-LaPadula is an example of a Mandatory Access Control (MAC) model. MAC enforces access control based on security labels assigned to subjects and objects, which aligns with Bell-LaPadula's focus on maintaining confidentiality in hierarchical security structures.

Question 85

B) Common Mode Noise (Correct Answer)

Explanation: Common Mode Noise refers to electromagnetic interference that appears equally and in phase on both conductors relative to ground. It's often caused by differences in ground potential between devices or systems.

Question 86

A) Bluebugging (Correct Answer)

Explanation: Bluebugging is a specific type of Bluetooth attack where hackers gain unauthorized access to a Bluetooth-enabled device, potentially controlling its features remotely. This can include activating the microphone, making calls, or accessing data.

Question 87

A) It limits what users can do or see based on privileges (Correct Answer)

Explanation: A constrained user interface restricts user actions and visible information based on their access

privileges. This approach enhances security by ensuring users only interact with system elements appropriate to their authorization level.

Question 88

D) Encapsulating Security Payload (Correct Answer)

Explanation: Encapsulating Security Payload (ESP) is an IPSec protocol that provides both authentication and encryption of the data being transmitted. It encapsulates the entire IP packet, offering a higher level of security than Authentication Header (AH) alone.

Question 89

C) Consistency (Correct Answer)

Explanation: In the ACID properties of database transactions, "C" stands for Consistency. This ensures that a transaction brings the database from one valid state to another, maintaining all predefined rules and constraints.

Question 90

D) Direct Addressing (Correct Answer)

Explanation: Direct Addressing is a method where the CPU is provided with the actual memory address of the data to be accessed. This allows for faster memory access as the CPU doesn't need to perform additional calculations to find the data location.

Question 91

D) DNS Poisoning (Correct Answer)

Explanation: DNS Poisoning, also known as DNS Cache Poisoning, involves corrupting a DNS server's cache with false information. This causes the server to return an incorrect IP address, redirecting traffic to malicious sites.

Question 92

C) Boolean (Correct Answer)

Explanation: A Boolean data type represents two truth values - true and false. It's fundamental in computer science for logical operations and control structures, named after mathematician George Boole.

Question 93

A) A gateway (Correct Answer)

Explanation: A gateway is the most appropriate device for connecting networks using different protocols, such as IPv4 and IPv6. It can translate between these protocols, allowing communication between the two different network types.

Question 94

B) Release control (Correct Answer)

Explanation: Release control is the change management process that encompasses user acceptance testing. It manages the final stages of development, including testing and deployment of new software versions.

Question 95

B) Handshake (Correct Answer)

Explanation: The TCP handshake, also known as the three-way handshake, is the process used to establish a connection between two hosts in a TCP/IP network. It involves three steps: SYN, SYN-ACK, and ACK.

Question 96

A) Fuzzy Logic (Correct Answer)

Explanation: Fuzzy Logic is a computational approach that attempts to mimic human-like reasoning. Unlike traditional binary logic, it can handle partial truths and uncertainties, making it more suitable for complex, real-world problems.

Question 97

D) Limit check (Correct Answer)

Explanation: A limit check is a control that ensures input values fall within a predefined acceptable range. For a BMI calculator, it would prevent unrealistic weight values, improving data accuracy and application reliability.

Question 98

B) A CDN (Correct Answer)

Explanation: A Content Delivery Network (CDN) is the best solution for providing low latency, high performance, and high availability for global content delivery. CDNs use distributed servers worldwide to cache and serve content closer to end-users.

Question 99

A) Gray box (Correct Answer)

Explanation: Gray box testing combines elements of both black box and white box testing. The tester has partial knowledge of the internal workings (source code in this case) while also testing from an end-user perspective.

Question 100

C) Encrypting the files (Correct Answer)

Explanation: Encrypting the files is an effective risk mitigation strategy against data theft. It ensures that even if unauthorized access occurs, the data remains unreadable without the decryption key, thus protecting sensitive information.

Question 101

B) Implicit deny (Correct Answer)

Explanation: The implicit deny principle is a fundamental concept in access control. It states that if there's no explicit permission granted to a user for an object, access is automatically denied. In Donald Blake's implementation, users are denied access to objects they don't have rights to,

even without an explicit rule, which aligns perfectly with the implicit deny principle.

Question 102

C) Vigilante methodology (Correct Answer)

Explanation: When IT personnel make security decisions independently without consulting senior management, it's considered a vigilante methodology. This approach bypasses proper channels and authority, potentially leading to inconsistent or unauthorized security practices. It's not a bottom-up approach as that implies a structured flow of ideas, nor is it mutiny or an inside attack which have more severe implications.

Question 103

D) Cloud Shared-Responsibility Model (Correct Answer)

Explanation: The Cloud Shared-Responsibility Model is a concept in cloud computing where both the cloud service provider and the customer share responsibilities for security and compliance. The provider typically secures the infrastructure, while the customer is responsible for data, access management, and application-level controls. This model ensures a clear division of security duties between the two parties.

Question 104

C) Bind (Correct Answer)

Explanation: In LDAP (Lightweight Directory Access Protocol), the Bind operation is used for authentication. It allows a client to identify itself to the LDAP server using credentials, typically a username and password. This operation establishes the authentication state for the LDAP session, making it crucial for secure access to the directory service.

Question 105

A) RTO (Correct Answer)

Explanation: RTO stands for Recovery Time Objective, which is the maximum tolerable length of time a computer, system, network, or application can be down after a failure or disaster occurs. In business continuity planning, minimizing RTO is crucial as it represents how quickly an organization needs to recover its IT systems to avoid unacceptable consequences associated with a break in business continuity.

Question 106

D) Use Case Testing (Correct Answer)

Explanation: Use Case Testing involves testing the software against realistic scenarios that represent how end-users will interact with the system. In this case, Quan Yaozu is inputting data into actual tax forms to verify the software's accuracy, which directly simulates how the end-users (tax preparers or individuals) would use the software. This approach ensures that the software performs correctly under real-world conditions.

Question 107

B) Cryptosystem (Correct Answer)

Explanation: A cryptosystem is a suite of algorithms for cryptographic key generation, encryption, and decryption. It's designed to provide secure communication between parties using either shared secret keys (symmetric cryptography) or pairs of public and private keys (asymmetric cryptography). This system encompasses all the necessary components to facilitate secure communication, making it the most accurate term for the described scenario.

Question 108

C) Remote Mirroring (Correct Answer)

Explanation: Remote Mirroring is a data backup technique where data is copied in real-time from one location to another, typically over a network or the internet. This method maintains an exact, up-to-date copy of the primary database at a secondary location, making it the most advanced database backup solution. It ensures minimal data loss and quick recovery in case of a disaster at the primary site.

Question 109

B) 100BaseTX (Correct Answer)

Explanation: 100BaseTX is a form of twisted-pair Ethernet cable capable of supporting network traffic at a nominal rate of 100 Mbit/s. It uses two pairs of high-quality twisted-pair copper wires, making it suitable for Fast Ethernet networks. This standard is widely used in local area networks and provides a good balance between speed and cost-effectiveness.

Question 110

D) UDP Protocol (Correct Answer)

Explanation: UDP (User Datagram Protocol) is a connectionless protocol that does not establish a connection before sending data and does not guarantee packet delivery. It's designed for speed and efficiency rather than reliability. UDP is often used for real-time applications like video streaming or online gaming where speed is more critical than ensuring every packet arrives.

Question 111

D) Dictionary Attack (Correct Answer)

Explanation: A Dictionary Attack is a method used to break into a password-protected computer or server by systematically entering every word in a dictionary as a password. It's an attack against a system designed to uncover passwords associated with known usernames. This

method often employs scripts or programs that automate the process of trying common passwords and dictionary words, making it an efficient way to crack weak passwords.

Question 112

B) Smart card (Correct Answer)

Explanation: While the image is not provided, the description suggests a Smart card. Smart cards contain an embedded integrated circuit chip that can process data, providing secure storage of data and robust authentication capabilities. They are commonly used for physical access control in organizations due to their advanced security features and ability to store multiple credentials or access rights.

Question 113

C) USA Patriot Act (Correct Answer)

Explanation: The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) was enacted in response to the September 11, 2001 terrorist attacks. This act significantly expanded law enforcement and intelligence agencies' powers, including enhanced surveillance capabilities, easier information sharing between agencies, and broadened definitions of terrorism-related activities.

Question 114

A) United States (Correct Answer)

Explanation: The International Safe Harbor Privacy Principles were primarily designed to regulate data transfers between the European Union and the United States. The onward transfer provision specifically addresses the transfer of personal data to third parties outside the EU. As LexCorp is an Irish company (within the EU), transferring data to the United States would activate these provisions, as the U.S. is

not considered to have adequate data protection laws by EU standards.

Question 115

C) Full-Interruption Test (Correct Answer)

Explanation: A Full-Interruption Test, also known as a full-scale test, involves completely shutting down operations at the primary site and fully activating the disaster recovery site. This type of test is the most comprehensive and realistic disaster recovery test, as it simulates a real disaster scenario where the primary site becomes completely unavailable. It allows organizations to evaluate their ability to continue operations from the recovery site under real-world conditions.

Question 116

C) Log Analysis (Correct Answer)

Explanation: Log Analysis is the process of systematically reviewing and interpreting log data to identify patterns, anomalies, or security incidents. It involves examining various system, application, and network logs to detect unauthorized access attempts, policy violations, or other security-relevant events. This thorough examination of logged information helps in understanding system behavior, troubleshooting issues, and maintaining security compliance.

Question 117

C) Manual (Correct Answer)

Explanation: Manual code review is the most appropriate type for considering business logic. Unlike automated tools (used in static or dynamic analysis), human reviewers can understand and evaluate the context, intent, and business rules implemented in the code. Manual review allows for a comprehensive assessment of how well the code aligns with

business requirements and can identify logical flaws that automated tools might miss.

Question 118

A) The most efficient method of conveying information is electronic. (Correct Answer)

Explanation: This statement is not a principle of the Agile approach. Agile methodologies emphasize face-to-face communication and interactions over formal documentation or electronic communication. The other options (simplicity, working software as a measure of progress, and daily collaboration between business people and developers) are all key principles of Agile development, focusing on flexibility, continuous delivery, and close collaboration.

Question 119

B) Blackboxing (Correct Answer)

Explanation: Blackboxing is not a common attack vector for VoIP systems. The other options - Caller ID spoofing (manipulating caller identification), Denial of Service (overwhelming the system to disrupt service), and Eavesdropping (intercepting voice communications) - are all significant security concerns for VoIP. Blackboxing typically refers to a testing method where the internal structure of a system is not known, which is not directly related to VoIP security threats.

Question 120

A) DSA (Correct Answer)

Explanation: The Digital Signature Algorithm (DSA) matches all the characteristics described. It was developed by the National Institute of Standards and Technology (NIST) in 1991 specifically for digital signatures. DSA uses modular exponentiation and is based on the discrete logarithm problem. It's primarily used for signing and verification, making it a key component in many digital signature

schemes. Unlike RSA, which can be used for both encryption and signatures, DSA is specifically designed for digital signatures.

Question 121

B) Port (Correct Answer)

Explanation: In networking and protocols, a port is a logical construct that identifies a specific process or a type of network service. It acts as a connection address within a protocol, allowing multiple services or applications to coexist on a single IP address. Ports are crucial for directing network traffic to the correct application or service on a device, enabling efficient communication in complex networked environments.

Question 122

A) Malware (Correct Answer)

Explanation: Malware, short for malicious software, is the broad term used to describe any software designed to cause harm to a computer system. This includes viruses, worms, trojans, ransomware, and spyware. Malware can perform various unwanted or unauthorized activities, such as stealing data, disrupting operations, or gaining unauthorized access to systems. It's a significant threat in information security, requiring constant vigilance and protection measures.

Question 123

C) dd (Correct Answer)

Explanation: The 'dd' (data duplicator) command is a powerful and versatile Unix utility that can create exact, bit-for-bit copies of storage devices. It's widely used in digital forensics for creating forensic images of hard drives because it can copy data at the lowest level, preserving all information including deleted files and slack space. Unlike xcopy or ImageMagik, which are file-level copying tools, 'dd'

creates a complete, unaltered copy suitable for forensic analysis.

Question 124

D) Degaussing (Correct Answer)

Explanation: Degaussing is the process of using a strong magnetic field to erase data stored on magnetic media. This method is highly effective for securely erasing data from hard drives, tapes, and other magnetic storage devices. Degaussing disrupts the magnetic domains on the storage medium, making the data unrecoverable. It's often used when physical destruction of the media is not feasible or when the storage device needs to be reused securely.

Question 125

D) AND (Correct Answer)

Explanation: In the context of Information Systems Security and boolean logic, the ^ symbol typically represents the AND operation. The AND operation returns true only if both input values are true. It's commonly used in programming, database queries, and access control rules to combine multiple conditions. In some contexts, ^ can represent XOR (exclusive OR), but given the options and the security context, AND is the most appropriate answer.

Question 126

C) RAM (Correct Answer)

Explanation: RAM (Random Access Memory) is classified as volatile memory. Volatile memory requires constant power to maintain stored information. When power is removed, all data in RAM is lost. This is in contrast to non-volatile memory types like EEPROM, EPROM, and Flash, which retain data even when power is removed.

Question 127

B) Fiber optic (Correct Answer)

Explanation: For a network cable spanning over a kilometer, fiber optic is the best choice. Fiber optic cables can transmit data over much longer distances than copper-based alternatives without signal degradation. They're immune to electromagnetic interference, have higher bandwidth capacity, and are more secure. Other options like 10Base5 or 10BaseT are limited in distance and prone to interference over long runs.

Question 128

B) Integrity (Correct Answer)

Explanation: Integrity in cryptography ensures that the message has not been altered during transmission. When Alice wants James to know the message wasn't changed, she's aiming for integrity. This is typically achieved through methods like digital signatures or message authentication codes (MACs). Confidentiality protects the content from unauthorized viewing, authentication proves the sender's identity, and non-repudiation prevents denial of sending.

Question 129

A) Automated recovery (Correct Answer)

Explanation: Automated recovery is a process where the system can recover from a failure without administrator intervention. However, this type of recovery may result in some data loss as it prioritizes quick restoration of services over complete data preservation. It's a balance between rapid recovery and potential data loss, suitable for systems where immediate availability is crucial.

Question 130

A) Keystroke Patterns (Correct Answer)

Explanation: Keystroke Patterns, also known as keystroke dynamics, is a biometric authentication method that analyzes the unique way an individual types. It measures factors like typing speed, pressure, and the time between

keystrokes. This behavioral biometric can provide an additional layer of security, as each person's typing pattern is unique, much like a fingerprint.

Question 131

B) Grudge Attack (Correct Answer)

Explanation: A Grudge Attack is motivated by resentment and carried out with the intention to harm an organization or individual. It's often perpetrated by disgruntled current or former employees, or others with a personal vendetta. Unlike other types of attacks that may be financially motivated or aimed at data theft, grudge attacks are primarily driven by a desire for revenge or to cause damage.

Question 132

B) Harrison–Ruzzo–Ullman Model (Correct Answer)

Explanation: The Harrison–Ruzzo–Ullman (HRU) Model is an integrity model based on predetermining the set of objects a subject can access. It focuses on the concept of access rights and how they can be transferred between subjects. The model is used to analyze the safety of protection systems, particularly in terms of whether it's possible to leak privileges in a given access control configuration.

Question 133

B) Intrusion Detection System (Correct Answer)

Explanation: An Intrusion Detection System (IDS) is a security product that automates the inspection of audit logs and real-time system events. It's primarily used to detect intrusion attempts by analyzing patterns of suspicious activity. IDSs can also identify system failures and assess overall performance. They play a crucial role in network security by providing early warning of potential security breaches.

Question 134

C) Badges (Correct Answer)

Explanation: Badges are a common form of physical identification and electronic access control in information security. They can range from simple visual identification cards to sophisticated smart cards with embedded chips for electronic access control. Badges provide a tangible means of identifying authorized personnel and controlling access to physical spaces or digital resources.

Question 135

C) Data Definition Language (DDL) (Correct Answer)

Explanation: Data Definition Language (DDL) is the subset of SQL used to define, modify, and delete database objects such as tables, indexes, and schemas. DDL commands like CREATE, ALTER, and DROP are used to manage the structure of the database. This is distinct from Data Manipulation Language (DML) which is used to manipulate data within the database, and Data Control Language (DCL) which manages permissions.

Question 136

C) Ensure that the tapes are handled in the same manner as the original media would be, based on their classification. (Correct Answer)

Explanation: When sending backup tapes offsite, it's crucial to maintain the same level of security as the original data. The classification level should not change just because the tapes are leaving the premises. Decrypting or purging the tapes would defeat the purpose of backup. The correct approach is to handle the backup tapes with the same security measures as the original data, based on their existing classification level.

Question 137

A) Salt reuse (Correct Answer)

Explanation: While the image is not provided, the description suggests that the flaw in Lucky's password hashing implementation is salt reuse. Salt is a random value added to each password before hashing to prevent rainbow table attacks and to ensure that identical passwords don't produce the same hash. Reusing the same salt for multiple passwords negates these benefits and weakens the security of the hashing process.

Question 138

C) Pass around (Correct Answer)

Explanation: For a remote worker on a different schedule, the "Pass around" review process is most suitable. In this method, the code is circulated electronically to reviewers who can examine it at their convenience. This asynchronous approach accommodates different time zones and work schedules, allowing each reviewer to provide feedback independently without requiring real-time collaboration.

Question 139

C) Machine languages (Correct Answer)

Explanation: First generation programming languages are machine languages. These are the lowest-level programming languages, consisting of binary code (1s and 0s) that directly instruct the computer's hardware. They are specific to the particular computer architecture and are extremely difficult for humans to read or write, but they are the only language that computers directly understand without interpretation or compilation.

Question 140

A) Switch (Correct Answer)

Explanation: A switch is the network device described in the question. It's considered an intelligent hub because it can

learn and remember the MAC addresses of devices connected to each of its ports. Unlike a hub that broadcasts data to all ports, a switch can direct traffic only to the specific port where the destination device is connected, improving network efficiency and security.

Question 141

C) URL Hijacking (Correct Answer)

Explanation: URL Hijacking, also known as URL redirection, is the practice of redirecting users from their intended destination to a malicious or fraudulent website. This is often achieved by altering hyperlink URLs in HTML documents sent to clients. The attacker's goal is typically to trick users into revealing sensitive information or to install malware on their systems. It's a common technique in phishing attacks.

Question 142

D) Parol Evidence Rule (Correct Answer)

Explanation: The Parol Evidence Rule is a legal concept stating that when a contract is in written form, it is presumed to contain all the terms of the agreement. This rule prevents the introduction of external evidence (like prior negotiations or verbal agreements) that contradicts or adds to the written contract. It's crucial in contract law to ensure the finality and reliability of written agreements.

Question 143

D) Media analysis (Correct Answer)

Explanation: Timothy is performing media analysis, a type of digital forensic analysis focused on examining storage media like hard drives. This process involves recovering deleted files, analyzing file systems, and reconstructing data from damaged or formatted drives. Media analysis is crucial in digital forensics for retrieving evidence that may have been intentionally or accidentally erased.

Question 144

B) API (Correct Answer)

Explanation: An API (Application Programming Interface) is the most direct solution for Fran's task. APIs allow different software systems to communicate and interact programmatically. By developing an API, Fran can enable customers to check inventory, place orders, and check order status without accessing the web page directly. APIs provide a structured way for external systems to interact with the company's backend systems securely and efficiently.

Question 145

D) Type 2 Error (Correct Answer)

Explanation: In biometric systems, a False Rejection Rate (FRR) is classified as a Type 2 Error. This occurs when the system incorrectly rejects an authorized user, failing to recognize a valid biometric input. Type 2 Errors are also known as "false negatives" in statistical hypothesis testing. In contrast, a Type 1 Error (false positive) would be incorrectly accepting an unauthorized user.

Question 146

B) Vulnerabilities (Correct Answer)

Explanation: Both CVE (Common Vulnerabilities and Exposures) and NVD (National Vulnerability Database) provide information about vulnerabilities. CVE is a list of publicly disclosed cybersecurity vulnerabilities, each with a unique identifier. NVD is the U.S. government repository of standards-based vulnerability management data, which includes CVE entries along with additional analysis, severity scores, and impact ratings.

Question 147

C) Agile Methodology (Correct Answer)

Explanation: Agile Methodology is characterized by incremental, rapid development cycles with a focus on customer collaboration and responding to change. It emphasizes flexibility, continuous delivery, and close teamwork between developers and business stakeholders. Agile methods, like Scrum or Kanban, prioritize working software over comprehensive documentation and adapt quickly to changing requirements.

Question 148

B) Primary Evidence (Correct Answer)

Explanation: Primary Evidence refers to the original document or item presented in court. In legal contexts, primary evidence is considered the best and most reliable form of evidence. It's the actual document or object in question, rather than a copy or description of it. This type of evidence is given the highest evidentiary value in legal proceedings.

Question 149

B) Declassification (Correct Answer)

Explanation: Declassification is the process of reducing the security classification level of information or resources. This occurs when the sensitivity of the information decreases over time or when the need for high-level protection no longer justifies the resources required to maintain it. Declassification is crucial for managing information lifecycle and ensuring that security measures are proportionate to the current value and sensitivity of the information.

Question 150

B) Wave pattern (Correct Answer)

Explanation: Wave pattern motion detectors, specifically those using microwave technology, employ high-frequency electromagnetic waves to detect movement. These detectors emit microwave radiation and measure the

reflections. When an object moves within the protected area, it causes a change in the reflected wave pattern, triggering the alarm. Microwave detectors are effective for large areas and can penetrate thin walls, making them useful in certain security applications.

Question 151

A) Repudiation and Tampering (Correct Answer)

Explanation: Altering audit logs involves two STRIDE categories: Repudiation and Tampering. Repudiation is involved because modifying logs can allow an attacker to deny their actions. Tampering is directly related to the act of altering the logs. This combination best describes the security implications of modifying audit logs.

Question 152

C) Least privilege (Correct Answer)

Explanation: The principle of least privilege states that users should only have the minimum level of access necessary to perform their job functions. Running an application with full administrative privileges violates this principle, as it grants excessive permissions that may not be required for the application's operation, potentially increasing security risks.

Question 153

C) Data owner (Correct Answer)

Explanation: The data owner, typically a senior executive or department head, bears ultimate responsibility for data protection within an organization. They determine data classification levels, access rights, and overall data governance policies. While other roles like data custodians implement these policies, the data owner remains accountable for the overall protection strategy.

Question 154

D) IaaS (Correct Answer)

Explanation: Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet. Object-based storage systems managed by vendors and accessed through APIs are a characteristic of IaaS. This model allows organizations to use storage resources without managing the underlying hardware infrastructure, fitting the IaaS paradigm.

Question 155

A) Stenography (Correct Answer)

Explanation: The correct term is actually "Steganography," but "Stenography" is the closest option provided. Steganography is the practice of concealing messages or information within other non-secret text, images, or audio files. This technique aims to hide the existence of the message, making it different from encryption, which makes the message unreadable but doesn't hide its existence.

Question 156

C) The KDC confirms the validity of the Ticket Granting Ticket and verifies the user's privileges for the requested resource. (Correct Answer)

Explanation: In Kerberos authentication, when a client requests a service ticket, the Key Distribution Center (KDC) first validates the Ticket Granting Ticket (TGT) presented by the client. It then checks if the user has the necessary privileges to access the requested resource. This step ensures that only authorized users receive service tickets for resources they are permitted to access.

Question 157

A) The logs will only retain the most recent 20 megabytes of data. (Correct Answer)

Explanation: When log settings are configured with a maximum size and set to overwrite as needed, the system will continuously overwrite the oldest log entries once the

maximum size is reached. This means that only the most recent 20 megabytes of log data will be retained, potentially losing important historical information and making it difficult to conduct thorough audits or investigations.

Question 158

C) Enrollment (Correct Answer)

Explanation: In the user provisioning process, "enrollment" typically refers to the initial creation of a user account. This step involves collecting necessary user information and setting up their account in the system. It's the first step in granting a user access to organizational resources and precedes other actions like background checks or clearance verification.

Question 159

C) LDAP (Correct Answer)

Explanation: Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, standards-based protocol used for accessing and maintaining distributed directory information services over an IP network. It provides a centralized method for storing and querying information about users and services, making it ideal for the IT manager's requirements of a centralized, easily queryable system.

Question 160

C) DBMS application (Correct Answer)

Explanation: A Database Management System (DBMS) application is specifically designed to interact with databases, allowing for the storage, retrieval, modification, and management of data. While SQL is a language used to communicate with databases, and SAML is used for exchanging authentication and authorization data, a DBMS application provides the comprehensive functionality described in the question.

Question 161

C) Cookie-based SSO (Correct Answer)

Explanation: Cookie-based Single Sign-On (SSO) uses HTTP cookies to store and transmit user credentials between the browser and server. This method automatically gathers and encrypts existing credentials on the client machine, storing them in cookies, which are then sent to the destination server without requiring additional user input. This matches the description provided in the question.

Question 162

D) Plaintext (Correct Answer)

Explanation: Plaintext refers to information in its original, unencrypted form. It's the raw data before any cryptographic operations have been applied. When a message is encrypted, the plaintext is converted into ciphertext. Therefore, a message that has not been encrypted is referred to as plaintext.

Question 163

B) Work Breakdown Structure (Correct Answer)

Explanation: A Work Breakdown Structure (WBS) is a project management tool that breaks down the project into smaller, more manageable components. It typically includes tasks, subtasks, and work packages, providing a hierarchical decomposition of the project scope. This matches the description of the document received by the project manager in the question.

Question 164

B) A credential management system (Correct Answer)

Explanation: A credential management system is the most comprehensive solution for the described problem. It allows for centralized storage, management, and rotation of passwords across multiple systems with varying security

requirements. This approach ensures proper password handling, logging, and automated rotation, addressing the challenges faced by the system administrators more effectively than the other options.

Question 165

B) Bell-LaPadula (Correct Answer)

Explanation: The Bell-LaPadula model is a state machine model for computer security that focuses on protecting confidentiality. One of its key properties is the "no write down" rule, which states that a subject at a higher security level cannot write information to a lower security level. This property precisely matches the description given in the question.

Question 166

D) Egress Monitoring (Correct Answer)

Explanation: Egress Monitoring refers to the process of monitoring and controlling outbound network traffic. Its primary purpose is to detect and prevent unauthorized data transfer from inside an organization to external entities. This aligns perfectly with the description provided in the question, focusing on outgoing traffic and data transfer prevention.

Question 167

C) SHA (Correct Answer)

Explanation: SHA (Secure Hash Algorithm) is a family of cryptographic hash functions developed by the National Institute of Standards and Technology (NIST) and published as a U.S. Federal Information Processing Standard (FIPS). It's widely used for various security applications and protocols, making it the correct answer among the options provided.

Question 168

A) $100,000 (Correct Answer)

Explanation: To calculate the Annualized Loss Expectancy (ALE), we use the formula: ALE = Annual Rate of Occurrence (ARO) × Single Loss Expectancy (SLE). Here, ARO = 1/200 (as it's a 200-year flood plain), and SLE = $20 million (the expected damage from a flood). Thus, ALE = (1/200) × $20,000,000 = $100,000.

Question 169

A) Social Engineering (Correct Answer)

Explanation: Social engineering attacks rely on human interaction and often involve tricking people into breaking normal security procedures. The preventive measures described - requiring proof of identity, callback authorizations, and prohibiting password changes via voice communications - are specifically designed to counter social engineering tactics that exploit human trust and manipulate individuals into divulging sensitive information.

Question 170

C) Trace (Correct Answer)

Explanation: Structural coverage in software testing typically includes statement coverage, branch coverage, path coverage, and sometimes data flow coverage. "Trace" is not a standard type of structural coverage. Statement, data flow, and loop coverage are all valid types of structural testing, making "trace" the odd one out in this list.

Question 171

A) Jailbreaking (Correct Answer)

Explanation: Jailbreaking is the process of removing software restrictions imposed by Apple on iOS devices. This process allows root access to the iOS file system and manager, enabling the installation of software that Apple would otherwise restrict. It precisely matches the description given in the question for removing restrictions and gaining root-level access on iOS devices.

Question 172

A) Data Loss Prevention (DLP) (Correct Answer)

Explanation: Data Loss Prevention (DLP) systems are specifically designed to detect and prevent the unauthorized exfiltration of sensitive data from an organization. DLP solutions monitor data in use, in motion, and at rest, identifying and blocking attempts to transfer sensitive information outside the organization's network, which aligns perfectly with the description in the question.

Question 173

B) Fiber-optic (Correct Answer)

Explanation: Fiber-optic cabling is immune to electromagnetic interference (EMI) because it uses light signals instead of electrical signals to transmit data. This makes it ideal for environments with high EMI, such as industrial facilities with large motors. While it may be more expensive and difficult to install, the question specifies that these concerns are outweighed by the need for EMI resistance.

Question 174

A) Bit Flipping (Correct Answer)

Explanation: Bit flipping is a technique used in software testing and security analysis where individual bits in a data stream or storage are changed from 0 to 1 or vice versa. This method is commonly used in fuzzing, where input data is slightly modified to test how a system handles unexpected or malformed inputs. The description in the question precisely matches the definition of bit flipping.

Question 175

A) Gray-Box Testing (Correct Answer)

Explanation: Gray-Box Testing is a software testing method that combines elements of both black-box and white-box

testing. It involves partial knowledge of an application's internal workings, allowing testers to design test cases based on high-level descriptions of the system's behavior while also considering its implementation details. This approach is particularly effective for identifying defects related to improper code structure or functionality, as described in the question.

Question 176

D) Optimizing (Correct Answer)

Explanation: The Software Capability Maturity Model (SW-CMM) has five levels of maturity: Initial, Repeatable, Defined, Managed, and Optimizing. The Optimizing level is the highest and final stage, where the organization focuses on continuous process improvement and optimization of existing practices.

Question 177

B) Exposure Factor (EF) (Correct Answer)

Explanation: The Exposure Factor (EF) is a measure used in risk assessment that represents the percentage of loss an organization would experience if a specific asset were compromised. It's expressed as a percentage and helps quantify the potential impact of a realized risk on a particular asset.

Question 178

D) Electrical Spikes (Correct Answer)

Explanation: Atmospheric lightning can cause electrical spikes, which are sudden, brief increases in voltage. These spikes can be extremely damaging to electronic equipment and are a common result of lightning strikes. While lightning can indirectly cause other disturbances, electrical spikes are the most direct and immediate effect.

Question 179

D) Horizontal Distribution System (Correct Answer)

Explanation: The Horizontal Distribution System refers to the cabling and associated hardware that extends from telecommunications rooms to individual work areas. It includes the cables, cross-connection blocks, patch panels, and other supporting infrastructure that connects end-user devices to the network backbone.

Question 180

A) International Organization for Standardization (ISO) (Correct Answer)

Explanation: The International Organization for Standardization (ISO) is an independent, non-governmental international organization that develops and publishes a wide range of proprietary, industrial, and commercial standards. It covers various fields, including technology, manufacturing, and management systems.

Question 181

A) Transfer (Correct Answer)

Explanation: Purchasing insurance is a classic example of risk transfer. In this approach, the organization shifts the potential financial impact of a risk to another party (the insurance company) in exchange for a premium. The risk itself isn't eliminated, but its financial consequences are transferred to the insurer.

Question 182

B) Bell-LaPadula Model (Correct Answer)

Explanation: The Bell-LaPadula Model is a state machine model focused on maintaining confidentiality. It employs mandatory access controls and uses a lattice structure to represent security levels. This model is known for its "no read up, no write down" policy, which helps prevent information leakage to lower security levels.

Question 183

C) User (Correct Answer)

Explanation: In the subject/object model of access control, the subject is the entity requesting access to a resource. In this scenario, the user attempting to log into the VPN is the subject, as they are initiating the action and seeking access to the remote file server (the object).

Question 184

D) Secret (Correct Answer)

Explanation: While "Secret" is a common classification level in government systems, it's not typically used in commercial data classification schemes. Commercial organizations usually use levels like Public, Internal Use Only, Confidential, and Restricted. "Secret" is more associated with government and military classification systems.

Question 185

D) Deliver working software infrequently, with an emphasis on creating accurate code over longer timelines. (Correct Answer)

Explanation: This statement contradicts the agile principle of delivering working software frequently. Agile methodologies emphasize rapid, iterative development with frequent deliveries of functional software. The focus on infrequent delivery and longer timelines is more characteristic of traditional waterfall approaches, not agile development.

Question 186

B) Object-Oriented Programming (Correct Answer)

Explanation: Object-Oriented Programming (OOP) is a programming paradigm that uses "objects" – data structures consisting of data fields and methods – to design and organize code. It's particularly well-suited for modeling real-

world scenarios due to its ability to represent complex systems as interacting objects. OOP also facilitates error tracking and propagation through its hierarchical structure and encapsulation principles.

Question 187

C) High-Speed Serial Interface (HSSI) (Correct Answer)

Explanation: The High-Speed Serial Interface (HSSI) is a Layer 1 protocol designed for high-speed communication between routers and other network devices. It's commonly used to connect routers and multiplexers to ATM (Asynchronous Transfer Mode) or frame relay connection devices, providing a standardized interface for high-speed data transmission.

Question 188

B) Manual (Correct Answer)

Explanation: Manual code review is most effective for identifying flaws in business logic. This is because business logic often involves complex decision-making processes and rules that are specific to the application's domain. Human reviewers can better understand and evaluate these logical flows, considering various scenarios and edge cases that automated tools might miss.

Question 189

D) Primary Memory (Correct Answer)

Explanation: Primary Memory, also known as main memory, refers to the high-performance storage directly accessible by the CPU. It typically consists of volatile Random Access Memory (RAM). This type of memory provides fast read and write access, making it crucial for storing actively used data and instructions for immediate processing by the CPU.

Question 190

B) Access Accounting (Correct Answer)

Explanation: Access Accounting refers to the practice of recording and analyzing user activities within an information system. This includes auditing, logging, and monitoring attempted accesses and actions performed by subjects (users or processes) in the system. It's a crucial aspect of security management, providing a trail of user activities for security analysis and compliance purposes.

Question 191

C) Administrative Physical Security Controls (Correct Answer)

Explanation: Administrative Physical Security Controls encompass a wide range of non-technical measures aimed at protecting physical assets and environments. These include policies and procedures related to facility construction and selection, site management, personnel controls (like background checks), security awareness training, and emergency response procedures. These controls form a crucial part of an organization's overall security strategy.

Question 192

A) Data Analytics (Correct Answer)

Explanation: Data Analytics is the field of study that focuses on examining raw data to extract meaningful insights and draw conclusions. It involves various techniques and processes to analyze large datasets, identify patterns, and derive valuable information. This field encompasses statistical analysis, predictive modeling, and data visualization to support decision-making processes.

Question 193

D) All three would be the same size (Correct Answer)

Explanation: In an incremental backup strategy, each backup only includes the data that has changed since the last backup. Assuming the same amount of data changes

each day, the size of each incremental backup (Monday's, Tuesday's, and Wednesday's) would be the same. This is because each backup is capturing the same volume of daily changes, regardless of the day.

Question 194

A) Logging into a workstation (Correct Answer)

Explanation: While logging privileged administrative actions is crucial for security and auditing purposes, logging into a workstation is typically not considered a privileged action that requires automatic logging. The other options – restoring systems, purging logs, and managing user accounts – are sensitive activities that should be logged to maintain accountability and track potential security incidents.

Question 195

A) Testing Methodology (Correct Answer)

Explanation: Testing Methodology refers to the comprehensive approach and strategies used to ensure an application meets client expectations. It encompasses various testing types and levels, including unit testing, integration testing, system testing, and performance testing. This term describes the overall framework and processes used to plan, design, and execute tests throughout the software development lifecycle.

Question 196

D) Session-based SSO (Correct Answer)

Explanation: Session-based Single Sign-On (SSO) is a method where the initial login to an HTTP server generates a session token, which is then stored as an in-memory cookie in the user's browser. This token is used for subsequent authentication requests, allowing the user to access multiple applications without re-entering credentials.

This approach matches the description provided in the question.

Question 197

C) TOCTOU (Correct Answer)

Explanation: TOCTOU (Time-of-Check to Time-of-Use) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This type of attack exploits the time gap between when a system checks for authorization and when it actually uses that authorization, relying on precise timing to bypass security measures.

Question 198

B) Due care (Correct Answer)

Explanation: The action described demonstrates due care. Due care refers to taking reasonable steps to prevent foreseeable harm or to mitigate known risks, even if it's not explicitly part of one's job description. By closing the door to a secure area, despite it not being their direct responsibility, the information security professional is exercising due care to protect the organization's assets and maintain security.

Question 199

A) Bit Flipping (Correct Answer)

Explanation: Bit Flipping is a technique used in software testing and security analysis where individual bits in a data stream or file are changed from 0 to 1 or vice versa. This method is often used in fuzzing tests to create slightly modified versions of input data, helping to identify how systems handle unexpected or malformed inputs.

Question 200

A) Logging into a workstation (Correct Answer)

Explanation: While logging privileged administrative actions is important for security auditing, logging into a workstation is generally not considered a privileged administrative activity that requires automatic logging. The other actions listed – restoring systems, purging log entries, and managing user accounts – are sensitive activities that should be logged to maintain accountability and track potential security incidents.

Question 201

C) Separation of duties (Correct Answer)

Explanation: Separation of duties is a security principle that enforces the concept of two-person control by dividing critical tasks or responsibilities among different individuals. This prevents a single person from having complete control over sensitive operations, reducing the risk of fraud, errors, or malicious activities. It ensures that multiple people are involved in critical processes, enhancing accountability and security.

Question 202

A) Reconnaissance (Correct Answer)

Explanation: This type of attack is known as a port scan, which is a form of reconnaissance. By attempting to connect to all 65,536 TCP ports on a single system within a brief timeframe, the attacker is gathering information about open ports and potential vulnerabilities. This is typically an initial step in the attack process, allowing the adversary to map out the target system's structure and identify potential entry points for further exploitation.

Question 203

D) PASTA (Correct Answer)

Explanation: PASTA (Process for Attack Simulation and Threat Analysis) is a risk-centric threat modeling methodology that consists of seven stages. These stages

include defining objectives, technical scope, application decomposition, threat analysis, vulnerability assessment, attack modeling, and risk impact analysis. PASTA provides a comprehensive approach to identifying and analyzing potential threats to an application or system.

Question 204

B) Firmware (Correct Answer)

Explanation: Firmware refers to software that is stored in a Read-Only Memory (ROM) chip or other non-volatile memory. It is a type of low-level software that provides control, monitoring, and data manipulation functions for devices. Firmware is typically used in embedded systems and is essential for the basic operation of hardware devices, acting as an interface between the hardware and higher-level software.

Question 205

B) Responsibility Assignment Matrix (Correct Answer)

Explanation: A Responsibility Assignment Matrix (RAM), also known as a RACI matrix (Responsible, Accountable, Consulted, Informed), is a tool used in project management and organizational planning. It clearly outlines roles and responsibilities for various activities or groups of tasks within a project or organization. This matrix helps in clarifying expectations, avoiding duplication of efforts, and ensuring that all necessary tasks are assigned to specific individuals or teams.

Question 206

D) An RFC 1918 address (Correct Answer)

Explanation: The IP address 10.11.45.170 falls under the category of an RFC 1918 address. RFC 1918 defines private IP address ranges for use in private networks. The address 10.11.45.170 is part of the 10.0.0.0/8 range, which is one of the three private IP address ranges specified in RFC 1918.

These addresses are not routable on the public internet and are commonly used in local area networks (LANs) and for internal network addressing.

Question 207

A) Personal Identity Verification (PIV) (Correct Answer)

Explanation: Personal Identity Verification (PIV) is the term used for smart cards issued to US government personnel. These cards include a photograph and other identifying information, serving as both a badge for physical access and a smart card for logical access to computer systems. PIV cards are part of a standardized identity credentialing system used across federal agencies to enhance security and interoperability.

Question 208

B) Application firewall (Correct Answer)

Explanation: An application firewall, also known as a Web Application Firewall (WAF), operates at the application layer (Layer 7) of the OSI model. It has the capability to inspect traffic at this level and perform protocol-specific analysis for malicious content. Unlike packet filtering or stateful inspection firewalls, application firewalls can understand and filter HTTP traffic, detect SQL injection attempts, cross-site scripting, and other application-layer attacks.

Question 209

A) Qualitative Risk Analysis (Correct Answer)

Explanation: Qualitative Risk Analysis is an approach to risk assessment that involves scenario-based evaluation using ranking and grading for exposure ratings and decision-making. This method uses subjective criteria to categorize risks, often employing scales like "low," "medium," and "high" to assess likelihood and impact. It's particularly useful when numerical data is limited or when a quick

assessment is needed, providing a general understanding of relative risk levels to guide decision-making.

Question 210

A) TOCTOU (Correct Answer)

Explanation: TOCTOU stands for Time-of-Check to Time-of-Use, which is a timing vulnerability that occurs when a program verifies access permissions too far in advance of a resource request. This creates a window of opportunity for an attacker to manipulate the resource between the time of the check and the time of use. TOCTOU vulnerabilities can lead to privilege escalation or unauthorized access to resources in multi-threaded or time-shared systems.

Question 211

B) Hashed Message Authentication Code (HMAC) (Correct Answer)

Explanation: A Hashed Message Authentication Code (HMAC) provides a partial digital signature, ensuring message integrity during transmission but not offering non-repudiation. HMAC uses a cryptographic hash function in combination with a secret key to produce a message authentication code. This technique verifies both the data integrity and the authenticity of a message, but since it uses a shared secret key, it doesn't provide non-repudiation like a full digital signature would.

Question 212

C) Information Flow Model (Correct Answer)

Explanation: The Information Flow Model is a security model that focuses on controlling how information moves within a system, maintaining and enforcing security regardless of the information's path. It is based on a State Machine Model, which represents the system as a set of states and transitions. This model ensures that information flows only in authorized ways, preventing unauthorized access or

leakage of sensitive data across different security levels or compartments.

Question 213

C) Compiler (Correct Answer)

Explanation: A compiler is a programming tool that converts high-level language code into an executable file designed for a specific operating system. It translates human-readable source code into machine code or lower-level code that can be directly executed by the computer's processor. Compilers perform various optimizations and error checks during this process, producing efficient and platform-specific executable programs.

Question 214

C) Attackers may use XSS filter evasion techniques against this approach (Correct Answer)

Explanation: Filtering out only the <SCRIPT> tag on the server side is insufficient to prevent cross-site scripting (XSS) attacks. Attackers can use various XSS filter evasion techniques to bypass this simple protection. For example, they might use other HTML tags that can execute JavaScript (like <img> with an onerror attribute), or employ encoding tricks to disguise malicious scripts. A comprehensive approach to XSS prevention requires more robust input validation and output encoding techniques.

Question 215

D) Authentication (Correct Answer)

Explanation: Authentication is the process of verifying or testing the validity of an identity claimed by a subject. It involves confirming that an entity (user, system, or device) is who or what it claims to be. This process typically involves checking credentials, such as passwords, biometrics, or security tokens, against stored information to ensure the authenticity of the claimed identity. Authentication is a

crucial component of access control and information security.

Question 216

D) Multilayer (Correct Answer)

Explanation: Multilayer protocols rely on encapsulation as their core concept. Encapsulation is the process of wrapping data from one protocol inside another protocol's data unit. This layered approach allows for the separation of networking functions and enables data to be transmitted across different network types. The OSI (Open Systems Interconnection) model and the TCP/IP model are examples of multilayer protocol suites that extensively use encapsulation to facilitate communication between different layers and across networks.

Question 217

C) Inappropriate Activities (Correct Answer)

Explanation: Inappropriate Activities refer to actions that occur on a computer or over IT infrastructure that may not be criminal but often result in internal disciplinary measures or termination. These activities violate organizational policies, ethical standards, or acceptable use guidelines. Examples might include accessing inappropriate content, excessive personal use of company resources, or minor security policy violations. While not necessarily illegal, these actions can compromise productivity, security, or the organization's reputation.

Question 218

D) The CA's private key (Correct Answer)

Explanation: When a Certificate Authority (CA) creates a digital signature for a certificate, it uses its private key to sign the completed certificate. This process ensures the authenticity and integrity of the certificate. The CA's private key is kept secret and is used to create signatures that can

be verified using the CA's public key. This mechanism allows anyone with the CA's public key to verify that the certificate was indeed issued and signed by the trusted CA.

Question 219

D) Generational (Correct Answer)

Explanation: Generational fuzzing, also known as intelligent fuzzing, is an advanced fuzzing technique that generates test cases based on understanding the format or structure of the input data. Unlike mutation-based fuzzing, which randomly modifies existing inputs, generational fuzzing creates new inputs from scratch using knowledge of the input format. This approach allows for more targeted and efficient testing, potentially uncovering deeper and more complex vulnerabilities in the system under test.

Question 220

D) Asset (Correct Answer)

Explanation: An asset is anything within an environment that should be protected. In the context of information security, assets can include physical items (like computers, servers, or network devices), digital assets (such as data, software, or intellectual property), and even intangible assets (like reputation or business processes). Identifying and classifying assets is a crucial step in risk management and security planning, as it helps organizations prioritize their protection efforts and allocate resources effectively.

Question 221

B) SLA (Correct Answer)

Explanation: SLA stands for Service Level Agreement, which is a contractual obligation that often requires the implementation of sound Business Continuity Planning (BCP) practices for clients. An SLA is a formal agreement between a service provider and a client that defines the level of service expected, including aspects of availability,

performance, and disaster recovery. By including BCP requirements in SLAs, organizations ensure that their service providers have adequate measures in place to maintain operations and recover from disruptions, thus protecting the client's interests.

Question 222

B) Visual Card (Correct Answer)

Explanation: A Visual Card is a human-readable only card ID typically featuring a photo and written information about the authorized bearer. These cards are used in environments where automated controls are impractical but security guards are available to visually verify identities. Visual cards rely on physical inspection rather than electronic scanning, making them suitable for low-tech security environments or as a backup to more sophisticated access control systems.

Question 223

A) Risk Management (Correct Answer)

Explanation: Risk Management is the comprehensive process of identifying potential threats, evaluating their impact, and implementing cost-effective solutions to mitigate or reduce risk. This ongoing process involves risk assessment, risk treatment (including mitigation, transfer, acceptance, or avoidance), and continuous monitoring. Risk management aims to balance the costs of protective measures against the potential losses from security incidents, ensuring that an organization's resources are used efficiently to address the most significant risks.

Question 224

B) Hot Site (Correct Answer)

Explanation: A Hot Site is a backup facility maintained in constant working order, with a full complement of servers, workstations, and communication links ready to assume primary operations responsibilities. It is designed for

immediate takeover of critical business functions in the event of a disaster or major disruption at the primary site. Hot sites are the most expensive type of backup facility but offer the fastest recovery time, typically allowing operations to resume within hours of activation.

Question 225

D) Aggregate Functions (Correct Answer)

Explanation: Aggregate Functions in SQL are functions that accumulate values and return a single result. These functions operate on a set of rows and return a single output value. Common aggregate functions include COUNT(), MIN(), MAX(), SUM(), and AVG(). They are typically used in combination with GROUP BY clauses to perform calculations across a set of rows that match specified criteria. Aggregate functions are essential for data analysis and reporting in database systems.

Question 226

A) Operational investigation (Correct Answer)

Explanation: Operational investigations typically have the most relaxed standards for information collection and preservation. These investigations are internal to an organization and are often conducted to improve processes, identify inefficiencies, or address minor policy violations. Unlike criminal, civil, or regulatory investigations, operational investigations don't usually require strict chain of custody or evidence preservation protocols, as the findings are primarily used for internal decision-making and process improvement rather than legal proceedings.

Question 227

D) Auxiliary Alarm System (Correct Answer)

Explanation: An Auxiliary Alarm System is an additional function that can be added to local or centralized alarm systems to automatically notify police or fire services when

an alarm is triggered. This system creates a direct link between the alarm system and emergency services, reducing response time in case of a security breach or emergency. It enhances the effectiveness of the primary alarm system by ensuring that appropriate authorities are immediately alerted without relying on human intervention.

Question 228

C) Misuse case testing (Correct Answer)

Explanation: Misuse case testing involves diagramming potential hacker approaches to an application and determining how the system would respond to likely attacker behavior. This type of testing focuses on identifying and exploring potential security vulnerabilities by simulating malicious user actions. It helps developers and security professionals understand how an attacker might attempt to exploit the system, allowing them to implement appropriate countermeasures and improve overall security.

Question 229

C) Sunday's full backup (Correct Answer)

Explanation: In a backup strategy involving full backups on Sundays and differential backups Monday through Friday, the Sunday full backup should be applied first when restoring data after a server failure. A full backup contains a complete copy of all data, serving as the baseline for subsequent differential backups. After applying the full backup, the most recent differential backup would then be applied to bring the system up to date. This approach ensures a complete and efficient restoration of the system to its latest state.

Question 230

A) Evil Twin (Correct Answer)

Explanation: An Evil Twin attack is where a hacker operates a false access point that automatically clones the identity of

another access point based on a client device's automatic reconnection request. This type of attack exploits the tendency of devices to automatically connect to known networks. The attacker sets up a rogue access point with the same SSID as a legitimate one, tricking users into connecting to the malicious network. This allows the attacker to intercept traffic and potentially steal sensitive information.

Question 231

D) Frame (Correct Answer)

Explanation: In networking, a frame is the combination of the Data Link Layer header, payload, and footer. The frame is the basic unit of communication at the Data Link Layer (Layer 2) of the OSI model. It encapsulates the data from higher layers and includes addressing information and error-checking mechanisms. The frame structure allows for reliable point-to-point communication between network devices, managing data transfer across the physical link.

Question 232

B) Watermarking (Correct Answer)

Explanation: Watermarking is the most effective security control for tracing the source of sensitive documents if they appear in a public forum. This technique involves embedding a unique, often invisible, identifier into a document. Watermarks can contain information such as the document's origin, owner, or intended recipient. If a watermarked document is leaked or shared inappropriately, the watermark can be used to trace it back to its source, helping to identify the point of compromise or the individual responsible for the breach.

Question 233

A) Broadband (Correct Answer)

Explanation: Cable modems, ISDN (Integrated Services Digital Network), and DSL (Digital Subscriber Line) fall under the category of broadband technologies. Broadband refers to high-speed internet access that is always on and faster than traditional dial-up access. These technologies use wide bandwidth data transmission to provide faster internet speeds, allowing for the simultaneous transmission of various types of data signals. Broadband technologies have largely replaced older, slower internet connection methods due to their superior speed and capacity.

Question 234

C) Bracketed (Correct Answer)

Explanation: "Bracketed" is not a recognized design in Mandatory Access Control (MAC) systems. The common designs in MAC systems include hierarchical (where access levels are arranged in a strict hierarchy) and compartmentalized (where access is based on separate, non-hierarchical categories). Some systems may use a hybrid approach combining both hierarchical and compartmentalized elements. The term "bracketed" is not a standard classification in MAC design, making it the incorrect option among the given choices.

Question 235

B) TLS, VPN, IPsec (Correct Answer)

Explanation: TLS (Transport Layer Security), VPN (Virtual Private Network), and IPsec (Internet Protocol Security) are commonly employed methods to protect data in transit. These protocols provide encryption and authentication mechanisms to secure data as it travels across networks. TLS secures web communications, VPNs create secure tunnels for remote access, and IPsec secures IP communications. Together, these technologies ensure the confidentiality, integrity, and authenticity of data during transmission, protecting it from interception and tampering.

Question 236

B) Private Branch Exchange (PBX) (Correct Answer)

Explanation: A Private Branch Exchange (PBX) is a sophisticated local telephone exchange often used by organizations for inbound call support, extension-to-extension calling, conference calling, and voicemail. PBX systems manage internal communications within an organization and connect to external telephone networks. They offer features like call routing, voicemail, call forwarding, and interactive voice response systems. PBX systems can be traditional hardware-based or modern software-based (IP PBX) solutions, providing flexible and cost-effective communication solutions for businesses.

Question 237

D) Real Memory (Correct Answer)

Explanation: Real Memory, also known as physical memory or main memory, is typically the largest RAM storage resource available to a computer. It is composed of dynamic RAM chips that require periodic refreshing by the CPU to maintain data. Real memory is the actual physical memory installed in a computer, as opposed to virtual memory which uses hard disk space to simulate additional RAM. It provides fast, direct access to data and instructions for the CPU, playing a crucial role in system performance.

Question 238

A) Turnstile (Correct Answer)

Explanation: A turnstile is a security control indicated by an arrow pointing to a unidirectional gate that prevents more than one person from entering a facility at a time. Turnstiles are physical access control devices that allow only one person to pass through at a time, typically rotating in one direction. They are commonly used in entrances to secure areas, public transportation systems, and stadiums to

control and count the flow of people. Turnstiles can be integrated with electronic access control systems for enhanced security.

Question 239

D) SMTP (Correct Answer)

Explanation: SMTP (Simple Mail Transfer Protocol) is primarily used for moving email messages from clients to servers and between servers. It is the standard protocol for sending email across the Internet. SMTP handles the transmission of emails from the sender's mail client to the mail server, and then from server to server until it reaches the recipient's mail server. While other protocols like POP3 and IMAP are used for retrieving emails, SMTP is specifically designed for sending and routing email messages.

Question 240

D) False acceptance will be very high (Correct Answer)

Explanation: On a biometric authentication curve, false acceptance rates would be very high at the point where the system is set to be highly permissive. This occurs when the threshold for accepting a biometric match is set very low. In this scenario, the system is more likely to incorrectly accept unauthorized users (false positives), trading off security for convenience. This point on the curve represents a high risk of unauthorized access but a low risk of rejecting authorized users.

Question 241

A) 15 (Correct Answer)

Explanation: In a system with 6 users where any 2 users should be able to communicate securely, 15 symmetric encryption keys are needed. This number is calculated using the combination formula: n(n-1)/2, where n is the number of users. In this case, 6(6-1)/2 = 15. Each pair of users needs a unique shared key for secure communication, resulting in 15

distinct key pairs. This approach ensures that each pair of users has a unique encryption key, maintaining security even if one key is compromised.

Question 242

A) Highly cohesive (Correct Answer)

Explanation: An object that can perform a task with minimal assistance from other objects is described as highly cohesive. In object-oriented programming, cohesion refers to the degree to which the elements of a module or class work together to perform a single, well-defined task. A highly cohesive object encapsulates related functionality, making it more independent, easier to understand, maintain, and reuse. This design principle promotes modularity and reduces dependencies between different parts of a system.

Question 243

D) Boot Sector (Correct Answer)

Explanation: The boot sector is the portion of a storage device used to load the operating system. It's also a common target for certain types of viruses, known as boot sector viruses. The boot sector contains critical information needed to start the system, including the Master Boot Record (MBR) on traditional disk layouts. Boot sector viruses infect this area, potentially gaining control of the system before the operating system loads, making them particularly dangerous and difficult to detect or remove.

Question 244

B) Open networks are unencrypted, making traffic easily sniffable (Correct Answer)

Explanation: In open wireless networks, the vulnerability that allows users to potentially capture other customers' web traffic, including usernames and passwords, is that these networks are unencrypted, making traffic easily

sniffable. Without encryption, data transmitted over the network is sent in plain text, allowing anyone within range to intercept and read the information using packet sniffing tools. This vulnerability highlights the importance of using encrypted connections (like HTTPS) when accessing sensitive information on public Wi-Fi networks.

Question 245

C) Longer passwords and salting (Correct Answer)

Explanation: Longer passwords and salting are the most effective controls in preventing password cracking attacks against a system. Longer passwords increase the complexity and time required for brute-force attacks. Salting involves adding random data to each password before hashing, ensuring that even identical passwords have different hash values. This combination significantly increases the difficulty of cracking passwords, as it defeats rainbow table attacks and requires each password to be cracked individually, greatly increasing the time and computational resources needed for a successful attack.

Question 246

C) Packets with the source address from the public IP address block (Correct Answer)

Explanation: When configuring egress monitoring, packets with source addresses from the public IP address block should be allowed to leave the network for the Internet. This ensures that only legitimate outbound traffic from the organization's public IP range is permitted, preventing IP spoofing and maintaining network integrity. Private addresses should not be seen on the public Internet, and allowing only public source addresses helps in maintaining proper network address translation (NAT) and security policies.

Question 247

B) Impact (Correct Answer)

Explanation: Using encryption to protect sensitive business information during transmission over the Internet primarily reduces the impact of a potential data breach. While encryption doesn't necessarily decrease the likelihood of an attack, it significantly mitigates the consequences if data is intercepted. Encrypted data remains unreadable to unauthorized parties, thus reducing the potential damage or impact of a successful interception. This protection is crucial for maintaining data confidentiality and integrity during transmission.

Question 248

D) Patent (Correct Answer)

Explanation: A patent is the most suitable form of intellectual property protection for a company wanting to license a newly developed manufacturing process while preventing unauthorized use. Patents grant exclusive rights to the inventor for a limited period, typically 20 years, in exchange for public disclosure of the invention. This allows the company to license the process to others while maintaining legal protection against unauthorized use or replication. Patents are particularly well-suited for protecting novel processes, methods, and technologies.

Question 249

B) Protocol (Correct Answer)

Explanation: A protocol is the set of rules and restrictions that define how data is transmitted over a network medium, enabling computer-to-computer communications. Protocols specify the format, timing, sequencing, and error control in data communication. They govern various aspects of network communication, including how data is packaged, addressed, transmitted, routed, and received. Examples include TCP/IP, HTTP, and FTP. Protocols are essential for

ensuring interoperability and standardized communication between different devices and systems on a network.

Question 250

D) Aggregate Functions (Correct Answer)

Explanation: Aggregate functions in SQL, such as COUNT(), MIN(), MAX(), SUM(), and AVG(), are used to perform calculations on a set of values and return a single result. These functions operate on multiple rows and produce a summarized output. They are particularly useful for data analysis, reporting, and summarizing large datasets. Aggregate functions can be used in combination with GROUP BY clauses to perform calculations across groups of data, providing valuable insights into the overall characteristics of the data in a database.

Question 201

C) Separation of duties (Correct Answer)

Explanation: Separation of duties is a security principle that enforces the concept of two-person control by dividing critical tasks or responsibilities among different individuals. This prevents a single person from having complete control over sensitive operations, reducing the risk of fraud, errors, or malicious activities. It ensures that multiple people are involved in critical processes, enhancing accountability and security.

Question 202

A) Reconnaissance (Correct Answer)

Explanation: This type of attack is known as a port scan, which is a form of reconnaissance. By attempting to connect to all 65,536 TCP ports on a single system within a brief timeframe, the attacker is gathering information about open ports and potential vulnerabilities. This is typically an initial step in the attack process, allowing the adversary to map

out the target system's structure and identify potential entry points for further exploitation.

Question 203

D) PASTA (Correct Answer)

Explanation: PASTA (Process for Attack Simulation and Threat Analysis) is a risk-centric threat modeling methodology that consists of seven stages. These stages include defining objectives, technical scope, application decomposition, threat analysis, vulnerability assessment, attack modeling, and risk impact analysis. PASTA provides a comprehensive approach to identifying and analyzing potential threats to an application or system.

Question 204

B) Firmware (Correct Answer)

Explanation: Firmware refers to software that is stored in a Read-Only Memory (ROM) chip or other non-volatile memory. It is a type of low-level software that provides control, monitoring, and data manipulation functions for devices. Firmware is typically used in embedded systems and is essential for the basic operation of hardware devices, acting as an interface between the hardware and higher-level software.

Question 205

B) Responsibility Assignment Matrix (Correct Answer)

Explanation: A Responsibility Assignment Matrix (RAM), also known as a RACI matrix (Responsible, Accountable, Consulted, Informed), is a tool used in project management and organizational planning. It clearly outlines roles and responsibilities for various activities or groups of tasks within a project or organization. This matrix helps in clarifying expectations, avoiding duplication of efforts, and ensuring that all necessary tasks are assigned to specific individuals or teams.

Question 206

D) An RFC 1918 address (Correct Answer)

Explanation: The IP address 10.11.45.170 falls under the category of an RFC 1918 address. RFC 1918 defines private IP address ranges for use in private networks. The address 10.11.45.170 is part of the 10.0.0.0/8 range, which is one of the three private IP address ranges specified in RFC 1918. These addresses are not routable on the public internet and are commonly used in local area networks (LANs) and for internal network addressing.

Question 207

A) Personal Identity Verification (PIV) (Correct Answer)

Explanation: Personal Identity Verification (PIV) is the term used for smart cards issued to US government personnel. These cards include a photograph and other identifying information, serving as both a badge for physical access and a smart card for logical access to computer systems. PIV cards are part of a standardized identity credentialing system used across federal agencies to enhance security and interoperability.

Question 208

B) Application firewall (Correct Answer)

Explanation: An application firewall, also known as a Web Application Firewall (WAF), operates at the application layer (Layer 7) of the OSI model. It has the capability to inspect traffic at this level and perform protocol-specific analysis for malicious content. Unlike packet filtering or stateful inspection firewalls, application firewalls can understand and filter HTTP traffic, detect SQL injection attempts, cross-site scripting, and other application-layer attacks.

Question 209

A) Qualitative Risk Analysis (Correct Answer)

Explanation: Qualitative Risk Analysis is an approach to risk assessment that involves scenario-based evaluation using ranking and grading for exposure ratings and decision-making. This method uses subjective criteria to categorize risks, often employing scales like "low," "medium," and "high" to assess likelihood and impact. It's particularly useful when numerical data is limited or when a quick assessment is needed, providing a general understanding of relative risk levels to guide decision-making.

Question 210

A) TOCTOU (Correct Answer)

Explanation: TOCTOU stands for Time-of-Check to Time-of-Use, which is a timing vulnerability that occurs when a program verifies access permissions too far in advance of a resource request. This creates a window of opportunity for an attacker to manipulate the resource between the time of the check and the time of use. TOCTOU vulnerabilities can lead to privilege escalation or unauthorized access to resources in multi-threaded or time-shared systems.

Question 211

B) Hashed Message Authentication Code (HMAC) (Correct Answer)

Explanation: A Hashed Message Authentication Code (HMAC) provides a partial digital signature, ensuring message integrity during transmission but not offering non-repudiation. HMAC uses a cryptographic hash function in combination with a secret key to produce a message authentication code. This technique verifies both the data integrity and the authenticity of a message, but since it uses a shared secret key, it doesn't provide non-repudiation like a full digital signature would.

Question 212

C) Information Flow Model (Correct Answer)

Explanation: The Information Flow Model is a security model that focuses on controlling how information moves within a system, maintaining and enforcing security regardless of the information's path. It is based on a State Machine Model, which represents the system as a set of states and transitions. This model ensures that information flows only in authorized ways, preventing unauthorized access or leakage of sensitive data across different security levels or compartments.

Question 213

C) Compiler (Correct Answer)

Explanation: A compiler is a programming tool that converts high-level language code into an executable file designed for a specific operating system. It translates human-readable source code into machine code or lower-level code that can be directly executed by the computer's processor. Compilers perform various optimizations and error checks during this process, producing efficient and platform-specific executable programs.

Question 214

C) Attackers may use XSS filter evasion techniques against this approach (Correct Answer)

Explanation: Filtering out only the <SCRIPT> tag on the server side is insufficient to prevent cross-site scripting (XSS) attacks. Attackers can use various XSS filter evasion techniques to bypass this simple protection. For example, they might use other HTML tags that can execute JavaScript (like <img> with an onerror attribute), or employ encoding tricks to disguise malicious scripts. A comprehensive approach to XSS prevention requires more robust input validation and output encoding techniques.

Question 215

D) Authentication (Correct Answer)

Explanation: Authentication is the process of verifying or testing the validity of an identity claimed by a subject. It involves confirming that an entity (user, system, or device) is who or what it claims to be. This process typically involves checking credentials, such as passwords, biometrics, or security tokens, against stored information to ensure the authenticity of the claimed identity. Authentication is a crucial component of access control and information security.

Question 216

D) Multilayer (Correct Answer)

Explanation: Multilayer protocols rely on encapsulation as their core concept. Encapsulation is the process of wrapping data from one protocol inside another protocol's data unit. This layered approach allows for the separation of networking functions and enables data to be transmitted across different network types. The OSI (Open Systems Interconnection) model and the TCP/IP model are examples of multilayer protocol suites that extensively use encapsulation to facilitate communication between different layers and across networks.

Question 217

C) Inappropriate Activities (Correct Answer)

Explanation: Inappropriate Activities refer to actions that occur on a computer or over IT infrastructure that may not be criminal but often result in internal disciplinary measures or termination. These activities violate organizational policies, ethical standards, or acceptable use guidelines. Examples might include accessing inappropriate content, excessive personal use of company resources, or minor security policy violations. While not necessarily illegal, these actions can compromise productivity, security, or the organization's reputation.

Question 218

D) The CA's private key (Correct Answer)

Explanation: When a Certificate Authority (CA) creates a digital signature for a certificate, it uses its private key to sign the completed certificate. This process ensures the authenticity and integrity of the certificate. The CA's private key is kept secret and is used to create signatures that can be verified using the CA's public key. This mechanism allows anyone with the CA's public key to verify that the certificate was indeed issued and signed by the trusted CA.

Question 219

D) Generational (Correct Answer)

Explanation: Generational fuzzing, also known as intelligent fuzzing, is an advanced fuzzing technique that generates test cases based on understanding the format or structure of the input data. Unlike mutation-based fuzzing, which randomly modifies existing inputs, generational fuzzing creates new inputs from scratch using knowledge of the input format. This approach allows for more targeted and efficient testing, potentially uncovering deeper and more complex vulnerabilities in the system under test.

Question 220

D) Asset (Correct Answer)

Explanation: An asset is anything within an environment that should be protected. In the context of information security, assets can include physical items (like computers, servers, or network devices), digital assets (such as data, software, or intellectual property), and even intangible assets (like reputation or business processes). Identifying and classifying assets is a crucial step in risk management and security planning, as it helps organizations prioritize their protection efforts and allocate resources effectively.

Question 221

B) SLA (Correct Answer)

Explanation: SLA stands for Service Level Agreement, which is a contractual obligation that often requires the implementation of sound Business Continuity Planning (BCP) practices for clients. An SLA is a formal agreement between a service provider and a client that defines the level of service expected, including aspects of availability, performance, and disaster recovery. By including BCP requirements in SLAs, organizations ensure that their service providers have adequate measures in place to maintain operations and recover from disruptions, thus protecting the client's interests.

Question 222

B) Visual Card (Correct Answer)

Explanation: A Visual Card is a human-readable only card ID typically featuring a photo and written information about the authorized bearer. These cards are used in environments where automated controls are impractical but security guards are available to visually verify identities. Visual cards rely on physical inspection rather than electronic scanning, making them suitable for low-tech security environments or as a backup to more sophisticated access control systems.

Question 223

A) Risk Management (Correct Answer)

Explanation: Risk Management is the comprehensive process of identifying potential threats, evaluating their impact, and implementing cost-effective solutions to mitigate or reduce risk. This ongoing process involves risk assessment, risk treatment (including mitigation, transfer, acceptance, or avoidance), and continuous monitoring. Risk management aims to balance the costs of protective measures against the potential losses from security

incidents, ensuring that an organization's resources are used efficiently to address the most significant risks.

Question 224

B) Hot Site (Correct Answer)

Explanation: A Hot Site is a backup facility maintained in constant working order, with a full complement of servers, workstations, and communication links ready to assume primary operations responsibilities. It is designed for immediate takeover of critical business functions in the event of a disaster or major disruption at the primary site. Hot sites are the most expensive type of backup facility but offer the fastest recovery time, typically allowing operations to resume within hours of activation.

Question 225

D) Aggregate Functions (Correct Answer)

Explanation: Aggregate Functions in SQL are functions that accumulate values and return a single result. These functions operate on a set of rows and return a single output value. Common aggregate functions include COUNT(), MIN(), MAX(), SUM(), and AVG(). They are typically used in combination with GROUP BY clauses to perform calculations across a set of rows that match specified criteria. Aggregate functions are essential for data analysis and reporting in database systems.

Question 226

A) Operational investigation (Correct Answer)

Explanation: Operational investigations typically have the most relaxed standards for information collection and preservation. These investigations are internal to an organization and are often conducted for business purposes, such as improving processes or addressing performance issues. Unlike criminal, civil, or regulatory investigations, operational investigations are not bound by strict legal

requirements for evidence handling and can be more flexible in their approach.

Question 227

D) Auxiliary Alarm System (Correct Answer)

Explanation: An Auxiliary Alarm System is an additional function that can be added to local or centralized alarm systems to automatically notify police or fire services when an alarm is triggered. This system creates a direct link between the alarm system and emergency services, reducing response time and enhancing overall security. It's particularly useful in situations where immediate professional response is crucial.

Question 228

C) Misuse case testing (Correct Answer)

Explanation: Misuse case testing involves diagramming potential hacker approaches to an application and determining how the system would respond to likely attacker behavior. This type of testing focuses on identifying potential security vulnerabilities by simulating malicious user actions. It helps developers understand how their application might be exploited and allows them to implement appropriate countermeasures.

Question 229

C) Sunday's full backup (Correct Answer)

Explanation: In a backup strategy involving full backups on Sundays and differential backups Monday through Friday, the Sunday full backup should be applied first when restoring data after a server failure. A full backup contains all the data, while differential backups only contain changes since the last full backup. To restore, you start with the most recent full backup (Sunday's) and then apply the most recent differential backup to get the latest data state.

Question 230

A) Evil Twin (Correct Answer)

Explanation: An Evil Twin attack is where a hacker operates a false access point that automatically clones the identity of another access point based on a client device's automatic reconnection request. This type of attack exploits the tendency of devices to automatically connect to known networks, allowing the attacker to intercept data or conduct man-in-the-middle attacks. It's particularly effective in public Wi-Fi scenarios.

Question 231

D) Frame (Correct Answer)

Explanation: In networking, a frame is the combination of the Data Link Layer header, payload, and footer. The frame is the basic unit of communication at the Data Link Layer (Layer 2) of the OSI model. It encapsulates the data from higher layers and includes addressing and error-checking information specific to the Data Link Layer protocol being used, such as Ethernet or Wi-Fi.

Question 232

B) Watermarking (Correct Answer)

Explanation: Watermarking is the most effective security control for tracing the source of sensitive documents if they appear in a public forum. It involves embedding a unique, often invisible, identifier into a document. This identifier can be used to trace the origin or ownership of the document. Unlike hashing or digital signatures, watermarks remain intact even if the document is partially altered or shared in different formats, making them ideal for tracking leaked documents.

Question 233

A) Broadband (Correct Answer)

Explanation: Cable modems, ISDN (Integrated Services Digital Network), and DSL (Digital Subscriber Line) all fall under the category of broadband technology. Broadband refers to high-speed internet access that is always on and faster than traditional dial-up access. These technologies use wide bandwidth data transmission to carry multiple signals and traffic types, allowing for faster data transfer rates compared to narrowband technologies.

Question 234

C) Bracketed (Correct Answer)

Explanation: "Bracketed" is not a recognized design in Mandatory Access Control (MAC) systems. The common designs in MAC systems include hierarchical (based on security levels) and compartmentalized (based on categories or need-to-know). Some systems also use a hybrid approach combining both. "Bracketed" is not a term used in the context of MAC system designs.

Question 235

B) TLS, VPN, IPsec (Correct Answer)

Explanation: TLS (Transport Layer Security), VPN (Virtual Private Network), and IPsec (Internet Protocol Security) are commonly employed methods to protect data in transit. These protocols provide encryption and authentication for data as it moves across networks. TLS secures web traffic, VPNs create secure tunnels for data transmission, and IPsec provides security at the IP layer. Together, they offer comprehensive protection for data during transmission.

Question 236

B) Private Branch Exchange (PBX) (Correct Answer)

Explanation: A Private Branch Exchange (PBX) is a sophisticated local telephone exchange often used by organizations for inbound call support, extension-to-extension calling, conference calling, and voicemail. It acts

as a private telephone network within an organization, allowing for internal communication and shared external phone lines. Modern PBX systems can be hardware-based or software-based (IP PBX) and offer advanced features like call routing, voicemail-to-email, and integration with other business systems.

Question 237

D) Real Memory (Correct Answer)

Explanation: Real Memory, also known as physical memory or main memory, is typically the largest RAM storage resource available to a computer. It is composed of dynamic RAM chips that require periodic refreshing by the CPU to maintain data. Real memory is the actual hardware RAM installed in the computer, as opposed to virtual memory which uses hard disk space to supplement physical RAM.

Question 238

A) Turnstile (Correct Answer)

Explanation: A turnstile is a security control indicated by an arrow pointing to a unidirectional gate that prevents more than one person from entering a facility at a time. Turnstiles are physical access control devices that allow only one person to pass through at a time, often used in conjunction with card readers or other authentication methods. They help prevent tailgating and unauthorized access to secure areas.

Question 239

D) SMTP (Correct Answer)

Explanation: SMTP (Simple Mail Transfer Protocol) is primarily used for moving email messages from clients to servers and between servers. It is the standard protocol for sending email across the Internet. While other protocols like POP3 and IMAP are used for retrieving emails from servers,

SMTP handles the task of sending emails and relaying them between mail servers.

Question 240

D) False acceptance will be very high (Correct Answer)

Explanation: On a biometric authentication curve, false acceptance rates would be very high at the point where the system is set to be highly permissive. This typically occurs when the threshold for accepting a match is set very low. In this scenario, the system is more likely to incorrectly accept unauthorized users, leading to a high false acceptance rate. This trade-off is often visualized in a ROC (Receiver Operating Characteristic) curve, showing the relationship between false acceptance and false rejection rates.

Question 241

A) 15 (Correct Answer)

Explanation: For a system with 6 users where any 2 users should be able to communicate securely using symmetric encryption, 15 keys are needed. This is calculated using the combination formula: $n(n-1)/2$, where n is the number of users. In this case, $6(6-1)/2 = 15$. Each pair of users needs a unique shared key for secure communication, resulting in 15 different key combinations.

Question 242

A) Highly cohesive (Correct Answer)

Explanation: An object that can perform a task with minimal assistance from other objects is described as highly cohesive. In object-oriented programming, cohesion refers to the degree to which the elements of a module belong together. High cohesion means that the methods and properties of a class are closely related and focused on a single purpose, making the object more independent and easier to maintain.

Question 243

D) Boot Sector (Correct Answer)

Explanation: The boot sector is the portion of a storage device used to load the operating system. It's a critical part of the boot process, containing code that initiates the loading of the operating system. Boot sector viruses are a type of malware that specifically target this area, infecting it to gain control of the system during the boot process. These viruses can be particularly dangerous as they activate before antivirus software loads.

Question 244

B) Open networks are unencrypted, making traffic easily sniffable (Correct Answer)

Explanation: In open wireless networks, the vulnerability that allows users to potentially capture other customers' web traffic, including usernames and passwords, is that the network traffic is unencrypted. Open networks do not use encryption protocols like WPA or WPA2, meaning data transmitted over the network is sent in clear text. This makes it easy for anyone on the same network to intercept and read the traffic using packet sniffing tools.

Question 245

C) Longer passwords and salting (Correct Answer)

Explanation: Longer passwords and salting are the two most effective controls in preventing password cracking attacks against a system. Longer passwords increase the complexity and time required for brute-force attacks. Salting involves adding random data to each password before hashing, which prevents the use of rainbow tables and makes each hash unique even for identical passwords. This combination significantly increases the difficulty of cracking passwords.

Question 246

C) Packets with the source address from the public IP address block (Correct Answer)

Explanation: When configuring egress monitoring on a network, packets with the source address from the public IP address block assigned to the organization should be allowed to leave the network headed for the Internet. This ensures that only legitimate outbound traffic from the organization's public IP range is permitted, preventing IP spoofing and helping to maintain network security. Packets with private or unassigned source addresses should typically be blocked to prevent potential abuse.

Question 247

B) Impact (Correct Answer)

Explanation: When using encryption to protect sensitive business information during transmission over the Internet, the risk metric that is reduced is the impact. Encryption doesn't necessarily reduce the likelihood of an attack or interception attempt, but it significantly reduces the impact if data is intercepted. Even if an attacker captures the encrypted data, they cannot read or use it without the decryption key, thus minimizing the potential damage or data breach impact.

Question 248

D) Patent (Correct Answer)

Explanation: A patent is the most suitable type of intellectual property protection for a company wanting to license a newly developed manufacturing process to other companies while preventing unauthorized use. Patents provide exclusive rights to the inventor for a limited period, typically 20 years, in exchange for public disclosure of the invention. This allows the company to license the process to others while maintaining legal protection against unauthorized use or replication.

Question 249

B) Protocol (Correct Answer)

Explanation: A protocol is the set of rules and restrictions that define how data is transmitted over a network medium, enabling computer-to-computer communications. Protocols specify the format, timing, sequencing, and error control in data communication. They are essential for ensuring that different devices and systems can understand each other and exchange information effectively across networks.

Question 250

D) Aggregate Functions (Correct Answer)

Explanation: Aggregate functions in SQL, such as COUNT(), MIN(), MAX(), SUM(), and AVG(), can be run against a database to produce an information set. These functions perform calculations on a set of values and return a single result. They are particularly useful for data analysis, reporting, and summarizing large datasets. Aggregate functions operate on multiple rows and can be used with GROUP BY clauses to perform calculations across groups of data.

Practice Tests 5

Question 1

A facilities manager named Hunter at OZ-Tech, a large data center management company, is assessing the installation of a flood prevention system at one of their facilities. The facility and its contents are valued at $100 million, and the new flood prevention system would cost $10 million to install. After consulting with flood experts, Hunter determined that the facility is located in a 200-year flood plain and that a flood would likely cause $20 million in damage to the facility.

Based on this information, what is the yearly probability of a flood occurring at the OZ-Tech data center?

A) 0.05

B) 0.005

C) 0.02

D) 0.002

Question 2

Two friends, Sanil and Richard, who are in different physical locations, want to start communicating using cryptography to protect the confidentiality of their messages. They exchange digital certificates to begin this process and plan to use an asymmetric encryption algorithm for secure email exchange.

When Sanil sends a message to Richard, which key should he use for encryption?

A) Sanil's public key

B) Richard's public key

C) Sanil's private key

D) Richard's private key

Question 3

Harry is worried that accountants in his organization might use Data Diddling Attacks to conceal fraudulent activities in accounts they regularly access.

Which of the following security measures would be most effective in preventing this type of attack?

A) Access Control

B) Firewalls

C) Encryption

D) Integrity Verification

Question 4

Complete the following sentence in the context of Information Systems Security:

"[?] is an attack where a malicious individual intercepts part of a communication between an authorized user and a resource, then uses a technique to take control of the session and assume the authorized user's identity."

A) Session Hijacking

B) Malware Attack

C) Drive-by Attack

D) Man-in-the-Middle Attack

Question 5

Fill in the blank in the following sentence within the context of Information Systems Security:

"The [?] is the highest level of administrative access in a system."

A) Header

B) Base

C) Core

D) Root

Question 6

Complete the following sentence in the context of Information Systems Security:

"A(n) [?] is an individual assigned or delegated the daily responsibilities of classifying and labeling objects, as well as properly storing and protecting them."

A) Program Analyst

B) Custodian

C) Program Manager

D) Business Analyst

Question 7

Which RAID level is also referred to as disk striping with parity?

A) RAID 0

B) RAID 5

C) RAID 1

D) RAID 10

Question 8

What is another term for active monitoring?

A) Passive

B) Reactive

C) Span-based

D) Synthetic

Question 9

Charles Xavier owns a coffee shop and wants to provide wireless internet service for his customers. His network is

simple, using a single customer-grade wireless router and cable modem connected via a commercial cable data contract.

How can Charles implement access control for his customers without having to set up user IDs in advance, while also collecting useful contact information for his business purposes?

A) A Captive Portal

B) Port Security

C) WPA2 PSK

D) Require customers to use a publicly posted password like "Charles Xavier's Coffee"

Question 10

Complete the following sentence in the context of Information Systems Security:

"A(n) [?] is the exploitation of a vulnerability by a threat agent."

A) Assault

B) Charge

C) Blunt-Force Attack

D) Attack

Question 11

Fill in the blank in the following sentence within the context of Information Systems Security:

"The [?] is legislation that amends the US Code to implement additional information security policies and procedures."

A) Government Information Security Reform Act of 2000

B) Government Information Act of 2009

C) Information Management Act of 2005

D) Freedom of Information Act of 1999

Question 12

Complete the following sentence in the context of Information Systems Security:

"A(n) [?] is an error that occurs when a biometric device is overly sensitive and fails to authenticate a valid subject."

A) False Rejection Rate (FRR)

B) False Acceptance Rate (FAR)

C) Unusual Rejection Rate (URR)

D) Unusual Acceptance Rate (UAR)

Question 13

Surveys, interviews, and audits are all examples of methods to measure which important aspect of an organization's security posture?

A) Attack surface

B) Awareness

C) Service vulnerabilities

D) Code quality

Question 14

Which of the following tools is most appropriate for the information gathering phase of a penetration test?

A) zzuf

B) Whois

C) Metasploit

D) Nessus

Question 15

In the OSI Model, which layer determines the physical path that data will take?

A) Datalink

B) Presentation

C) Network

D) Application

Question 16

Complete the following sentence in the context of Information Systems Security:

"[?] is the formal declaration by the Designated Approving Authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk."

A) Acceptance

B) Affirmation

C) Accreditation

D) Designation

Question 17

Which of the following is not a valid key length for the Advanced Encryption Standard?

A) 192 bits

B) 128 bits

C) 256 bits

D) 384 bits

Question 18

What type of testing is used to ensure that separately developed software modules properly exchange data?

A) Dynamic testing

B) API checksums

C) Interface testing

D) Fuzzing

Question 19

When Nico Minoru logs into his system, his password is compared to a hashed value stored in a database.

What is this process called?

A) Validation

B) Identification

C) Hashing

D) Authentication

Question 20

Proteus is building a fault-tolerant server and wants to implement RAID 1.

How many physical disks are required to create this solution?

A) 1

B) 5

C) 3

D) 2

Question 21

Fill in the blank in the following sentence within the context of Information Systems Security:

"A(n) [?] is any event that negatively impacts the confidentiality, integrity, or availability of an organization's assets."

A) Incident

B) Risk

C) Problem

D) Issue

Question 22

Complete the following sentence in the context of Information Systems Security:

"[?] is the concept of controlling access to an environment through strict adherence to and enforcement of a security policy. The goals of [?] are to prevent/reduce zero-day attacks, enforce security policy compliance throughout the network, and use identities to perform access control."

A) Discretionary Access Control (DAC)

B) Network Access Control (NAC)

C) Role-Based Access Control (RBAC)

D) Mandatory Access Control (MAC)

Question 23

Fill in the blank in the following sentence within the context of Information Systems Security:

"A(n) [?] is the human-friendly name of a system or resource that is associated with an IP address. A(n) [?] is composed of a host name, a registered domain name, and a Top Level Domain name (TLD)."

A) Uniform Resource Locator (URL)

B) Main Level Domain Name (MLDN)

C) Internet Protocol Address (IPA)

D) Fully Qualified Domain Name (FQDN)

Question 24

Complete the following sentence in the context of Information Systems Security:

"A(n) [?] attack is a standard term used to describe an attack that exploits new vulnerabilities. These [?] DDoS vulnerabilities do not have patches or effective defensive mechanisms."

A) Armada

B) Zero Day

C) Teardrop

D) Ping-of-Death

Question 25

Kabuki is a database security administrator for Aircraft Systems, Inc. (ASI), a military contractor involved in the design and analysis of aircraft avionics systems. ASI regularly handles classified information for the government and other government contractors. Kabuki is concerned about ensuring the security of information stored in ASI databases. The database is multi-level security, with different ASI employees having different security clearances. It contains information on the location of military aircraft with ASI systems to allow ASI staff to monitor those systems. Kabuki wants to create a key that enforces referential integrity for the database.

What type of key does she need to create?

A) Candidate key

B) Primary key

C) Foreign key

D) Master key

Question 26

Fill in the blank in the following sentence within the context of Information Systems Security:

"A(n) [?] is an algorithm that relies on a 'shared secret' encryption key distributed to all members participating in communications. This key is used by all parties to both encrypt and decrypt messages."

A) Symmetric Key

B) Public Key

C) Asymmetric Key

D) Private Key

Question 27

Complete the following sentence in the context of Information Systems Security:

"[?] is an email or electronic communications scam targeted towards a specific individual, organization or business."

A) Spear Phishing

B) Whaling

C) Spamming

D) Pharming

Question 28

The Avengers organization needs to use a non-IP protocol on their VPN.

Which of the common VPN protocols should be chosen to natively support non-IP protocols?

A) L2F

B) L2TP

C) IPSec

D) PPTP

Question 29

The following are all types of what?

Direct

Circumstantial

Primary

Secondary

Documentary

A) Evidence

B) Responsibility

C) Data

D) Management

Question 30

Which group is best suited to evaluate and report on the effectiveness of administrative controls an organization has put in place to a third party?

A) Penetration testers

B) Employees who design, implement, and monitor the controls

C) Internal auditors

D) External auditors

Question 31

Which of the following tools might an attacker use to best identify vulnerabilities in a targeted system?

A) nessus

B) ipconfig

C) traceroute

D) nmap

Question 32

Which of the following is not a mode of operation for the Data Encryption Standard?

A) AES

B) CFB

C) OFB

D) CBC

Question 33

RIP, OSPF, and BGP are all examples of protocols associated with what type of network device?

A) Routers

B) Gateways

C) Switches

D) Bridges

Question 34

Carol Danvers's SMTP server does not authenticate senders before accepting and relaying email.

What is this security configuration issue known as?

A) An email gateway

B) An open relay

C) An SMTP relay

D) An X.400-compliant gateway

Question 35

Fill in the blank in the following sentence within the context of Information Systems Security:

"[?] are the records created by recording information about events and occurrences into a database or log file."

A) Audit trails

B) Transaction ledger

C) Transaction Lifecycle history

D) XAT report

Question 36

Complete the following sentence in the context of Information Systems Security:

"[?] is a platform-independent programming language developed by Sun Microsystems."

A) Python

B) Java

C) SQL

D) Jira

Question 37

The company that Lenny works for is reviewing the security of their issued cell phones. They provide 4G-capable smartphones running Android or iOS and use a mobile device management solution to deploy company software to the phones. The mobile device management software also allows the company to remotely wipe the phones if they are lost.

What security consideration should Lenny's company require for sending sensitive data over the cellular network?

A) Cellular provider networks are private networks and should not require special consideration

B) Encrypt all traffic to ensure confidentiality

C) They should use the same requirements as data over any public network

D) Require the use of WAP for all data sent from the phone

Question 38

What is the process that occurs when the session layer removes the header from data sent by the transport layer?

A) De-encapsulation

B) Payloading

C) Packet unwrapping

D) Encapsulation

Question 39

Fill in the blank in the following sentence within the context of Information Systems Security:

"A(n) [?] is a cloud deployment model that uses cloud-based assets for a single organization. Organizations can create host exclusive deployments using their own resources."

A) Platform-as-a-Service (PaaS)

B) Hybrid Cloud

C) Private Cloud

D) Public Cloud

Question 40

Complete the following sentence in the context of Information Systems Security:

"[?] is a software testing technique in which the internal structure, design, and coding of software are tested to verify the flow of input-output and to improve design, usability, and security."

A) Black-Box Testing

B) Blue-Box Testing

C) White-Box Testing

D) Gray-Box Testing

Question 41

Fill in the blank in the following sentence within the context of Information Systems Security:

"A(n) [?] is a component of an expert system; it contains the rules known by an expert system and seeks to codify the knowledge of human experts in a series of 'if/then' statements."

A) Dictionary

B) Manual

C) Knowledgebase

D) Structured Content Query

Question 42

Complete the following sentence in the context of Information Systems Security:

"[?] is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers."

A) Bluefishing

B) Bluejacking

C) Blueprinting

D) Bludgeoning

Question 43

Fill in the blank in the following sentence within the context of Information Systems Security:

"[?] is a skill by which an unauthorized person gains the trust of someone inside an organization and encourages the victim to make a change to the system in order to grant the attacker access. It can also be used as a means to trick a victim into disclosing information to the attacker."

A) Shoulder Surfing

B) Brute Force Assault

C) DoS Manipulation

D) Social Engineering

Question 44

Billy implemented RAID level 5 on a server that he operates using a total of three discs.

How many discs may fail without the loss of data?

A) Zero

B) One

C) Two

D) Three

Question 45

Complete the following sentence in the context of Information Systems Security:

"The [?] is a law that establishes the prohibition of attempts to circumvent copyright protection mechanisms placed on a protected work by the copyright holder and limits the liability of Internet service providers when their circuits are used by criminals violating the copyright law."

A) Millennium Digital Copyright Act

B) Federal Media Copyright Act

C) Global Correspondence Copyright Act

D) International Publishing Copyright Act

Question 46

Ed is tasked with protecting information about his organization's customers, including their name, Social Security number, birthdate, and place of birth, as well as a variety of other information.

What is this information known as?

A) PID

B) PII

C) PHI

D) Personal Protected Data

Question 47

Fill in the blank in the following sentence within the context of Information Systems Security:

"A(n) [?] is a standby facility large enough to handle the processing load of an organization and with appropriate electrical and environmental support systems."

A) Emergency Site

B) Cold Site

C) Virtual Site

D) Parallel Site

Question 48

Complete the following sentence in the context of Information Systems Security:

"A(n) [?] is a collection of resource services deployed in numerous data centers across the internet in order to provide low latency, high performance, and high availability of the hosted content."

A) Global Data Allocation (GDA)

B) Dynamic Load Balancing (DLB)

C) Cloud Content Harmonization (CCH)

D) Content-Distribution Network (CDN)

Question 49

The company that Loki works for is reviewing the security of their issued cell phones. They provide 4G-capable smartphones running Android or iOS and use a mobile device management solution to deploy company software to the phones. The mobile device management software also allows the company to remotely wipe the phones if they are lost. Loki plans to attend a major hacker conference this year.

What should he do when connecting to his cellular provider's 4G network while at the conference?

A) Only use trusted Wi-Fi networks

B) Connect to his company's encrypted VPN service

C) Discontinue all usage; Towers can be spoofed

D) Continue normal usage

Question 50. What type of diagram used in application threat modelling incorporates malicious users and descriptions such as "mitigates" and "threatens"?

A) Misuse case diagrams

B) STRIDE charts

C) Threat trees

D) DREAD diagrams

Question 51. How should samples be generated when evaluating account management practices?

A) Validate accounts from the last 180 days

B) Have administrators generate the samples

C) Audit all accounts as sampling is ineffective

D) Conduct random sampling

Question 52. Which software development methodology emphasizes customer needs and rapid, iterative development of new functionality?

A) Agile software development

B) Kanban software development

C) Lean software development

D) Waterfall software development

Question 53. In database terminology, what term refers to a record or role?

A) Relation

B) Field

C) Attribute

D) Tuple

Question 54. Which RAID level is commonly referred to as disk striping with parity?

A) RAID 1

B) RAID 0

C) RAID 5

D) RAID 10

Question 55. What is the term for a central repository that stores information about data elements, their relationships, usage, sources, and formats?

A) Data Element Wiki

B) Data Dictionary

C) Data Glossary

D) Data Definitions Table

Question 56. In a virtualized computing environment, which component is responsible for maintaining separation between guest machines?

A) Kernel

B) Protection manager

C) Guest operating system

D) Hypervisor

Question 57. Which testing method is characterized by being performed by non-employee clients or end users, typically in a real-time environment without a lab setup, and focusing on reliability, security, and robustness?

A) Delta Testing

B) Beta Testing

C) Omega Testing

D) Alpha Testing

Question 58. What process helps prevent unintended outages by requiring personnel to submit requests for configuration changes, which are then reviewed, approved, tested, implemented, and documented?

A) Change Management

B) Release Management

C) Deployment Management

D) Update Management

Question 59. What type of chart displays the interrelationships between projects and schedules over time, providing a graphical illustration to help plan, coordinate, and track specific tasks in a project?

A) Scrum Board

B) Gantt Chart

C) PDLC Chart

D) Kanban Board

Question 60. When preparing to solicit bids for a penetration test of networking systems, which type of test should be required to maximize effectiveness rather than realism?

A) Zero box

B) Black box

C) Grey box

D) Crystal box

Question 61. Which single sign-on (SSO) method allows for secure storage of information typically filled into documents through template completion?

A) Kerberos-based SSO

B) NTLM-based SSO

C) SPNEGO-based SSO

D) Form-filling SSO

Question 62. When implementing a Network Access Control (NAC) solution with a post-admission philosophy, what type

of issues cannot be addressed by a strict post-admission policy?

A) Preventing exploitation of an unpatched laptop immediately after network connection

B) Out-of-band monitoring

C) Denying access when user behavior doesn't match an authorized matrix

D) Allowing user access when user behavior aligns with an authorization matrix

Question 63. What is the process of attempting to discover the original message that has been hashed by generating potential messages, hashing them, and comparing their hash to the original?

A) Public Key Decryption

B) Symmetric Decryption

C) Asymmetric Decryption

D) Reverse Hash Matching

Question 64. Which term best describes an attack that uses stolen or falsified authentication credentials to bypass an authentication mechanism?

A) Masquerading

B) Modification

C) Spoofing

D) Replay

Question 65. What end-to-end encryption technique provides encrypted alternatives to common Internet applications such as FTP, Telnet, and rlogin?

A) SHA

B) SAML

C) SSH

D) SSL

Question 66. When reviewing a system assigned an EAL2 evaluation assurance level under common criteria, what is the highest level of assurance that can be expected?

A) It has been semi-formally designed and tested

B) It has been functionally tested

C) It has been formally verified, designed, and tested

D) It has been structurally tested

Question 67. When tasked with deploying an authentication, authorization, and accounting server for wireless network services while avoiding proprietary technology, which solution should be selected?

A) OAuth

B) TACACS+

C) XTACACS

D) RADIUS

Question 68. What method involves storing duplicate data on two or more hard drives for purposes such as data backup, fault tolerance, improved throughput, increased storage functions, and enhanced performance?

A) Cold Storage

B) Hot Storage

C) RAID

D) SAVED

Question 69. Which code review process is characterized by a highly formalized approach involving planning, overview, preparation, inspection, rework, and follow-up steps?

A) Dynamic inspection

B) Static inspection

C) Fagan inspection

D) Interface testing

Question 70. What term describes an organization's ability to absorb losses associated with realized risks?

A) Risk Capacity

B) Risk Acceptance

C) Risk Tolerance

D) Risk Diffusion

Question 71. In a scenario where a hacker might use an SQL injection attack to deface a web server due to a missing patch in a company's web application, what is considered the risk?

A) Web defacement

B) Unpatched web application

C) Hacker

D) Operating system

Question 72. What term is used to describe non-fluctuating pure power?

A) A Reserve

B) Nuclear Power

C) A Power Block

D) Clean Power

Question 73. What type of crypto processor is used to manage and store digital encryption keys, accelerate crypto operations, support faster digital signatures, and improve authentication?

A) Hardware Security Module (HSM)

B) Kubeflow

C) Kubernetes

D) Equinix Cloud Exchange Fabric (ECX Fabric)

Question 74. In the context of network protocols, what term describes data from an application sent into a protocol stack, which becomes the initial payload of the top layer protocol?

A) Data Trail

B) Data Line

C) Data Loop

D) Data Stream

Question 75. When needing to transfer files from a PC to a remote server securely, which protocol should be used instead of FTP?

A) SCP

B) SSH

C) Telnet

D) HTTP

Question 76. Which type of document provides a detailed, step-by-step description of the exact actions individuals must complete?

A) Policy

B) Standard

C) Guideline

D) Procedure

Question 77. What markup language is used to define access control policies within an XML format and commonly implements role-based access controls?

A) XACML

B) ACXML

C) XMLAC

D) ACML

Question 78. What term describes a new way of communication between two systems at a given point in time, where one system is called a "Client" and the other a "Server"?

A) REST

B) SSL

C) SQL

D) SAML

Question 79. During which phase of the electronic discovery process does an organization perform an initial filtering of gathered information to discard irrelevant data?

A) Processing

B) Identification

C) Preservation

D) Collection

Question 80. What is the minimum number of cryptographic keys required to achieve strong security when using the 3DES algorithm?

A) 3

B) 4

C) 2

D) 1

Question 81. Which type of access control is designed to discover unwanted or unauthorized activity by providing information after an event has occurred?

A) Directive

B) Detective

C) Preventative

D) Corrective

Question 82. What term describes a disaster recovery site that serves as a middle ground, containing necessary equipment and data circuits for rapid establishment of operations but typically not housing copies of client data?

A) Warm Site

B) Parallel Site

C) Cold Site

D) Hot Site

Question 83. What type of web attack exploits a trusted user to execute commands via their browser against a vulnerable server?

A) Cross-Site Request Forgery (CSRF)

B) Blunt-Force Attack (BFA)

C) Guerilla Website Attack (GWA)

D) Browser-to-Browser Hijacking (BBHJ)

Question 84. What activity transforms a zero-day vulnerability into a less dangerous attack vector?

A) Reconfiguration of a firewall

B) Implementation of transport-layer encryption

C) Release of a security patch

D) Discovery of the vulnerability

Question 85. What is the process of reversing a cryptographic algorithm that was used to encrypt a message?

A) Encrypting

B) Reverse Engineering

C) Ciphering

D) Decrypting

Question 86. Which model, originally published in 1977, was the first to address integrity concerns and includes properties such as simple integrity, star integrity, and invocation?

A) Integrity Flow Model

B) Biba Model

C) Information Flow Model

D) Bell-LaPadula Model

Question 87. What automated cash-management service is used to deter check fraud by matching the checks a company issues with those presented for payment?

A) Fraud Recovery TDR Report

B) Bust Out Referrals

C) Positive Pay

D) Loss-Prevention Automation

Question 88. What is the most effective method to ensure data is not recoverable from a Solid State Drive (SSD)?

A) Use a random pattern wipe of 1s and 0s

B) Use the built-in erase commands

C) Physically destroy the drive

D) Degauss the drive

Question 89. What type of software is used by an intruder to probe active systems on a network and determine the public services running on each machine?

A) SMB Scanner

B) NetBIOS Reader

C) Portal X-Ray

D) Port Scan

Question 90. When allowing a partner organization's Active Directory forest to access resources in your domain forest without reciprocal access and preventing trust flow upward through the domain tree, what type of trust should be established?

A) Set up a one-way nontransitive trust

B) Set up a one-way transitive trust

C) Set up a two-way nontransitive trust

D) Set up a two-way transitive trust

Question 91. What is the process which ensures that a requested activity or object access is possible given the rights and privileges assigned to an authenticated identity?

A) Permissioning

B) Identification

C) Justification

D) Authorization

Question 92. What term describes the removal of an employee's identity from the identity and access management system after they have left the organization?

A) Deletion

B) Purging

C) Offboarding

D) Erasing

Question 93. What risk rating system is designed to provide a flexible solution based on asking five main questions about each threat?

A) DEATH

B) DREAD

C) LANCE

D) FIGHT

Question 94. When Smart Card based locks are ineffective due to staff propping doors open, and signs are placed reminding staff of security issues along with alarms for doors left open, what type of controls have been implemented?

A) Compensation

B) Administrative

C) Recovery

D) Physical

Question 95. What is a central repository of data elements and their relationships that stores critical information about data usage, relationships, sources, and formats?

A) Data Element Wiki

B) Data Dictionary

C) Data Glossary

D) Data Definitions Table

Question 96. In a virtualized computing environment, which component is responsible for enforcing separation between guest machines?

A) Kernel

B) Protection manager

C) Guest operating system

D) Hypervisor

Question 97. What characteristics describe a testing method performed by non-employee clients or end users, typically in a real-time environment, focusing on reliability, security, and robustness?

A) Delta Testing

B) Beta Testing

C) Omega Testing

D) Alpha Testing

Question 98. What process helps prevent unintended outages by requiring personnel to submit requests for configuration changes, which are then reviewed, approved, tested, implemented, and documented?

A) Change Management

B) Release Management

C) Deployment Management

D) Update Management

Question 99. What type of chart displays the interrelationships between projects and schedules over time, providing a graphical illustration to help plan, coordinate, and track specific tasks in a project?

A) Scrum Board

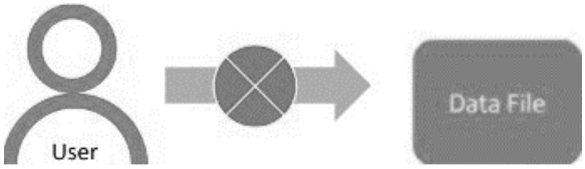
B) Gantt Chart

C) PDLC Chart

D) Kanban Board

Question 100

What security model prohibits a user from accessing files with a higher classification level than their clearance?



A) Clark-Wilson

B) Brewer-Nash

C) Biba

D) Bell-LaPadula

Question 101

Which of these is considered a man-in-the-middle attack technique?

A) Session hijacking

B) IP spoofing

C) Replay attack

D) All of the above

Question 102

What type of industrial control system distributes control elements across a monitored environment while centralizing monitoring and command functions?

A) Discretionary Access Control Systems

B) Distributed Control Systems

C) Distributed Access Control Systems

D) Directive Access Control Systems

Question 103

After detecting a potential security incident, what should be the next step in the incident response process?

A) Activate the incident response team

B) File a written report

C) Investigate the root cause

D) Attempt to restore system operations

Question 104

Which RAID level is commonly referred to as disk striping?

A) RAID 5

B) RAID 1

C) RAID 0

D) RAID 10

Question 105

What mobile device security feature allows for remote deletion of data and configuration settings?

A) Remote wipe

B) Unlocking a bootloader

C) Bricking

D) Jailbreaking

Question 106

Which network protocol uses a three-way handshake, performs error checking, and provides reliable data delivery?

A) UDP

B) TCP

C) SQL

D) SAML

Question 107

What type of non-volatile storage media can be electronically erased and rewritten in blocks or pages?

A) RAM

B) SSD

C) HDD

D) Flash memory

Question 108

Which data security standard is specific to the payment card industry?

A) PCI DSS

B) SOX

C) HIPAA

D) FERPA

Question 109

What term describes server configurations that provide backup options in case of disaster?

A) Cloud servers

B) Shared servers

C) Redundant servers

D) On-premise servers

Question 110

Which business process typically requires managerial approval before system modifications?

A) Release management

B) Versioning

C) Change management

D) SDN

Question 111

What database property ensures that committed transactions remain in the system even after failures?

A) Durability

B) Isolation

C) Atomicity

D) Consistency

Question 112

Which access control type aims to prevent unauthorized activities before they occur?

A) Deterrent access control

B) Security access control

C) Responsive access control

D) Preventive access control

Question 113

What legacy network technology used token-passing and dual counter-rotating rings?

A) Fiber Distributed Data Interface (FDDI)

B) Synchronous Optical Network (SONET)

C) Synchronous Digital Hierarchy (SDH)

D) Unilateral Flow Data Interface (UFDI)

Question 114

Who should receive initial business continuity plan training in an organization?

A) First responders

B) Those with specific business continuity roles

C) Senior executives

D) Everyone in the organization

Question 115

Which denial-of-service attack is similar to a Smurf attack but uses UDP packets?

A) Rumpelstiltskin

B) Bo-Peep

C) Red Riding Hood

D) Fraggle

Question 116

What risk management strategy involves taking action to ensure a potential risk cannot materialize?

A) Risk acceptance

B) Risk transfer

C) Risk avoidance

D) Risk mitigation

Question 117

What programming language serves as an intermediate step between machine code and high-level languages?

A) C+++

B) Assembly language

C) SAML

D) Fourth-generation language

Question 118

Which access control type aims to restore systems to normal after an unauthorized activity has occurred?

A) Corrective access control

B) Deterrent access control

C) Booby-trap access control

D) Repellant access control

Question 119

What team or department is primarily responsible for an organization's information security?

A) Senior management

B) IT

C) DevOps

D) InfoSec

Question 120

What security issue can arise when an employee changes roles multiple times within an organization?

A) Account creep

B) Least privilege violation

C) Privilege creep

D) Account termination

Question 121

What principle states that users should be granted minimal access necessary for their job functions?

A) Principle of required permissions

B) Principle of least privilege

C) Principle of basic access

D) Principle of minimal rights

Question 122

What term describes the practice of searching through an organization's discarded materials to find sensitive information?

A) Interrogation

B) Interpretation

C) Recycling

D) Dumpster diving

Question 123

What type of firewall tracks communication status and allows responses based on connection state?

A) Stateful packet inspection firewall

B) Static packet filtering firewall

C) Application-level gateway firewall

D) Circuit-level gateway firewall

Question 124

What capability allows a system to continue operating despite component failures?

A) Fault rebound

B) Fault acceptance

C) Fault forgiveness

D) Fault tolerance

Question 125

Which security protocol, designed to address WEP vulnerabilities, was replaced by AES-based CCMP and 802.1x?

A) TKIP

B) PEAP

C) TLS

D) EAP

Question 126

What type of access control aims to guide or restrict subject actions to ensure security policy compliance?

A) Digital Signature Standard (DSS)

B) Directive Access Control (DAC)

C) Direct addressing

D) Direct Memory Access (DMA)

Question 127

Which data removal technique category includes degaussing?

A) Destroy

B) Shrink

C) Clear

D) Purge

Question 128

What type of firewall lacks the ability to track connection status across packets?

A) Application proxy

B) Stateful inspection

C) Packet filter

D) Next generation

Question 129

In an Infrastructure as a Service (IaaS) cloud environment, what component is typically the vendor's responsibility?

A) Maintaining the host firewall

B) Maintaining the hypervisor

C) Configuring server access control

D) Managing operating system security settings

Question 130

Which access control mechanism uses security labels to regulate subject access to objects?

A) Policy-Based Access Control (PBAC)

B) Discretionary Access Control (DAC)

C) Mandatory Access Control (MAC)

D) Role-Based Access Control (RBAC)

Question 131

What technical term describes data remaining on storage media after attempted removal?

A) Data permanence

B) Data remanence

C) Data pooling

D) Failed clearing

Question 132

What term describes the mixing of data with different classification levels or need-to-know requirements?

A) Contamination

B) Contagion

C) Corruption

D) Pestilence

Question 133

What metric represents the cost associated with a single occurrence of a specific risk to an asset?

A) SLE

B) PLV

C) LVP

D) ELV

Question 134

What cryptographic technique involves adding random data to a password before hashing?

A) Key stretching

B) Seed

C) Nonce

D) Salt

Question 135

What type of network typically uses dedicated leased lines to connect geographically distant components?

A) FAN

B) WAN

C) KAN

D) LAN

Question 136

What term describes an automated program that crawls websites to retrieve and process data for users?

A) Cyborg

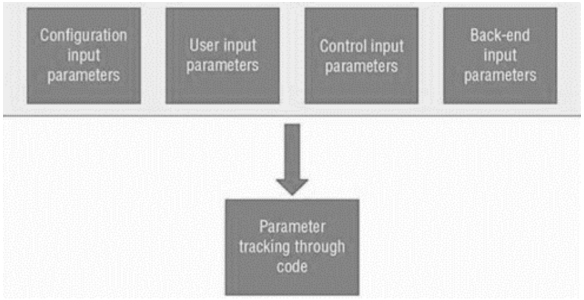
B) Bot

C) Android

D) AutoBot

Question 137

Which part of a security review process involves analyzing input parameters to identify potential vulnerabilities?



A) SQL injection review

B) Fagan inspection

C) Sprint review

D) Attack surface identification

Question 138

Under the Digital Millennium Copyright Act (DMCA), which group can receive safe harbor protection?

A) Book publishers

B) Music producers

C) Internet Service Providers

D) Banks

Question 139

What term describes the expected frequency of a specific threat or risk occurring within a year?

A) Annualized Loss Expectancy (ALE)

B) Single Loss Expectancy (SLE)

C) Break-Even Point (BEP)

D) Annual Rate of Occurrence (ARO)

Question 140

What cloud service involves using vendor-provided storage capacity to host organizational data?

A) Server farm

B) Shared cloud computing

C) Community storage

D) Cloud storage

Question 141

Which CPU protection rings were affected by the Meltdown bug announced in early 2018?

A) Rings 0 and 3

B) Rings 0 and 1

C) Rings 1 and 3

D) Rings 1 and 2

Question 142

What cryptographic method uses a pair of keys for message encryption and decryption?

A) Primary-key cryptography

B) Public-key cryptography

C) Index-key cryptography

D) Private-key cryptography

Question 143

What term describes a brief burst of electromagnetic energy that can disrupt electronic equipment?

A) Electrical spikes

B) Electromagnetic pulse

C) Common mode noise

D) Dips and surges

Question 144

What type of denial-of-service attack exploits Internet services by sending numerous packets with a spoofed source address?

A) Distributed Reflective Denial of Service (DRDoS)

B) Lightweight Directory Access Protocol (LDAP)

C) Cross-Site Scripting (XSS)

D) OS Command Injection (OSCI)

Question 145

What term describes the malicious gathering of confidential information for disclosure to competitors or other interested parties?

A) Espionage

B) Surveillance

C) Politics

D) Corruption

Question 146

In virtualization, what term describes an operating system running within a virtual machine?

A) Temporary OS

B) Core OS

C) Guest OS

D) Remote OS

Question 147

Where can one find the text of federal criminal and civil laws in the United States?

A) Supreme Court rulings

B) Compendium of laws

C) United States Code

D) Code of Federal Regulations

Question 148

What security issue arises when a user has more access or privileges than necessary for their job tasks?

A) Excessive privilege

B) Privilege mirroring

C) Privilege creep

D) Privilege transfer

Question 149: What is the term for information appended by a protocol to the beginning of a payload received from a higher-layer protocol?

A. Starter

B. Begin

C. <HEAD>

D. Header

Question 150: Which type of monitoring is employed when using a span port to observe traffic to a production website and identify performance issues in real-time?

A. Passive monitoring

B. Signature based monitoring

C. Active monitoring

D. Synthetic monitoring

Question 151: According to NIST SP800-53A guidelines for assessing security controls in federal information systems, what assessment methods are associated with mechanisms and activities?

A. Examine and test

B. Examine an interview

C. Test and assess

D. Test and interview

Question 152: What kind of risk evaluation utilizes tools like the one depicted in the image?

A. Quantitative

B. Financial

C. Loss expectancy

D. Qualitative

Question 153: What is the name of the device that detects authorized personnel and grants physical entry into a facility using field-powered technology?

A. Magnetic Reader

B. Proximity Reader

C. Circuit Reader

D. Memory Reader

Question 154: What security measure disables a user account after a specified number of failed login attempts as part of a password policy's programmatic controls?

A. User account bypass

B. Account lockout

C. Misuse prevention

D. Lost password recovery

Question 155: Which program does a United States federal government employee participate in to ensure acquired devices and components are not compromised?

A. MITRE

B. GovBuy

C. Trusted Foundry

D. TEMPEST

Question 156: In which development model is a large project divided into smaller parts, with each part undergoing multiple iterations of the waterfall model?

A. Kanban Development

B. Iterative Development

C. SCRUM Development

D. Agile Development

Question 157: What networking technology uses packet-switching to create virtual circuits for customers on a shared connection medium?

A. SMDS

B. ISDN

C. ATM

D. Frame Relay

Question 158: As a system owner for a healthcare organization, what is your primary responsibility regarding data on the systems you manage?

A. Classify the data

B. Grant appropriate access to personnel

C. Ensure appropriate security controls are in place to protect the data

D. Bear sole responsibility for data protection at rest, in transit, and in use

Question 159: What is the default subnet mask for a Class B network?

A. 255.0.0.0

B. 255.255.0.0

C. 255.254.0.0

D. 255.255.255.0

Question 160: What network utility is used to test the accessibility of a specific IP address when troubleshooting a connection?

A. Echo

B. Ping

C. CDN

D. SAML

Question 161: Which database programming language allows users to interact with data within the schema?

A. Data Control Language (DCL)

B. Data Definition Language (DDL)

C. Transaction Control Language (TCL)

D. Data Manipulation Language (DML)

Question 162: What term describes the monetary value assigned to an asset based on actual costs and non-monetary expenses?

A. Market Value

B. Equity Value

C. Asset Value

D. Liquidation Value

Question 163: What type of governmental grant gives an inventor the exclusive right to make, use, and sell their invention for a set period?

A. Patent

B. Copyright

C. Trademark

D. Permit

Question 164: When a system is assigned to EAL7 evaluation assurance level under the Common Criteria, what

is the highest level of assurance that can be claimed about it?

A. It has been formally verified, designed, and tested

B. It has been methodically tested and checked

C. It has been methodically designed, tested, and reviewed

D. It has been functionally tested

Question 165: What term describes any data item that can be easily traced back to its person of origin or concern?

A. Personally Identifiable Information (PII)

B. Individually Concealed Documentation (ICD)

C. Confidential Traceable Content (CTC)

D. Universally Discreet Data (UDD)

Question 166: Which rule of evidence requires system administrators to testify about how they gathered logs when presenting them as evidence in court?

A. Hearsay Rule

B. Best Evidence Rule

C. Parol Evidence Rule

D. Testimonial Evidence Rule

Question 167: If an organization switches from differential to incremental backups while maintaining the same schedule, how many backups would need to be applied to restore data to its most current state after a server failure on Wednesday at 3:00 PM?

A. 3

B. 1

C. 2

D. 4

Question 168: What protocol is used to transfer email messages from an email server to an email client?

A. Google Mail Services

B. Internet Message Access Protocol (IMAP)

C. AOL Mail Protocol (AOLMP)

D. Standard Mail Transfer Protocol (SMTP)

Question 169: In which cloud service model does the customer have the least responsibility for security?

A. PaaS

B. IaaS

C. SaaS

D. TaaS

Question 170: What is the term for a placeholder used in SQL for literal values such as numbers or string characters?

A. NULL

B. Bind Variable

C. Zero (0)

D. N/A

Question 171: When building an Ethernet network that needs to span over 150 meters with 1000Base-T, what technology should be used to address this distance?

A. Use STP cable to handle the longer distance at high speeds

B. Install a repeater or a concentrator before 100 metres

C. Use Category 7 cable, which has better shielding for higher speeds

D. Install a gateway to handle the distance

Question 172: What type of evidence is based on inference rather than personal knowledge or observation?

A. Opinion Evidence

B. Hearsay Evidence

C. Secondary Evidence

D. Circumstantial Evidence

Question 173: To effectively prevent a Smurf attack, what firewall configuration change should a network administrator implement?

A. Block the source IP address of the attack

B. Block the destination IP address of the attack

C. Block inbound ICMP traffic

D. Block inbound UDP traffic

Question 174: What is the name of the device that generates one-time passwords after a user enters a PIN, with the PIN provided by a server as a challenge?

A. Asynchronous Dynamic Password Token

B. Synchronous Dynamic Password Token

C. Asymmetric Dynamic Password Token

D. Symmetric Dynamic Password Token

Question 175: When developing a business continuity plan for a company in North Dakota that chooses to accept the risk of earthquakes, which action aligns with this strategy?

A. Relocating the data centre to a safer area

B. Reengineering the facility to withstand earthquake shocks

C. Purchasing earthquake insurance

D. Documenting the decision-making process

Question 176: What is the term for the legal process where each party must preserve and share evidence related to a case, including both paper and electronic records?

A. Digital Deposition

B. Privileged Information

C. Electronic Discovery

D. The Electronic Evidence Procedure

Question 177: What type of attack has become prevalent in database-driven websites, where a malicious actor executes a query to the database via input data from the client to server?

A. SQL injection attack

B. Cross-site scripting attack

C. Malware attack

D. Man-in-the-Middle

Question 178: Which software development methodology emphasizes short development cycles, dividing projects into simple tasks, and frequent customer feedback?

A. Kanban

B. LEAN

C. Extreme programming

D. SCRUM

Question 179: What term describes an incident where a security mechanism is bypassed or thwarted by a threat agent?

A. Login

B. Frontdoor

C. Breach

D. Virus

Question 180: What network devices are responsible for transmitting data over a frame relay and maintaining virtual circuits for customers?

A. Access Point Device

B. Bridging Router Device

C. Data Circuit-Terminating Equipment

D. Gateway Hub

Question 181: What type of device generates passwords that users must carry with them, representing a "something you have" (Type 2) authentication factor?

A. 2FR Device

B. MMFA Device

C. Passphrase Device

D. Token Device

Question 182: What two types of attacks are VoIP call managers and VoIP phones most susceptible to?

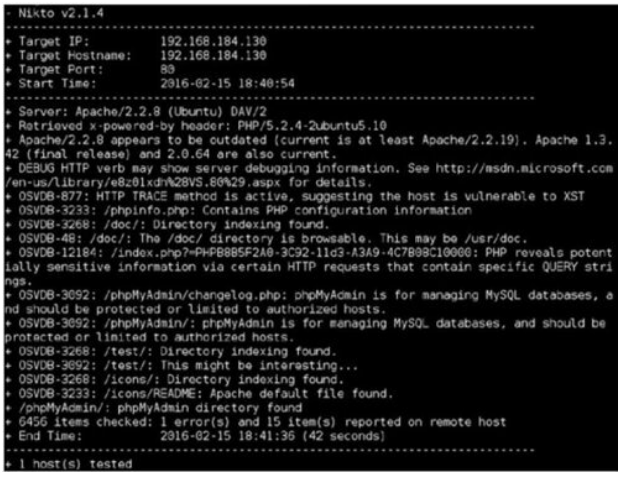
A. DoS and malware

B. Host OS attacks and buffer overflows

C. DoS and host OS attacks

D. Worms and Trojans

Question 183: During a web application vulnerability scan, why does Nikto identify directory indexing as an issue?



A. It may allow for XDRF

B. It lists files in a directory

C. Directory indexing is off by default, potentially indicating compromise

D. Directory indexing can result in a denial of service attack

Question 184: When an organization decides not to take action against a small risk because the cost of implementing controls is not justified, what risk management strategy are they employing?

A. Risk mitigation

B. Risk transference

C. Risk acceptance

D. Risk avoidance

Question 185: What is the term for a portion of a message containing data and the destination address, typically located at the network layer?

A. Pad

B. Pack

C. Pocket

D. Packet

Question 186: Which logical operation, represented by the ¬ symbol, reverses the value of an input variable and operates on only one variable at a time?

A. LIST

B. NOT

C. DIM

D. SEQ

Question 187: How often should an organization conduct Business Continuity Plan refresher training for individuals with specific business continuity roles?

A. Weekly

B. Semi-annually

C. Monthly

D. Annually

Question 188: What U.S. law was specifically created to address computer crimes that cross state boundaries without infringing on states' rights?

A. Border State Computer Fraud Act

B. Interstate Computer Crimes Act

C. Computer Fraud and Abuse Act

D. Federal Electronic Criminal Act

Question 189: What password security technique involves adding a username to a password before hashing the combined string of characters?

A. Scrabling

B. Spoofing

C. Jacking

D. Salting

Question 190: What security principle ensures that authorized subjects have timely and uninterrupted access to objects?

A. Connectivity

B. Availability

C. Accessibility

D. Granted Access

Question 191: What type of identification card technology is shown in the image, featuring a black strip across the card?

A. Magnetic stripe card

B. Phase two card

C. Proximity card

D. Smart card

Question 192: What term describes a type of web program that users download to their own computer for execution instead of using server-side resources?

A. Local Deployment

B. Active Content

C. Dynamic Programming

D. User-side Application

Question 193: To comply with the California Online Privacy Protection Act, what must a New York-based commercial web service that collects personal information from California residents do?

A. Encrypt all personal data received

B. Provide notice and choice for website users

C. Comply with the EU DPD

D. Have a conspicuously posted privacy policy on the site

Question 194: What type of attack uses third-party web resources to run scripts in the victim's web browser or scriptable application by injecting malicious JavaScript into a website's database?

A. SQL injection attack

B. Drive-by attack

C. Cross-site scripting attack

D. Denial-of-service

Question 195: Gertrude Yorkes utilizes a span port to monitor traffic to her production website and employs a monitoring tool to identify performance issues in real-time. What type of monitoring is she conducting?

A. Passive monitoring

B. Signature based monitoring

C. Active monitoring

D. Synthetic monitoring

Question 196: What is the default subnet mask for a Class B network?

A. 255.0.0.0

B. 255.255.0.0

C. 255.254.0.0

D. 255.255.255.0

Question 197: What type of governmental grant bestows upon an invention's creator the exclusive right to make, use, and sell that invention for a set period?

A. Patent

B. Copyright

C. Trademark

D. Permit

Question 198

In the context of Information Systems Security, what computational system is designed to perform numerous calculations simultaneously, often going beyond basic multi-

processing capabilities and dividing large tasks into smaller elements for parallel computation?

A) Realtime Data Structures

B) AI Computing

C) Near-Quantum Data Processing

D) Parallel Data Systems

Question 199

What term describes an intelligent code object that performs actions on behalf of a user, typically taking initial instructions and then carrying on its activity unattended for a predetermined period or until certain conditions are met?

A) Parasite

B) Agent

C) Android

D) Symbiont

Question 200

According to the OSI model, what format does the Data Link Layer employ to structure messages received from higher layers in the stack?

A) A frame

B) A segment

C) A datastream

D) A datagram

Question 201

In a biometric authentication system for high-security building access control, what does the point where False Acceptance Rate (FAR) and False Rejection Rate (FRR) intersect represent?

A) The CER

B) The FAR point

C) The CFR

D) The FRR crossover

Question 202

When conducting a STRIDE threat assessment, which categories best describe an issue allowing transactions to be altered between a web browser and its application server?

A) Tampering and Repudiation

B) Tampering and Information disclosure

C) Spoofing and Tampering

D) Information Disclosure and Elevation of Privilege

Question 203

What protocol is utilized to transmit webpage elements from a web server to web browsers, typically over TCP/UDP port 80?

A) Intranet Protocol

B) Python Protocol

C) Hypertext Transfer Protocol over Secure Sockets Layer

D) Hypertext Transfer Protocol

Question 204

What type of smart lock employs a credential reader, an electromagnet, and a door-closed sensor?

A) Computerized Permission Limiters (CPLs)

B) Electronic Access Controls (EACs)

C) Mortise Lock Cylinder & Thumbturns (MLCTs)

D) Yale Electric Tumblers (YETs)

Question 205

What term describes malicious code that infects a system and remains inactive until triggered by specific conditions?

A) Logic Bomb

B) Ransomware Code

C) Trojan Horse

D) Malware Code

Question 206

What addressing scheme uses a value stored in a CPU register as the base location, then adds a supplied value to compute the memory location for retrieving an operand?

A) SaltBase Addressing

B) Core+Value Addressing

C) Base+Offset Addressing

D) Base+Salt Addressing

Question 207

Which scoring system incorporates metrics such as attack vector, complexity, exploit maturity, and required user interaction?

A) CVE

B) NVD

C) CVSS

D) CAN

Question 208

What term describes the maximum duration a business function can be non-operational without causing irreversible damage to the organization?

A) Maximum Tolerable Downtime (MTD)

B) Maximum Liquidity Threshold (MLT)

C) Maximum Breakpoint

D) Maximum Business Chokepoint (MBC)

Question 209

What is the process of dividing a database into smaller sections or individual databases called?

A) Data Shadowing

B) Data Dissecting

C) Database Partitioning

D) Database Sectoring

Question 210

When using cryptography for secure communication, what security goal do digital signatures primarily enforce?

A) Nonrepudiation

B) Secrecy

C) Availability

D) Confidentiality

Question 211

Which type of virus alters the system boot process to redirect the BIOS to load malware before the operating system?

A) Polymorphic

B) MBR

C) File infector

D) Service injection

Question 212

What kind of attack is characterized by repeated login attempts with slight variations in the password?

```
Jan 31 11:39:12 ip-10-0-0-2 sshd[29092]: Invalid user
admin from remotehost passwd=aaaaaaaa

Jan 31 11:39:20 ip-10-0-0-2 sshd[29098]: Invalid user
admin from remotehost passwd=aaaaaaab

Jan 31 11:39:23 ip-10-0-0-2 sshd[29100]: Invalid user
admin from remotehost passwd=aaaaaaac

Jan 31 11:39:31 ip-10-0-0-2 sshd[29106]: Invalid user
admin from remotehost passwd=aaaaaaad

Jan 31 20:40:53 ip-10-0-0-254 sshd[30520]: Invalid
user admin from remotehost passwd=aaaaaaae
```

A) A Pasta Hash Attack

B) A Brute Force Attack

C) A Man-in-the-Middle Attack

D) A Dictionary Attack

Question 213

When selecting a disaster recovery facility that balances recovery time and cost, what type of site should be chosen?

A) Cold site

B) Hot site

C) Warm site

D) Red site

Question 214

What type of policy outlines acceptable behaviors and activities while defining consequences for violations?

A) Advisory Policy

B) Legal Policy

C) Guideline Policy

D) Mandate Policy

Question 215

When sending a message, what cryptography goal ensures that unauthorized parties cannot read the contents during transmission?

A) Confidentiality

B) Authentication

C) Integrity

D) Nonrepudiation

Question 216

Which law is least likely to apply to a federal government agency working closely with the Defense Department on classified matters?

A) FISMA

B) HAS

C) CFAA

D) HIPAA

Question 217

What authentication method allows users to provide credentials once during a computer session and not be asked again when accessing other resources?

A) True SSO

B) Session-based SSO

C) Enrollment-based SSO

D) Kerberos-based SSO

Question 218

In a Mandatory Access Control environment where security domains are isolated and unrelated, what is this type of setup called?

A) Classified Access Control Element

B) Access Control Categorization

C) Insulated Query Platform

D) Compartmentalized MAC Environment

Question 219

What type of coaxial cable, often used to connect systems to backbone trunks, has a maximum span of 185 meters and throughput of 10 Mbps?

A) 10BaseT

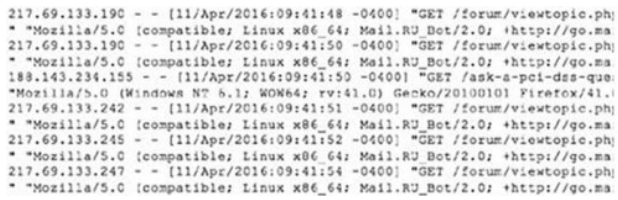
B) 10/185Base2

C) 10Base2

D) 10.0Base2

Question 220

What type of log primarily contains HTTP requests and GET commands?



A) Application log

B) Firewall log

C) System log

D) Changelog

Question 221

What kind of attack involves sending a packet with identical source and destination IP addresses?

A) Fraggle

B) Smurf

C) Land

D) Teardrop

Question 222

What database model combines records and fields in a logical tree structure where each field can have multiple or

no children but only a single parent?

A) Object Based Data Model

B) Record Based Data Model

C) Hierarchical Data Model

D) Holacratic Data Model

Question 223

What type of testing would be most appropriate for validating support across multiple web browsers for a web application?

A) White box testing

B) Fuzzing

C) Interface testing

D) Regression testing

Question 224

What is Microsoft's component object model technology used in web applications called?

A) OAuth

B) SSO

C) ActiveX

D) SAML

Question 225

What policy allows employees to connect their personal devices to an organization's network while maintaining organizational ownership of data stored on those devices?

A) CYOD

B) SSID

C) BYOD

D) BYOB

Question 226

What term describes the number of binary digits in a value such as a key, block size, or hash?

A) Boolean Attribute

B) Byte Magnitude

C) Bit Size

D) Root Weight

Question 227

Which class of fire extinguisher is most effective against liquid-based fires?

A) Class A

B) Class B

C) Class D

D) Class C

Question 228

What process is used to verify a dial-up user's connection from a preauthorized phone number while avoiding spoofing?

A) Callback

B) CHAP

C) PPP

D) Caller ID

Question 229

What open SSO standard, maintained by its namesake foundation, can be used in conjunction with OAuth or independently?

A) Apereo CAS

B) OpenID

C) ActiveX

D) Persona

Question 230

What is the primary advantage of Decentralized Access Control?

A) It provides control of access to people closer to resources.

B) It provides more granular control of access.

C) It is less expensive.

D) It provides better redundancy.

Question 231

What cloud computing concept provides a computing platform and software solution stack as a virtual or cloud-based service?

A) Platform as a Service (PaaS)

B) Infrastructure as a Service (IaaS)

C) Software as a Service (SaaS)

D) Content Distribution as a Service (CDaaS)

Question 232

What is the process of reconfiguring a system to have the IP address of a trusted system in order to gain access to external resources called?

A) DDoS Attacks

B) IP Spoofing

C) Web-App Attacks

D) Phishing Attacks

Question 233

Which technology provides a functional interface allowing developers to interact with systems without knowing

implementation details?

A) Object model

B) Source code

C) Data dictionary

D) API

Question 234

For a multinational non-profit with small offices in developing countries and poor internet connectivity, what type of access control design is most suitable?

A) Rule-Based Access Control

B) Decentralized Access Control

C) Centralized Access Control

D) Mandatory Access Control

Question 235

In an access control matrix, what column specifies the level of access each subject has over an object?

A) Role

B) User Allocation

C) Access Control List

D) Permissions

Question 236

What term describes a malicious user intent on attacking a person or system?

A) Shark

B) Cracker

C) Wolf

D) Olive

Question 237

What type of attack involves a malicious user positioning themselves between a client and server, interrupting the session, and taking it over while impersonating the client?

A) Spoofing Attack

B) Man-in-the-Middle Attack

C) Eavesdropping Attack

D) Hijack Attack

Question 238

What is a simple three-position shifting mono-alphabetic substitution cipher called?

A) Mudd Cipher

B) Caesar Cipher

C) Hiawatha Cipher

D) Napoleon Cipher

Question 239

What is a software simulation of a computer within which a process executes, with its own memory address space and controlled communication between instances?

A) Virtual Machine

B) Quantum Mirroring

C) Quantum Computing

D) Virtual Reality

Question 240

In transaction processing, what does the "I" in ACID stand for?

A) Irrevocable

B) Irremediable

C) Isolation

D) Identifiable

Question 241

What approach to application control blocks certain prohibited packages while allowing the installation of other software on systems?

A) Whitelist

B) Antivirus

C) Blacklist

D) Heuristic

Question 242

What term describes the situation when someone is forced to perform an action under threat?

A) Knife-point hacking

B) Antisocial engineering

C) Duress

D) Distress

Question 243

What type of Intrusion Detection System is installed on a single computer and can monitor activities on that specific machine?

A) Isolated Detective System

B) Cyber-Defined IDS

C) Stand-Alone Detection System

D) Host-Based IDS

Question 244

When calculating the Annualized Loss Expectancy (ALE) for a potential disaster, what formula is used?

A) ALE = Single Loss Expectancy x Annualized Rate of Occurrence

B) ALE = Total Asset Value x Probability of Occurrence

C) ALE = Cost of Countermeasure x Frequency of Threat

D) ALE = Impact of Loss x Likelihood of Event

Question 245

What is the protocol used to transmit webpage elements from a web server to web browsers over port 80 called?

A) File Transfer Protocol (FTP)

B) Simple Mail Transfer Protocol (SMTP)

C) Hypertext Transfer Protocol (HTTP)

D) Secure Shell (SSH)

Correct Answers & Explanations

Question 1

D) 0.002 (Correct Answer)

Explanation: The facility is located in a 200-year flood plain, meaning the probability of a flood occurring in any given year is 1/200 = 0.005. However, the question asks for the yearly probability, which is half of this value: 0.005/2 = 0.002 or 0.2%. This calculation accounts for the average occurrence of a flood over the 200-year period.

Question 2

B) Richard's public key (Correct Answer)

Explanation: In asymmetric encryption, the sender uses the recipient's public key to encrypt the message. Only the recipient's corresponding private key can decrypt it. Therefore, Sanil should use Richard's public key to encrypt the message, ensuring that only Richard can read it with his private key.

Question 3

D) Integrity Verification (Correct Answer)

Explanation: Data Diddling Attacks involve making unauthorized changes to data. Integrity Verification is the most effective measure against this type of attack as it ensures that data has not been altered or tampered with. This can be achieved through checksums, hashing, or digital signatures, which would detect any unauthorized modifications to the data.

Question 4

A) Session Hijacking (Correct Answer)

Explanation: Session Hijacking is precisely the attack described in the question. It involves an attacker intercepting a legitimate user's session, taking control of it, and then impersonating the authorized user. This allows the attacker to assume the identity of the authorized user and potentially gain unauthorized access to resources.

Question 5

D) Root (Correct Answer)

Explanation: In most operating systems, particularly Unix-like systems, the "root" account is the superuser account with the highest level of administrative access. It has unrestricted access to all commands and files on the system, making it the most powerful and potentially dangerous account if misused.

Question 6

B) Custodian (Correct Answer)

Explanation: A custodian in information security is responsible for the day-to-day management of information assets. This includes classifying and labeling objects, ensuring proper storage, and implementing protection measures. Custodians play a crucial role in maintaining the

security and integrity of an organization's information resources.

Question 7

B) RAID 5 (Correct Answer)

Explanation: RAID 5 is commonly referred to as disk striping with parity. It distributes data and parity information across all drives in the array, providing improved performance and fault tolerance. This configuration allows the system to continue operating even if one drive fails, making it a popular choice for balancing performance and data protection.

Question 8

C) Span-based (Correct Answer)

Explanation: Active monitoring, also known as span-based monitoring, involves creating a copy of network traffic and sending it to a monitoring tool for analysis. This approach allows for real-time analysis of network traffic without interfering with the actual data flow, making it an effective method for network security and performance monitoring.

Question 9

A) A Captive Portal (Correct Answer)

Explanation: A Captive Portal is the ideal solution for Charles Xavier's coffee shop. It allows customers to connect to the Wi-Fi network without pre-configured user IDs while still collecting useful information. When customers attempt to access the internet, they are redirected to a web page where they can enter contact information or agree to terms of service before gaining access.

Question 10

D) Attack (Correct Answer)

Explanation: An attack in information security is defined as the exploitation of a vulnerability by a threat agent. This

encompasses any deliberate attempt to compromise the confidentiality, integrity, or availability of a system or network by taking advantage of known or unknown weaknesses.

Question 11

A) Government Information Security Reform Act of 2000 (Correct Answer)

Explanation: The Government Information Security Reform Act (GISRA) of 2000 is the legislation that amended the US Code to implement additional information security policies and procedures. It aimed to improve federal information security by requiring agencies to conduct annual IT security reviews and report the results to the Office of Management and Budget (OMB).

Question 12

A) False Rejection Rate (FRR) (Correct Answer)

Explanation: The False Rejection Rate (FRR) is the error that occurs when a biometric device is overly sensitive and fails to authenticate a valid subject. This type of error, also known as a Type I error, can be frustrating for legitimate users and may impact the efficiency of biometric systems if set too high.

Question 13

B) Awareness (Correct Answer)

Explanation: Surveys, interviews, and audits are methods commonly used to measure an organization's security awareness. These tools help assess how well employees understand and adhere to security policies, procedures, and best practices. Measuring awareness is crucial for identifying gaps in knowledge and improving an organization's overall security posture.

Question 14

B) Whois (Correct Answer)

Explanation: Whois is the most appropriate tool for the information gathering phase of a penetration test. It provides valuable information about domain registrations, including contact details, name servers, and registration dates. This information is crucial for reconnaissance and helps penetration testers understand the target's online presence and infrastructure.

Question 15

C) Network (Correct Answer)

Explanation: In the OSI Model, the Network layer (Layer 3) is responsible for determining the physical path that data will take. This layer handles logical addressing, routing, and path determination, ensuring that data packets are sent from the source to the destination across potentially multiple networks.

Question 16

C) Accreditation (Correct Answer)

Explanation: Accreditation is the formal declaration by the Designated Approving Authority (DAA) that an IT system is approved to operate in a particular security mode. This process involves a comprehensive evaluation of the system's security controls, risks, and safeguards to ensure it meets the required security standards and can operate at an acceptable level of risk.

Question 17

D) 384 bits (Correct Answer)

Explanation: The Advanced Encryption Standard (AES) supports key lengths of 128, 192, and 256 bits. 384 bits is not a valid key length for AES. This standardization ensures compatibility and security across different implementations of the AES algorithm.

Question 18

C) Interface testing (Correct Answer)

Explanation: Interface testing is used to ensure that separately developed software modules properly exchange data. This type of testing focuses on verifying the communication between different components or modules of a system, ensuring that data is correctly passed and interpreted across module boundaries.

Question 19

D) Authentication (Correct Answer)

Explanation: The process of comparing a user's entered password to a hashed value stored in a database is called authentication. This security measure verifies the identity of a user by checking if the provided credentials match the stored information, allowing access only to authorized individuals.

Question 20

D) 2 (Correct Answer)

Explanation: RAID 1, also known as disk mirroring, requires a minimum of two physical disks. In this configuration, data is written identically to both disks, creating a mirrored set. This provides fault tolerance and improved read performance, as the system can read from either disk.

Question 21

A) Incident (Correct Answer)

Explanation: An incident in information security refers to any event that negatively impacts the confidentiality, integrity, or availability of an organization's assets. This can include data breaches, system failures, malware infections, or any other occurrence that compromises the security of information systems or data.

Question 22

B) Network Access Control (NAC) (Correct Answer)

Explanation: Network Access Control (NAC) is the concept described in the question. It involves controlling access to a network environment through strict adherence to and enforcement of security policies. NAC aims to prevent zero-day attacks, enforce security compliance, and use identities for access control, enhancing overall network security.

Question 23

D) Fully Qualified Domain Name (FQDN) (Correct Answer)

Explanation: A Fully Qualified Domain Name (FQDN) is the complete, human-readable name of a system or resource associated with an IP address. It consists of a hostname, a registered domain name, and a Top Level Domain (TLD). FQDNs provide a unique, hierarchical naming structure for identifying and locating resources on the internet.

Question 24

B) Zero Day (Correct Answer)

Explanation: A Zero Day attack exploits previously unknown vulnerabilities in software or systems. These attacks are particularly dangerous because there are no patches or effective defensive mechanisms available at the time of exploitation. The term "zero day" refers to the fact that developers have had zero days to address and patch the vulnerability.

Question 25

C) Foreign key (Correct Answer)

Explanation: To enforce referential integrity in a database, Kabuki needs to create a foreign key. Foreign keys establish relationships between tables by referencing the primary key of another table. This ensures that data remains consistent across related tables and prevents orphaned records, which

is crucial for maintaining the integrity of classified information in a multi-level security database.

Question 26

A) Symmetric Key (Correct Answer)

Explanation: A symmetric key algorithm uses a single shared secret key for both encryption and decryption. All parties involved in the communication must have access to this key, which is used to both encrypt the plaintext and decrypt the ciphertext. This method is faster than asymmetric encryption but requires secure key distribution.

Question 27

A) Spear Phishing (Correct Answer)

Explanation: Spear phishing is a targeted form of phishing attack aimed at specific individuals, organizations, or businesses. Unlike general phishing attempts, spear phishing emails are customized to appear more credible to the target, often using personal information or posing as a trusted entity to increase the likelihood of success.

Question 28

B) L2TP (Correct Answer)

Explanation: Layer 2 Tunneling Protocol (L2TP) is designed to support non-IP protocols natively. It operates at the data link layer (Layer 2) of the OSI model, allowing it to encapsulate various types of network traffic, including non-IP protocols. This makes L2TP a versatile choice for organizations needing to transmit diverse types of data over their VPN.

Question 29

A) Evidence (Correct Answer)

Explanation: The listed items (Direct, Circumstantial, Primary, Secondary, and Documentary) are all types of evidence. In legal and investigative contexts, these

categories help classify different forms of proof used to support or refute claims. Each type of evidence has its own characteristics and weight in establishing facts or drawing conclusions.

Question 30

D) External auditors (Correct Answer)

Explanation: External auditors are best suited to evaluate and report on the effectiveness of administrative controls to a third party. They provide an independent, objective assessment of an organization's controls, free from internal biases or conflicts of interest. Their reports carry more credibility with third parties due to their independence and professional standards.

Question 31

A) nessus (Correct Answer)

Explanation: Nessus is a comprehensive vulnerability scanner that can identify a wide range of security issues in a targeted system. It performs thorough scans to detect vulnerabilities, misconfigurations, and potential security risks. While nmap is useful for network discovery and port scanning, Nessus provides more in-depth vulnerability assessment capabilities.

Question 32

A) AES (Correct Answer)

Explanation: AES (Advanced Encryption Standard) is not a mode of operation for the Data Encryption Standard (DES). AES is a separate encryption algorithm that replaced DES. The other options (CFB, OFB, CBC) are valid modes of operation for block ciphers like DES, used to enhance security and handle data that doesn't align with the block size.

Question 33

A) Routers (Correct Answer)

Explanation: RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol) are all routing protocols associated with routers. These protocols are used by routers to exchange routing information and determine the best paths for data to travel across networks, playing a crucial role in internet and large network infrastructures.

Question 34

B) An open relay (Correct Answer)

Explanation: An SMTP server that does not authenticate senders before accepting and relaying email is known as an open relay. This configuration poses a significant security risk as it allows anyone to send emails through the server, potentially leading to spam distribution and other malicious activities. Open relays are often exploited by spammers and should be secured to prevent abuse.

Question 35

A) Audit trails (Correct Answer)

Explanation: Audit trails are records created by logging information about events and occurrences in a system. These trails provide a chronological record of activities, helping to track user actions, system changes, and potential security incidents. Audit trails are crucial for maintaining accountability, detecting unauthorized activities, and conducting forensic analysis in case of security breaches.

Question 36

B) Java (Correct Answer)

Explanation: Java is a platform-independent programming language developed by Sun Microsystems (now owned by Oracle). It's designed to run on any platform that supports the Java Virtual Machine (JVM), adhering to the "write once,

run anywhere" principle. Java's platform independence has made it popular for developing cross-platform applications and enterprise software.

Question 37

B) Encrypt all traffic to ensure confidentiality (Correct Answer)

Explanation: To protect sensitive data transmitted over cellular networks, Lenny's company should encrypt all traffic. While cellular networks have some built-in security, they can still be vulnerable to interception. Encrypting all traffic ensures that even if data is intercepted, it remains confidential and unreadable to unauthorized parties, providing an additional layer of security for sensitive corporate information.

Question 38

A) De-encapsulation (Correct Answer)

Explanation: De-encapsulation is the process of removing headers (and sometimes trailers) from data as it moves up the OSI model layers. When the session layer removes the header from data sent by the transport layer, it's performing de-encapsulation. This process allows each layer to access and process the relevant information before passing the data to the next higher layer.

Question 39

C) Private Cloud (Correct Answer)

Explanation: A private cloud is a cloud deployment model that uses cloud-based assets exclusively for a single organization. It allows organizations to create and host their own cloud infrastructure, providing greater control over security, privacy, and customization. Private clouds can be hosted on-premises or by a third-party provider, but are dedicated to a single organization's use.

Question 40

C) White-Box Testing (Correct Answer)

Explanation: White-Box Testing is a software testing technique that examines the internal structure, design, and coding of software. Testers have full knowledge of the source code and internal workings of the application. This method allows for thorough testing of all code paths, improving design, usability, and security by identifying issues that may not be apparent from external behavior alone.

Question 41

C) Knowledgebase (Correct Answer)

Explanation: A knowledgebase is a key component of an expert system that contains the rules and information known by the system. It codifies the knowledge of human experts into a series of "if/then" statements or other logical structures. This allows the expert system to make decisions or provide recommendations based on the encoded expert knowledge, simulating human expertise in specific domains.

Question 42

B) Bluejacking (Correct Answer)

Explanation: Bluejacking is the practice of sending unsolicited messages over Bluetooth to Bluetooth-enabled devices. This typically involves sending text messages, contact information, or images to nearby devices without the recipient's consent. While often used for pranks or marketing, bluejacking can be a security concern as it may be used to distribute malicious content or gather information about nearby devices.

Question 43

D) Social Engineering (Correct Answer)

Explanation: Social Engineering is a technique used by attackers to manipulate individuals into divulging confidential information or performing actions that compromise security. It relies on psychological manipulation rather than technical hacking methods. Social engineers exploit human trust and behavior to gain unauthorized access to systems or information, often by posing as legitimate entities or creating scenarios that prompt victims to act against security protocols.

Question 44

B) One (Correct Answer)

Explanation: In a RAID 5 configuration with three discs, one disc can fail without data loss. RAID 5 uses distributed parity, allowing the system to reconstruct data from a failed drive using the parity information stored across the remaining drives. However, if more than one drive fails simultaneously, data loss will occur. This configuration provides a balance between performance, storage efficiency, and fault tolerance.

Question 45

A) Millennium Digital Copyright Act (Correct Answer)

Explanation: The correct name is actually the Digital Millennium Copyright Act (DMCA). This law, enacted in 1998, addresses copyright issues in the digital age. It prohibits circumvention of technological measures used to protect copyrighted works and limits the liability of internet service providers for copyright infringement by their users. The DMCA has significant implications for digital content, online platforms, and copyright enforcement in the internet era.

Question 46

B) PII (Correct Answer)

Explanation: PII stands for Personally Identifiable Information. This term refers to any data that can be used to

identify a specific individual, either alone or in combination with other information. Examples include names, Social Security numbers, birthdates, and places of birth. Protecting PII is crucial for maintaining privacy and preventing identity theft, and is often subject to strict regulatory requirements.

Question 47

D) Parallel Site (Correct Answer)

Explanation: A parallel site, also known as a hot site, is a fully equipped alternate facility capable of taking over operations immediately in case of a disaster. It has the necessary hardware, software, and network connections to handle the organization's full processing load, along with appropriate electrical and environmental support systems. Parallel sites provide the fastest recovery time but are also the most expensive disaster recovery option.

Question 48

D) Content-Distribution Network (CDN) (Correct Answer)

Explanation: A Content Distribution Network (CDN) is a geographically distributed network of servers that work together to provide fast delivery of Internet content. By storing copies of content across multiple locations, CDNs reduce latency and improve performance by serving content from servers closest to the end-user. This approach enhances website speed, reduces bandwidth costs, and improves availability and redundancy of content delivery.

Question 49

B) Connect to his company's encrypted VPN service (Correct Answer)

Explanation: When attending a hacker conference, connecting to the company's encrypted VPN service is the safest option for Loki. This ensures that all data transmitted between his device and the company network is encrypted, protecting it from potential interception or manipulation.

Using a VPN adds an extra layer of security, especially in potentially hostile environments like hacker conferences where network attacks are more likely to occur.

Question 50

A) Misuse case diagrams (Correct Answer)

Explanation: Misuse case diagrams are specifically designed for application threat modeling. They incorporate malicious users (also called misactors) and use descriptions like "mitigates" and "threatens" to show the relationships between threats and security measures. This makes them ideal for visualizing potential security risks and their countermeasures in software applications.

Question 51

D) Conduct random sampling (Correct Answer)

Explanation: Random sampling is the most effective and unbiased method for evaluating account management practices. It ensures a representative sample of accounts across the entire population, reducing the risk of overlooking potential issues. This approach is more reliable than focusing on a specific time frame, having administrators generate samples (which could introduce bias), or auditing all accounts (which is often impractical and time-consuming).

Question 52

A) Agile software development (Correct Answer)

Explanation: Agile software development is characterized by its focus on customer needs and rapid, iterative development of new functionality. It emphasizes flexibility, continuous improvement, and frequent delivery of working software. Agile methodologies, such as Scrum or Extreme Programming, prioritize customer collaboration and responsiveness to change over following a rigid plan.

Question 53

D) Tuple (Correct Answer)

Explanation: In database terminology, a tuple refers to a single row or record in a relational database table. It represents a complete set of related data elements that describe a single entity or instance. The term "tuple" is synonymous with "record" or "row" in this context, making it the correct answer for describing a record or role in a database.

Question 54

C) RAID 5 (Correct Answer)

Explanation: RAID 5 is commonly referred to as disk striping with parity. This RAID level distributes data and parity information across all drives in the array. It provides a good balance of performance, fault tolerance, and storage efficiency. RAID 5 requires a minimum of three drives and can withstand the failure of one drive without data loss.

Question 55

B) Data Dictionary (Correct Answer)

Explanation: A Data Dictionary is a centralized repository of information about data elements within an organization's information systems. It stores metadata about data elements, including their definitions, relationships, usage, sources, and formats. This comprehensive resource helps maintain data consistency, facilitates system integration, and supports data governance initiatives.

Question 56

D) Hypervisor (Correct Answer)

Explanation: In a virtualized computing environment, the hypervisor is responsible for maintaining separation between guest machines. Also known as a Virtual Machine Monitor (VMM), the hypervisor creates and manages virtual

machines, allocating resources and ensuring isolation between different guest operating systems running on the same physical hardware.

Question 57

B) Beta Testing (Correct Answer)

Explanation: Beta Testing is characterized by being performed by non-employee clients or end users in a real-time environment without a lab setup. It focuses on reliability, security, and robustness of the software. Beta testing occurs in the later stages of software development and aims to gather feedback from actual users in real-world conditions before the final release.

Question 58

A) Change Management (Correct Answer)

Explanation: Change Management is the process that helps prevent unintended outages by requiring personnel to submit requests for configuration changes. These requests are then reviewed, approved, tested, implemented, and documented. This systematic approach ensures that changes are carefully controlled, reducing the risk of disruptions and maintaining system stability.

Question 59

B) Gantt Chart (Correct Answer)

Explanation: A Gantt Chart is a type of bar chart that displays the interrelationships between projects and schedules over time. It provides a graphical illustration to help plan, coordinate, and track specific tasks in a project. Gantt charts show task dependencies, start and end dates, and overall project timelines, making them invaluable tools for project management and scheduling.

Question 60

D) Crystal box (Correct Answer)

Explanation: Crystal box testing, also known as white box or clear box testing, provides testers with full knowledge of the system's internal workings, including source code, architecture, and configuration. This approach maximizes effectiveness by allowing testers to thoroughly examine all aspects of the system, identifying potential vulnerabilities and weaknesses that might not be apparent in other testing methods.

Question 61

D) Form-filling SSO (Correct Answer)

Explanation: Form-filling Single Sign-On (SSO) is a method that allows for secure storage of information typically filled into documents through template completion. This SSO technique automatically populates form fields with stored user credentials, reducing the need for manual input and enhancing user convenience while maintaining security.

Question 62

A) Preventing exploitation of an unpatched laptop immediately after network connection (Correct Answer)

Explanation: A strict post-admission Network Access Control (NAC) policy cannot address the issue of preventing exploitation of an unpatched laptop immediately after network connection. Post-admission NAC focuses on monitoring and controlling access after a device has already joined the network. To prevent immediate exploitation of vulnerabilities, pre-admission checks and quarantine procedures would be necessary.

Question 63

D) Reverse Hash Matching (Correct Answer)

Explanation: Reverse Hash Matching is the process of attempting to discover the original message that has been hashed by generating potential messages, hashing them, and comparing their hash to the original. This technique,

also known as a "rainbow table attack" or "pre-image attack," is used to crack hashed passwords or recover original data from hash values.

Question 64

A) Masquerading (Correct Answer)

Explanation: Masquerading is an attack that uses stolen or falsified authentication credentials to bypass an authentication mechanism. In this type of attack, the attacker impersonates a legitimate user or system by presenting valid-looking credentials, gaining unauthorized access to protected resources or systems.

Question 65

C) SSH (Correct Answer)

Explanation: SSH (Secure Shell) is an end-to-end encryption technique that provides encrypted alternatives to common Internet applications such as FTP, Telnet, and rlogin. SSH creates a secure channel over an unsecured network, allowing for secure remote login, file transfer, and command execution. It offers strong authentication and encryption, making it a preferred choice for secure remote access and management.

Question 66

B) It has been functionally tested (Correct Answer)

Explanation: For a system assigned an EAL2 (Evaluation Assurance Level 2) under Common Criteria, the highest level of assurance that can be expected is that it has been functionally tested. EAL2 provides a low to moderate level of independently assured security, including independent testing of security functions and a review of the developer's vulnerability analysis.

Question 67

D) RADIUS (Correct Answer)

Explanation: RADIUS (Remote Authentication Dial-In User Service) is the recommended solution for deploying an authentication, authorization, and accounting server for wireless network services while avoiding proprietary technology. RADIUS is an open standard protocol widely supported by various vendors, making it ideal for interoperability and avoiding vendor lock-in.

Question 68

C) RAID (Correct Answer)

Explanation: RAID (Redundant Array of Independent Disks) is a method that involves storing duplicate data on two or more hard drives for purposes such as data backup, fault tolerance, improved throughput, increased storage functions, and enhanced performance. RAID combines multiple disk drive components into a logical unit for data redundancy and performance improvement.

Question 69

C) Fagan inspection (Correct Answer)

Explanation: Fagan inspection is a code review process characterized by a highly formalized approach involving planning, overview, preparation, inspection, rework, and follow-up steps. Developed by Michael Fagan at IBM, this method provides a structured and thorough approach to identifying defects in software artifacts, including code, design documents, and requirements specifications.

Question 70

C) Risk Tolerance (Correct Answer)

Explanation: Risk Tolerance describes an organization's ability to absorb losses associated with realized risks. It represents the level of risk that an organization is willing and able to accept in pursuit of its objectives. Risk tolerance helps guide decision-making processes and determines the

appropriate risk response strategies for different types of risks.

Question 71

A) Web defacement (Correct Answer)

Explanation: In this scenario, web defacement is considered the risk. The risk is the potential negative outcome or impact of a threat exploiting a vulnerability. Here, the unpatched web application is the vulnerability, the hacker using SQL injection is the threat, and the resulting web defacement is the risk or potential consequence of the threat exploiting the vulnerability.

Question 72

D) Clean Power (Correct Answer)

Explanation: Clean Power is the term used to describe non-fluctuating pure power. It refers to a stable, consistent electrical supply free from voltage spikes, sags, or other distortions. Clean power is essential for sensitive electronic equipment and can be achieved through various power conditioning and filtering technologies.

Question 73

A) Hardware Security Module (HSM) (Correct Answer)

Explanation: A Hardware Security Module (HSM) is a type of crypto processor used to manage and store digital encryption keys, accelerate crypto operations, support faster digital signatures, and improve authentication. HSMs provide a secure, tamper-resistant environment for performing cryptographic operations and protecting sensitive key material.

Question 74

D) Data Stream (Correct Answer)

Explanation: In the context of network protocols, a Data Stream describes data from an application sent into a

protocol stack, which becomes the initial payload of the top layer protocol. This continuous flow of data is processed and encapsulated by each layer of the protocol stack before being transmitted over the network.

Question 75

A) SCP (Correct Answer)

Explanation: SCP (Secure Copy Protocol) should be used instead of FTP when needing to transfer files from a PC to a remote server securely. SCP is built on top of SSH and provides encrypted file transfer capabilities, ensuring the confidentiality and integrity of data during transmission. Unlike FTP, which sends data in clear text, SCP offers a secure alternative for file transfers.

Question 76

D) Procedure (Correct Answer)

Explanation: A procedure provides a detailed, step-by-step description of the exact actions individuals must complete to perform a specific task or process. Unlike policies, standards, or guidelines, procedures offer precise instructions, ensuring consistency and reducing errors in task execution.

Question 77

A) XACML (Correct Answer)

Explanation: XACML (eXtensible Access Control Markup Language) is used to define access control policies within an XML format and commonly implements role-based access controls. It provides a standardized way to express and interpret access control rules, allowing for fine-grained, attribute-based access control across various systems and applications.

Question 78

A) REST (Correct Answer)

Explanation: REST (Representational State Transfer) describes a new way of communication between two systems at a given point in time, where one system is called a "Client" and the other a "Server". It is an architectural style for designing networked applications, emphasizing scalability, simplicity, and statelessness in client-server interactions.

Question 79

A) Processing (Correct Answer)

Explanation: During the processing phase of the electronic discovery process, an organization performs an initial filtering of gathered information to discard irrelevant data. This phase involves analyzing, categorizing, and reducing the volume of collected data to focus on potentially relevant information for the legal matter at hand.

Question 80

C) 2 (Correct Answer)

Explanation: The minimum number of cryptographic keys required to achieve strong security when using the 3DES (Triple Data Encryption Standard) algorithm is 2. While 3DES uses three rounds of encryption, it can be configured to use either two or three unique keys. The two-key variant (K1, K2, K1) provides adequate security for most applications.

Question 81

B) Detective (Correct Answer)

Explanation: Detective access control is designed to discover unwanted or unauthorized activity by providing information after an event has occurred. Unlike preventative controls that aim to stop incidents before they happen, detective controls focus on identifying and reporting security breaches, policy violations, or suspicious activities after they have taken place.

Question 82

A) Warm Site (Correct Answer)

Explanation: A warm site serves as a middle ground in disaster recovery, containing necessary equipment and data circuits for rapid establishment of operations but typically not housing copies of client data. It offers a balance between the minimal preparedness of a cold site and the full readiness of a hot site, allowing for quicker recovery than a cold site but at a lower cost than a hot site.

Question 83

A) Cross-Site Request Forgery (CSRF) (Correct Answer)

Explanation: Cross-Site Request Forgery (CSRF) is a type of web attack that exploits a trusted user to execute commands via their browser against a vulnerable server. It tricks the victim's browser into sending malicious requests to a website where the user is authenticated, potentially leading to unauthorized actions being performed on behalf of the victim.

Question 84

C) Release of a security patch (Correct Answer)

Explanation: The release of a security patch transforms a zero-day vulnerability into a less dangerous attack vector. A zero-day vulnerability is unknown to the software vendor and has no available fix. Once a patch is released, the vulnerability becomes known and can be mitigated, reducing its potential for exploitation and overall risk to systems.

Question 85

D) Decrypting (Correct Answer)

Explanation: Decrypting is the process of reversing a cryptographic algorithm that was used to encrypt a message. It involves using the appropriate key and

algorithm to convert encrypted ciphertext back into its original, readable plaintext form. Decryption is essential for accessing protected information by authorized parties.

Question 86

B) Biba Model (Correct Answer)

Explanation: The Biba Model, originally published in 1977, was the first to address integrity concerns in computer systems. It includes properties such as simple integrity, star integrity, and invocation. The model focuses on preventing unauthorized users from modifying data at higher integrity levels and preventing data from flowing from lower to higher integrity levels.

Question 87

C) Positive Pay (Correct Answer)

Explanation: Positive Pay is an automated cash-management service used to deter check fraud by matching the checks a company issues with those presented for payment. This system allows companies to send their bank a list of issued checks, which the bank then compares against checks presented for payment, helping to identify and prevent fraudulent transactions.

Question 88

C) Physically destroy the drive (Correct Answer)

Explanation: Physically destroying the drive is the most effective method to ensure data is not recoverable from a Solid State Drive (SSD). Due to the way SSDs store and manage data, traditional data wiping methods may not be fully effective. Physical destruction, such as shredding or crushing, ensures that the storage medium is rendered completely inoperable and unreadable.

Question 89

D) Port Scan (Correct Answer)

Explanation: A port scan is a type of software used by an intruder to probe active systems on a network and determine the public services running on each machine. It systematically checks a range of port numbers on a host to find open ports, which can reveal information about the services and potential vulnerabilities of the target system.

Question 90

A) Set up a one-way nontransitive trust (Correct Answer)

Explanation: To allow a partner organization's Active Directory forest to access resources in your domain forest without reciprocal access and preventing trust flow upward through the domain tree, a one-way nontransitive trust should be established. This type of trust allows access in one direction only and does not extend to other domains in the forest.

Question 91

D) Authorization (Correct Answer)

Explanation: Authorization is the process which ensures that a requested activity or object access is possible given the rights and privileges assigned to an authenticated identity. It determines what actions or resources a user, program, or device is allowed to access based on predefined permissions and security policies.

Question 92

C) Offboarding (Correct Answer)

Explanation: Offboarding describes the process of removing an employee's identity from the identity and access management system after they have left the organization. This comprehensive process includes revoking access rights, disabling accounts, and removing or archiving user data to ensure security and compliance when an employee departs.

Question 93

B) DREAD (Correct Answer)

Explanation: DREAD is a risk rating system designed to provide a flexible solution based on asking five main questions about each threat. The acronym stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. This model helps assess and prioritize security risks in software development and system design.

Question 94

B) Administrative (Correct Answer)

Explanation: When signs are placed reminding staff of security issues along with alarms for doors left open, administrative controls have been implemented. These are management-level controls that include policies, procedures, and guidelines aimed at influencing employee behavior and awareness to enhance security. They complement physical and technical controls in a comprehensive security strategy.

Question 95

B) Data Dictionary (Correct Answer)

Explanation: A Data Dictionary is a central repository of data elements and their relationships that stores critical information about data usage, relationships, sources, and formats. It serves as a comprehensive catalog of an organization's data assets, providing metadata and context to support data governance, system integration, and application development.

Question 96

D) Hypervisor (Correct Answer)

Explanation: In a virtualized computing environment, the hypervisor is responsible for enforcing separation between guest machines. Also known as a virtual machine monitor

(VMM), the hypervisor manages the allocation of physical resources to virtual machines and ensures isolation between different guest operating systems running on the same physical hardware.

Question 97

B) Beta Testing (Correct Answer)

Explanation: Beta Testing is characterized by being performed by non-employee clients or end users, typically in a real-time environment, focusing on reliability, security, and robustness. It occurs in the later stages of software development, allowing actual users to test the product in real-world conditions before its final release.

Question 98

A) Change Management (Correct Answer)

Explanation: Change Management is the process that helps prevent unintended outages by requiring personnel to submit requests for configuration changes, which are then reviewed, approved, tested, implemented, and documented. This systematic approach ensures that changes are carefully controlled and monitored, reducing the risk of disruptions to IT services.

Question 99

B) Gantt Chart (Correct Answer)

Explanation: A Gantt Chart displays the interrelationships between projects and schedules over time, providing a graphical illustration to help plan, coordinate, and track specific tasks in a project. It shows tasks, their durations, and dependencies on a timeline, making it an essential tool for project managers to visualize project schedules and progress.

Question 100

D) Bell-LaPadula (Correct Answer)

Explanation: The Bell-LaPadula model is a state machine model for computer security that enforces access control in government and military applications. It focuses on data confidentiality and controlled access to classified information. This model implements a "no read up, no write down" policy, which means that a subject at a given security level cannot read data at a higher security level (no read up) or write data to a lower security level (no write down).

Question 101

D) All of the above (Correct Answer)

Explanation: Man-in-the-middle (MITM) attacks involve an attacker secretly relaying and possibly altering the communication between two parties. Session hijacking, IP spoofing, and replay attacks are all techniques used in MITM attacks. Session hijacking involves taking over a valid user session, IP spoofing involves disguising the source of IP packets, and replay attacks involve retransmitting valid data transmissions. All these techniques can be used to intercept and manipulate communication between two parties.

Question 102

B) Distributed Control Systems (Correct Answer)

Explanation: Distributed Control Systems (DCS) are used in industrial settings to control production systems within the same geographic location. They distribute control of different components of the system to various control elements throughout the operation while maintaining centralized supervision and coordination. This allows for more efficient and flexible control of complex industrial processes.

Question 103

A) Activate the incident response team (Correct Answer)

Explanation: After detecting a potential security incident, the next immediate step should be to activate the incident

response team. This team is specifically trained to handle security incidents and will coordinate the response efforts. They will assess the situation, contain the incident, investigate its root cause, and guide the organization through the recovery process. Activating this team ensures a prompt and organized response to the security incident.

Question 104

C) RAID 0 (Correct Answer)

Explanation: RAID 0, also known as disk striping, is a RAID configuration that splits data evenly across two or more disks without parity information for redundancy. This technique improves performance by allowing multiple drives to read and write data simultaneously. However, it provides no fault tolerance, as the failure of any disk in the array results in complete data loss.

Question 105

A) Remote wipe (Correct Answer)

Explanation: Remote wipe is a security feature that allows an administrator or user to send a command to a mobile device to delete all data stored on the device. This feature is particularly useful in cases where a device is lost or stolen, as it helps prevent unauthorized access to sensitive information. Remote wipe can be triggered remotely through a mobile device management (MDM) system or through specific applications designed for this purpose.

Question 106

B) TCP (Correct Answer)

Explanation: Transmission Control Protocol (TCP) is a connection-oriented protocol that uses a three-way handshake to establish a reliable connection between two devices. It performs error checking to ensure data integrity and provides reliable, ordered, and error-checked delivery of data. TCP is designed to guarantee the delivery of data

packets in the same order they were sent, making it suitable for applications that require high reliability.

Question 107

D) Flash memory (Correct Answer)

Explanation: Flash memory is a type of non-volatile storage media that can be electronically erased and reprogrammed. It is organized into blocks or pages, which can be individually erased and rewritten. This characteristic makes flash memory ideal for use in solid-state drives (SSDs), USB flash drives, and memory cards. Unlike RAM, flash memory retains data even when power is removed, and unlike HDDs, it has no moving parts.

Question 108

A) PCI DSS (Correct Answer)

Explanation: The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. This standard is specific to the payment card industry and is mandated by card brands but administered by the Payment Card Industry Security Standards Council. PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.

Question 109

C) Redundant servers (Correct Answer)

Explanation: Redundant servers are backup server configurations designed to take over in case the primary server fails. This setup ensures business continuity and disaster recovery by providing a failover mechanism. Redundant servers can be configured in various ways, such as active-active (where both servers actively handle requests) or active-passive (where one server is on

standby). This redundancy helps minimize downtime and ensures that critical services remain available even in the event of hardware failure or other disasters.

Question 110

C) Change management (Correct Answer)

Explanation: Change management is a systematic approach to dealing with the transition or transformation of an organization's goals, processes, or technologies. In IT, it typically requires managerial approval before system modifications are implemented. This process ensures that changes are introduced in a controlled and coordinated manner, minimizing the risk of disruptions to IT services. Change management helps organizations balance the need for change with the potential risks and impacts on the business.

Question 111

A) Durability (Correct Answer)

Explanation: Durability is one of the four key properties of ACID (Atomicity, Consistency, Isolation, Durability) transactions in database systems. It ensures that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In other words, all completed transactions are recorded in non-volatile memory and are not undone by system failures. This property is crucial for maintaining data integrity and reliability in database systems.

Question 112

D) Preventive access control (Correct Answer)

Explanation: Preventive access control is a type of access control that aims to stop unauthorized activities before they occur. It works by implementing measures that prevent users from accessing resources or performing actions they are not authorized to do. Examples include user

authentication, encryption, and access control lists (ACLs). By proactively blocking unauthorized access attempts, preventive access control helps maintain the security and integrity of systems and data.

Question 113

A) Fiber Distributed Data Interface (FDDI) (Correct Answer)

Explanation: Fiber Distributed Data Interface (FDDI) was a standard for data transmission in local area networks that used fiber optic cable. It was based on token ring technology and employed a dual counter-rotating ring topology. This design provided redundancy: if one ring failed, the other could take over, ensuring continued network operation. FDDI was capable of transmitting data at speeds of 100 Mbps over distances up to 200 kilometers. While largely obsolete now, FDDI was an important technology in the evolution of high-speed networking.

Question 114

D) Everyone in the organization (Correct Answer)

Explanation: Initial business continuity plan training should be provided to everyone in the organization. This approach ensures that all employees understand their roles and responsibilities during a crisis or disruption. While certain individuals may have specific roles in executing the plan, everyone needs to be aware of the basic procedures, communication channels, and expectations during an emergency. This widespread understanding helps in faster and more effective implementation of the plan when needed.

Question 115

D) Fraggle (Correct Answer)

Explanation: A Fraggle attack is a type of denial-of-service (DoS) attack that is similar to a Smurf attack but uses User Datagram Protocol (UDP) packets instead of ICMP echo

requests. In a Fraggle attack, the attacker sends a large number of UDP echo packets to IP broadcast addresses, with the source IP spoofed to be the victim's address. This causes all hosts on the target network to send responses to the victim, overwhelming their system. The name "Fraggle" comes from a character in the TV show "Fraggle Rock," following the naming convention of the Smurf attack.

Question 116

C) Risk avoidance (Correct Answer)

Explanation: Risk avoidance is a risk management strategy that involves taking actions to eliminate a specific threat or risk entirely. This approach aims to prevent the risk from materializing by changing plans, altering business processes, or avoiding certain activities altogether. For example, a company might decide not to expand into a certain market due to high political instability, thereby avoiding the associated risks. While effective for high-impact risks, risk avoidance may also result in missed opportunities, so it should be applied judiciously.

Question 117

B) Assembly language (Correct Answer)

Explanation: Assembly language is a low-level programming language that provides a symbolic representation of machine code instructions. It serves as an intermediate step between high-level programming languages (like C++ or Java) and machine code (binary instructions directly executed by the CPU). Assembly language uses mnemonics to represent machine instructions and memory locations, making it more readable for humans than raw machine code. While still close to the hardware, it allows programmers more control over the system's resources compared to high-level languages.

Question 118

A) Corrective access control (Correct Answer)

Explanation: Corrective access control is a type of access control mechanism that aims to restore systems to a normal state after an unauthorized activity has occurred. Unlike preventive controls that try to stop incidents before they happen, corrective controls are reactive measures. They are designed to reverse the impact of a security incident, limit the extent of any damage, and facilitate a return to normal operations. Examples include system backups, redundant systems, and disaster recovery plans.

Question 119

D) InfoSec (Correct Answer)

Explanation: The Information Security (InfoSec) team or department is primarily responsible for an organization's information security. This team is dedicated to protecting the confidentiality, integrity, and availability of the organization's data and information systems. Their responsibilities typically include developing and implementing security policies, conducting risk assessments, managing security technologies, responding to incidents, and ensuring compliance with relevant regulations. While other departments like IT and senior management play important roles in supporting security efforts, the InfoSec team specializes in and leads these initiatives.

Question 120

C) Privilege creep (Correct Answer)

Explanation: Privilege creep is a security issue that occurs when an employee accumulates access rights beyond what is necessary for their current role, often as a result of changing positions within an organization over time. As employees move between different roles or departments, they may retain access permissions from previous positions,

even if these are no longer relevant to their current responsibilities. This gradual accumulation of unnecessary privileges can lead to security vulnerabilities, as it violates the principle of least privilege and increases the potential impact of a compromised account.

Question 121

B) Principle of least privilege (Correct Answer)

Explanation: The Principle of Least Privilege (PoLP) is a fundamental concept in information security that states users should be granted the minimum levels of access or permissions necessary to perform their job functions. This principle aims to limit the potential damage from accidents, errors, or malicious actions by restricting users' access rights to only what is absolutely necessary for their roles. By minimizing the attack surface and reducing the risk of privilege abuse, the principle of least privilege helps enhance overall system security.

Question 122

D) Dumpster diving (Correct Answer)

Explanation: Dumpster diving is a technique used by malicious actors to gather sensitive information by searching through an organization's discarded materials. This can include rifling through trash bins, recycling containers, or other disposal areas to find documents, electronic media, or other items that may contain valuable data. Organizations often underestimate the risk of carelessly discarded information, making dumpster diving a surprisingly effective method for gathering intelligence. To counter this threat, organizations should implement proper document destruction policies and raise awareness about the importance of securely disposing of sensitive materials.

Question 123

A) Stateful packet inspection firewall (Correct Answer)

Explanation: A stateful packet inspection (SPI) firewall, also known as a dynamic packet filtering firewall, is a network security system that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. Unlike static packet filtering, which makes decisions based solely on individual packets, SPI firewalls keep track of the state of network connections (such as TCP streams) traversing them. This allows the firewall to detect and prevent certain types of attacks that might elude a simple packet filter, providing a higher level of security.

Question 124

D) Fault tolerance (Correct Answer)

Explanation: Fault tolerance is the capability of a system to continue operating properly in the event of the failure of one or more of its components. This is achieved through redundancy in critical components and systems designed to automatically detect, isolate, and compensate for failures. Fault-tolerant systems aim to prevent system failures from causing data loss or system downtime. This capability is crucial in environments where continuous operation is essential, such as in financial systems, healthcare, and critical infrastructure.

Question 125

A) TKIP (Correct Answer)

Explanation: Temporal Key Integrity Protocol (TKIP) was a security protocol introduced as part of the Wi-Fi Protected Access (WPA) standard to address the vulnerabilities in the older Wired Equivalent Privacy (WEP) protocol. TKIP provided a way to wrap the WEP encryption system with stronger encryption and authentication methods. However, TKIP itself was later found to have weaknesses and was subsequently replaced by more robust security measures in WPA2, which uses the Advanced Encryption Standard (AES)

based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and 802.1x authentication.

Question 126

B) Directive Access Control (DAC) (Correct Answer)

Explanation: Directive Access Control (DAC) is an access control mechanism designed to guide or restrict subject actions to ensure compliance with security policies. Unlike other access control methods that focus on granting or denying access, DAC provides guidelines and restrictions on how subjects should interact with objects. It often involves implementing security policies, procedures, and best practices to direct user behavior and ensure that actions align with the organization's security objectives.

Question 127

D) Purge (Correct Answer)

Explanation: Degaussing falls under the "Purge" category of data removal techniques. Purging involves using advanced sanitization methods to render data recovery infeasible, even with sophisticated laboratory techniques. Degaussing is a process that uses strong magnetic fields to erase data from magnetic storage media, such as hard drives or tapes. This method is more thorough than simple data clearing and is considered a secure way to remove sensitive information from storage devices before disposal or reuse.

Question 128

C) Packet filter (Correct Answer)

Explanation: A packet filter firewall is the simplest type of firewall architecture that lacks the ability to track connection status across packets. It operates at the network layer of the OSI model and filters traffic based on predefined rules that examine packet headers. Unlike stateful inspection firewalls, packet filters make decisions on each

packet individually, without considering the context of previous packets or the overall connection state. This limitation makes packet filter firewalls less secure against certain types of attacks but also makes them faster and less resource-intensive.

Question 129

B) Maintaining the hypervisor (Correct Answer)

Explanation: In an Infrastructure as a Service (IaaS) cloud environment, the vendor is typically responsible for maintaining the hypervisor. The hypervisor, also known as a virtual machine monitor (VMM), is the software layer that enables multiple operating systems to share a single hardware host. It's a critical component of the virtualization infrastructure that the IaaS provider manages. The vendor ensures the hypervisor's security, performance, and updates, while customers are usually responsible for managing their virtual machines, including operating systems, applications, and data.

Question 130

C) Mandatory Access Control (MAC) (Correct Answer)

Explanation: Mandatory Access Control (MAC) is an access control mechanism that uses security labels to regulate subject access to objects. In a MAC system, every subject (user or process) and object (file, device, or resource) is assigned a security label. Access decisions are made by comparing these labels according to a set of rules defined by a central authority. MAC is often used in high-security environments, such as government and military systems, where strict control over information flow is crucial. It enforces access control policies that cannot be altered by individual users, ensuring a high level of security and compliance with organizational policies.

Question 131

B) Data remanence (Correct Answer)

Explanation: Data remanence refers to the residual representation of data that remains even after attempts have been made to remove or erase it. This phenomenon occurs because standard data deletion methods often only remove references to the data in the file system, leaving the actual data intact on the storage medium. Data remanence can pose a significant security risk, as sensitive information may be recoverable from disposed or repurposed storage devices. To address this issue, organizations often employ specialized data sanitization techniques, such as multiple overwrites or physical destruction of storage media.

Question 132

A) Contamination (Correct Answer)

Explanation: In information security, contamination refers to the mixing of data with different classification levels or need-to-know requirements. This situation can occur when data of a higher security classification is introduced into a system or environment cleared for lower-level data, or when data is improperly combined across different security domains. Contamination poses a significant security risk as it can lead to unauthorized access to sensitive information. To prevent contamination, organizations implement strict data handling procedures, access controls, and data segregation policies.

Question 133

A) SLE (Correct Answer)

Explanation: SLE stands for Single Loss Expectancy, which represents the monetary value associated with a single occurrence of a specific risk to an asset. It is calculated by multiplying the value of the asset by the exposure factor (the percentage of the asset's value that would be lost in a single incident). SLE is a crucial metric in risk assessment

and management, helping organizations understand the potential financial impact of various risks and prioritize their risk mitigation efforts accordingly.

Question 134

D) Salt (Correct Answer)

Explanation: In cryptography, a salt is a random string of data that is added to a password before it is hashed. The purpose of salting is to defend against dictionary attacks and rainbow table attacks. By adding unique, random data to each password before hashing, salting ensures that even if two users have the same password, their hashed values will be different. This technique significantly increases the complexity and computational cost of cracking passwords, enhancing overall security. Salts are typically stored alongside the hashed password in a database.

Question 135

B) WAN (Correct Answer)

Explanation: A Wide Area Network (WAN) typically uses dedicated leased lines to connect geographically distant components. WANs are designed to span large geographic areas, connecting multiple Local Area Networks (LANs) or other network types across cities, countries, or even continents. The use of leased lines in WANs provides several advantages, including guaranteed bandwidth, improved security, and better performance compared to public internet connections. Common WAN technologies include MPLS (Multiprotocol Label Switching), SD-WAN (Software-Defined WAN), and various types of VPN (Virtual Private Network) solutions.

Question 136

B) Bot (Correct Answer)

Explanation: A bot, short for robot, is an automated program designed to perform specific tasks on the internet without

human intervention. In the context of web crawling, a bot (also known as a web crawler or spider) is programmed to systematically browse websites, retrieve content, and process data for various purposes. These can include search engine indexing, data mining, or monitoring websites for updates. Bots can be beneficial (like search engine crawlers) or malicious (like those used in DDoS attacks or spam operations). Their behavior is governed by algorithms and can be customized for specific tasks or websites.

Question 137

D) Attack surface identification (Correct Answer)

Explanation: Attack surface identification is a crucial part of the security review process that involves analyzing input parameters and other potential entry points to identify vulnerabilities in a system. This process aims to map out all the ways an attacker could potentially interact with the system, including user inputs, APIs, network protocols, and file uploads. By thoroughly examining these potential attack vectors, security professionals can identify weaknesses, prioritize security efforts, and implement appropriate controls to reduce the overall attack surface of the system.

Question 138

C) Internet Service Providers (Correct Answer)

Explanation: Under the Digital Millennium Copyright Act (DMCA), Internet Service Providers (ISPs) can receive safe harbor protection. This provision shields ISPs from copyright infringement liability for simply transmitting information over the internet. To qualify for this protection, ISPs must meet certain conditions, including having a policy for terminating repeat infringers and complying with standard technical measures. The safe harbor provision is crucial for ISPs, as it allows them to operate without the constant threat of copyright lawsuits while still providing a

mechanism for copyright holders to address infringement concerns.

Question 139

D) Annual Rate of Occurrence (ARO) (Correct Answer)

Explanation: The Annual Rate of Occurrence (ARO) is a risk assessment metric that describes the estimated frequency of a specific threat or risk occurring within a year. It is typically expressed as a number or a probability. For example, an ARO of 0.1 suggests that the risk is expected to occur once every ten years on average. ARO is a crucial component in calculating the Annualized Loss Expectancy (ALE) and helps organizations prioritize their risk management efforts by focusing on threats that are more likely to occur frequently.

Question 140

D) Cloud storage (Correct Answer)

Explanation: Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is managed, maintained, and operated by a cloud storage service provider. Organizations can use cloud storage to store and access their data without having to manage the storage infrastructure themselves. This service offers several advantages, including scalability, accessibility from anywhere with an internet connection, and often improved reliability through data replication across multiple locations. Common examples of cloud storage services include Amazon S3, Google Cloud Storage, and Microsoft Azure Blob Storage.

Question 141

A) Rings 0 and 3 (Correct Answer)

Explanation: The Meltdown bug, announced in early 2018, primarily affected CPU protection rings 0 and 3. In the x86 architecture, Ring 0 is the most privileged level where the

kernel operates, while Ring 3 is the least privileged level where user applications run. Meltdown exploited a vulnerability in the way modern processors handle speculative execution, allowing processes running in Ring 3 to potentially read kernel memory in Ring 0. This breach of the fundamental isolation between user applications and the operating system posed a significant security risk, potentially exposing sensitive data and requiring substantial changes in operating system design to mitigate.

Question 142

B) Public-key cryptography (Correct Answer)

Explanation: Public-key cryptography, also known as asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This method allows users to communicate securely without having to share a secret key. The public key is used for encryption or signature verification, while the private key is used for decryption or signature generation. This system forms the basis for secure communication protocols like HTTPS, digital signatures, and secure key exchange methods used in various internet security applications.

Question 143

B) Electromagnetic pulse (Correct Answer)

Explanation: An Electromagnetic Pulse (EMP) is a short burst of electromagnetic energy that can disrupt, degrade, or destroy electronic equipment. EMPs can be caused by natural phenomena like solar flares or man-made sources such as nuclear explosions or specialized EMP weapons. The intense electromagnetic fields generated by an EMP can induce currents in electrical conductors, potentially damaging or destroying electronic devices. EMPs are a significant concern in both military and civilian contexts due

to the potential for widespread disruption of critical infrastructure and communication systems.

Question 144

A) Distributed Reflective Denial of Service (DRDoS) (Correct Answer)

Explanation: A Distributed Reflective Denial of Service (DRDoS) attack is a type of DoS attack that exploits Internet services by sending numerous packets with a spoofed source address. In this attack, the attacker sends requests to a large number of servers (reflectors) using the spoofed IP address of the intended victim. These servers then send their responses to the victim, overwhelming their system. This technique amplifies the attack's power and makes it harder to trace back to the original attacker. DRDoS attacks often exploit protocols like DNS, NTP, or SSDP, which can produce large responses to small queries, further increasing the attack's effectiveness.

Question 145

A) Espionage (Correct Answer)

Explanation: Espionage refers to the practice of obtaining secret or confidential information through clandestine means, typically for military, political, or commercial advantage. In the context of information security, corporate or industrial espionage involves the malicious gathering of confidential information from businesses or organizations for disclosure to competitors or other interested parties. This can include stealing trade secrets, proprietary technologies, strategic plans, or customer data. Espionage can be conducted through various methods, including insider threats, social engineering, hacking, or physical infiltration, and poses a significant threat to an organization's competitive advantage and overall security.

Question 146

C) Guest OS (Correct Answer)

Explanation: In virtualization, a Guest OS refers to an operating system that runs within a virtual machine (VM). The guest OS operates as if it were installed on a standalone hardware platform, unaware that it's running in a virtualized environment. This allows multiple operating systems to run concurrently on a single physical machine, each within its own VM. The guest OS is managed by the hypervisor, which allocates physical resources to it as needed. This architecture enables efficient use of hardware resources, improved isolation between applications, and greater flexibility in managing and deploying software environments.

Question 147

C) United States Code (Correct Answer)

Explanation: The United States Code (U.S.C.) is the official compilation and codification of the general and permanent federal statutes of the United States. It contains the text of federal criminal and civil laws, organized by subject matter into 53 titles. The U.S. Code is published every six years by the Office of the Law Revision Counsel of the U.S. House of Representatives, with annual cumulative supplements. It serves as the authoritative source for federal legislation and is widely used by legal professionals, government officials, and the public to access and understand federal laws.

Question 148

A) Excessive privilege (Correct Answer)

Explanation: Excessive privilege is a security issue that arises when a user is granted more access rights or permissions than necessary for their job tasks. This violates the principle of least privilege, which states that users should only have the minimum level of access required to perform their duties. Excessive privileges increase the

potential impact of a compromised account, as an attacker gaining control of such an account would have broader access to sensitive systems and data. This situation can occur due to improper access management, lack of regular access reviews, or inadequate role-based access control implementation. Addressing excessive privileges is crucial for maintaining a strong security posture and minimizing potential damage from insider threats or external attacks.

Question 149

D) Header (Correct Answer)

Explanation: A header is information added by a protocol to the beginning of a payload received from a higher-layer protocol. It contains essential data for processing the payload, such as source and destination addresses, protocol type, and sequence numbers. Headers are crucial for proper data transmission and interpretation in network communication.

Question 150

A) Passive monitoring (Correct Answer)

Explanation: Passive monitoring involves observing network traffic without interfering with it. Using a span port to observe traffic to a production website and identify performance issues in real-time is a classic example of passive monitoring. This method allows for continuous observation without affecting the network's normal operation.

Question 151

A) Examine and test (Correct Answer)

Explanation: According to NIST SP800-53A guidelines, examining and testing are the primary assessment methods associated with mechanisms and activities in federal information systems. Examining involves the inspection of policies, procedures, and documentation, while testing

involves the hands-on verification of security controls' functionality and effectiveness.

Question 152

D) Qualitative (Correct Answer)

Explanation: Qualitative risk evaluation uses non-numerical methods to assess risks, often employing tools like risk matrices or heat maps. These tools typically use color-coding or descriptive terms (e.g., low, medium, high) to represent risk levels, which is characteristic of qualitative analysis.

Question 153

B) Proximity Reader (Correct Answer)

Explanation: A proximity reader is a device that detects authorized personnel and grants physical entry into a facility using field-powered technology. It works by detecting a proximity card or token when it's brought near the reader, allowing for contactless access control.

Question 154

B) Account lockout (Correct Answer)

Explanation: Account lockout is a security measure that disables a user account after a specified number of failed login attempts. This is a common programmatic control in password policies, designed to prevent brute-force attacks by temporarily or permanently locking the account after multiple unsuccessful login attempts.

Question 155

C) Trusted Foundry (Correct Answer)

Explanation: The Trusted Foundry program is a U.S. Department of Defense initiative that ensures the integrity of electronic components used in critical systems. It provides a trusted supply chain for microelectronics, helping

to prevent the introduction of compromised or counterfeit components into sensitive government systems.

Question 156

B) Iterative Development (Correct Answer)

Explanation: Iterative development is a model where a large project is divided into smaller parts, with each part undergoing multiple iterations of the waterfall model. This approach allows for incremental development, feedback incorporation, and risk mitigation throughout the project lifecycle.

Question 157

D) Frame Relay (Correct Answer)

Explanation: Frame Relay is a networking technology that uses packet-switching to create virtual circuits for customers on a shared connection medium. It provides a cost-effective way to transmit data over wide area networks by allowing multiple logical connections over a single physical link.

Question 158

C) Ensure appropriate security controls are in place to protect the data (Correct Answer)

Explanation: As a system owner in a healthcare organization, the primary responsibility regarding data is to ensure appropriate security controls are in place to protect it. This includes implementing measures to safeguard data confidentiality, integrity, and availability, in compliance with regulations like HIPAA.

Question 159

B) 255.255.0.0 (Correct Answer)

Explanation: The default subnet mask for a Class B network is 255.255.0.0. This mask allows for 16 bits of network address and 16 bits of host address, providing a balance

between the number of networks and hosts per network in the Class B address space.

Question 160

B) Ping (Correct Answer)

Explanation: Ping is a network utility used to test the accessibility of a specific IP address when troubleshooting a connection. It sends ICMP echo request packets to the target host and waits for ICMP echo reply packets, providing information about network latency and packet loss.

Question 161

D) Data Manipulation Language (DML) (Correct Answer)

Explanation: Data Manipulation Language (DML) is the subset of SQL that allows users to interact with data within the database schema. It includes commands like SELECT, INSERT, UPDATE, and DELETE, which are used to retrieve, add, modify, and remove data from database tables.

Question 162

C) Asset Value (Correct Answer)

Explanation: Asset Value is the term that describes the monetary value assigned to an asset based on actual costs and non-monetary expenses. It includes the original purchase price, any improvements made, and other factors that contribute to the asset's overall worth to the organization.

Question 163

A) Patent (Correct Answer)

Explanation: A patent is a type of governmental grant that gives an inventor the exclusive right to make, use, and sell their invention for a set period. It provides legal protection for new and non-obvious inventions, encouraging innovation by allowing inventors to profit from their creations.

Question 164

A) It has been formally verified, designed, and tested (Correct Answer)

Explanation: EAL7 is the highest evaluation assurance level under the Common Criteria. A system assigned to EAL7 has undergone the most rigorous evaluation, including formal verification of the design and comprehensive testing. This level provides the highest assurance of security in the evaluated system.

Question 165

A) Personally Identifiable Information (PII) (Correct Answer)

Explanation: Personally Identifiable Information (PII) refers to any data item that can be easily traced back to its person of origin or concern. This includes information such as names, social security numbers, addresses, and other data that can be used to identify an individual, either alone or in combination with other information.

Question 166

B) Best Evidence Rule (Correct Answer)

Explanation: The Best Evidence Rule requires that the most reliable form of evidence be presented in court. For digital evidence like system logs, this often means system administrators must testify about how they gathered and preserved the logs to establish their authenticity and reliability as evidence.

Question 167

D) 4 (Correct Answer)

Explanation: With incremental backups, you need to restore the last full backup and all subsequent incremental backups up to the point of failure. Assuming a full backup on Sunday and incremental backups on Monday, Tuesday, and Wednesday, you would need to restore 4 backups: Sunday's

full backup and the incremental backups from Monday, Tuesday, and Wednesday.

Question 168

B) Internet Message Access Protocol (IMAP) (Correct Answer)

Explanation: The Internet Message Access Protocol (IMAP) is used to transfer email messages from an email server to an email client. IMAP allows users to access their emails from multiple devices while keeping the messages stored on the server, providing more flexibility than other protocols like POP3.

Question 169

C) SaaS (Correct Answer)

Explanation: In the Software as a Service (SaaS) model, the customer has the least responsibility for security. The service provider manages the entire stack, including the application, runtime, middleware, operating system, virtualization, servers, storage, and networking. The customer is only responsible for data and access management.

Question 170

B) Bind Variable (Correct Answer)

Explanation: A bind variable in SQL is a placeholder used for literal values such as numbers or string characters. It allows for the creation of parameterized queries, improving performance and security by preventing SQL injection attacks and enabling query plan reuse.

Question 171

B) Install a repeater or a concentrator before 100 metres (Correct Answer)

Explanation: The maximum cable length for 1000Base-T Ethernet is 100 meters. To span over 150 meters, you need to install a repeater or concentrator before the 100-meter

mark. This device will amplify and retransmit the signal, allowing it to cover the extended distance while maintaining signal integrity.

Question 172

D) Circumstantial Evidence (Correct Answer)

Explanation: Circumstantial evidence is based on inference rather than personal knowledge or observation. It requires the drawing of conclusions from related facts or circumstances. While not as direct as eyewitness testimony, circumstantial evidence can be powerful when multiple pieces point to the same conclusion.

Question 173

C) Block inbound ICMP traffic (Correct Answer)

Explanation: To prevent a Smurf attack, which exploits ICMP echo requests (ping) to flood a target network, the most effective firewall configuration is to block inbound ICMP traffic. This prevents the attacker from using broadcast ICMP packets to amplify their attack, effectively mitigating the Smurf attack vector.

Question 174

A) Asynchronous Dynamic Password Token (Correct Answer)

Explanation: An Asynchronous Dynamic Password Token generates one-time passwords after a user enters a PIN, with the PIN provided by a server as a challenge. This type of token doesn't need to be synchronized with the authentication server, making it more flexible but potentially less secure than synchronous tokens.

Question 175

D) Documenting the decision-making process (Correct Answer)

Explanation: When a company chooses to accept a risk, such as earthquakes in North Dakota, the action that aligns

with this strategy is documenting the decision-making process. This involves recording the reasons for accepting the risk, the potential impacts, and any mitigating factors considered. It's a crucial step in risk management and ensures transparency in decision-making.

Question 176

C) Electronic Discovery (Correct Answer)

Explanation: Electronic Discovery, often abbreviated as e-discovery, is the legal process where parties involved in litigation must preserve and share all relevant evidence, including both paper and electronic records. This process ensures that all potentially relevant information is available for the legal proceedings, regardless of its format.

Question 177

A) SQL injection attack (Correct Answer)

Explanation: SQL injection is a type of attack that has become prevalent in database-driven websites. In this attack, a malicious actor executes unauthorized SQL queries by manipulating input data sent from the client to the server. This can allow attackers to read, modify, or delete database contents, potentially compromising the entire system.

Question 178

C) Extreme programming (Correct Answer)

Explanation: Extreme Programming (XP) is a software development methodology that emphasizes short development cycles, dividing projects into simple tasks, and frequent customer feedback. It focuses on improving software quality and responsiveness to changing customer requirements through practices like pair programming, extensive code review, and continuous integration.

Question 179

C) Breach (Correct Answer)

Explanation: A breach is an incident where a security mechanism is bypassed or thwarted by a threat agent. It represents a successful attempt to circumvent security controls, potentially resulting in unauthorized access, data theft, or system compromise. Breaches are serious security incidents that often require immediate response and mitigation.

Question 180

C) Data Circuit-Terminating Equipment (Correct Answer)

Explanation: Data Circuit-Terminating Equipment (DCE) is responsible for transmitting data over a frame relay network and maintaining virtual circuits for customers. DCEs act as the interface between the customer's equipment and the frame relay network, handling tasks such as packet switching, addressing, and error control.

Question 181

D) Token Device (Correct Answer)

Explanation: A token device is a type of authentication factor that generates passwords that users must carry with them, representing a "something you have" (Type 2) authentication factor. These devices produce one-time passwords or codes that change frequently, adding an extra layer of security to the authentication process.

Question 182

C) DoS and host OS attacks (Correct Answer)

Explanation: VoIP call managers and VoIP phones are most susceptible to Denial of Service (DoS) and host operating system (OS) attacks. DoS attacks can disrupt voice services, while host OS attacks exploit vulnerabilities in the underlying operating system of VoIP devices, potentially leading to unauthorized access or control.

Question 183

B) It lists files in a directory (Correct Answer)

Explanation: Nikto identifies directory indexing as an issue during web application vulnerability scans because it allows the listing of files in a directory. This can potentially expose sensitive information or provide attackers with valuable information about the website's structure and contents, which could be used to plan further attacks.

Question 184

C) Risk acceptance (Correct Answer)

Explanation: When an organization decides not to take action against a small risk because the cost of implementing controls is not justified, they are employing a risk acceptance strategy. This approach involves acknowledging the existence of a risk but choosing not to mitigate it, typically because the potential impact is low and the cost of mitigation outweighs the potential benefits.

Question 185

D) Packet (Correct Answer)

Explanation: A packet is a portion of a message containing data and the destination address, typically located at the network layer. Packets are the fundamental units of data transmission in computer networks, allowing for efficient routing and delivery of information across complex network infrastructures.

Question 186

B) NOT (Correct Answer)

Explanation: The NOT logical operation, represented by the ¬ symbol, reverses the value of an input variable and operates on only one variable at a time. In boolean algebra, it changes TRUE to FALSE and vice versa, serving as a fundamental operation in logic circuits and programming.

Question 187

D) Annually (Correct Answer)

Explanation: Organizations should conduct Business Continuity Plan refresher training for individuals with specific business continuity roles annually. This frequency ensures that all relevant personnel remain familiar with their roles and responsibilities in the event of a disruption, while also allowing for updates to the plan based on changes in the business environment or lessons learned from exercises.

Question 188

C) Computer Fraud and Abuse Act (Correct Answer)

Explanation: The Computer Fraud and Abuse Act (CFAA) was specifically created to address computer crimes that cross state boundaries without infringing on states' rights. This federal law criminalizes various computer-related activities, including unauthorized access to protected computers and the spread of malicious code, providing a legal framework for prosecuting cybercrime at the federal level.

Question 189

D) Salting (Correct Answer)

Explanation: Salting is a password security technique that involves adding additional data (such as a username) to a password before hashing the combined string of characters. This practice enhances security by making it more difficult for attackers to use precomputed hash tables (rainbow tables) to crack passwords, as each salt creates a unique hash even for identical passwords.

Question 190

B) Availability (Correct Answer)

Explanation: Availability is the security principle that ensures authorized subjects have timely and uninterrupted access to objects. It is one of the three core principles of

information security (along with confidentiality and integrity) and focuses on maintaining system uptime, preventing service disruptions, and ensuring that resources are accessible when needed by authorized users.

Question 191

A) Magnetic stripe card (Correct Answer)

Explanation: The image shows a magnetic stripe card, which features a black strip across the card containing encoded information. This technology is commonly used in credit cards, hotel key cards, and employee ID badges. The magnetic stripe stores data that can be read by swiping the card through a card reader.

Question 192

B) Active Content (Correct Answer)

Explanation: Active Content refers to a type of web program that users download to their own computer for execution instead of using server-side resources. This includes technologies like Java applets, ActiveX controls, and JavaScript, which can enhance web functionality but also pose potential security risks if not properly managed.

Question 193

D) Have a conspicuously posted privacy policy on the site (Correct Answer)

Explanation: To comply with the California Online Privacy Protection Act, a New York-based commercial web service that collects personal information from California residents must have a conspicuously posted privacy policy on the site. This policy should clearly state what personal information is collected, how it is used, and with whom it may be shared, ensuring transparency for California users.

Question 194

C) Cross-site scripting attack (Correct Answer)

Explanation: A cross-site scripting (XSS) attack uses third-party web resources to run malicious scripts in the victim's web browser or scriptable application. This is often achieved by injecting malicious JavaScript into a website's database, which is then served to unsuspecting users. XSS attacks can lead to theft of sensitive information, session hijacking, or defacement of websites.

Question 195

A) Passive monitoring (Correct Answer)

Explanation: Gertrude Yorkes is conducting passive monitoring. By utilizing a span port to observe traffic to her production website and employing a monitoring tool to identify performance issues in real-time, she is observing network activity without interfering with it. This non-intrusive approach allows for continuous monitoring of network performance and behavior without affecting the normal operation of the system.

Question 196

B) 255.255.0.0 (Correct Answer)

Explanation: The default subnet mask for a Class B network is 255.255.0.0. This subnet mask allocates 16 bits for the network portion and 16 bits for the host portion of the IP address, allowing for a large number of hosts within each network while still providing a significant number of possible networks.

Question 197

A) Patent (Correct Answer)

Explanation: A patent is a type of governmental grant that bestows upon an invention's creator the exclusive right to make, use, and sell that invention for a set period. Patents encourage innovation by providing inventors with a temporary monopoly on their creations, allowing them to

profit from their inventions while also requiring public disclosure of the invention's details.

Question 198

D) Parallel Data Systems (Correct Answer)

Explanation: Parallel Data Systems are designed to perform numerous calculations simultaneously, dividing large tasks into smaller elements for parallel computation. This goes beyond basic multi-processing capabilities, allowing for efficient handling of complex computational tasks in Information Systems Security.

Question 199

B) Agent (Correct Answer)

Explanation: An agent is an intelligent code object that performs actions on behalf of a user. It takes initial instructions and then carries on its activity unattended for a predetermined period or until certain conditions are met, making it an autonomous entity in information systems.

Question 200

A) A frame (Correct Answer)

Explanation: In the OSI model, the Data Link Layer employs frames to structure messages received from higher layers. Frames encapsulate data with addressing and error-checking information, facilitating reliable point-to-point communication between network nodes.

Question 201

A) The CER (Correct Answer)

Explanation: The point where False Acceptance Rate (FAR) and False Rejection Rate (FRR) intersect is called the Crossover Error Rate (CER) or Equal Error Rate (EER). This point represents the optimal balance between security and usability in a biometric authentication system.

Question 202

B) Tampering and Information disclosure (Correct Answer)

Explanation: In a STRIDE threat assessment, altering transactions between a web browser and its application server falls under Tampering (modifying data) and Information Disclosure (unauthorized access to information). These categories best describe the vulnerability allowing such alterations.

Question 203

D) Hypertext Transfer Protocol (Correct Answer)

Explanation: HTTP (Hypertext Transfer Protocol) is the standard protocol used to transmit webpage elements from a web server to web browsers. It typically operates over TCP/UDP port 80 and is fundamental to data communication on the World Wide Web.

Question 204

B) Electronic Access Controls (EACs) (Correct Answer)

Explanation: Electronic Access Controls (EACs) are smart locks that employ a credential reader, an electromagnet, and a door-closed sensor. These components work together to provide secure, controlled access to restricted areas in buildings.

Question 205

A) Logic Bomb (Correct Answer)

Explanation: A Logic Bomb is malicious code that infects a system and remains inactive until triggered by specific conditions. It's designed to execute when certain criteria are met, potentially causing significant damage to the infected system.

Question 206

C) Base+Offset Addressing (Correct Answer)

Explanation: Base+Offset Addressing is an addressing scheme that uses a value stored in a CPU register as the base location, then adds a supplied value (offset) to compute the memory location for retrieving an operand. This method allows for efficient memory access in computer systems.

Question 207

C) CVSS (Correct Answer)

Explanation: The Common Vulnerability Scoring System (CVSS) incorporates metrics such as attack vector, complexity, exploit maturity, and required user interaction to assess the severity of vulnerabilities. It provides a standardized method for rating IT vulnerabilities and security risks.

Question 208

A) Maximum Tolerable Downtime (MTD) (Correct Answer)

Explanation: Maximum Tolerable Downtime (MTD) is the maximum duration a business function can be non-operational without causing irreversible damage to the organization. It's a crucial metric in business continuity and disaster recovery planning.

Question 209

C) Database Partitioning (Correct Answer)

Explanation: Database Partitioning is the process of dividing a database into smaller sections or individual databases. This technique improves database performance, manageability, and availability by distributing data across multiple storage units.

Question 210

A) Nonrepudiation (Correct Answer)

Explanation: Digital signatures primarily enforce nonrepudiation in secure communication. They ensure that

the sender cannot deny having sent the message, providing proof of origin and integrity of the communication.

Question 211

B) MBR (Correct Answer)

Explanation: An MBR (Master Boot Record) virus alters the system boot process to redirect the BIOS to load malware before the operating system. This type of virus infects the critical boot sector, allowing it to gain control of the system early in the boot process.

Question 212

B) A Brute Force Attack (Correct Answer)

Explanation: A Brute Force Attack is characterized by repeated login attempts with slight variations in the password. This method systematically checks all possible passwords until the correct one is found, often using automated tools to try numerous combinations.

Question 213

C) Warm site (Correct Answer)

Explanation: A warm site balances recovery time and cost in disaster recovery. It provides some equipment and data connections but may not have full data replication, offering a middle ground between the more expensive hot site and the less prepared cold site.

Question 214

D) Mandate Policy (Correct Answer)

Explanation: A Mandate Policy outlines acceptable behaviors and activities while defining consequences for violations. It is a formal, enforceable policy that sets clear expectations and penalties for non-compliance within an organization.

Question 215

A) Confidentiality (Correct Answer)

Explanation: Confidentiality is the cryptography goal that ensures unauthorized parties cannot read the contents of a message during transmission. It protects the privacy of the communication, typically through encryption methods.

Question 216

D) HIPAA (Correct Answer)

Explanation: HIPAA (Health Insurance Portability and Accountability Act) is least likely to apply to a federal government agency working on classified matters with the Defense Department. HIPAA primarily regulates healthcare information privacy, which is not typically the focus of defense-related agencies.

Question 217

A) True SSO (Correct Answer)

Explanation: True Single Sign-On (SSO) allows users to provide credentials once during a computer session and not be asked again when accessing other resources. This method enhances user convenience and security by reducing the number of times a user must enter their credentials.

Question 218

D) Compartmentalized MAC Environment (Correct Answer)

Explanation: A Compartmentalized MAC (Mandatory Access Control) Environment refers to a setup where security domains are isolated and unrelated. This strict separation ensures that information and resources in one compartment cannot interact with or influence those in another, enhancing overall security.

Question 219

C) 10Base2 (Correct Answer)

Explanation: 10Base2 is a type of coaxial cable used to connect systems to backbone trunks. It has a maximum

span of 185 meters and a throughput of 10 Mbps, making it suitable for certain network configurations where longer cable runs are needed.

Question 220

A) Application log (Correct Answer)

Explanation: An Application log primarily contains HTTP requests and GET commands. These logs record interactions between users and web applications, providing valuable information for troubleshooting, security analysis, and performance monitoring.

Question 221

C) Land (Correct Answer)

Explanation: A Land attack involves sending a packet with identical source and destination IP addresses. This type of attack can cause some systems to crash or become unresponsive, exploiting vulnerabilities in TCP/IP stack implementations.

Question 222

C) Hierarchical Data Model (Correct Answer)

Explanation: The Hierarchical Data Model combines records and fields in a logical tree structure where each field can have multiple or no children but only a single parent. This model organizes data in a parent-child relationship, suitable for representing naturally hierarchical information.

Question 223

C) Interface testing (Correct Answer)

Explanation: Interface testing would be most appropriate for validating support across multiple web browsers for a web application. This type of testing focuses on how the application's user interface behaves and appears across different browsers, ensuring consistent functionality and appearance.

Question 224

C) ActiveX (Correct Answer)

Explanation: ActiveX is Microsoft's component object model technology used in web applications. It allows for the creation of reusable software components that can be embedded in web pages, providing enhanced functionality and interactivity in Internet Explorer browsers.

Question 225

C) BYOD (Correct Answer)

Explanation: BYOD (Bring Your Own Device) is a policy that allows employees to connect their personal devices to an organization's network while maintaining organizational ownership of data stored on those devices. This approach can increase productivity and employee satisfaction while presenting unique security challenges.

Question 226

C) Bit Size (Correct Answer)

Explanation: Bit Size refers to the number of binary digits (bits) in a value such as a key, block size, or hash. It's a crucial measure in cryptography and computer science, determining the complexity and security level of various algorithms and data structures.

Question 227

B) Class B (Correct Answer)

Explanation: Class B fire extinguishers are specifically designed for liquid-based fires, including flammable liquids like gasoline, oil, and grease. They work by smothering the fire and interrupting the chemical reaction causing the fire, making them most effective against liquid fuel fires.

Question 228

A) Callback (Correct Answer)

Explanation: Callback is a security process used to verify dial-up users' connections from preauthorized phone numbers. After initial contact, the system terminates the connection and calls back the user at a predetermined number, preventing unauthorized access through spoofed phone numbers.

Question 229

B) OpenID (Correct Answer)

Explanation: OpenID is an open standard for decentralized authentication, maintained by the OpenID Foundation. It can be used independently or in conjunction with OAuth for authentication and authorization. OpenID allows users to be authenticated by cooperating sites using a third-party service.

Question 230

A) It provides control of access to people closer to resources. (Correct Answer)

Explanation: Decentralized Access Control's primary advantage is that it places control closer to the resources being protected. This allows for more responsive and context-aware access decisions, as those managing access are more familiar with local needs and conditions.

Question 231

A) Platform as a Service (PaaS) (Correct Answer)

Explanation: Platform as a Service (PaaS) provides a computing platform and software solution stack as a virtual or cloud-based service. It offers developers a framework they can build upon to develop or customize applications, without the complexity of maintaining the underlying infrastructure.

Question 232

B) IP Spoofing (Correct Answer)

Explanation: IP Spoofing is the process of reconfiguring a system to have the IP address of a trusted system to gain access to external resources. This technique involves creating IP packets with a forged source IP address, deceiving the receiving system about the origin of the communication.

Question 233

D) API (Correct Answer)

Explanation: An API (Application Programming Interface) provides a functional interface allowing developers to interact with systems without knowing implementation details. It defines a set of protocols and tools for building software applications, enabling communication between different software components.

Question 234

B) Decentralized Access Control (Correct Answer)

Explanation: For a multinational non-profit with small offices in developing countries and poor internet connectivity, Decentralized Access Control is most suitable. This approach allows local offices to manage access independently, reducing reliance on potentially unreliable internet connections to a central authority.

Question 235

C) Access Control List (Correct Answer)

Explanation: In an access control matrix, the Access Control List (ACL) specifies the level of access each subject has over an object. It's a column that defines permissions for various users or groups, detailing what operations they can perform on the associated resource.

Question 236

B) Cracker (Correct Answer)

Explanation: A cracker is a term used to describe a malicious user intent on attacking a person or system. Unlike hackers, who may have benign or even beneficial intentions, crackers specifically aim to breach security measures for malicious purposes.

Question 237

D) Hijack Attack (Correct Answer)

Explanation: A Hijack Attack involves a malicious user positioning themselves between a client and server, interrupting the session, and taking it over while impersonating the client. This type of attack allows the attacker to gain unauthorized access to the ongoing communication session.

Question 238

B) Caesar Cipher (Correct Answer)

Explanation: The Caesar Cipher is a simple three-position shifting mono-alphabetic substitution cipher. Named after Julius Caesar, who used it for military communications, it involves shifting each letter in the plaintext by a fixed number of positions in the alphabet.

Question 239

A) Virtual Machine (Correct Answer)

Explanation: A Virtual Machine is a software simulation of a computer within which a process executes, with its own memory address space and controlled communication between instances. It allows multiple operating systems to run on a single physical machine, providing isolation and resource management.

Question 240

C) Isolation (Correct Answer)

Explanation: In the ACID properties of transaction processing, "I" stands for Isolation. This principle ensures

that concurrent execution of transactions leaves the database in the same state that would have been obtained if the transactions were executed sequentially.

Question 241

C) Blacklist (Correct Answer)

Explanation: A Blacklist approach to application control blocks certain prohibited packages while allowing the installation of other software on systems. This method specifies which applications or types of applications are not allowed to run, while permitting everything else by default.

Question 242

C) Duress (Correct Answer)

Explanation: Duress describes the situation when someone is forced to perform an action under threat. In information security, it's important to consider duress scenarios, such as implementing duress codes that allow users to signal they're acting under coercion without alerting the threat actor.

Question 243

D) Host-Based IDS (Correct Answer)

Explanation: A Host-Based Intrusion Detection System (HIDS) is installed on a single computer and can monitor activities on that specific machine. It analyzes system calls, application logs, file-system modifications, and other host activities to detect potential security breaches.

Question 244

A) ALE = Single Loss Expectancy x Annualized Rate of Occurrence (Correct Answer)

Explanation: The formula for calculating Annualized Loss Expectancy (ALE) is ALE = Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO). This calculation helps

organizations quantify the potential yearly cost of a specific threat or risk, aiding in risk management decisions.

Question 245

C) Hypertext Transfer Protocol (HTTP) (Correct Answer)

Explanation: Hypertext Transfer Protocol (HTTP) is the protocol used to transmit webpage elements from a web server to web browsers, typically over port 80. It's the foundation of data communication on the World Wide Web, defining how messages are formatted and transmitted between web browsers and servers.

Practice Tests 6

Question 1

What method is employed to adequately erase media that will be utilized again within the same protected environment?

A) Degaussing

B) Reformatting

C) Clearing

D) Partitioning

Question 2

What kind of solution is Nick Fury implementing for his organization when he sets up an IDaaS system?

A) Employee ID as a Service

B) Cloud based RADIUS

C) OAth

D) Identity as a Service

Question 3

What term describes the hardware or software used to regulate access to resources and systems while providing protection? Examples include encryption, smart cards, passwords, biometrics, constrained inferences, access control lists, protocols, firewalls, routers, intrusion detection systems, and clipping levels.

A) Discretionary Access Control

B) Attribute-Based Access Control

C) Role-Based Access Control

D) Logical Access Control

Question 4

What type of program for mobile devices provides users with a selection of approved devices to choose from for implementation?

A) CYOD

B) PYOM

C) BYOB

D) BYOD

Question 5

What is the term for the practice of falsifying DNS information used by a client to reach a desired system, typically accomplished by inserting false data into a zone file, caching DNS system, or HOSTS file?

A) Phantom Domain Attack

B) Distributed Reflection Denial of Service

C) DNS Tunneling

D) DNS Poisoning

Question 6

What strategy involves choosing alternative options or activities that carry less associated risk compared to the default, common, expedient, or inexpensive option?

A) Risk Acceptance

B) Risk Avoidance

C) Risk Transfer

D) Risk Reduction

Question 7

Which type of firewall employs multiple proxy servers to filter traffic based on analysis of the protocols used for each service?

A) A static packet filtering firewall

B) An application level-gateway firewall

C) A stateful inspection firewall

D) A circuit-level gateway firewall

Question 8

What is the term for the practice of intercepting packets from a network with the intention of extracting useful information from their contents?

A) Packet Sniffing

B) Packetjacking

C) Packet-Snatching

D) Packet Boosting

Question 9

In which data model is information stored across multiple databases while remaining logically connected, with users perceiving it as a single entity despite consisting of numerous interconnected parts over a network, and each field potentially having multiple children and parents, resulting in a many-to-many data mapping relationship?

A) Remote Data Model

B) Distributed Data Model

C) Standard Data Model

D) Consolidated Data Model

Question 10

Which of the following is an example of a biometric factor that utilizes a unique behavioral or physiological characteristic of an individual?

A) Passphrase

B) Iris Scan

C) RFID

D) Pattern Recognition

Question 11

What protocol is a full-duplex system used for transmitting TCP/IP packets over various non-LAN connections such as modems, ISDN, VPNs, and Frame Relay, and is widely supported as the preferred transport protocol for dial-up Internet connections?

A) Network Control Protocols (NCPs)

B) Link Control Protocols (LCPs)

C) Encapsulation Component Protocols (ECPs)

D) Point-to-Point Protocol (PPP)

Question 12

Which network and distributed application solution divides tasks and workloads among equal participants?

A) Hierarchical Distributed Network

B) System Area Network

C) Peer-to-Peer (P2P)

D) Grid Computing

Question 13

In an asymmetric cryptosystem where Mike and Renee are communicating using digital certificates signed by a mutually trusted certificate authority, which key does Mike use to verify the authenticity of Renee's digital certificate?

A) Renee's public key

B) CA's public key

C) Renee's private key

D) CA's private key

Question 14

What U.S. law, enacted in 2002, mandates that federal agencies implement an information security program covering their operations and includes the activities of contractors in their security management programs?

A) Patriot Act

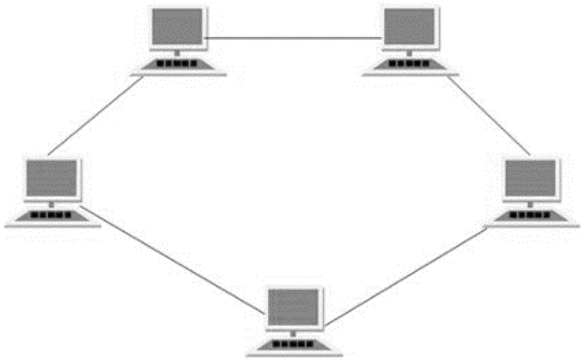
B) Federal Information Security Management Act (FISMA)

C) Human Rights and Privacy Act (HRPA)

D) Family Educational Rights and Privacy Act (FERPA)

Question 15

What type of network topology is characterized by each computer being connected to another in a circular formation, with the last one linked back to the first?



A) Bus

B) Star

C) Ring

D) Mesh

Question 16

Which principle in cryptography advocates for the public availability of all algorithms while maintaining the privacy of all keys?

A) Schrödinger principle

B) Heisenberg principle

C) Satoshi principle

D) Kerckchoff principle

Question 17

What type of backup stores only the files that have been modified since the most recent full or incremental backup?

A) Incremental Backup

B) Differential Backup

C) Partial Backup

D) Synthetic Backup

Question 18

Which data mining technique develops models of normal user behavior based on factors such as organizational affiliation, distance between the data center and user's physical location, day of the week, hour of the day, and other attributes?

A) Outlier detection

B) Classification

C) Expectation Maximization (EM)

D) Regression

Question 19

What term describes a total loss of electrical power?

A) Freeze

B) Blackout

C) Knockout

D) Outage

Question 20

What is the term for the malicious redirection of a legitimate website's URL or IP address to a fake site hosting a false version of the original valid site?

A) URL Phishing

B) 404 Redirects

C) Website Referral

D) DNS Pharming

Question 21

What type of attacks are directed against hash algorithms used to verify the integrity of messages, software, or digital signatures?

A) Eavesdropping attack

B) Cross-site scripting attack

C) Birthday attack

D) Drive-by attack

Question 22

Why are iris scans considered superior to most other biometric factors?

A) Iris scanners are more difficult to deceive

B) Irises remain more consistent over time compared to other factors

C) Iris scans are challenging to replicate

D) Iris scanners are more cost-effective than other factors

Question 23

When conducting a qualitative risk assessment for an organization, which two crucial risk elements should be given the most weight in the analysis?

A) Likelihood and History

B) Probability and Impact

C) History and Impact

D) Cost and Likelihood

Question 24

What type of testing is performed by actual users of a software application in a real environment and can be considered a form of external User Acceptance Testing?

A) Beta Testing

B) Omega Testing

C) Alpha Testing

D) Delta Testing

Question 25

What technology ensures that an operating system allocates distinct memory spaces for each application running on a system?

A) Data Hiding

B) Layering

C) Process Isolation

D) Abstraction

Question 26

What term describes a statement, either oral or written, made by someone other than a witness in a proceeding, which is based on third-party content?

A) Opinion Evidence

B) Hearsay Evidence

C) Secondary Evidence

D) Circumstantial Evidence

Question 27

What security mechanism aims to ensure that information stored in a database is always accurate or at least has its integrity and availability protected, using a "lock" feature to allow an authorized user to make changes and then "unlocks" data elements only after all changes are complete?

A) Contravention

B) Congruency

C) Concurrency

D) Consignation

Question 28

Which term describes a brief period of abnormally high voltage?

A) Sag

B) Surge

C) Brownout

D) Spike

Question 29

What standard specifies that all federally approved digital signature algorithms must employ a secure hashing function?

A) Digital Signature Standard (DSS)

B) Digital Signature Act (DSA)

C) Digital Signature Protocol (DSP)

D) Digital Signature Policy (DSP)

Question 30

What early implementation of the spread spectrum concept involves a wireless access technology that transmits data in a series while continuously changing the frequency in use?

A) Alternating Spread Spectrum (ASS)

B) Frequency Hopping Spread Spectrum (FHSS)

C) Variable Spread Spectrum (VSS)

D) Oscillating Spread Spectrum (OSS)

Question 31

What type of authenticator, classified as a Type 2 Authentication Factor, generates dynamic passwords based on a time or algorithm-based system?

A) PIV

B) CAC

C) Smart Card

D) Token

Question 32

What term describes the level of confidence that security requirements are met?

A) Insurance

B) Verification

C) Assertation

D) Assurance

Question 33

Which specialized privacy bill affects educational institutions accepting federal funding and grants certain privacy rights to students over 18 and parents of minor students?

A) Family Educational Rights and Privacy Act (FERPA)

B) Human Rights and Privacy Act (HRPA)

C) Educational Institution Privacy Act (EIPA)

D) Children's Educational Privacy Protection Act (CEPPA)

Question 34

SYN floods exploit implementations of which protocol to cause Denial of Service conditions?

A) TCP

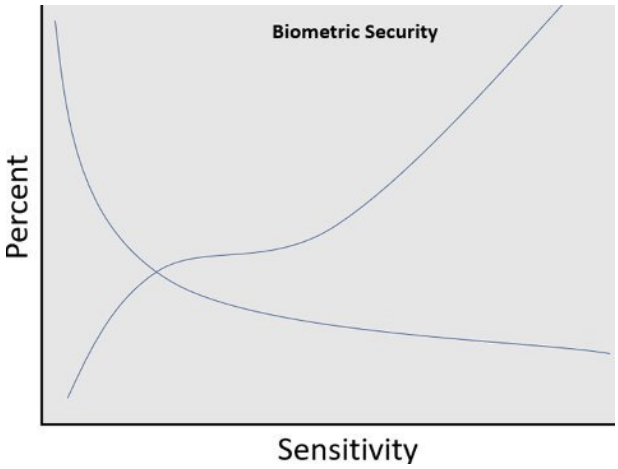
B) IGMP

C) ICMP

D) UDP

Question 35

What metric is used to summarize the operating characteristics of a biometric security system, where a smaller value indicates better performance?



A) CER

B) FAR

C) FRR

D) FNMR

Question 36

What security technique creates a boundary for applications and prevents them from interacting with other applications?

A) Walling

B) Sandboxing

C) Caging

D) Corralling

Question 37

Which public key encryption algorithm was developed by Adi Shamir, Leonard Adleman, and Ron Rivest?

A) RSA

B) ARS

C) DSA

D) SAR

Question 38

What type of network device should Freddy Krueger deploy to connect his network to other networks while controlling traffic on his network?

A) Gateway

B) Switch

C) Router

D) Bridge

Question 39

What 2009 congressional amendment to HIPAA updated many privacy and security requirements, changed how Business Associates are treated, and introduced new data breach notification requirements?

A) Health Insurance Portability and Accountability Act Revision of 2009 (HIPAAR)

B) Health Information Technology for Economic and Clinical Health Act (HITECH)

C) Health Insurance Privacy Rule (HIPR)

D) Rights and Protections for Participants and Healthcare Beneficiaries Act (RPPHB)

Question 40

Which type of penetration testing provides information on the scope of the test, including target systems, but doesn't offer full visibility into the configuration or other details of the systems or networks being tested?

A) Gray box

B) Black box

C) White box

D) Crystal box

Question 41

Which of the following cryptographic algorithms supports the goal of nonrepudiation?

A) AES

B) DES

C) Blowfish

D) RSA

Question 42

What term describes any component of an infrastructure – such as a device, service, protocol, or communication link – that would cause significant or total downtime if compromised, violated, or destroyed, affecting the ability of organization members to perform essential work tasks?

A) Weakest Link

B) Single Point of Failure

C) Root Cause

D) Source of Incident

Question 43

What type of attack involves the attacker using an unknown plaintext message, encrypting it with every possible key (k1), while simultaneously decrypting the equivalent ciphertext using all possible keys (k2)?

A) Meet-in-the-Middle Attack

B) Eavesdropping Attack

C) Man-in-the-Middle Attack

D) Drive-by Attack

Question 44

What term describes a controlled exit and entry point in a fence?

A) Gate

B) Turnstile

C) Portal

D) Mantrap

Question 45

What type of testing is used to verify that a system complies with laws, regulations, baselines, guidelines, standards, and policies as an important part of maintaining security in any environment?

A) Traceability Testing

B) Compliance Testing

C) Scope Testing

D) User Acceptance Testing

Question 46

What type of new system deployment testing involves running the new system and the old system simultaneously?

A) Simultaneous Cutover

B) Parallel Run

C) Start-to-Start Testing

D) Cloned Changeover

Question 47

What form of malicious code is self-replicating but not designed to directly harm host systems, with its primary purpose being to replicate itself to other systems and gather information?

A) Bot

B) Trojan

C) Virus

D) Worm

Question 48

In a packet captured by Bill Foster's protocol analyzer showing both PSH and URG flags set, what type of packet is it and what do these flags signify?

A) A TCP packet; PSH and URG are used to present the header and indicate that the speed of the network is unregulated

B) A UDP packet; PSH and URG indicate that the UDP buffer should be cleared and that the data is urgent

C) A TCP packet; PSH and URG are used to clear the buffer and indicate that the data is urgent

D) A UDP packet; PSH and URG indicate that the data should be sent at high speed

Question 49

If Tom's suspicion is correct that a customer of his Internet service provider has been exploiting a vulnerability to read other customers' email messages, which law would the customer most likely have violated?

A) HITECH

B) CALEA

C) Privacy Act

D) ECPA

Question 50

Which security model is designed to allow access controls to change dynamically based on a user's previous activity, making it a type of state machine model as well?

A) Bell-Lapadula Model

B) Clark-Wilson Model

C) Biba Model

D) Brewer and Nash Model

Question 51

Harold is searching for a software development approach that will address a significant issue in his organization. At present, developers and operations personnel do not collaborate and are often perceived as passing problems to each other without taking responsibility.

Which technology management strategy is specifically designed to resolve this issue?

A) ITSM

B) DevOps

C) ITIL

D) Lean

Question 52

Complete the following sentence in the context of Information Systems Security:

The _____ is an alternative name for the Emergency Response Team, which consists of InfoSec professionals capable of addressing incidents and system issues.

A) Federal InfoSec Fraud Group (FIFG)

B) Special Computer Fraud Responders (SCFR)

C) International Informational Security Response Team (ITSRT)

D) Computer Incident Response Team (CIRT)

Question 53

Fill in the blank in the following sentence within the context of Information Systems Security:

____ is a widely used shared media LAN technology.

A) SDD

B) USB

C) HDD

D) Ethernet

Question 54

Complete the following sentence in the context of Information Systems Security:

A(n) _____ refers to any individual who attempts to carry out a malicious action against a system.

A) Attacker

B) Player

C) Predator

D) Militia

Question 55

Gordon is performing a risk evaluation for his company and has calculated the expected annual damage that flooding would cause to his facilities.

Which metric has Gordon identified?

A) SLE

B) EF

C) ARO

D) ALE

Question 56

Fill in the blank in the following sentence within the context of Information Systems Security:

A(n) _____ is a procedure in which disaster recovery checklists are distributed to disaster recovery team members for their examination.

A) Soft DR Test

B) Executive DR Test

C) Parallel Disaster Recovery Test

D) Checklist Test

Question 57

Sue's organization recently failed a security audit because their network was configured as a single flat broadcast domain, allowing traffic sniffing between different functional groups.

What solution should she propose to address the identified issues?

A) Enable port security

B) Modify the subnet mask for all systems

C) Implement gateways

D) Utilize VLANs

Question 58

Which of the following is not considered a code review process?

A) Over-the-shoulder

B) IDE forcing

C) Email pass-around

D) Pair programming

Question 59

Complete the following sentence in the context of Information Systems Security:

____ explains how the mathematical principles underlying the Diffie-Hellman key exchange algorithm could be extended to support a complete public cryptosystem for message encryption and decryption.

A) Isa

B) ElGamal

C) Kasab

D) McEliece

Question 60

Fill in the blank in the following sentence within the context of Information Systems Security:

____ refers to the network of devices capable of communicating with each other or a control console via the Internet to influence and monitor the physical world.

A) OMG Network

B) Basic Attention Token

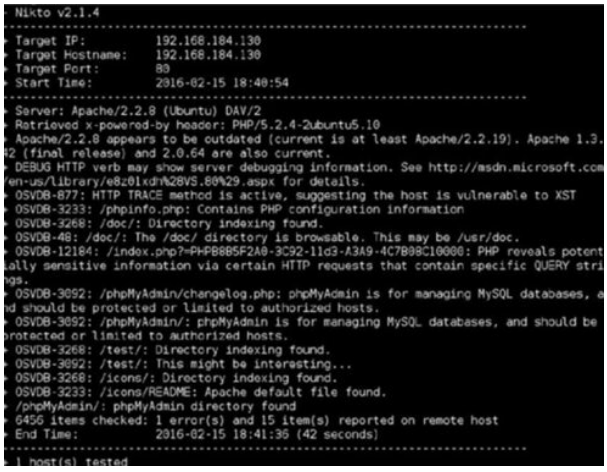
C) Internet of Things (IoT)

D) Advanced Internet Blocks

Question 61

During a web application vulnerability scan, Steve runs Nikto against a web server that he suspects may be vulnerable to attacks.

Why might he be concerned about this vulnerability?



A) It is used to store sensitive data

B) It indicates a potential compromise

C) The /test directory allows administrative access to PHP

D) Test directories often contain scripts that can be exploited

Question 62

Complete the following sentence in the context of Information Systems Security:

____ refers to the number of rows in a relational database.

A) Horizontal Reference

B) Vertical Reference

C) Cardinality

D) Coordinates

Question 63

Which OASIS standard markup language is employed to generate provisioning requests both within organizations and with third parties?

A) SOA

B) XACML

C) SPML

D) SAML

Question 64

Fill in the blank in the following sentence within the context of Information Systems Security:

A(n) _____ is a type of attack where malicious users position themselves between two communication endpoints. The client and server are unaware that a third party is intercepting and facilitating their communication session.

A) Phishing Attack

B) Man-in-the-Middle (MitM) Attack

C) Drive-by Attack

D) Eavesdropping Attack

Question 65

Complete the following sentence in the context of Information Systems Security:

A(n) _____ is a sophisticated attack exploiting a known vulnerability, where bots with valid IPs establish a legitimate connection with a web server. The bots then split packets into tiny fragments and send them to the target as slowly as possible before timing out. This method allows attackers to maintain an active connection for an extended period without triggering defense mechanisms.

A) Ping-of-Death Attack

B) Teardrop Attack

C) Zero Day Attack

D) Fragmented HTTP Flood

Question 66

Fill in the blank in the following sentence within the context of Information Systems Security:

____ is a software testing methodology that evaluates the entire software from start to finish, including its integration with external interfaces. The purpose of this testing is to assess the software's dependencies, data integrity, and communication with other systems, interfaces, and databases to simulate a complete production-like scenario.

A) Begin-To-Finish Testing

B) Floor-To-Ceiling Testing

C) Start-To-End Testing

D) End-To-End Testing

Question 67

NIST SP 800-53 discusses a set of security controls as what type of security tool?

A) The CIS standard

B) A configuration list

C) A baseline

D) A threat management strategy

Question 68

An attack that alters a symlink on a Linux system between the time when an account's rights to the file are verified and when the file is accessed is an example of what type of attack?

A) TOCTOU

B) Tick/tock

C) Unlinking

D) setuid

Question 69

Complete the following sentence in the context of Information Systems Security:

____ is an intrusion detection mechanism used by IDS that learns about normal activities and events on your system through observation and analysis.

A) Silicone-Based Recognition

B) Artificial Intelligence Unmasking

C) Behaviour-Based Detection

D) Synthetic Learning Protocol

Question 70

Which protocol possesses the following characteristics?

Connectionless, sending data without checking if the receiving system is ready

Unreliable, not guaranteeing packet delivery

Faster due to lack of delivery guarantees

8-byte packet size

No acknowledgment waiting; data is sent immediately

No flow control mechanism

No error checking or resending of lost packets

Used for applications requiring fast communication without prioritizing reliability, such as VoIP, game streaming, and video/music streaming

A) UDP

B) SAML

C) SQL

D) TCP

Question 71

Fill in the blank in the following sentence within the context of Information Systems Security:

____ is the process of integrating new employees into an organization's identity and access management system. This process is also used when an employee's role or position changes, or when they are granted additional levels of privilege or access.

A) Hiring

B) Promotion

C) Onboarding

D) Modification

Question 72

While monitoring traffic at two points of a network connection, Lauren observes inbound traffic to a public IP

address appearing inside the production network, destined for an internal host using an RFC 1918 reserved address.

What technology should she expect to be in use at the network border?

A) BGP

B) S/NAT

C) VLANs

D) NAT

Question 73

The type of access granted to an object and the actions that can be performed on or with the object are examples of what?

A) Permissions

B) Privileges

C) Roles

D) Rights

Question 74

Complete the following sentence in the context of Information Systems Security:

A(n) _____ is the hacker who controls a botnet.

A) AndroidChief

B) Botmaster

C) Cyborg

D) Botboss

Question 75

Fill in the blank in the following sentence within the context of Information Systems Security:

The _____ is an integrity-focused security model based on the state machine model, employing mandatory access

controls and the lattice model.

A) Information Flow Model

B) Integrity Flow Model

C) Biba Model

D) Bell-LaPadula Model

Question 76

Complete the following sentence in the context of Information Systems Security:

____ is a cloud computing concept that provides on-demand online access to specific software applications or suites without requiring local installation.

A) PaaS

B) IaaS

C) GaaS

D) SaaS

Question 77

D'Ken Neramani is working on integrating a federated identity management system and needs to exchange authentication and authorization information for browser-based single sign-on.

Which technology is the most suitable option for his needs?

A) SPML

B) XACML

C) HTML

D) SAML

Question 78

Fill in the blank in the following sentence within the context of Information Systems Security:

A(n) _____ is a string of characters typically much longer than a password. Once entered, the system converts it into a virtual password for use in the authentication process. It is often a natural-language sentence to facilitate easier memorization.

A) Bio-Key

B) Screen Scraping Authenticator

C) Passphrase

D) Cookie-based Key

Question 79

During which phase of the incident response process would an organization determine if it is obligated to notify law enforcement officials or other regulators about the incident?

A) Remediation

B) Recovery

C) Reporting

D) Detection

Question 80

In which phase of the incident response process would security professionals analyze the process itself to identify potential areas for improvement?

A) Remediation

B) Lessons learned

C) Recovery

D) Reporting

Question 81

Complete the following sentence in the context of Information Systems Security:

The _____ represents the annual cost associated with a specific realized threat against a particular asset.

A) Annualized Loss Expectancy (ALE)

B) Annual Rate of Occurrence (ARO)

C) Break-Even Point (BEP)

D) Single Loss Expectancy (SLE)

Question 82

Pete Wisdom has a flash memory card containing sensitive information that he wishes to reuse.

Which technique can he employ to securely remove data from the card while allowing for its reuse?

A) Degaussing

B) Reformatting

C) Physical destruction

D) Overwriting

Question 83

Kabuki, a database security administrator for Aircraft Systems, Inc. (ASI), is concerned about safeguarding information stored in ASI databases. ASI is a military contractor dealing with classified information, and different employees have varying security clearances. The database contains information on military aircraft locations with ASI systems for monitoring purposes.

Kabuki has learned of a classified military mission involving some ASI aircraft and worries that employees without proper clearance might deduce the mission by noticing the movement of numerous aircraft to a specific region.

What technique can Kabuki use to prevent employees without proper clearance from discovering the true location of the aircraft?

A) Input validation

B) Server-side validation

C) Parameterization

D) Polyinstantiation

Question 84

Which US government classification label is applied to information that, if disclosed, could cause serious damage to national security, and requires that the potential damage be describable or identifiable by the classification authority?

A) Top Secret

B) Confidential

C) Secret

D) Classified

Question 85

What term describes a software testing process aimed at uncovering new bugs introduced by patches or configuration changes?

A) Nonregression testing

B) Regression testing

C) Evolution testing

D) Smoke testing

Question 86

Fill in the blank in the following sentence within the context of Information Systems Security:

A(n) _____ is an attack that repeatedly sends ping requests to a system. It can originate from a single system as a DoS attack but is more commonly launched against a target by multiple systems in a DDoS attack.

A) SYN Flood Attack

B) UDP Flood Attack

C) Ping Flood Attack

D) HTTP Flood Attack

Question 87

Complete the following sentence in the context of Information Systems Security:

With _____, it is possible for a user to prove knowledge of their password without actually providing the password itself. This is achieved using a challenge and response protocol that first determines the mutually supported types and encryption mechanisms between the client and server, then cryptographically hashes the user's password and sends it to the server requiring authentication.

A) SPNEGO-based SSO

B) Form-filling SSO

C) NTLM-based SSO

D) Kerberos-based SSO

Question 88

Galia is utilizing IPSec's ESP component in transport mode.

What crucial information should she be aware of regarding transport mode?

A) Transport mode adds a new, unencrypted header to ensure packets reach their destination

B) Transport mode provides full encryption of the entire IP packet

C) Transport mode offers no encryption; only tunnel mode provides encryption

D) Transport mode does not encrypt the header of the packet

Question 89

Fill in the blank in the following sentence within the context of Information Systems Security:

____ refers to the act of making minor alterations to data, typically with malicious intent.

A) Data Diddling

B) Data Mixing

C) Data Augmenting

D) Data Jiggling

Question 90

Jackie is designing a database that includes a Customers table. She is creating a new table to store Orders and plans to link the Company ID from the Customers table to uniquely identify the customer associated with each order.

What role does the Company ID field play in the Orders table?

Company ID	Company Name	Address	City	State/Province	Postal Code	Telephone	Sales Rep
1	Stark Industries	1 Stark Avenue	New York	New York	10001	(212) 989-2654	12
2	Daily Bugle	203 39th Street	New York	New York	10028	(312) 302-5689	18
3	Mel's Diner	140 University Avenue W	Waterloo	Ontario	N2L 6J3	(519) 579-6357	33

A) Candidate key

B) Primary key

C) Referential key

D) Foreign key

Question 91

Complete the following sentence in the context of Information Systems Security:

____ is one of the four essential characteristics of all database transactions. A database transaction must be an "all-or-nothing" affair. If any part of the transaction fails, the entire transaction must be rolled back as if it never occurred.

A) Durability

B) Isolation

C) Atomicity

D) Consistency

Question 92

Adam is processing an access request for an end user.

Which two factors should he verify before granting access?

A) Clearance and endorsement

B) Separation and need to know

C) Second factor and clearance

D) Clearance and need to know

Question 93

Fill in the blank in the following sentence within the context of Information Systems Security:

____ involve the use of human physiological or behavioral characteristics as authentication factors for logical access and identification for physical access.

A) Genetics

B) Celebrealitics

C) Biometrics

D) Gestations

Question 94

Mark is planning a disaster recovery test for his organization. He wants to conduct a live test of the disaster recovery facility without disrupting operations at the primary facility.

What type of test should Mark choose?

A) Parallel test

B) Checklist review

C) Tabletop exercise

D) Full interruption test

Question 95

Gwen Stacy wants to integrate her website to allow users to use accounts from sites like Google.

Which technology should she implement?

A) SESAME

B) OpenID

C) Kerberos

D) LDAP

Question 96

Complete the following sentence in the context of Information Systems Security:

The _____ is a type of attack that prevents a system from processing or responding to legitimate traffic or requests for resources and objects.

A) Denial of Service (DoS) attack

B) Cross-site scripting (XSS) attack

C) SQL injection attack

D) Malware attack

Question 97

Clint Barton owns a coffeehouse and wants to provide wireless internet service for his customers. Clint's network is simple, using a single consumer-grade wireless router and cable modem connected via a commercial cable data contract. Clint intends to run an open, unencrypted wireless network.

How should he connect his business devices?

A) Set up a separate wireless network using WEP

B) Set up a separate SSID using WPA2

C) Run WPA2 on the same SSID

D) Run the open network in enterprise mode

Question 98

Fill in the blank in the following sentence within the context of Information Systems Security:

____ are a common method of spreading malware. Hackers identify insecure websites and insert a malicious script into the HTTP or PHP code on one of the pages.

A) Drive-by attacks

B) SQL injection attacks

C) Man-in-the-middle attacks

D) Eavesdropping attacks

Question 99

Complete the following sentence in the context of Information Systems Security:

____ is a special type of secondary memory managed by the operating system in such a way that it appears to be real memory.

A) Virtual Memory

B) Parallel Memory

C) Memory Reserve

D) Reverse

Question 100

In the realm of Information Systems Security, what term describes an attack aimed at uncovering the password associated with a known user identity?

A) Phishing Attack

B) Whaling Attack

C) Brute-Force Attack

D) Trojan Attack

Question 101

Which of the following provides the most intricate decoy environment for an intruder to explore during an attempted breach?

A) Pseudo flaw

B) Darknet

C) Honeynet

D) Honeypot

Question 102

What is the process of erasing media to enable its reuse in a less secure setting called?

A) Cleanup

B) Ejection

C) Purging

D) Deleting

Question 103

What term is used to describe the information appended by a protocol to the end of a payload received from a higher-layer protocol?

A) Footer

B) Close

C) Footnote

D) <END>

Question 104

When configuring network devices to use syslog, what should be set to ensure notification of issues without receiving messages about normal operational matters?

A) The log priority

B) The security level

C) The facility code

D) The severity level

Question 105

In risk assessment, what term refers to the anticipated monetary loss each time an asset is exposed to risk?

A) Annual Rate of Occurrence (ARO)

B) Annualized Loss Expectancy (ALE)

C) Break-Even Point (BEP)

D) Single Loss Expectancy (SLE)

Question 106

How many ports of each type must be scanned to thoroughly examine all possible TCP and UDP ports on a system?

A) 65,535 TCP ports and 32,768 UDP ports

B) 1024 common TCP ports and 32,768 ephemeral UDP ports

C) 65,536 TCP and 65,536 UDP ports

D) 16,384 TCP ports, and 16,384 UDP ports

Question 107

What term describes a system that conceals the true meaning of a message by employing various techniques to alter or rearrange characters or words to achieve confidentiality?

A) Private Key

B) Mirror

C) Cipher

D) Cryptographic Hash

Question 108

What is the term for a system's response to a failure that results in defaulting to an "allow" posture?

A) Fail-Closed

B) Fail-Safe

C) Fail-Over

D) Fail-Open

Question 109

What key feature distinguishes Frame Relay from X.25?

A) Frame Relay does not provide a Committed Information rate (CIR).

B) Frame relay supports multiple PVCs or a single WAN carrier connection.

C) Frame Relay only requires a DTE on the provider side.

D) Frame Relay is a cell switching technology instead of packet switching technology like X.25.

Question 110

Which protocol utilizes port 443 to establish encrypted communication sessions between web servers and browser clients?

A) Hypertext Transfer Protocol

B) Intranet Protocol

C) Python Protocol

D) Hypertext Transfer Protocol over Secure Sockets Layer

Question 111

What is the most effective method to ensure the confidentiality of email content while in transit?

A) Use a signal signature.

B) Use TLS between the client and server.

C) Use SSL between the client and the server.

D) Encrypt the email content.

Question 112

What type of access control involves authorization verification performed by a single entity within a system?

A) Bottom-Up Access Control

B) Distributed Access Control

C) Centralized Access Control

D) Top-Down Access Control

Question 113

What network device is used to amplify signals on network cabling, allowing for greater distances between nodes?

A) Radio

B) Augmentor

C) Repeater

D) Slipstream

Question 114

In the context of transaction processing, what does the "D" in the ACID acronym stand for?

A) Dichotomous

B) Defensive

C) Durability

D) Dependent

Question 115

What term describes a number, also known as a message digest, generated by a hash function?

A) Private Address

B) Public Address

C) Hash

D) Key

Question 116

Which type of Windows audit record documents events such as operating system shutdowns or services being halted?

A) An application log

B) A setup log

C) A security log

D) A system log

Question 117

What type of testing is characterized by verifying a system against functional requirements provided by the client, being executed first, and potentially using manual or automation tools?

A) Functional Testing

B) Generic Testing

C) Non-Functional Testing

D) Focused Testing

Question 118

According to NIST Special Publication 800-53A, if someone is reviewing a password standard, which of the four types of objects are they assessing?

A) A mechanism

B) A specification

C) An activity

D) An individual

Question 119

What alternative term is commonly used to refer to a forensic drive controller?

A) Write blocker

B) SCSI terminator

C) Forensic device analyzer

D) RAID controller

Question 120

Which technology is specifically designed to prevent a hard drive from becoming a single point of failure in a system?

A) Load balancing

B) RAID

C) IPS

D) Dual power supplies

Question 121

During an account management assessment, which type of accounts are typically the primary focus?

A) Recently generated accounts

B) Accounts that have existed for long periods of time

C) A random sample

D) Highly privileged accounts

Question 122

In legal proceedings, what term describes physical evidence, such as an object presented in court, that is examined as a means of proving a fact?

A) Direct Evidence

B) Primary Evidence

C) Real Evidence

D) Best Evidence

Question 123

What protocol is responsible for assigning TCP/IP configuration settings to systems upon bootup, using UDP ports 67 and 68 for server and client communications respectively?

A) Dynamic Host Configuration Protocol (DHCP)

B) Automatic Server Configuration Protocol (ASCP)

C) Dedicated Script Internet Protocol (DSIP)

D) Process Application Setting Protocol (PASP)

Question 124

What term describes the act of substituting valid source and/or destination IP addresses and node numbers with false ones?

A) Spoofing

B) Spamming

C) Spear Phishing

D) Pharming

Question 125

When a network receives a packet larger than its maximum allowable size, into what does it break the packet?

A) Clones

B) Fragments

C) Clusters

D) Partitions

Question 126

What type of testing aims to verify that a system meets stated criteria for functionality and possibly security

capabilities, determining if end users or customers will accept the completed product?

A) UAT

B) CAC

C) MAP

D) DAT

Question 127

What networking device acts like a router or switch, providing the customer's network access to the Frame Relay Network?

A) Data Circuit-Terminating Equipment

B) Bridging Router Device

C) Gateway Hub

D) Data Terminal Equipment (DTE)

Question 128

What term describes a system where a long chain of computational decisions feed into each other, ultimately producing the desired output?

A) Positronic Brain

B) Neural Network

C) Symbolic Regression Optimization

D) Support Vector Machine

Question 129

Which of the following should not be a concern when penetration testers propose using Metasploit during their assessment?

A) Penetration testing only covers a point-in-time view of the organization's security.

B) Tools like Metasploit can cause denial of service issues.

C) Metasploit can only test vulnerabilities it has plugins for.

D) Penetration testing cannot test processes and policy.

Question 130

What term describes a mechanism that copies packets from one network to another, altering source and destination addresses to protect the identity of the internal or private network?

A) Virtual Drive

B) Proxy

C) Remote Backup

D) CDN

Question 131

What is the process of categorizing data under labels for the purpose of applying security controls and access restrictions called?

A) Security Controls & Access Formatting

B) Data Classification

C) Content Structuring

D) Terminology

Question 132

For a small college's information security officer responsible for safeguarding student record privacy, which law is most directly applicable?

A) HITECH

B) COPPA

C) FERPA

D) HIPAA

Question 133

What technique can best protect hashed passwords against automated cracking attacks that use precomputed values?

A) Salting

B) Double-hashing

C) Using the SHA-1 hashing algorithm

D) Using the MD5 hashing algorithm

Question 134

What open SSO standard designed to work with HTTP allows users to log on with one account across multiple sites or locations?

A) HTTPSO

B) OAuth

C) iAuth

D) O-SSO

Question 135

What fire-suppressant material, known to convert to toxic gases at 900 degrees Fahrenheit and deplete the ozone layer, is typically replaced by alternative substances?

A) ABC Dry Chemical

B) Purple K (BC Dry Chemical)

C) Novec 1230

D) Halon

Question 136

What type of protected information includes an individual's name, Social Security Number, date and place of birth, or mother's maiden name?

A) PII

B) Proprietary Data

C) EDI

D) PHI

Question 137

Who is most likely to lead a regulatory investigation?

A) CIO

B) Private detective

C) CISO

D) Government agent

Question 138

What term describes an organized group of highly motivated, skilled, and patient attackers, often government-sponsored, that focus on a specific target and persist until achieving their goal?

A) Bitcoin Development Core (BDC)

B) Advanced Persistent Threat (APT)

C) Blockchain Hacker Foundation (BHF)

D) Society Reform Liberators (SRL)

Question 139

What technology uses electromagnetic or electrostatic coupling in the radio frequency spectrum to identify specific devices, with each tag containing a unique identifier?

A) Kanban

B) QR-Codes

C) Barcodes

D) RFID

Question 140

What type of SSO is created by a trusted claims issuer and typically packaged into a digitally signed token sent over the network using Security Assertion Markup Language (SAML)?

A) Claims-based SSO

B) Screen Scraping SSO

C) Cookie-based SSO

D) Kerberos-based SSO

Question 141

What solution provides a secure storage space for users to keep their credentials when single sign-on (SSO) is unavailable?

A) Virtual Private Keys

B) Microsoft VUE

C) Cryptographic Assignment

D) Credential Management System

Question 142

Which disaster recovery test type has the least impact on business operations?

A) Parallel test

B) Full interruption test

C) Checklist review

D) Tabletop exercise

Question 143

Which of the following is not a typical function of a forensic device controller?

A) Blocking read commands sent to the device

B) Preventing the modification of data on a storage device

C) Reporting errors sent by the device to the forensic host

D) Returning data requested from the device

Question 144

What network device is used to control traffic flow between networks, often connecting similar networks and utilizing static or dynamic routing tables?

A) Fiber Optic Connector

B) Modem

C) Router

D) Switch

Question 145

What Internet-based single sign-on solution operates over the OAuth protocol and can be used for web services, cloud resources, and smart device apps?

A) ActiveX Connect

B) Apereo CAS Connect

C) OpenID Connect

D) Persona Connect

Question 146

What term describes a mechanism separate from a motion detector that triggers a deterrent, repellent, or notification?

A) Escalation

B) Routine

C) Query

D) Alarm

Question 147

When decommissioning archival DVD-ROMs containing Top Secret data, what method should be used to ensure the data cannot be exposed?

A) Degauss

B) Pulverize

C) Zero wipe

D) Secure erase

Question 148

What is the term for a table that indicates the actions or functions each subject can perform on each object in a system?

A) Subject Rights Matrix

B) Access Control Matrix

C) User Access Matrix

D) Permissions Matrix

Question 149

In planning the layout for a data center inside a newly constructed four-story office building, consisting of a basement and three above-ground floors, where should the data center be optimally situated?

A) Third floor

B) Basement

C) First floor

D) Second floor

Question 150. What is the term for regulations that encompass various topics, from internal agency procedures to immigration enforcement policies for laws enacted by Congress?

A. Federal Policy laws

B. Executive-order laws

C. Administrative laws

D. Procedural laws

Question 151. Which technique is specifically designed to counteract the use of Rainbow Tables in password security?

A. User education

B. Password expiration policies

C. Salting

D. Password complexity policies

Question 152. What cloud model incorporates a blend of two or more cloud types, which may include public, private, and/or community clouds?

A. Hybrid Cloud

B. Remote Cloud

C. Virtual Cloud

D. On-line Cloud

Question 153. What is the process of removing a layer's header and footer from a Protocol Data Unit as it ascends through the OSI model layers?

A. Incapacitation

B. Enveloping

C. Abridging

D. Deencapsulation

Question 154. At which layer of the OSI model do TCP and UDP operate?

A. Layer 4

B. Layer 3

C. Layer 2

D. Layer 5

Question 155. What type of twisted-pair wire includes a metallic foil wrapper within the outer sheath to provide enhanced protection against electromagnetic interference?

A. Ethernet

B. STP

C. USB

D. COAXE

Question 156. What is the comprehensive service for managing chargebacks and disputes, performed by a team of highly knowledgeable specialists?

A. TSYS Dispute Resolution (TDS)

B. Loss-Prevention Automation (LPA)

C. Bust-Out Reporting (BOR)

D. Positive Pay (PP)

Question 157. What term describes management's assessment of the cost-benefit analysis for potential safeguards, determining that the expense of countermeasures significantly outweighs the potential cost of loss due to a risk?

A. Risk mitigation

B. Risk Transfer

C. Risk acceptance

D. Risk avoidance

Question 158. What power supply fluctuations are typically caused by switching large electric loads on or off?

A. Common Mode Noise

B. Electromagnetic Pulse

C. Dips and Surges

D. Electrical Spikes

Question 159. What technique is being employed when a security monitoring system is configured to report failed login attempts only if there are five unsuccessful attempts to access the same account within a one-hour period?

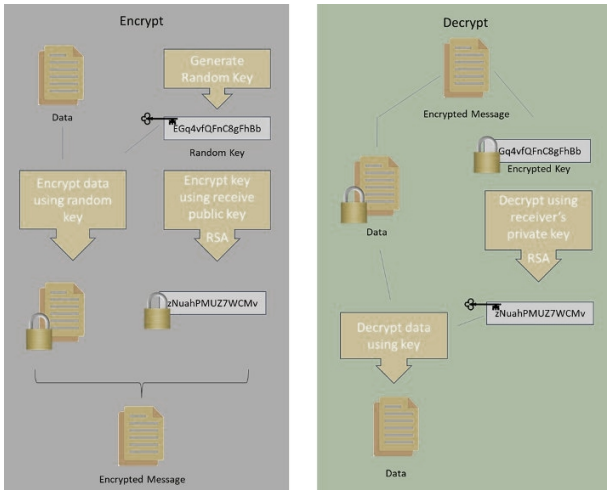
A. Account lockout

B. Sampling

C. Clipping

D. Thresholding

Question 160. Which email encryption method is depicted in the provided figure?



A. S/MIME

B. MD5

C. PGP

D. Thunderbird

Question 161. When decrypting a message that was encrypted using symmetric cryptography, which key should be utilized?

A. Melody's public key

B. Shared secret key

C. Barry's private key

D. Barry's public key

Question 162. What legal instrument should be employed to safeguard a company's data when an employee with access to trade secrets and confidential information leaves to work for a competitor?

A. An NDA

B. Encryption

C. An AUP

D. A stop loss order

Question 163. What is the sub-protocol of the TCP/IP protocol suite that functions at the Data Link layer to identify the MAC address of a system?

A. Media Address Control lookup

B. MAC TCP/IP protocol

C. Address Resolution Protocol

D. Media Access Control lookup

Question 164. What layer two protocol, developed by IBM for remote communications with NSA systems, is used in networks with dedicated or leased lines?

A. Spiral Defence Layer Capacity (SDLC)

B. Sandbox Decryption Link Cast (SDLC)

C. Synchronous Data Link Control (SDLC)

D. Software Development Life Cycle (SDLC)

Question 165. What has occurred when a Windows system displays an IP address in the 169.254.x.x range? Or Ed’s Windows system can't connect to the network and ipconfig image shows shown below, what has occurred on the system?

A. The system has failed to obtain a DHCP address and has assigned itself an address.

B. The subnet mask is incorrectly set, preventing communication with the gateway.

C. The system has a manually assigned IP address.

D. The system has been assigned an invalid IP address by its DHCP server.

Question 166. What information can be gathered by using ping to probe a remote network where pings are allowed through the target's border firewall?

A. Router advertisements, echo request responses, and potentially which hosts are tarpitted.

B. The host names and time to live (TTL) for each pingable system, and the ICMP types allowed through the firewall.

C. Which systems respond to ping, a rough network topology, and potentially the location of additional firewalls.

D. A list of all the systems behind the target's firewall.

Question 167. What term describes the operating system-independent primitive instructions that a computer requires to start up and load the operating system from disk?

A. WinOS

B. AOS

C. BIOS

D. DOS

Question 168. When a computer security specialist provides testimony in court about whether logs and records indicate a hacking attempt, what type of evidence are they offering?

A. Documentary evidence

B. Real evidence

C. Expert opinion

D. Direct evidence

Question 169. What is the term for code that is downloaded and installed on a user's system without their knowledge, often through modified code on legitimate websites or through phishing and redirection methods?

A. Random Subdomain Attack

B. Drive-by Download

C. TCP SYN Floods

D. Botnet-based Attacks

Question 170. In a scenario where a company uses mobile device management software to remotely wipe lost phones, what is the most likely circumstance that would cause a remote wipe to fail?

A. The phone has a passcode on it.

B. The phone is in use.

C. The provider has not unlocked the phone.

D. The phone cannot contact a network.

Question 171. In a backup scenario with full backups on Mondays and incremental backups on other days, how many files will be copied in Wednesday's backup given a specific set of file modifications?

A. 5

B. 1

C. 2

D. 6

Question 172. What term describes the physical or behavioral characteristics of an individual that can be used for identification or authentication purposes?

A. Biometric Factors

B. Physiological Characteristics

C. Habitual Mannerisms

D. Behavioural Tendencies

Question 173. What authentication method requires two distinct factors for verification?

A. SSO

B. SAML

C. 2FA

D. OAth

Question 174. When implementing an access control system to prevent developers from moving code from development to production environments, which information security principle is being most directly enforced?

A. Two-person control

B. Separation of duties

C. Least privilege

D. Job rotation

Question 175. What term describes the planned actions an organization intends to take to resume normal operations following a disruptive event?

A. Disaster Recovery Planning (DRP)

B. Virtualization Disaster Recovery (VDR)

C. Disaster Recovery as a Service (DRaS)

D. Cloud-Based Disaster Recovery (CBDR)

Question 176. What is the system by which subjects are granted or restricted access to objects, including hardware, software, and organizational policies?

A. Access control

B. Spam filters

C. SSO

D. Firewalls

Question 177. Which network port is typically associated with MSSQL?

A. TCP port 22

B. TCP port 443

C. UDP port 53

D. TCP port 1433

Question 178. What type of software testing aims to uncover vulnerabilities, threats, and risks in an application to prevent malicious attacks and identify potential weaknesses?

A. Beta Testing

B. QAQC Testing

C. Functional Testing

D. Security Testing

Question 179. What term refers to the algorithms applied to data designed to ensure confidentiality, integrity, authentication, and/or non-repudiation?

A. Transient Keys

B. Key Salting

C. Cryptography

D. Nonce

Question 180. What process is typically employed to ensure data security for workstations being removed from service but intended for resale or reuse?

A. Sanitization

B. Destruction

C. Clearing

D. Erasing

Question 181. What digital process conceals information within a file, known only to its creator, which can be used to detect unauthorized copies and trace them back to their source?

A. Window

B. Signature

C. Watermark

D. Breadcrumb

Question 182. What form of program testing examines the input and output of a program without focusing on its internal logical structures?

A. Black-Box Testing

B. Green-Box Testing

C. Blue-Box Testing

D. Orange-Box Testing

Question 183. What should be true regarding the salt used in password hashes?

A. Unique salts should be stored for each user.

B. Unique salts should be created every time a user logs in.

C. A single salt should be set so passwords can be dehashed as needed.

D. A single salt should be used so the original salt can be used to check passwords against their hash.

Question 184. Which of the following tools can be used to achieve the goal of non-repudiation?

A. Digital Signature

B. Firewall

C. IDS

D. Symmetric Encryption

Question 185. What term describes electromagnetic or radio frequency signals that may contain data susceptible to interception through eavesdropping?

A. Drive-by Signals

B. Cyphons

C. Leeching

D. Emanations

Question 186. What type of testing should be conducted to verify that a recent patch for a critical application did not introduce issues elsewhere in the system?

A. Unit Testing

B. Black Box

C. Regression Testing

D. White Box

Question 187. What is the layer of the OSI model that is responsible for end-to-end communication between devices, including segmentation of data and flow control?

A. Network Layer

B. Transport Layer

C. Session Layer

D. Presentation Layer

Question 188. Which OSI model layer is responsible for translating data between the network format and the application format?

A. Application Layer

B. Presentation Layer

C. Session Layer

D. Transport Layer

Question 189. What is the term for the layer of the OSI model that establishes, manages, and terminates connections between applications?

A. Network Layer

B. Transport Layer

C. Session Layer

D. Data Link Layer

Question 190. In the OSI model, which layer is responsible for routing and forwarding data packets between different networks?

A. Physical Layer

B. Data Link Layer

C. Network Layer

D. Transport Layer

Question 191. What OSI model layer is responsible for transmitting raw bit streams over a physical medium?

A. Physical Layer

B. Data Link Layer

C. Network Layer

D. Transport Layer

Question 192. Which layer of the OSI model is responsible for logical addressing and path determination?

A. Physical Layer

B. Data Link Layer

C. Network Layer

D. Session Layer

Question 193. What is the term for the OSI model layer that provides reliable data transfer services to the upper layers?

A. Network Layer

B. Transport Layer

C. Session Layer

D. Presentation Layer

Question 194. In the context of network security, what is the purpose of a firewall operating at the Transport layer of the OSI model?

A. To filter packets based on IP addresses

B. To encrypt data

C. To control access based on port numbers

D. To manage physical connections

Question 195. What type of attack targets the Transport layer of the OSI model by exploiting the TCP three-way handshake?

A. ARP spoofing

B. SQL injection

C. SYN flood

D. DNS cache poisoning

Question 196. Which protocol operates at the Transport layer and provides connectionless, unreliable data transfer?

A. TCP

B. UDP

C. IP

D. HTTP

Question 197. What is the primary function of the Network layer in the OSI model?

A. Establishing end-to-end connections

B. Routing data between networks

C. Providing reliable data transfer

D. Managing physical media

Question 198. Which of the following is NOT typically a concern addressed by the Transport layer of the OSI model?

A. Flow control

B. Error detection

C. Routing

D. Segmentation and reassembly

Question 199:

In the context of Information Systems Security, what term describes software that employs various methods to display advertisements on compromised computers?

A) AdMalware

B) Adware

C) Adpush

D) Advirus

Question 200:

Within Information Systems Security, who is responsible for examining and confirming that security policies are correctly implemented and the resulting security measures are sufficient?

A) Accountant

B) Tester

C) Inspector

D) Auditor

Question 201:

Which IPSec protocol provides authentication, integrity, and non-repudiation in Information Systems Security?

A) Sequence Number

B) Authentication Digest

C) Authentication Header

D) Security Parameter Index

Question 202:

In legal proceedings, what term refers to any statement made in a document presented to the court as proof of a disputed fact?

A) Circumstantial Evidence

B) Supreme Evidence

C) Documentary Evidence

D) Non-circumstantial Evidence

Question 203:

James Kirk has been assigned to create a policy outlining the duration for which data should be retained and when it should be eliminated. What concept does this policy address?

A) Data reduction

B) Data retention

C) Data remanence

D) Audit logging

Question 204:

Under the Children's Online Privacy Protection Act (COPPA), which category of websites is subject to regulation?

A) Financial websites not operated by financial institutions

B) Healthcare websites that gather personal information

C) Websites that collect information from children

D) Financial websites operated by financial institutions

Question 205:

In Information Systems Security, what term describes an algebraic manipulation aimed at reducing the complexity of a cryptographic algorithm by focusing on the logic of the algorithm itself?

A) Dynamic Attack

B) Analytic Attack

C) Cipher Attack

D) Math Attack

Question 206:

What system of access control in Information Systems Security involves authorization verification performed by various entities distributed throughout a system?

A) Decentralized Access Control

B) Asymmetric Access Control

C) Centralized Access Control

D) Public Access Control

Question 207:

James Kirk is configuring egress filtering on his network, examining outbound traffic to the Internet. His organization uses the public address range 12.8.195.0 /24. Which of the following destination addresses should be allowed to leave the network?

A) 10.8.15.9

B) 12.8.195.15

C) 192.168.109.55

D) 129.53.44.124

Question 208:

Which networking protocol is responsible for translating between MAC addresses and IP addresses?

A) ARP

B) DNS

C) TCP

D) UDP

Question 209:

When Obadiah Stane enters his organization's data center, he must use a smart card to pass through one set of doors, wait for them to close, and then use his card again to access a second set of doors that lock behind him. What type of security control is this, and what is it called?

A) A preventative access control; a mantrap

B) A physical control; a one-way trap door

C) A logical control; dual-swipe authorization

D) A directive control; one-way access corridor

Question 210:

What cell-switching technology, unlike packet-switching technologies such as Frame Relay, uses virtual circuits and fixed-size frames or cells to guarantee throughput, making it ideal for voice and video conferencing in WANs?

A) Symmetric Transfer Mode (STM)

B) Synchronous Transfer Mode (STM)

C) Asymmetric Transfer Mode (ATM)

D) Asynchronous Transfer Mode (ATM)

Question 211:

When labeling media based on the classification of the data it contains, what principle is typically applied regarding the labels?

A) The media is labeled with the lowest level of classification the data it contains

B) The media is labeled based on the highest classification level of the data it contains

C) The media is labeled with all levels of classification of the data it contains

D) The data is labeled based on its integrity requirements

Question 212:

Which of the following describes a single system designed to lure attackers by appearing to contain sensitive information or other valuable resources?

A) Pseudoflaw

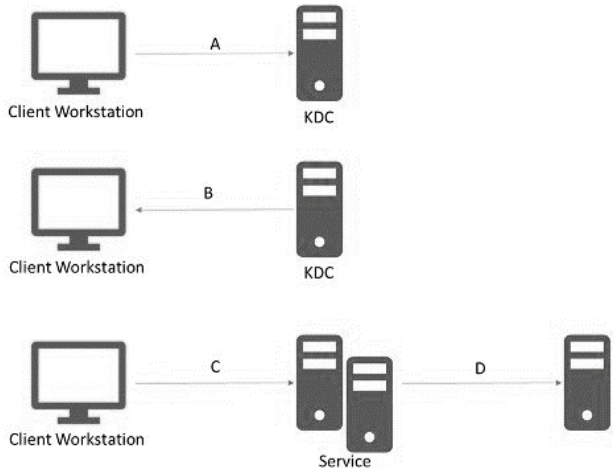
B) Honeynet

C) Darknet

D) Honeypot

Question 213:

In Kerberos authentication and authorization, what component(s) does a service being accessed use to validate the ticket?



A) The client workstation and the KDC

B) The KVS

C) The client workstation supplies it in the form of a client-to-server ticket and an authenticator

D) The KDC

Question 214:

Which encryption protocol, developed by Netscape, is designed to secure communications between a web server and a browser?

A) SSH

B) SSL

C) SHA

D) SAML

Question 215:

What type of DoS attack occurs when an attacker sends numerous SYN packets to a victim with spoofed source and destination IP addresses matching the victim's, causing the system to believe it sent a TCP/IP session opening packet to itself?

A) Land Attack

B) Protocol Attack

C) UDP Attack

D) ICMP Attack

Question 216:

Harry Osborn handles access control requests for his organization. A user explains that they need access to the human resources database to complete a headcount analysis requested by the CFO. What principle has the user successfully demonstrated to Harry?

A) Isolation

B) Clearance

C) Separation of Duties

D) Need to Know

Question 217:

Uptown Records Management recently contracted with a hospital for secure storage of medical records. The hospital is a HIPAA-covered entity. What type of agreement must the two organizations sign to comply with HIPAA?

A) NCA

B) BAA

C) NDA

D) SLA

Question 218:

Allen's Wrenches has developed a new manufacturing process for its product. They plan to use this technology internally without sharing it with others and want it to remain protected for as long as possible. Which type of intellectual property protection is best suited for this situation?

A) Copyright

B) Trademark

C) Patent

D) Trade Secret

Question 219:

In Information Systems Security, what term describes a database of pre-computed hashes for guessed passwords that can be used in a password attack?

A) Malware Table

B) Dictionary List

C) Drive-by Attack

D) Rainbow Table

Question 220:

Which of the following actions is not mandated by the EU General Data Protection Regulation?

A) Organizations must have a dispute resolution process for privacy issues

B) Organizations must provide individuals with lists of employees with access to information

C) Organizations must use proper mechanisms to protect data against unauthorized disclosure

D) Organizations must allow individuals to opt out of information sharing

Question 221:

What type of firewall filters traffic based on the Internet service (or application) used to transmit or receive data?

A) First-Generation firewall

B) Web-Service Gateway firewall

C) Root-Level firewall

D) Application-Level Gateway firewall

Question 222:

What technique or tool allows analysts to search through data warehouses and identify potentially correlated information within historical data?

A) Data Abstraction

B) Data Extraction

C) Data Mining

D) Data Tapping

Question 223:

In network infrastructure, what term describes the system that provides wired connections between the equipment room and telecommunications rooms, including cross-floor connections?

A) Physical Distribution Matrix

B) Hardwired Relay

C) Underlying Cable Network

D) Backbone Distribution System

Question 224:

Which markup language defines rules for document formatting and encoding that is both human and machine-

readable?

A) ASCII

B) XML

C) HTML

D) SQL

Question 225:

IP addresses such as 10.10.10.10 and 172.19.24.21 are examples of what type of IP address?

A) Public IP addresses

B) Private IP addresses

C) Prohibited IP addresses

D) Class B IP ranges

Question 226:

What cloud computing concept can provide not only on-demand operating solutions but also complete outsourcing of IT infrastructure?

A) Software as a Service (SaaS)

B) IT as a Service (ITaaS)

C) Infrastructure as a Service (IaaS)

D) Fundamentals as a Service (FaaS)

Question 227:

What type of network cable consists of four pairs of wires twisted around each other and then sheathed in a PVC insulator?

A) 10-4Base

B) 4BaseT

C) 10/4BaseT

D) 10BaseT

Question 228:

In Information Systems Security, what term describes an evaluation to determine if a safeguard effectively improves security without excessive cost?

A) ROI Analysis

B) Break-Even Analysis

C) Payback Period Analysis

D) Cost/Benefit Analysis

Question 229:

What term in Information Systems Security refers to an agreement between multiple individuals to perform an unauthorized or illegal action?

A) A Conspiracy

B) Collusion

C) Mutiny

D) Larceny

Question 230:

What common characteristic do Python, C++, Java, and C# share?

A) Imperative and procedural programming languages

B) High-level programming languages

C) Compiled imperative programming languages

D) Object-oriented languages

Question 231:

What term describes a registered word, slogan, or logo used to identify a company and its products or services?

A) Brand

B) Copyright

C) Patent

D) Trademark

Question 232:

What practice involves an organization improving its overall security by rotating employees among various job positions?

A) Staff Attrition

B) Job Shadowing

C) Job Rotation

D) Position Sharing

Question 233:

What type of cabling transmits light instead of electrical signals?

A) Twisted Pair

B) Crossover

C) Fiber-Optic

D) Coaxial

Question 234:

Frank Castle wants to allow a partner organization's Active Directory forest (B) to access his domain's forest resources but doesn't want to allow users in his domain to access B's resources. He also doesn't want the trust to flow upward through the domain tree as it is formed. What should he do?

A) Set up a two-way non-transitive trust

B) Set up a one-way non-transitive trust

C) Set up a one-way transitive trust

D) Set up a two-way transitive trust

Question 235:

In Information Systems Security, what process is used when a traveler presents their ticket and driver's license at the

airport to check bags and receive a boarding pass?

A) Authorization

B) Encryption

C) Identification

D) Authentication

Question 236:

Which mathematical operation, when substituted for the [?] shown here, would make the equations correct?

8 [?] 6 = 2

8 [?] 4 = 0

10 [?] 3 = 1

10 [?] 2 = 0

A) XOR

B) NAND

C) DIV

D) MOD

Question 237:

What form of social engineering attack uses the threat of malicious code to trick users into damaging their own system?

A) Trojan

B) Eavesdropping

C) Spoof

D) Hoax

Question 238:

What term refers to the practice of gathering multiple pieces of non-sensitive information and combining or

aggregating them to obtain sensitive information, often used in reconnaissance attacks?

A) Password attack

B) Eavesdropping attack

C) Access aggregation

D) Birthday attack

Question 239:

In Information Systems Security, what term describes any security mechanism, tool, or practice that can deter and mitigate undesirable actions or events?

A) Responsive Control

B) Detective Control

C) Preventative Control

D) Security Control

Question 240:

Hannibal King wants to ensure that third-party users of his services' API can be tracked to prevent abuse. What should he implement to help with this?

A) Session IDs

B) API buffer

C) API firewall

D) API keys

Question 241:

Which Kerberos service generates a new ticket and session keys and sends them to the client?

A) TGT

B) TGS

C) AS

D) KDC

Question 242:

The removal of a hard drive from a PC before it is retired and sold as surplus is an example of what type of action?

A) Purging

B) Sanitization

C) Destruction

D) Degaussing

Question 243:

What document is used to protect confidential information within an organization from being exposed by a former employee or other person with privileged information?

A) Non-Solicitation Agreement (NSA)

B) Noncompete Agreement (NCA)

C) Nondisclosure Agreement (NDA)

D) Master Protection Agreement (MPA)

Question 244:

What layer 2 protocol is used to transmit data over synchronous communication lines, supports full-duplex communications, both point-to-point and multipoint connections, offers flow control, and includes error detection and correction?

A) High-Level Data Link Control (HDLC)

B) Synchronous Data Encryption (SDE)

C) Centralized Data Synchronous Control (CDSC)

D) Asynchronous Data Encryption (ADE)

Question 245:

Which US law mandates that government agencies maintain only necessary records for conducting their business,

destroy those records when no longer needed, and provides a formal procedure for individuals to access and request amendments to their records?

A) Health Insurance Portability and Accountability Act of 1996

B) Global Data Privacy Act of 1985

C) Privacy Act of 1974

D) Data Protection and Privacy Legislation Act

Question 246:

At which layer of the OSI model is data sent as bits?

A) Transport

B) Data link

C) Physical

D) Network

Question 247:

What is the primary function of the Presentation Layer in the OSI model?

A) Interact directly with user data

B) Prepare data for use by the Application Layer

C) Manage network connections

D) Handle physical transmission of data

Correct Answers & Explanations

Question 1

C) Clearing (Correct Answer)

Explanation: Clearing is the appropriate method for erasing media that will be reused within the same protected

environment. It involves overwriting all addressable storage locations with a single character or zeros, making the data unrecoverable through simple data recovery methods. This process is sufficient for media that will remain within the same security boundary, as it prevents casual access to the previous data while allowing the media to be reused.

Question 2

D) Identity as a Service (Correct Answer)

Explanation: IDaaS stands for Identity as a Service, which is a cloud-based authentication infrastructure that allows organizations to manage user identities and access control. By implementing an IDaaS system, Nick Fury is adopting a cloud-based solution for identity and access management, which can provide scalable, flexible, and centralized control over user authentication and authorization across various applications and services.

Question 3

D) Logical Access Control (Correct Answer)

Explanation: Logical Access Control refers to the use of hardware or software mechanisms to manage access to resources and systems. This encompasses a wide range of technologies and methods, including encryption, smart cards, passwords, biometrics, access control lists, firewalls, and intrusion detection systems. These controls are designed to protect digital assets and information systems by regulating who or what can view or use resources in a computing environment.

Question 4

A) CYOD (Correct Answer)

Explanation: CYOD stands for "Choose Your Own Device," which is a mobile device program that provides users with a selection of approved devices to choose from for implementation in the workplace. This approach allows

organizations to maintain some control over the types of devices used while still offering employees a degree of choice. It strikes a balance between security and user preference, unlike BYOD (Bring Your Own Device) which allows any personal device, or company-issued devices which offer no choice.

Question 5

D) DNS Poisoning (Correct Answer)

Explanation: DNS Poisoning, also known as DNS cache poisoning or DNS spoofing, is the practice of falsifying DNS information used by a client to reach a desired system. This is typically accomplished by inserting false data into a DNS cache or zone file. The attacker's goal is to redirect traffic intended for legitimate websites to malicious sites, potentially leading to phishing attacks, malware distribution, or unauthorized access to sensitive information.

Question 6

B) Risk Avoidance (Correct Answer)

Explanation: Risk Avoidance is the strategy of choosing alternative options or activities that carry less associated risk compared to the default, common, expedient, or inexpensive option. This approach involves completely eliminating exposure to specific threats by avoiding the risk-causing activity altogether. It's often employed when the potential impact of a risk is deemed too high and no other risk management strategies are deemed sufficient.

Question 7

B) An application level-gateway firewall (Correct Answer)

Explanation: An application level-gateway firewall, also known as a proxy firewall, employs multiple proxy servers to filter traffic based on analysis of the protocols used for each service. This type of firewall operates at the application layer of the OSI model, allowing it to inspect the content of

the traffic and make decisions based on the specific application protocols being used. It provides a high level of security by understanding and filtering the traffic of specific applications.

Question 8

A) Packet Sniffing (Correct Answer)

Explanation: Packet Sniffing is the practice of intercepting and logging traffic passing over a digital network. It involves capturing packets of data flowing across a computer network and analyzing their contents. This technique can be used legitimately by network administrators for troubleshooting and monitoring network performance, but it can also be employed maliciously to capture sensitive information like passwords, email contents, or other private data transmitted over the network.

Question 9

B) Distributed Data Model (Correct Answer)

Explanation: The Distributed Data Model is a database architecture where information is stored across multiple databases while remaining logically connected. Users perceive it as a single entity despite it consisting of numerous interconnected parts over a network. In this model, each field can have multiple children and parents, resulting in many-to-many data mapping relationships. This approach allows for improved scalability, reliability, and performance in large-scale systems.

Question 10

B) Iris Scan (Correct Answer)

Explanation: An Iris Scan is a biometric factor that utilizes a unique physiological characteristic of an individual. The iris, which is the colored part of the eye surrounding the pupil, has complex patterns that are unique to each person and remain stable throughout life. Iris recognition systems

capture and analyze these patterns, providing a highly accurate and reliable method of biometric identification. Unlike passphrases or RFID, which are knowledge or possession factors, iris scans directly measure a physical attribute of the person.

Question 11

D) Point-to-Point Protocol (PPP) (Correct Answer)

Explanation: The Point-to-Point Protocol (PPP) is a full-duplex protocol used for transmitting TCP/IP packets over various non-LAN connections such as modems, ISDN, VPNs, and Frame Relay. It's widely supported as the preferred transport protocol for dial-up Internet connections. PPP provides a standard method for transporting multi-protocol datagrams over point-to-point links, offering features like authentication, encryption, and compression.

Question 12

C) Peer-to-Peer (P2P) (Correct Answer)

Explanation: Peer-to-Peer (P2P) is a network and distributed application solution that divides tasks and workloads among equal participants. In a P2P network, each node (peer) acts as both a client and a server, sharing resources directly with other nodes without the need for central coordination by servers. This decentralized approach allows for efficient distribution of resources and workloads, making it popular for file sharing, cryptocurrency networks, and distributed computing projects.

Question 13

B) CA's public key (Correct Answer)

Explanation: In an asymmetric cryptosystem using digital certificates, Mike would use the Certificate Authority's (CA's) public key to verify the authenticity of Renee's digital certificate. The CA's public key is used to decrypt the digital signature on the certificate, which was encrypted with the

CA's private key. This process verifies that the certificate was indeed issued by the trusted CA and hasn't been tampered with, thus confirming Renee's identity and public key.

Question 14

B) Federal Information Security Management Act (FISMA) (Correct Answer)

Explanation: The Federal Information Security Management Act (FISMA), enacted in 2002, mandates that federal agencies implement an information security program covering their operations and includes the activities of contractors in their security management programs. FISMA aims to enhance the security of federal information systems by requiring agencies to develop, document, and implement agency-wide information security programs. It also emphasizes the importance of continuous monitoring and risk assessment in maintaining the security of federal information systems.

Question 15

C) Ring (Correct Answer)

Explanation: A Ring topology is a network configuration where each computer is connected to another in a circular formation, with the last one linked back to the first. In this arrangement, data travels from one device to the next in a circular path until it reaches its destination. Ring topologies typically use token passing to control network access, where a token circulates around the ring and a device can only transmit data when it possesses the token.

Question 16

D) Kerckchoff principle (Correct Answer)

Explanation: The Kerckhoffs principle, named after Auguste Kerckhoffs, is a fundamental concept in cryptography that states the security of a cryptosystem should rely solely on

the secrecy of the key, not on the secrecy of the algorithm. This principle advocates for the public availability of all algorithms while maintaining the privacy of all keys. It encourages the use of well-known, thoroughly tested algorithms rather than relying on "security through obscurity," which can lead to vulnerabilities if the secret algorithm is discovered or reverse-engineered.

Question 17

B) Differential Backup (Correct Answer)

Explanation: A Differential Backup is a type of data backup that stores only the files that have been modified since the most recent full backup. Unlike incremental backups, which only store changes since the last backup of any type, differential backups always reference the last full backup. This method provides a balance between storage efficiency and ease of restoration, as only the last full backup and the most recent differential backup are needed to restore all data.

Question 18

A) Outlier detection (Correct Answer)

Explanation: Outlier detection is a data mining technique that develops models of normal user behavior based on various factors such as organizational affiliation, physical location, time of day, and other attributes. This method is used to identify patterns or data points that do not conform to expected behavior. In the context of security, outlier detection can be used to identify potentially suspicious activities or anomalies that deviate from established norms, which could indicate security threats or unauthorized access attempts.

Question 19

B) Blackout (Correct Answer)

Explanation: A Blackout refers to a complete loss of electrical power in a particular area. It's a more severe and widespread power outage compared to localized failures. Blackouts can be caused by various factors including equipment failure, natural disasters, or overloading of the power grid. In the context of information security and business continuity, understanding and preparing for blackouts is crucial as they can significantly impact operations and the availability of critical systems.

Question 20

D) DNS Pharming (Correct Answer)

Explanation: DNS Pharming is a cyber attack that involves the malicious redirection of a legitimate website's URL or IP address to a fake site hosting a false version of the original valid site. This is typically accomplished by exploiting vulnerabilities in DNS server software or through DNS cache poisoning. Unlike phishing, which relies on users clicking on deceptive links, pharming can redirect users to malicious sites even when they correctly type the intended URL, making it a more sophisticated and dangerous form of attack.

Question 21

C) Birthday attack (Correct Answer)

Explanation: A Birthday attack is a type of cryptographic attack against hash functions. It exploits the mathematics behind the birthday problem in probability theory to find collisions in hashing algorithms. The goal is to find two different inputs that produce the same hash output, which can be used to compromise the integrity of digital signatures or other security mechanisms that rely on hash functions. This attack is particularly relevant to the security of hash algorithms used in verifying the integrity of messages, software, or digital signatures.

Question 22

B) Irises remain more consistent over time compared to other factors (Correct Answer)

Explanation: Iris scans are considered superior to most other biometric factors primarily because irises remain more consistent over time compared to other physical characteristics. The complex patterns in the iris are formed by 8 months of age and remain stable throughout a person's lifetime, unlike fingerprints which can wear or be altered, or facial features which change with age. This consistency ensures long-term reliability and accuracy in identification, making iris scans a highly effective biometric method.

Question 23

B) Probability and Impact (Correct Answer)

Explanation: In a qualitative risk assessment, the two crucial risk elements that should be given the most weight are Probability and Impact. Probability refers to the likelihood of a risk event occurring, while Impact assesses the potential consequences if the risk does materialize. By focusing on these two factors, organizations can prioritize risks effectively, allocating resources to address high-probability, high-impact risks first. This approach provides a comprehensive view of the risk landscape, enabling more informed decision-making in risk management strategies.

Question 24

A) Beta Testing (Correct Answer)

Explanation: Beta Testing is a type of software testing performed by actual users of a software application in a real environment. It is considered a form of external User Acceptance Testing because it involves end-users or customers testing the product in real-world conditions before its official release. Beta testing helps identify issues that may not have been caught during internal testing,

provides feedback on user experience, and verifies if the product meets customer expectations. This phase is crucial for gathering real-world usage data and uncovering any remaining bugs or usability issues.

Question 25

C) Process Isolation (Correct Answer)

Explanation: Process Isolation is a technology that ensures an operating system allocates distinct memory spaces for each application running on a system. This security measure prevents one process from accessing or interfering with the memory space of another process. By isolating processes, the operating system enhances system stability and security, preventing malicious or faulty applications from affecting other running programs or the system as a whole. This is a fundamental concept in modern operating systems, crucial for maintaining the integrity and confidentiality of data across different applications.

Question 25

C) Process Isolation (Correct Answer)

Explanation: Process Isolation is a crucial security technology in operating systems that ensures each application runs in its own distinct memory space. This prevents one application from accessing or interfering with the memory of another, enhancing system stability and security. It's fundamental in protecting against malicious software and preventing errors in one application from affecting others.

Question 26

B) Hearsay Evidence (Correct Answer)

Explanation: Hearsay Evidence refers to statements made outside of court by someone other than the witness testifying, offered to prove the truth of the matter asserted. It's generally inadmissible in court due to its potential

unreliability, as the original declarant isn't present for cross-examination. However, there are numerous exceptions to the hearsay rule in legal proceedings.

Question 27

C) Concurrency (Correct Answer)

Explanation: Concurrency in database management is a mechanism that ensures data integrity and availability when multiple users are accessing or modifying the same data simultaneously. It uses locking mechanisms to prevent conflicting changes, allowing an authorized user to make modifications while temporarily blocking others from accessing the same data. This process helps maintain data consistency and prevents data corruption in multi-user environments.

Question 28

D) Spike (Correct Answer)

Explanation: A Spike in electrical terms refers to a brief, sudden increase in voltage, typically lasting microseconds. Unlike a surge, which lasts longer, a spike is a very short duration event. Spikes can be caused by lightning strikes, power outages, or switching of large electrical loads. They can potentially damage sensitive electronic equipment, making surge protectors an important safeguard for valuable devices.

Question 29

A) Digital Signature Standard (DSS) (Correct Answer)

Explanation: The Digital Signature Standard (DSS) is a Federal Information Processing Standard that specifies algorithms for digital signatures. It mandates that all federally approved digital signature algorithms must employ a secure hashing function. This requirement ensures the integrity and non-repudiation of digital signatures used in government and many private sector applications,

enhancing the security and trustworthiness of electronic transactions and documents.

Question 30

B) Frequency Hopping Spread Spectrum (FHSS) (Correct Answer)

Explanation: Frequency Hopping Spread Spectrum (FHSS) is an early implementation of spread spectrum technology. It transmits radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver. This technique improves resistance to interference and interception, and allows multiple devices to share the same frequency band. FHSS was initially developed for military communications but is now used in various civilian applications, including Bluetooth technology.

Question 31

D) Token (Correct Answer)

Explanation: A Token, classified as a Type 2 Authentication Factor (something you have), generates dynamic passwords based on time or algorithm-based systems. These devices produce one-time passwords that change frequently, typically every 30 to 60 seconds. Tokens enhance security by providing a second factor of authentication beyond just a username and password, making it much harder for unauthorized users to gain access even if they obtain the user's static credentials.

Question 32

D) Assurance (Correct Answer)

Explanation: Assurance refers to the degree of confidence that security requirements are met. It involves the processes, procedures, and methodologies implemented to ensure that a system or organization meets its security objectives. Assurance activities can include security audits,

testing, formal verification methods, and compliance checks. Higher levels of assurance typically require more rigorous and comprehensive evaluation processes.

Question 33

A) Family Educational Rights and Privacy Act (FERPA) (Correct Answer)

Explanation: The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. It applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's educational records and transfers these rights to the student when they reach the age of 18 or attend a school beyond the high school level. The act regulates how schools handle student information and who can access it.

Question 34

A) TCP (Correct Answer)

Explanation: SYN floods exploit the implementation of the Transmission Control Protocol (TCP). In a SYN flood attack, an attacker sends a succession of SYN (synchronize) requests to a target's system, often with a spoofed source IP address. This floods the target with half-open connections, exhausting its resources and preventing legitimate users from establishing connections. TCP's three-way handshake process is specifically targeted in this type of Denial of Service attack.

Question 35

A) CER (Correct Answer)

Explanation: CER stands for Crossover Error Rate, a metric used to summarize the operating characteristics of a biometric security system. It's the point at which the False Acceptance Rate (FAR) equals the False Rejection Rate

(FRR). A smaller CER indicates better overall system performance, as it represents a balance between falsely accepting unauthorized users and falsely rejecting authorized ones. The CER is crucial for comparing and evaluating different biometric systems or configurations.

Question 36

B) Sandboxing (Correct Answer)

Explanation: Sandboxing is a security technique that creates an isolated environment for running applications, preventing them from interacting with other applications or the underlying system. This containment strategy allows potentially unsafe or untrusted programs to be executed without risking harm to the host system or other applications. Sandboxing is commonly used in web browsers, for testing new software, and in cybersecurity for analyzing malware behavior in a controlled environment.

Question 37

A) RSA (Correct Answer)

Explanation: RSA (Rivest-Shamir-Adleman) is a widely used public-key cryptosystem developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. It's based on the practical difficulty of factoring the product of two large prime numbers. RSA is used for secure data transmission and digital signatures. Its security relies on the assumption that factoring large numbers is computationally infeasible, making it a cornerstone of many secure communication protocols on the internet.

Question 38

C) Router (Correct Answer)

Explanation: A Router is the most appropriate network device for Freddy Krueger to deploy to connect his network to other networks while controlling traffic. Routers operate at the network layer (Layer 3) of the OSI model, making

decisions about where to send data packets based on IP addresses. They can connect different types of networks, implement access control lists for basic traffic filtering, and provide a barrier between internal and external networks, making them essential for network connectivity and basic security.

Question 39

B) Health Information Technology for Economic and Clinical Health Act (HITECH) (Correct Answer)

Explanation: The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, significantly expanded HIPAA rules. It strengthened privacy and security protections for health information, increased potential legal liability for non-compliance, and provided for more enforcement. HITECH also promoted the adoption and meaningful use of health information technology, and introduced new breach notification requirements for covered entities and business associates.

Question 40

A) Gray box (Correct Answer)

Explanation: Gray box penetration testing is an approach where the tester is provided with partial knowledge about the target systems, including information on the scope and target systems, but without full visibility into configurations or other details. This method balances the realistic approach of black box testing (where the tester has no prior knowledge) with the efficiency of white box testing (where the tester has full information). Gray box testing allows for more focused and efficient testing while still simulating a semi-realistic attack scenario.

Question 41

D) RSA (Correct Answer)

Explanation: RSA (Rivest-Shamir-Adleman) supports the goal of nonrepudiation in cryptography. As a public key algorithm, RSA allows for the creation of digital signatures. When a message is signed with a user's private key, anyone can verify the signature using the corresponding public key. This process ensures that the sender cannot deny having sent the message, as only they should have access to their private key. This property of RSA makes it crucial for applications requiring nonrepudiation, such as legal documents and financial transactions.

Question 42

B) Single Point of Failure (Correct Answer)

Explanation: A Single Point of Failure (SPOF) refers to any component in an infrastructure that, if it fails, would cause a significant disruption or complete system failure. This could be a critical server, a main power supply, or a key network link. Identifying and mitigating SPOFs is crucial in system design and disaster recovery planning. Redundancy and fault-tolerant designs are often employed to address SPOFs, ensuring continuity of operations even if a critical component fails.

Question 43

A) Meet-in-the-Middle Attack (Correct Answer)

Explanation: A Meet-in-the-Middle Attack is a cryptographic attack that targets systems using multiple rounds of encryption. The attacker encrypts the plaintext with all possible keys (k1) and decrypts the ciphertext with all possible keys (k2), looking for a match in the middle. This approach can significantly reduce the time needed to break certain encryption schemes compared to a brute-force attack. It's particularly relevant to some block ciphers and has influenced the design of many modern cryptographic protocols to resist such attacks.

Question 44

A) Gate (Correct Answer)

Explanation: A Gate is a controlled exit and entry point in a fence or barrier. In physical security, gates play a crucial role in managing access to protected areas. They can be equipped with various security measures such as locks, access control systems, or guards to regulate who can enter or exit. Gates are essential components of perimeter security, allowing for controlled movement while maintaining the integrity of the protected boundary.

Question 45

B) Compliance Testing (Correct Answer)

Explanation: Compliance Testing is used to verify that a system adheres to laws, regulations, baselines, guidelines, standards, and policies. This type of testing is crucial in maintaining security and ensuring that an organization meets both internal and external requirements. It involves checking systems and processes against specific criteria set by regulatory bodies or industry standards. Compliance testing helps organizations avoid legal issues, maintain certifications, and ensure that their security practices meet required standards.

Question 46

B) Parallel Run (Correct Answer)

Explanation: A Parallel Run is a type of new system deployment testing where both the new system and the old system are run simultaneously for a period of time. This approach allows for direct comparison of outputs and performance between the two systems. It's particularly useful for critical systems where any discrepancies or issues with the new system can be identified without disrupting ongoing operations. Parallel runs provide a safety net during

transitions, ensuring that the new system performs as expected before fully replacing the old one.

Question 47

D) Worm (Correct Answer)

Explanation: A Worm is a type of malicious code that is self-replicating and designed to spread from system to system without direct user interaction. Unlike viruses, which require a host file to propagate, worms can operate independently. Their primary purpose is often to replicate and spread, consuming network bandwidth and resources. While not always directly harmful to host systems, worms can carry payloads that perform malicious actions, gather information, or create backdoors for future access. Their ability to spread rapidly makes them particularly dangerous in networked environments.

Question 48

C) A TCP packet; PSH and URG are used to clear the buffer and indicate that the data is urgent (Correct Answer)

Explanation: This packet is a TCP packet with both PSH (Push) and URG (Urgent) flags set. In TCP, the PSH flag instructs the receiving system to push all buffered data to the receiving application immediately, without waiting for the buffer to fill. The URG flag indicates that the packet contains urgent data that should be processed immediately. Together, these flags signal that the data in this packet is important and should be handled promptly, bypassing normal buffering procedures.

Question 49

D) ECPA (Correct Answer)

Explanation: The Electronic Communications Privacy Act (ECPA) of 1986 would likely be the law violated in this scenario. ECPA extends government restrictions on wire taps to include transmitted electronic data, making it illegal to

intercept or access stored electronic communications without authorization. If a customer is exploiting a vulnerability to read other customers' emails, they would be violating the provisions of ECPA that protect the privacy of stored electronic communications. This act covers various forms of electronic communication, including email, and prohibits unauthorized access or interception.

Question 50

D) Brewer and Nash Model (Correct Answer)

Explanation: The Brewer and Nash Model, also known as the Chinese Wall Model, is designed to allow access controls to change dynamically based on a user's previous activity. It's a type of state machine model that prevents conflicts of interest in commercial organizations. The model ensures that a user who has accessed information from one dataset cannot access conflicting information from another dataset. This dynamic approach to access control makes it particularly useful in scenarios where maintaining confidentiality and preventing conflicts of interest are crucial, such as in financial or consulting firms.

Question 51

B) DevOps (Correct Answer)

Explanation: DevOps is specifically designed to address the issue of collaboration between developers and operations personnel. It promotes a culture of shared responsibility, continuous integration, and automated deployment, breaking down silos between teams and fostering better communication and cooperation throughout the software development lifecycle.

Question 52

D) Computer Incident Response Team (CIRT) (Correct Answer)

Explanation: CIRT is an alternative name for the Emergency Response Team in information security. It consists of InfoSec professionals who are trained and equipped to handle various security incidents and system issues, providing rapid response and mitigation strategies during cybersecurity crises.

Question 53

D) Ethernet (Correct Answer)

Explanation: Ethernet is a widely used shared media LAN technology. It provides a standardized method for connecting multiple devices in a local area network, allowing for efficient data transmission and communication between networked devices using a shared medium.

Question 54

A) Attacker (Correct Answer)

Explanation: In the context of information systems security, an attacker refers to any individual who attempts to carry out malicious actions against a system. This term encompasses various types of malicious actors, including hackers, cybercriminals, and other threat agents who seek to compromise system security.

Question 55

D) ALE (Correct Answer)

Explanation: ALE stands for Annual Loss Expectancy, which is the metric Gordon has identified. It represents the expected annual damage that flooding would cause to his facilities. ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annual Rate of Occurrence (ARO), providing a quantitative measure of potential yearly losses due to a specific risk.

Question 56

D) Checklist Test (Correct Answer)

Explanation: A Checklist Test is a procedure in disaster recovery planning where disaster recovery checklists are distributed to team members for their examination. This type of test helps ensure that all team members are familiar with their roles and responsibilities during a disaster recovery scenario without actually simulating the disaster.

Question 57

D) Utilize VLANs (Correct Answer)

Explanation: To address the security audit failure due to a single flat broadcast domain, Sue should propose implementing VLANs (Virtual Local Area Networks). VLANs allow for the logical segmentation of a network, creating separate broadcast domains. This solution prevents traffic sniffing between different functional groups, enhancing network security and performance.

Question 58

B) IDE forcing (Correct Answer)

Explanation: IDE forcing is not considered a standard code review process. The other options (over-the-shoulder, email pass-around, and pair programming) are recognized code review methods. IDE forcing typically refers to enforcing coding standards through integrated development environment settings, which is not a review process but a preventive measure.

Question 59

B) ElGamal (Correct Answer)

Explanation: ElGamal is the cryptosystem that extends the mathematical principles of the Diffie-Hellman key exchange algorithm to support a complete public key cryptosystem for message encryption and decryption. It provides both encryption and digital signature capabilities based on the difficulty of computing discrete logarithms.

Question 60

C) Internet of Things (IoT) (Correct Answer)

Explanation: The Internet of Things (IoT) refers to the network of interconnected devices that can communicate with each other or a control console via the Internet. These devices are capable of influencing and monitoring the physical world, ranging from smart home appliances to industrial sensors and beyond.

Question 61

D) Test directories often contain scripts that can be exploited (Correct Answer)

Explanation: Steve is concerned about the vulnerability because test directories often contain scripts that can be exploited. These directories may include development or debugging scripts that were not intended for production use and might have security flaws. Attackers can potentially leverage these scripts to gain unauthorized access or execute malicious code on the server.

Question 62

C) Cardinality (Correct Answer)

Explanation: In the context of relational databases, cardinality refers to the number of rows in a table. It is an important concept in database design and query optimization, as it affects the performance and efficiency of database operations.

Question 63

C) SPML (Correct Answer)

Explanation: SPML (Service Provisioning Markup Language) is the OASIS standard markup language used to generate provisioning requests both within organizations and with third parties. It provides a standardized way to manage user

accounts, access rights, and resource allocation across different systems and organizations.

Question 64

B) Man-in-the-Middle (MitM) Attack (Correct Answer)

Explanation: A Man-in-the-Middle (MitM) attack is a type of cyberattack where malicious users position themselves between two communication endpoints. In this scenario, the attacker intercepts and potentially alters the communication between the client and server, while both parties remain unaware of the third-party interference.

Question 65

D) Fragmented HTTP Flood (Correct Answer)

Explanation: A Fragmented HTTP Flood is a sophisticated DDoS attack that exploits known vulnerabilities. In this attack, bots with valid IP addresses establish legitimate connections with a web server and then send packets in tiny fragments at a very slow rate, just before timing out. This technique allows attackers to maintain active connections for extended periods without triggering defense mechanisms, potentially overwhelming the target server.

Question 66

D) End-To-End Testing (Correct Answer)

Explanation: End-To-End Testing is a software testing methodology that evaluates the entire software system from start to finish, including its integration with external interfaces. This comprehensive approach assesses the software's dependencies, data integrity, and communication with other systems, interfaces, and databases to simulate a complete production-like scenario.

Question 67

C) A baseline (Correct Answer)

Explanation: NIST SP 800-53 discusses a set of security controls as a baseline. This baseline serves as a starting point for organizations to implement a comprehensive set of security measures. It provides a foundation of security controls that can be tailored to meet specific organizational needs and risk profiles.

Question 68

A) TOCTOU (Correct Answer)

Explanation: TOCTOU (Time-of-Check to Time-of-Use) is the type of attack described. In this scenario, an attacker exploits the time gap between when a system checks a condition (like file permissions) and when it acts on that condition. By altering a symlink during this interval, an attacker can potentially gain unauthorized access or elevate privileges.

Question 69

C) Behaviour-Based Detection (Correct Answer)

Explanation: Behaviour-Based Detection is an intrusion detection mechanism used by IDS (Intrusion Detection Systems) that learns about normal activities and events on a system through observation and analysis. This approach allows the IDS to identify potential threats by detecting deviations from established normal behavior patterns, making it effective against both known and unknown threats.

Question 70

A) UDP (Correct Answer)

Explanation: UDP (User Datagram Protocol) possesses all the characteristics listed. It is connectionless, unreliable, faster due to lack of delivery guarantees, has an 8-byte packet size, doesn't wait for acknowledgments, lacks flow control, doesn't perform error checking or packet resending, and is commonly used for applications requiring fast

communication without prioritizing reliability, such as VoIP and streaming services.

Question 71

C) Onboarding (Correct Answer)

Explanation: Onboarding is the process of integrating new employees into an organization's identity and access management system. This process is also applied when an employee's role changes or when they are granted additional levels of privilege or access. It ensures that employees have the appropriate access rights and permissions needed for their roles within the organization.

Question 72

D) NAT (Correct Answer)

Explanation: NAT (Network Address Translation) is the technology Lauren should expect to be in use at the network border. NAT allows the translation of public IP addresses to private IP addresses (RFC 1918 reserved addresses) and vice versa. This explains why Lauren observes inbound traffic to a public IP address appearing inside the production network with an internal destination address.

Question 73

A) Permissions (Correct Answer)

Explanation: Permissions refer to the type of access granted to an object and the actions that can be performed on or with the object. In information security, permissions define the specific rights a user or system has to interact with files, directories, or other resources, controlling read, write, execute, or other types of access.

Question 74

B) Botmaster (Correct Answer)

Explanation: A Botmaster is the term used to describe the hacker who controls a botnet. This individual is responsible

for commanding and controlling a network of compromised computers (bots) to perform various malicious activities, such as DDoS attacks, spam distribution, or data theft.

Question 75

C) Biba Model (Correct Answer)

Explanation: The Biba Model is an integrity-focused security model based on the state machine model, employing mandatory access controls and the lattice model. It focuses on preventing unauthorized users from modifying data at higher integrity levels and preventing data from flowing from lower to higher integrity levels, thus maintaining data integrity in a system.

Question 76

D) SaaS (Correct Answer)

Explanation: SaaS (Software as a Service) is a cloud computing model that provides on-demand access to software applications over the internet without requiring local installation. Users can access these applications through a web browser, eliminating the need for complex software and hardware management on the client-side. Examples include Google Workspace, Salesforce, and Microsoft Office 365.

Question 77

D) SAML (Correct Answer)

Explanation: SAML (Security Assertion Markup Language) is the most suitable technology for D'Ken Neramani's needs. It is specifically designed for exchanging authentication and authorization information in federated identity management systems, particularly for browser-based single sign-on. SAML allows secure communication of identity information between identity providers and service providers across different security domains.

Question 78

C) Passphrase (Correct Answer)

Explanation: A passphrase is a string of characters typically longer than a password, often in the form of a natural-language sentence. It's designed to be more memorable than a complex password while still providing strong security. When entered, the system converts the passphrase into a virtual password for authentication, offering a balance between security and user-friendliness.

Question 79

C) Reporting (Correct Answer)

Explanation: During the reporting phase of the incident response process, an organization determines if it is obligated to notify law enforcement officials or other regulators about the incident. This phase involves documenting the incident, assessing its impact, and deciding on the necessary communications to stakeholders, including legal and regulatory bodies, based on the nature and severity of the incident.

Question 80

B) Lessons learned (Correct Answer)

Explanation: The lessons learned phase is where security professionals analyze the incident response process itself to identify potential areas for improvement. This phase involves reviewing the entire incident, from detection to resolution, to understand what worked well and what could be enhanced. The insights gained are used to refine and strengthen the organization's incident response capabilities for future incidents.

Question 81

A) Annualized Loss Expectancy (ALE) (Correct Answer)

Explanation: The Annualized Loss Expectancy (ALE) represents the annual cost associated with a specific realized threat against a particular asset. It is calculated by multiplying the Single Loss Expectancy (SLE) by the Annual Rate of Occurrence (ARO). ALE helps organizations quantify the potential financial impact of security risks and prioritize their risk mitigation efforts.

Question 82

D) Overwriting (Correct Answer)

Explanation: Overwriting is the most suitable technique for Pete Wisdom to securely remove data from the flash memory card while allowing for its reuse. This method involves writing new data (often random patterns) over the existing data multiple times, effectively making the original data unrecoverable. Unlike degaussing (which is ineffective on solid-state media) or physical destruction, overwriting allows the card to be reused while ensuring data security.

Question 83

D) Polyinstantiation (Correct Answer)

Explanation: Polyinstantiation is the technique Kabuki should use to prevent unauthorized access to sensitive information. In database security, polyinstantiation allows multiple instances of the same data to exist at different classification levels. This means that users with lower clearance levels would see a different (less sensitive) version of the aircraft location data, effectively hiding the true locations from those without proper clearance.

Question 84

C) Secret (Correct Answer)

Explanation: The "Secret" classification label is applied to information that, if disclosed, could cause serious damage to national security. This level requires that the potential damage be describable or identifiable by the classification

authority. It's the second-highest level of classification in the U.S. government system, below Top Secret but above Confidential.

Question 85

B) Regression testing (Correct Answer)

Explanation: Regression testing is the software testing process aimed at uncovering new bugs introduced by patches or configuration changes. It involves re-running previously completed tests to ensure that recent program or code changes have not adversely affected existing features. This type of testing is crucial for maintaining software quality and stability after modifications.

Question 86

C) Ping Flood Attack (Correct Answer)

Explanation: A Ping Flood Attack is a type of Denial of Service (DoS) attack that repeatedly sends ICMP Echo Request (ping) packets to a target system. This flood of ping requests can overwhelm the target's resources, preventing it from responding to legitimate traffic. When launched from multiple systems simultaneously, it becomes a Distributed Denial of Service (DDoS) attack, making it more potent and harder to mitigate.

Question 87

C) NTLM-based SSO (Correct Answer)

Explanation: NTLM (NT LAN Manager) based Single Sign-On (SSO) allows users to prove knowledge of their password without directly providing it. It uses a challenge-response protocol where the client and server first negotiate supported authentication types and encryption mechanisms. The user's password is then cryptographically hashed and sent to the server for authentication, enhancing security by never transmitting the actual password over the network.

Question 88

D) Transport mode does not encrypt the header of the packet (Correct Answer)

Explanation: In IPSec's ESP (Encapsulating Security Payload) transport mode, the crucial information Galia should be aware of is that it does not encrypt the header of the IP packet. Transport mode only encrypts the payload (data portion) of the IP packet, leaving the original IP header intact. This allows for routing but may expose some traffic information. It's typically used for end-to-end communications where the endpoints are the same as the security endpoints.

Question 89

A) Data Diddling (Correct Answer)

Explanation: Data Diddling refers to the act of making minor, often unauthorized alterations to data, typically with malicious intent. This can include changing data before or during input into a computer system, or altering the output of the system. It's a subtle form of data manipulation that can be difficult to detect but can have significant consequences, especially in financial or critical systems.

Question 90

D) Foreign key (Correct Answer)

Explanation: In Jackie's database design, the Company ID field in the Orders table plays the role of a Foreign Key. A foreign key is a field in one table that refers to the primary key in another table, establishing a link between the two tables. In this case, the Company ID in the Orders table references the primary key (Company ID) in the Customers table, allowing for the association of each order with a specific customer.

Question 91

C) Atomicity (Correct Answer)

Explanation: Atomicity is one of the four essential characteristics of database transactions (ACID properties). It ensures that a transaction is treated as a single, indivisible unit of work. In an atomic transaction, either all operations are completed successfully, or none of them are. If any part of the transaction fails, the entire transaction is rolled back, leaving the database in its original state as if the transaction never occurred.

Question 92

D) Clearance and need to know (Correct Answer)

Explanation: When processing an access request, Adam should verify both the user's clearance level and their need to know. Clearance refers to the user's security level or authorization, while need to know determines whether the user requires access to the specific information or resource to perform their job duties. This combination ensures that users only access information they are both authorized to see and actually need for their work.

Question 93

C) Biometrics (Correct Answer)

Explanation: Biometrics involve the use of human physiological or behavioral characteristics as authentication factors. These can include fingerprints, facial recognition, iris scans, voice patterns, or behavioral traits like typing patterns. Biometrics are used for both logical access (e.g., logging into computer systems) and physical access (e.g., entering secure areas), providing a high level of security by verifying the user's unique biological traits.

Question 94

A) Parallel test (Correct Answer)

Explanation: Mark should choose a Parallel test for his disaster recovery plan. A parallel test involves running the disaster recovery facility alongside the primary facility without disrupting normal operations. This allows for a live test of the disaster recovery systems and procedures while maintaining business continuity. It provides a realistic assessment of the disaster recovery capabilities without the risks associated with a full interruption test.

Question 95

B) OpenID (Correct Answer)

Explanation: OpenID is the technology Gwen Stacy should implement to allow users to use accounts from sites like Google on her website. OpenID is an open standard and decentralized authentication protocol that allows users to be authenticated by cooperating sites (known as Relying Parties) using a third-party identity provider service. This enables single sign-on across multiple websites without needing separate accounts for each.

Question 96

A) Denial of Service (DoS) attack (Correct Answer)

Explanation: A Denial of Service (DoS) attack is specifically designed to overwhelm a system or network, preventing it from processing legitimate requests or traffic. This type of attack floods the target with an excessive amount of traffic or requests, causing it to become unresponsive to genuine users. DoS attacks aim to disrupt normal operations and make resources or services unavailable.

Question 97

B) Set up a separate SSID using WPA2 (Correct Answer)

Explanation: For Clint's business devices, setting up a separate SSID (Service Set Identifier) using WPA2 is the most secure option. WPA2 provides robust encryption and authentication mechanisms, making it significantly more

secure than WEP or an open network. By creating a separate SSID for business devices, Clint can maintain a secure network for sensitive business operations while still offering an open network for customers. This approach balances security needs with customer service.

Question 98

A) Drive-by attacks (Correct Answer)

Explanation: Drive-by attacks, also known as drive-by downloads, are indeed a common method for spreading malware. In these attacks, cybercriminals exploit vulnerabilities in websites by inserting malicious scripts into the site's code. When unsuspecting users visit these compromised websites, the malicious code can automatically download and install malware onto their devices without any user interaction. This makes drive-by attacks particularly dangerous and effective for spreading malware.

Question 99

A) Virtual Memory (Correct Answer)

Explanation: Virtual memory is a memory management technique that uses both hardware and software to extend the computer's physical memory (RAM) by utilizing space on the hard drive. It creates the illusion of having more main memory than is physically present in the computer. The operating system manages virtual memory by swapping data between RAM and disk storage as needed, allowing the system to run larger programs or multiple programs simultaneously even when physical RAM is limited. This technique optimizes memory usage and improves overall system performance

Question 100

C) Brute-Force Attack (Correct Answer)

Explanation: A brute-force attack is a method used to uncover passwords by systematically trying all possible combinations of characters until the correct one is found. This type of attack is specifically aimed at discovering passwords for known user identities, making it the most appropriate answer in the context of Information Systems Security.

Question 101

C) Honeynet (Correct Answer)

Explanation: A honeynet is the most intricate decoy environment for an intruder. It consists of multiple interconnected honeypots, creating a network of decoy systems designed to attract and trap attackers. This complex setup provides a more realistic and engaging environment for intruders to explore, allowing security professionals to study their tactics and methods in detail.

Question 102

C) Purging (Correct Answer)

Explanation: Purging is the process of removing sensitive data from media to allow its reuse in a less secure environment. This method goes beyond simple deletion, often involving multiple overwrites of the entire storage medium to ensure that no residual data can be recovered. It's a crucial step in the lifecycle of data storage devices, especially when transitioning from high-security to lower-security environments.

Question 103

A) Footer (Correct Answer)

Explanation: In networking protocols, a footer refers to the information added at the end of a payload received from a higher-layer protocol. This additional data often includes error-checking information, sequence numbers, or other

protocol-specific details that help ensure the integrity and proper handling of the transmitted data.

Question 104

D) The severity level (Correct Answer)

Explanation: When configuring syslog, the severity level is crucial for filtering messages. By setting an appropriate severity level, administrators can ensure they receive notifications about important issues without being overwhelmed by routine operational messages. This allows for efficient monitoring and prompt response to significant events while minimizing unnecessary alerts.

Question 105

D) Single Loss Expectancy (SLE) (Correct Answer)

Explanation: Single Loss Expectancy (SLE) is the anticipated monetary loss each time an asset is exposed to a specific risk. It's a key component in risk assessment, helping organizations quantify potential losses and make informed decisions about risk mitigation strategies. SLE is typically calculated by multiplying the value of the asset by the exposure factor (the percentage of the asset's value that would be lost in a single incident).

Question 106

C) 65,536 TCP and 65,536 UDP ports (Correct Answer)

Explanation: To thoroughly examine all possible ports, both TCP and UDP port ranges from 0 to 65,535 must be scanned, totaling 65,536 ports for each protocol. This comprehensive scan ensures that no potential entry points are overlooked, although in practice, many organizations focus on commonly used ports to balance thoroughness with efficiency.

Question 107

C) Cipher (Correct Answer)

Explanation: A cipher is a system used to conceal the true meaning of a message by altering or rearranging its characters or words. It's a fundamental concept in cryptography, encompassing various techniques to achieve confidentiality. Ciphers can be simple (like substitution ciphers) or highly complex (like modern encryption algorithms), but all serve the purpose of protecting information from unauthorized access.

Question 108

D) Fail-Open (Correct Answer)

Explanation: Fail-Open refers to a system's response to failure where it defaults to an "allow" posture. In this state, the system permits access or operations when it cannot properly authenticate or authorize. While this can maintain system availability, it poses significant security risks and is generally not recommended for critical security systems.

Question 109

B) Frame relay supports multiple PVCs or a single WAN carrier connection. (Correct Answer)

Explanation: A key distinguishing feature of Frame Relay is its ability to support multiple Permanent Virtual Circuits (PVCs) over a single WAN carrier connection. This capability allows for more efficient use of network resources and greater flexibility in network design compared to X.25, which typically requires separate physical connections for each virtual circuit.

Question 110

D) Hypertext Transfer Protocol over Secure Sockets Layer (Correct Answer)

Explanation: HTTPS (Hypertext Transfer Protocol Secure) uses port 443 to establish encrypted communication sessions between web servers and browser clients. It combines HTTP with SSL/TLS protocols to provide secure,

encrypted web communications, protecting sensitive data from interception and tampering during transit.

Question 111

D) Encrypt the email content. (Correct Answer)

Explanation: Encrypting the email content is the most effective method to ensure confidentiality while in transit. This end-to-end encryption protects the message content from unauthorized access, even if intercepted during transmission. While TLS and SSL provide transport-level security, they don't protect the email content at rest or when it passes through intermediate servers.

Question 112

C) Centralized Access Control (Correct Answer)

Explanation: Centralized Access Control involves authorization verification performed by a single entity within a system. This approach centralizes the management and enforcement of access policies, providing consistent security across the system and simplifying administration. It's particularly useful in large organizations where maintaining uniform access controls is crucial.

Question 113

C) Repeater (Correct Answer)

Explanation: A repeater is a network device used to amplify or regenerate signals on network cabling, allowing for greater distances between nodes. It operates at the physical layer of the OSI model, receiving a signal and retransmitting it at a higher power level or to the other side of an obstruction, thus extending the reach of a network segment.

Question 114

C) Durability (Correct Answer)

Explanation: In the context of transaction processing, the "D" in ACID stands for Durability. This principle ensures that

once a transaction is committed, it will remain so, even in the event of power loss, crashes, or errors. Durability is typically achieved through the use of transaction logs and stable storage mechanisms.

Question 115

C) Hash (Correct Answer)

Explanation: A hash, also known as a message digest, is a fixed-size number generated by a hash function from an input of arbitrary size. Hashes are crucial in cryptography and data integrity verification, as they provide a unique fingerprint of the input data, allowing for quick comparisons and detection of changes.

Question 116

D) A system log (Correct Answer)

Explanation: The system log in Windows records events related to the operating system's core functions, including system shutdowns, service stoppages, and other critical system-level events. This log is essential for troubleshooting system issues and monitoring the overall health and stability of the Windows environment.

Question 117

A) Functional Testing (Correct Answer)

Explanation: Functional Testing is characterized by verifying a system against functional requirements provided by the client. It's typically executed first in the testing process and can be performed manually or using automation tools. This type of testing focuses on ensuring that the system behaves as expected and meets the specified functional requirements.

Question 118

B) A specification (Correct Answer)

Explanation: According to NIST Special Publication 800-53A, when reviewing a password standard, the object being assessed is a specification. Specifications are documented requirements, guidelines, or characteristics for materials, products, systems, or services. In this context, a password standard would fall under the category of a specification, outlining the rules and requirements for password creation and management.

Question 119

A) Write blocker (Correct Answer)

Explanation: A write blocker is commonly used as an alternative term for a forensic drive controller. This device is crucial in digital forensics as it allows read-only access to storage devices, preventing any accidental or intentional modification of the original data during the investigation process. Write blockers ensure the integrity of digital evidence by blocking all write commands to the storage device.

Question 120

B) RAID (Correct Answer)

Explanation: RAID (Redundant Array of Independent Disks) is specifically designed to prevent a hard drive from becoming a single point of failure in a system. RAID technologies use multiple drives to provide data redundancy and/or improve performance, ensuring that if one drive fails, the system can continue to operate using the remaining drives. This redundancy is crucial for maintaining data availability and system uptime.

Question 121

D) Highly privileged accounts (Correct Answer)

Explanation: During an account management assessment, highly privileged accounts are typically the primary focus. These accounts, such as administrator or root accounts,

have extensive access rights and capabilities within a system. They pose the greatest risk if compromised, making them critical targets for security audits and stringent access controls.

Question 122

C) Real Evidence (Correct Answer)

Explanation: In legal proceedings, real evidence refers to physical objects presented in court that are examined as a means of proving a fact. This type of evidence is tangible and can be directly observed or inspected by the court. Real evidence is particularly powerful as it provides concrete, physical proof that can support or refute claims made during a trial.

Question 123

A) Dynamic Host Configuration Protocol (DHCP) (Correct Answer)

Explanation: DHCP is responsible for assigning TCP/IP configuration settings to systems upon bootup. It uses UDP ports 67 for server communications and 68 for client communications. DHCP automates the process of configuring devices on IP networks, reducing administrative overhead and ensuring consistent network configurations across multiple devices.

Question 124

A) Spoofing (Correct Answer)

Explanation: Spoofing refers to the act of substituting valid source and/or destination IP addresses and node numbers with false ones. This technique is used to disguise the true origin of network traffic or to impersonate another system. Spoofing can be employed in various types of network attacks, including man-in-the-middle attacks and denial-of-service attacks.

Question 125

B) Fragments (Correct Answer)

Explanation: When a network receives a packet larger than its maximum allowable size (known as the Maximum Transmission Unit or MTU), it breaks the packet into smaller pieces called fragments. This process, known as fragmentation, allows large packets to be transmitted over networks with smaller MTUs. The receiving end then reassembles these fragments to reconstruct the original packet.

Question 126

A) UAT (Correct Answer)

Explanation: UAT stands for User Acceptance Testing. This type of testing aims to verify that a system meets stated criteria for functionality and security capabilities from the end-user perspective. It is typically the final stage of testing before a system is deployed, determining if users or customers will accept the completed product based on their requirements and expectations.

Question 127

A) Data Circuit-Terminating Equipment (Correct Answer)

Explanation: Data Circuit-Terminating Equipment (DCE) acts as the interface between the customer's network and the Frame Relay network. It functions like a router or switch, providing the necessary protocols and signaling to connect the customer's Data Terminal Equipment (DTE) to the Frame Relay network, enabling data transmission across the WAN.

Question 128

B) Neural Network (Correct Answer)

Explanation: A Neural Network is a computational model inspired by the human brain, where a long chain of interconnected nodes (neurons) process information in

layers. Each neuron receives inputs, applies weights, and passes the result to the next layer, ultimately producing the desired output. This architecture allows neural networks to learn complex patterns and make decisions based on input data.

Question 129

D) Penetration testing cannot test processes and policy. (Correct Answer)

Explanation: This should not be a concern because it's incorrect. Penetration testing can indeed assess the effectiveness of security processes and policies by attempting to exploit them. The other options are valid concerns: Metasploit can cause DoS issues, it's limited to known vulnerabilities, and pen-testing provides only a point-in-time view. However, testing processes and policies is within the scope of penetration testing.

Question 130

B) Proxy (Correct Answer)

Explanation: A proxy is a mechanism that acts as an intermediary between networks, copying packets from one network to another while altering source and destination addresses. This process helps protect the identity of the internal or private network by masking the original IP addresses, enhancing security and privacy for the protected network.

Question 131

B) Data Classification (Correct Answer)

Explanation: Data Classification is the process of categorizing data under specific labels for the purpose of applying appropriate security controls and access restrictions. This process helps organizations manage and protect their data more effectively by ensuring that sensitive information receives the appropriate level of

security and handling based on its importance and confidentiality.

Question 132

C) FERPA (Correct Answer)

Explanation: The Family Educational Rights and Privacy Act (FERPA) is the most directly applicable law for safeguarding student record privacy in educational institutions. It protects the privacy of student education records and applies to all schools that receive funds under an applicable program of the U.S. Department of Education, making it the primary concern for a small college's information security officer.

Question 133

A) Salting (Correct Answer)

Explanation: Salting is the best technique to protect hashed passwords against automated cracking attacks that use precomputed values (rainbow tables). A salt is a random string added to the password before hashing, ensuring that even identical passwords produce different hash values. This significantly increases the complexity and computational cost of cracking attempts, making precomputed attacks ineffective.

Question 134

B) OAuth (Correct Answer)

Explanation: OAuth (Open Authorization) is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. It works with HTTP and allows users to log on with one account across multiple sites or locations, making it a widely adopted SSO solution for web services.

Question 135

D) Halon (Correct Answer)

Explanation: Halon is a fire-suppressant material known to convert to toxic gases at high temperatures and deplete the ozone layer. Due to its environmental impact, Halon has been phased out and replaced by alternative substances in most applications. Its effectiveness in fire suppression made it popular in data centers, but environmental concerns led to the development of safer alternatives.

Question 136

A) PII (Correct Answer)

Explanation: PII stands for Personally Identifiable Information. This type of protected information includes data that can be used to identify, contact, or locate a specific individual, such as name, Social Security Number, date and place of birth, or mother's maiden name. PII is subject to strict privacy regulations and requires careful handling and protection to prevent identity theft and fraud.

Question 137

D) Government agent (Correct Answer)

Explanation: A government agent is most likely to lead a regulatory investigation. Regulatory investigations are typically conducted by authorized government agencies to ensure compliance with laws and regulations. These agents have the legal authority and resources to conduct thorough investigations, issue subpoenas, and enforce regulatory standards across various industries.

Question 138

B) Advanced Persistent Threat (APT) (Correct Answer)

Explanation: An Advanced Persistent Threat (APT) refers to a sophisticated, long-term cyber attack campaign typically carried out by highly skilled and well-resourced attackers, often with state sponsorship. APTs are characterized by their persistence, advanced techniques, and specific targeting of high-value assets or organizations. They maintain a low

profile to avoid detection while achieving their objectives over an extended period.

Question 139

D) RFID (Correct Answer)

Explanation: RFID (Radio-Frequency Identification) uses electromagnetic or electrostatic coupling in the radio frequency spectrum to identify specific devices. Each RFID tag contains a unique identifier and can be attached to or embedded in objects, animals, or people. RFID technology allows for non-contact, automatic identification and tracking of tagged items, making it widely used in inventory management, access control, and supply chain logistics.

Question 140

A) Claims-based SSO (Correct Answer)

Explanation: Claims-based SSO is created by a trusted claims issuer and typically packaged into a digitally signed token sent over the network using Security Assertion Markup Language (SAML). This approach allows for a more flexible and interoperable SSO solution, where identity providers issue claims about a user that service providers can trust and use for authentication and authorization decisions.

Question 141

D) Credential Management System (Correct Answer)

Explanation: A Credential Management System provides a secure storage space for users to keep their credentials when single sign-on (SSO) is unavailable. This solution allows users to securely store and manage multiple passwords, access tokens, and other authentication credentials in a centralized location, enhancing security and user convenience when SSO cannot be implemented or is temporarily unavailable.

Question 142

C) Checklist review (Correct Answer)

Explanation: A checklist review has the least impact on business operations among disaster recovery test types. It involves a paper-based review of disaster recovery plans and procedures without any actual system or operational disruption. This method allows for a thorough examination of the plan's completeness and accuracy without risking any interruption to normal business activities.

Question 143

A) Blocking read commands sent to the device (Correct Answer)

Explanation: Blocking read commands is not a typical function of a forensic device controller. These controllers are designed to prevent modification of data (write commands) while allowing read access to preserve evidence integrity. They typically allow read operations, report errors, and return requested data. Blocking read commands would hinder the forensic investigation process, which relies on the ability to read and analyze data from the device.

Question 144

C) Router (Correct Answer)

Explanation: A router is a network device used to control traffic flow between networks, often connecting similar or dissimilar networks. Routers operate at the network layer of the OSI model, using static or dynamic routing tables to make decisions about where to send data packets. They play a crucial role in directing traffic across different network segments and are essential for internet connectivity.

Question 145

C) OpenID Connect (Correct Answer)

Explanation: OpenID Connect is an Internet-based single sign-on (SSO) solution that operates over the OAuth 2.0 protocol. It can be used for web services, cloud resources, and smart device apps, providing a standardized way for clients to verify the identity of end-users based on the authentication performed by an authorization server. OpenID Connect extends OAuth 2.0 with an identity layer, making it suitable for a wide range of SSO scenarios.

Question 146

D) Alarm (Correct Answer)

Explanation: An alarm is a mechanism separate from a motion detector that triggers a deterrent, repellent, or notification. While motion detectors sense movement, alarms are the systems that respond to that detection (or other triggers) by activating audible warnings, silent alerts to security personnel, or other deterrent measures. Alarms play a crucial role in physical security systems by alerting to potential security breaches.

Question 147

B) Pulverize (Correct Answer)

Explanation: Pulverizing is the most effective method to ensure that data on archival DVD-ROMs containing Top Secret information cannot be exposed during decommissioning. This physical destruction method reduces the media to small particles, making data recovery impossible. For highly sensitive data like Top Secret information, complete physical destruction is preferred over other methods to guarantee that the data is irretrievable.

Question 148

B) Access Control Matrix (Correct Answer)

Explanation: An Access Control Matrix is a table that indicates the actions or functions each subject (user or process) can perform on each object (file, resource) in a

system. It provides a comprehensive view of the permissions and restrictions within a system, allowing administrators to manage and visualize access rights efficiently. This matrix is a fundamental concept in access control models and helps in implementing the principle of least privilege.

Question 149

C) First floor (Correct Answer)

Explanation: The first floor is often considered the optimal location for a data center in a multi-story building. It provides a balance between accessibility and security. The first floor reduces the risk of flooding compared to the basement, offers easier equipment delivery and maintenance access than upper floors, and provides better structural support for heavy equipment compared to higher floors. It also allows for more efficient cooling and power distribution compared to basement locations.

Question 150

C) Administrative laws (Correct Answer)

Explanation: Administrative laws are regulations created by government agencies to implement and enforce laws passed by Congress. These laws cover a wide range of topics, including internal agency procedures and immigration enforcement policies. They are more specific and detailed than the broader laws enacted by Congress, allowing agencies to adapt and apply laws to various situations.

Question 151

C) Salting (Correct Answer)

Explanation: Salting is a technique specifically designed to counter Rainbow Table attacks in password security. It involves adding random data (salt) to each password before hashing, ensuring that even identical passwords produce

different hash values. This makes it computationally infeasible to use pre-computed Rainbow Tables to crack passwords, as each salt-hash combination would be unique.

Question 152

A) Hybrid Cloud (Correct Answer)

Explanation: A Hybrid Cloud is a cloud computing environment that combines two or more different cloud deployment models, such as public, private, and/or community clouds. This model allows organizations to leverage the benefits of multiple cloud types, optimizing performance, security, and cost-effectiveness based on specific workload requirements.

Question 153

D) Deencapsulation (Correct Answer)

Explanation: Deencapsulation is the process of removing the header and footer information from a Protocol Data Unit (PDU) as it moves up through the OSI model layers. This process occurs at each layer, stripping away layer-specific information until the original data is retrieved at the application layer.

Question 154

A) Layer 4 (Correct Answer)

Explanation: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) operate at Layer 4, the Transport layer, of the OSI model. This layer is responsible for end-to-end communication, providing reliable (TCP) or unreliable (UDP) data transfer services to the upper layers.

Question 155

B) STP (Correct Answer)

Explanation: STP (Shielded Twisted Pair) is a type of twisted-pair cable that includes a metallic foil wrapper within the outer sheath. This additional shielding provides enhanced

protection against electromagnetic interference (EMI) and radio frequency interference (RFI), making it suitable for use in environments with high levels of electrical noise.

Question 156

A) TSYS Dispute Resolution (TDS) (Correct Answer)

Explanation: TSYS Dispute Resolution (TDS) is a comprehensive service for managing chargebacks and disputes in the payment card industry. It is performed by a team of highly knowledgeable specialists who handle the complex process of resolving disputes between merchants, cardholders, and issuing banks.

Question 157

C) Risk acceptance (Correct Answer)

Explanation: Risk acceptance is the term used when management, after conducting a cost-benefit analysis, determines that the expense of implementing countermeasures significantly outweighs the potential cost of loss due to a risk. In this scenario, the organization chooses to accept the risk rather than mitigate it, transfer it, or avoid it altogether.

Question 158

C) Dips and Surges (Correct Answer)

Explanation: Dips and surges are power supply fluctuations typically caused by switching large electric loads on or off. A dip is a brief decrease in voltage, while a surge is a brief increase. These fluctuations can occur when heavy machinery or large appliances are turned on or off, affecting the overall power supply to other connected devices.

Question 159

D) Thresholding (Correct Answer)

Explanation: Thresholding is the technique being employed when a security monitoring system is configured to report

failed login attempts only if a specific condition is met, such as five unsuccessful attempts to access the same account within a one-hour period. This approach helps reduce false positives and focuses attention on potentially significant security events.

Question 160

C) PGP (Correct Answer)

Explanation: Without seeing the provided figure, it's impossible to definitively answer this question. However, PGP (Pretty Good Privacy) is a widely used email encryption method that provides cryptographic privacy and authentication for data communication. It uses a combination of symmetric-key cryptography and public-key cryptography to ensure secure communication.

Question 161

B) Shared secret key (Correct Answer)

Explanation: In symmetric cryptography, the same key is used for both encryption and decryption. This key is known as the shared secret key. When decrypting a message that was encrypted using symmetric cryptography, the recipient must use this shared secret key to recover the original plaintext.

Question 162

A) An NDA (Correct Answer)

Explanation: An NDA (Non-Disclosure Agreement) is the appropriate legal instrument to safeguard a company's data when an employee with access to trade secrets and confidential information leaves to work for a competitor. This legally binding contract prohibits the employee from disclosing sensitive information to third parties, including their new employer.

Question 163

C) Address Resolution Protocol (Correct Answer)

Explanation: The Address Resolution Protocol (ARP) is a sub-protocol of the TCP/IP protocol suite that functions at the Data Link layer to identify the MAC address of a system. ARP is used to map IP addresses to MAC addresses, enabling communication between devices on a local network.

Question 164

C) Synchronous Data Link Control (SDLC) (Correct Answer)

Explanation: Synchronous Data Link Control (SDLC) is a layer two protocol developed by IBM for remote communications with NSA systems. It is used in networks with dedicated or leased lines, providing a reliable, full-duplex communication method for point-to-point and multipoint network configurations.

Question 165

A) The system has failed to obtain a DHCP address and has assigned itself an address. (Correct Answer)

Explanation: When a Windows system displays an IP address in the 169.254.x.x range, it indicates that the system has failed to obtain an IP address from a DHCP server and has assigned itself an Automatic Private IP Addressing (APIPA) address. This is a temporary solution that allows the system to communicate on the local network while it continues to attempt to obtain a proper IP address from a DHCP server.

Question 166

C) Which systems respond to ping, a rough network topology, and potentially the location of additional firewalls. (Correct Answer)

Explanation: When using ping to probe a remote network where pings are allowed through the target's border firewall, you can gather information about which systems respond to ping, infer a rough network topology based on response

times and IP addresses, and potentially identify the location of additional firewalls based on where ping responses stop or change significantly.

Question 167

C) BIOS (Correct Answer)

Explanation: BIOS (Basic Input/Output System) refers to the operating system-independent primitive instructions that a computer requires to start up and load the operating system from disk. It is firmware that initializes hardware during the booting process before control is passed to the operating system.

Question 168

C) Expert opinion (Correct Answer)

Explanation: When a computer security specialist provides testimony in court about whether logs and records indicate a hacking attempt, they are offering expert opinion evidence. This type of evidence is based on the specialist's professional knowledge, skills, and experience in interpreting technical data and drawing conclusions about cyber security incidents.

Question 169

B) Drive-by Download (Correct Answer)

Explanation: A drive-by download refers to the unintentional download of software (often malicious) onto a user's system without their knowledge or consent. This typically occurs through compromised websites or through phishing and redirection methods, exploiting vulnerabilities in web browsers or plugins to install malware on the victim's computer.

Question 170

D) The phone cannot contact a network. (Correct Answer)

Explanation: In a scenario where a company uses mobile device management software to remotely wipe lost phones, the most likely circumstance that would cause a remote wipe to fail is if the phone cannot contact a network. Remote wiping requires the device to be connected to a network (cellular or Wi-Fi) to receive and execute the wipe command. If the phone is offline or in an area without network coverage, the remote wipe cannot be performed.

Question 171

C) 2 (Correct Answer)

Explanation: In a backup scenario with full backups on Mondays and incremental backups on other days, Wednesday's backup would only include files that have been modified since the last backup (Tuesday's incremental backup). Without specific information about file modifications, we can assume that only files changed since Tuesday would be backed up on Wednesday, which is likely to be a small number, such as 2.

Question 172

A) Biometric Factors (Correct Answer)

Explanation: Biometric factors refer to the physical or behavioral characteristics of an individual that can be used for identification or authentication purposes. These include fingerprints, facial features, voice patterns, iris scans, and behavioral traits like typing patterns or gait analysis. Biometrics are increasingly used in security systems due to their uniqueness and difficulty to forge.

Question 173

C) 2FA (Correct Answer)

Explanation: 2FA (Two-Factor Authentication) is an authentication method that requires two distinct factors for verification. These factors typically come from different categories: something you know (like a password),

something you have (like a smartphone or token), or something you are (biometrics). By requiring two different types of authentication, 2FA significantly enhances security compared to single-factor authentication.

Question 174

B) Separation of duties (Correct Answer)

Explanation: When implementing an access control system to prevent developers from moving code from development to production environments, the information security principle being most directly enforced is separation of duties. This principle ensures that no single individual has complete control over a critical process, reducing the risk of unauthorized or accidental changes to production systems.

Question 175

A) Disaster Recovery Planning (DRP) (Correct Answer)

Explanation: Disaster Recovery Planning (DRP) is the term that describes the planned actions an organization intends to take to resume normal operations following a disruptive event. A DRP outlines procedures and instructions for responding to unplanned incidents, including natural disasters, cyber-attacks, or other business disruptions, with the goal of minimizing downtime and data loss.

Question 176

A) Access control (Correct Answer)

Explanation: Access control is the system that manages how subjects (users or processes) are granted or restricted access to objects (resources like hardware, software, or data). It encompasses various mechanisms, policies, and procedures to ensure that only authorized entities can interact with specific resources, maintaining security and privacy within an organization.

Question 177

D) TCP port 1433 (Correct Answer)

Explanation: TCP port 1433 is the default port associated with Microsoft SQL Server (MSSQL). This port is used for client-server communication in MSSQL database systems. It's important for network administrators to be aware of this port for security configurations and troubleshooting database connectivity issues.

Question 178

D) Security Testing (Correct Answer)

Explanation: Security Testing is a type of software testing specifically aimed at uncovering vulnerabilities, threats, and risks in an application. It focuses on identifying potential weaknesses that could be exploited by malicious attacks, ensuring the confidentiality, integrity, and availability of data. This testing helps in preventing security breaches and strengthening the overall security posture of the application.

Question 179

C) Cryptography (Correct Answer)

Explanation: Cryptography refers to the practice and study of techniques for secure communication in the presence of adversaries. It involves the use of algorithms to ensure confidentiality (keeping information secret), integrity (ensuring information hasn't been tampered with), authentication (verifying the identity of parties involved), and non-repudiation (preventing denial of actions). Cryptographic algorithms are fundamental to modern information security.

Question 180

A) Sanitization (Correct Answer)

Explanation: Sanitization is the process typically employed to ensure data security for workstations being removed from service but intended for resale or reuse. This process

involves thoroughly cleaning all storage devices to remove or destroy all data stored on them, making it unrecoverable. Sanitization methods can include secure overwriting, degaussing, or physical destruction of storage media, depending on the level of security required.

Question 181

C) Watermark (Correct Answer)

Explanation: A digital watermark is a process that conceals information within a file, known only to its creator. It's used to embed identifying data into digital media like images, audio, or video files. Watermarks can be visible or invisible and are designed to persist through various transformations of the file. They are commonly used to detect unauthorized copies and trace them back to their source, helping protect intellectual property rights.

Question 182

A) Black-Box Testing (Correct Answer)

Explanation: Black-Box Testing is a form of software testing that examines the functionality of an application without knowledge of its internal code structure. Testers focus solely on the inputs and outputs of the program, treating it as a "black box" whose contents are unknown. This approach is useful for simulating end-user experiences and identifying issues from a user's perspective.

Question 183

A) Unique salts should be stored for each user. (Correct Answer)

Explanation: In password hashing, unique salts should be stored for each user. A salt is a random string added to a password before hashing to make each hash unique, even for identical passwords. Storing unique salts for each user enhances security by preventing rainbow table attacks and making it significantly more difficult for attackers to crack

multiple passwords simultaneously, even if they obtain the password database.

Question 184

A) Digital Signature (Correct Answer)

Explanation: A Digital Signature is a cryptographic tool used to achieve non-repudiation. It provides a way to verify the authenticity and integrity of a digital message or document. By using public key cryptography, digital signatures ensure that the sender cannot deny sending the message (non-repudiation), as the signature can only be created with the sender's private key. This makes digital signatures crucial for secure electronic transactions and communications.

Question 185

D) Emanations (Correct Answer)

Explanation: Emanations refer to electromagnetic or radio frequency signals that may contain data susceptible to interception through eavesdropping. These unintentional emissions from electronic devices can potentially leak sensitive information. The study and prevention of such leaks is known as TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions). Protecting against emanations is crucial in high-security environments to prevent data theft through side-channel attacks.

Question 186

C) Regression Testing (Correct Answer)

Explanation: Regression Testing is the type of testing that should be conducted to verify that a recent patch for a critical application did not introduce issues elsewhere in the system. This testing ensures that new code changes or fixes haven't adversely affected existing functionalities. It involves re-running previously completed tests to ensure

that previously developed and tested software still performs correctly after changes.

Question 187

B) Transport Layer (Correct Answer)

Explanation: The Transport Layer (Layer 4) of the OSI model is responsible for end-to-end communication between devices. It handles the segmentation of data, flow control, and error correction. This layer ensures that data is delivered reliably and in the correct sequence, providing services such as connection-oriented communication (TCP) and connectionless communication (UDP).

Question 188

B) Presentation Layer (Correct Answer)

Explanation: The Presentation Layer (Layer 6) of the OSI model is responsible for translating data between the network format and the application format. It handles data formatting, encryption, compression, and protocol conversion. This layer ensures that data sent from the application layer of one system can be read by the application layer of another system, regardless of differences in data representation.

Question 189

C) Session Layer (Correct Answer)

Explanation: The Session Layer (Layer 5) of the OSI model is responsible for establishing, managing, and terminating connections between applications. It sets up, coordinates, and terminates conversations, exchanges, and dialogues between applications at each end of the communication. This layer handles session and connection coordination between applications on different devices.

Question 190

C) Network Layer (Correct Answer)

Explanation: In the OSI model, the Network Layer (Layer 3) is responsible for routing and forwarding data packets between different networks. It handles logical addressing (such as IP addresses) and determines the best path for data to travel from source to destination across multiple networks. This layer is crucial for internetworking and allows communication between devices on different networks.

Question 191

A) Physical Layer (Correct Answer)

Explanation: The Physical Layer (Layer 1) of the OSI model is responsible for transmitting raw bit streams over a physical medium. It defines the electrical, mechanical, and functional specifications for activating, maintaining, and deactivating physical connections. This layer deals with the actual hardware transmission technologies, including cables, switches, and network interface cards.

Question 192

C) Network Layer (Correct Answer)

Explanation: The Network Layer (Layer 3) of the OSI model is responsible for logical addressing and path determination. It handles the routing of data packets between different networks, using logical addresses (like IP addresses) to determine the best path for data to travel. This layer makes decisions about which physical path the data should take based on network conditions, priority of service, and other factors.

Question 193

B) Transport Layer (Correct Answer)

Explanation: The Transport Layer (Layer 4) of the OSI model provides reliable data transfer services to the upper layers. It ensures end-to-end communication, handling segmentation, flow control, and error correction. This layer offers both connection-oriented (TCP) and connectionless

(UDP) communication protocols, providing a reliable means of transferring data between applications on different hosts.

Question 194

C) To control access based on port numbers (Correct Answer)

Explanation: In the context of network security, a firewall operating at the Transport layer of the OSI model primarily controls access based on port numbers. This type of firewall, often called a stateful inspection firewall, can examine the header of TCP and UDP packets to determine which applications are communicating. By filtering traffic based on port numbers, it can allow or block specific types of network traffic associated with different applications or services.

Question 195

C) SYN flood (Correct Answer)

Explanation: A SYN flood is a type of attack that targets the Transport layer of the OSI model by exploiting the TCP three-way handshake. In this attack, the attacker sends a flood of TCP SYN packets with spoofed source IP addresses. This causes the server to send SYN-ACK responses and wait for the final ACK that never comes, eventually exhausting the server's resources and making it unresponsive to legitimate traffic.

Question 196

B) UDP (Correct Answer)

Explanation: UDP (User Datagram Protocol) operates at the Transport layer and provides connectionless, unreliable data transfer. Unlike TCP, UDP does not establish a connection before sending data, nor does it guarantee delivery or correct sequencing of packets. It's faster and more efficient for applications that can tolerate some data loss, such as streaming media, online gaming, or DNS lookups.

Question 197

B) Routing data between networks (Correct Answer)

Explanation: The primary function of the Network layer in the OSI model is routing data between networks. This layer is responsible for packet forwarding, including routing through intermediate routers. It uses logical addressing (such as IP addresses) to determine the best path for data to travel from source to destination across multiple networks. The Network layer enables internetworking and is crucial for communication between devices on different networks.

Question 198

C) Routing (Correct Answer)

Explanation: Routing is NOT typically a concern addressed by the Transport layer of the OSI model. Routing is primarily a function of the Network layer (Layer 3). The Transport layer (Layer 4) is concerned with end-to-end communication, including flow control, error detection, and segmentation and reassembly of data. It does not deal with the path data takes through the network, which is the domain of routing at the Network layer.

Question 199:

B) Adware (Correct Answer)

Explanation: Adware is software that displays unwanted advertisements on a user's computer, often without their consent. In the context of Information Systems Security, adware is considered a type of potentially unwanted program (PUP) that can compromise system performance and user privacy. Unlike malware, adware's primary purpose is to generate revenue through ad display rather than causing direct harm to the system.

Question 200:

D) Auditor (Correct Answer)

Explanation: In Information Systems Security, an auditor is responsible for examining and verifying that security policies are correctly implemented and that the resulting security measures are adequate. Auditors conduct independent assessments of an organization's security controls, processes, and practices to ensure compliance with established standards and regulations. They play a crucial role in identifying vulnerabilities, recommending improvements, and providing assurance to stakeholders about the effectiveness of security measures.

Question 201:

C) Authentication Header (Correct Answer)

Explanation: The Authentication Header (AH) is an IPSec protocol that provides authentication, integrity, and non-repudiation in Information Systems Security. It ensures that the data received is from the claimed sender and has not been altered during transmission. AH does not provide confidentiality (encryption) of the data, but it guarantees the authenticity of the entire IP packet, including the IP header.

Question 202:

C) Documentary Evidence (Correct Answer)

Explanation: In legal proceedings, documentary evidence refers to any statement made in a document presented to the court as proof of a disputed fact. This type of evidence includes written or printed materials such as contracts, letters, emails, photographs, or any other tangible items that contain information relevant to the case. Documentary evidence is considered more reliable than verbal testimony in many instances, as it provides a physical record of information that can be examined and verified.

Question 203:

B) Data retention (Correct Answer)

Explanation: Data retention refers to the policy that outlines how long an organization should keep data and when it should be deleted. This concept is crucial in Information Systems Security as it helps organizations manage their data effectively, comply with legal and regulatory requirements, and minimize security risks associated with storing unnecessary data. A well-defined data retention policy ensures that data is kept only for as long as it serves a legitimate business purpose or meets legal obligations.

Question 204:

C) Websites that collect information from children (Correct Answer)

Explanation: The Children's Online Privacy Protection Act (COPPA) specifically regulates websites that collect information from children under 13 years of age. COPPA aims to protect children's privacy online by requiring parental consent for the collection, use, or disclosure of personal information from children. This regulation applies to commercial websites, mobile apps, and online services directed at children or those that knowingly collect information from children.

Question 205:

B) Analytic Attack (Correct Answer)

Explanation: An analytic attack in Information Systems Security refers to an algebraic manipulation aimed at reducing the complexity of a cryptographic algorithm by focusing on the logic of the algorithm itself. This type of attack attempts to exploit mathematical weaknesses in the cryptographic system without relying on brute force methods. Analytic attacks often involve sophisticated mathematical analysis to find vulnerabilities in the underlying structure of the encryption algorithm.

Question 206:

A) Decentralized Access Control (Correct Answer)

Explanation: Decentralized Access Control in Information Systems Security involves authorization verification performed by various entities distributed throughout a system. In this model, access control decisions are not made by a single central authority but are instead delegated to multiple points within the network or system. This approach can improve scalability and reduce single points of failure, but it may also increase complexity in managing and coordinating access policies across the distributed system.

Question 207:

D) 129.53.44.124 (Correct Answer)

Explanation: In this scenario, James Kirk is configuring egress filtering for outbound traffic to the Internet. The organization uses the public address range 12.8.195.0/24, which means all IP addresses starting with 12.8.195 are internal. The correct answer is 129.53.44.124 because it's the only address that is not part of a private IP range (10.x.x.x, 172.16.x.x-172.31.x.x, 192.168.x.x) and is not within the organization's public IP range. This address represents a legitimate external destination that should be allowed to leave the network.

Question 208:

A) ARP (Correct Answer)

Explanation: The Address Resolution Protocol (ARP) is responsible for translating between MAC (Media Access Control) addresses and IP addresses in networking. ARP operates at the data link layer (Layer 2) of the OSI model and is crucial for communication within local area networks. When a device needs to send data to an IP address on the same network, it uses ARP to discover the corresponding

MAC address, allowing the data to be properly addressed at the hardware level.

Question 209:

A) A preventative access control; a mantrap (Correct Answer)

Explanation: The security control described in this scenario is a mantrap, which is a type of preventative access control. A mantrap is a physical security measure consisting of a small space with two sets of interlocking doors. It prevents tailgating by allowing only one person to enter at a time and requires authentication at each stage. This system is commonly used in high-security areas like data centers to ensure that only authorized individuals can access sensitive areas and to prevent unauthorized access through piggybacking or tailgating.

Question 210:

D) Asynchronous Transfer Mode (ATM) (Correct Answer)

Explanation: Asynchronous Transfer Mode (ATM) is a cell-switching technology that uses virtual circuits and fixed-size cells (53 bytes) to guarantee throughput. Unlike packet-switching technologies such as Frame Relay, ATM provides consistent, predictable performance, making it ideal for voice and video conferencing in Wide Area Networks (WANs). ATM's ability to handle different types of traffic (data, voice, video) with guaranteed quality of service (QoS) makes it suitable for applications requiring low latency and consistent bandwidth.

Question 211:

B) The media is labeled based on the highest classification level of the data it contains (Correct Answer)

Explanation: When labeling media based on the classification of the data it contains, the principle typically applied is to label the media with the highest classification

level of any data it contains. This approach, known as the "high water mark" principle, ensures that the most sensitive information on the media is protected according to its required security level. By labeling based on the highest classification, organizations can maintain appropriate security controls and handling procedures for all data on the media, even if some of the contained information is of a lower classification.

Question 212:

D) Honeypot (Correct Answer)

Explanation: A honeypot is a single system designed to lure attackers by appearing to contain sensitive information or other valuable resources. It is a security mechanism used to detect, deflect, or study attempts at unauthorized use of information systems. Honeypots are intentionally vulnerable systems that mimic legitimate targets to attract potential attackers, allowing security professionals to study their tactics and gather intelligence on new threats. Unlike a honeynet, which is a network of honeypots, a single honeypot is an isolated system set up for this specific purpose.

Question 213:

C) The client workstation supplies it in the form of a client-to-server ticket and an authenticator (Correct Answer)

Explanation: In Kerberos authentication and authorization, the service being accessed validates the ticket using information supplied by the client workstation. This information comes in two parts: the client-to-server ticket and an authenticator. The ticket, issued by the Ticket Granting Service (TGS), contains encrypted information about the client's identity and session key. The authenticator is created by the client and includes a timestamp and other information to prove the client's identity. Together, these elements allow the service to verify

the client's authenticity and authorization without directly communicating with the Key Distribution Center (KDC).

Question 214:

B) SSL (Correct Answer)

Explanation: SSL (Secure Sockets Layer) is the encryption protocol developed by Netscape to secure communications between a web server and a browser. SSL, and its successor TLS (Transport Layer Security), create an encrypted channel for sensitive data transmission over the internet, protecting against eavesdropping and tampering. SSL/TLS is widely used for securing various internet communications, including web browsing (HTTPS), email, instant messaging, and voice over IP (VoIP). It provides authentication, confidentiality, and integrity for data exchanged between clients and servers.

Question 215:

A) Land Attack (Correct Answer)

Explanation: A Land Attack is a type of Denial of Service (DoS) attack where an attacker sends numerous SYN packets to a victim with spoofed source and destination IP addresses matching the victim's. This causes the system to believe it sent a TCP/IP session opening packet to itself, creating a loop in the TCP handshake process. The victim system becomes overwhelmed trying to respond to these packets, potentially leading to a system crash or freeze. This attack exploits vulnerabilities in the TCP/IP stack implementation and can be particularly effective against older operating systems.

Question 216:

D) Need to Know (Correct Answer)

Explanation: The principle demonstrated in this scenario is "Need to Know." This principle is a fundamental concept in information security that states users should only have

access to the information and resources necessary to perform their job functions. By explaining the specific reason for needing access to the human resources database (to complete a headcount analysis requested by the CFO), the user has demonstrated a legitimate need for the information. The Need to Know principle helps minimize unnecessary access to sensitive data, reducing the risk of data breaches and unauthorized information disclosure.

Question 217:

B) BAA (Correct Answer)

Explanation: The type of agreement that must be signed between Uptown Records Management and the hospital to comply with HIPAA is a Business Associate Agreement (BAA). Under HIPAA, a covered entity (in this case, the hospital) must obtain satisfactory assurances from its business associates that they will appropriately safeguard the protected health information they receive or create on behalf of the covered entity. A BAA is a written contract that specifies each party's responsibilities in protecting the privacy and security of protected health information (PHI). This agreement is crucial for ensuring HIPAA compliance when a third party handles or has access to PHI.

Question 218:

D) Trade Secret (Correct Answer)

Explanation: The best type of intellectual property protection for Allen's Wrenches' new manufacturing process is a Trade Secret. Trade secrets are ideal for protecting processes, formulas, patterns, or compilations of information that give a business a competitive advantage and are kept confidential. Unlike patents, which require public disclosure and have a limited duration, trade secrets can potentially last indefinitely as long as they remain secret. This protection method is suitable for Allen's Wrenches because they plan to use the technology

internally without sharing it, and they want it to remain protected for as long as possible. Trade secret protection requires implementing strict confidentiality measures and non-disclosure agreements with employees and partners.

Question 219:

D) Rainbow Table (Correct Answer)

Explanation: In Information Systems Security, a Rainbow Table is a database of pre-computed hashes for guessed passwords that can be used in a password attack. Rainbow Tables are a time-memory trade-off technique, allowing attackers to crack hashed passwords more quickly than traditional brute-force methods. These tables contain a large number of possible plaintext passwords and their corresponding hash values, enabling rapid lookup of a password given its hash. Rainbow Tables are particularly effective against unsalted password hashes, which is why modern security practices emphasize the use of salt in password hashing to mitigate this type of attack.

Question 220:

B) Organizations must provide individuals with lists of employees with access to information (Correct Answer)

Explanation: The EU General Data Protection Regulation (GDPR) does not mandate that organizations provide individuals with lists of employees who have access to their information. While GDPR emphasizes transparency and individual rights regarding personal data, it does not require this level of detailed disclosure about internal access controls. The other options listed are generally in line with GDPR requirements: organizations must have dispute resolution processes, protect data against unauthorized disclosure, and in many cases, allow individuals to opt out of information sharing. The GDPR focuses on ensuring data protection by design and default, but does not require disclosing specific employee access details to data subjects.

Question 221:

D) Application-Level Gateway firewall (Correct Answer)

Explanation: An Application-Level Gateway firewall, also known as a proxy firewall, filters traffic based on the Internet service (or application) used to transmit or receive data. This type of firewall operates at the application layer (Layer 7) of the OSI model, allowing it to understand and filter traffic based on the specific protocols and content of applications such as HTTP, FTP, or SMTP. Application-Level Gateway firewalls can provide more granular control and deeper inspection of network traffic compared to simpler packet-filtering firewalls. They can examine the actual content of the data being transmitted, making decisions based on the application-specific information rather than just IP addresses and port numbers.

Question 222:

C) Data Mining (Correct Answer)

Explanation: Data Mining is the technique that allows analysts to search through data warehouses and identify potentially correlated information within historical data. It involves using advanced analytical tools and algorithms to discover patterns, relationships, and insights from large datasets. Data mining can uncover hidden trends, predict future outcomes, and support decision-making processes. In the context of data warehouses, which store vast amounts of historical data from various sources, data mining techniques can be particularly powerful for extracting valuable business intelligence, identifying customer behaviors, detecting fraud, or optimizing operations based on historical patterns.

Question 223:

D) Backbone Distribution System (Correct Answer)

Explanation: In network infrastructure, the Backbone Distribution System provides wired connections between the equipment room and telecommunications rooms, including cross-floor connections. This system forms the core of a building's network infrastructure, typically consisting of high-capacity fiber optic or copper cables that carry aggregated network traffic between different areas of a building or campus. The backbone distribution system is designed to support high-speed data transmission and serves as the main conduit for connecting various network segments, ensuring efficient communication between different floors or sections of a facility. It's a critical component in structured cabling systems, providing the foundation for reliable and scalable network connectivity.

Question 224:

B) XML (Correct Answer)

Explanation: XML (eXtensible Markup Language) is the markup language that defines rules for document formatting and encoding that is both human and machine-readable. XML is designed to store and transport data in a way that is self-descriptive and flexible. Unlike HTML, which is used primarily for displaying data, XML is used for describing and organizing data structure. It allows users to define their own tags, making it highly adaptable for various types of data representation. XML's ability to be easily read by both humans and machines makes it widely used for data exchange between different systems and applications, configuration files, and as a basis for other markup languages like XHTML and RSS.

Question 225:

B) Private IP addresses (Correct Answer)

Explanation: IP addresses such as 10.10.10.10 and 172.19.24.21 are examples of private IP addresses. These addresses are part of the ranges reserved for private

networks as defined in RFC 1918. Specifically, 10.0.0.0 to 10.255.255.255 (10.0.0.0/8) and 172.16.0.0 to 172.31.255.255 (172.16.0.0/12) are two of the three ranges designated for private use. Private IP addresses are not routable on the public internet and are used within local networks to allow devices to communicate internally. They are commonly used in home and corporate networks and are typically translated to public IP addresses by Network Address Translation (NAT) when communicating with the internet.

Question 226:

C) Infrastructure as a Service (IaaS) (Correct Answer)

Explanation: Infrastructure as a Service (IaaS) is a cloud computing model that provides virtualized computing resources over the internet. IaaS offers complete outsourcing of IT infrastructure, including servers, storage, networking, and virtualization. It allows businesses to rent these resources on-demand, scaling up or down as needed, without having to invest in and maintain physical hardware. This model provides flexibility, cost-efficiency, and the ability to quickly deploy and manage IT resources, making it ideal for organizations looking to outsource their entire IT infrastructure.

Question 227:

D) 10BaseT (Correct Answer)

Explanation: 10BaseT is a type of Ethernet cable that consists of four pairs of wires twisted around each other and then sheathed in a PVC insulator. The "10" refers to the maximum data transmission speed of 10 Mbps, "Base" indicates baseband transmission (using a single frequency), and "T" stands for twisted pair. This cable type is commonly used in local area networks (LANs) and is known for its durability, flexibility, and ease of installation. While modern networks often use faster variants like 100BaseT or

1000BaseT (Gigabit Ethernet), the basic twisted pair structure remains the same.

Question 228:

D) Cost/Benefit Analysis (Correct Answer)

Explanation: In Information Systems Security, a Cost/Benefit Analysis is an evaluation to determine if a safeguard effectively improves security without excessive cost. This analysis compares the cost of implementing and maintaining a security measure against the potential benefits it provides in terms of risk reduction and loss prevention. It helps organizations make informed decisions about which security controls to implement by weighing the financial investment against the expected security improvements. This approach ensures that security spending is justified and aligned with the organization's risk management strategy.

Question 229:

B) Collusion (Correct Answer)

Explanation: In Information Systems Security, collusion refers to an agreement between multiple individuals to perform an unauthorized or illegal action. This term is particularly relevant in the context of insider threats, where two or more people with different levels of access or authority might work together to bypass security controls or commit fraud. Collusion can be especially dangerous because it can potentially circumvent security measures designed to prevent individual misconduct, such as separation of duties. Detecting and preventing collusion often requires more sophisticated monitoring and auditing processes than those used to detect individual malicious actions.

Question 230:

D) Object-oriented languages (Correct Answer)

Explanation: The common characteristic shared by Python, C++, Java, and C# is that they are all object-oriented programming languages. Object-oriented programming (OOP) is a programming paradigm based on the concept of "objects," which can contain data and code. These languages support key OOP concepts such as encapsulation, inheritance, and polymorphism. While they may also support other paradigms (e.g., Python is multi-paradigm, supporting procedural and functional programming as well), their strong support for OOP is a defining feature. This approach allows for modular, reusable code and is widely used in software development for its flexibility and ability to model real-world entities.

Question 231:

D) Trademark (Correct Answer)

Explanation: A trademark is a registered word, slogan, or logo used to identify a company and its products or services. It is a form of intellectual property protection that gives the owner exclusive rights to use the mark in connection with specific goods or services. Trademarks serve to distinguish a company's products or services from those of competitors and help consumers identify the source of goods. They can include names, logos, phrases, symbols, designs, or a combination of these elements. Unlike patents or copyrights, trademarks can be renewed indefinitely as long as they remain in use and are properly maintained.

Question 232:

C) Job Rotation (Correct Answer)

Explanation: Job Rotation is the practice where an organization improves its overall security by rotating employees among various job positions. This approach serves multiple purposes in information security:

It helps prevent fraud by ensuring that no single employee has prolonged control over sensitive processes.

It increases the number of employees familiar with different aspects of the organization's operations, improving overall resilience.

It can help detect and prevent long-term fraudulent activities that might go unnoticed if an employee remains in the same position indefinitely.

It broadens employees' skills and knowledge, potentially improving their ability to identify security issues across different areas of the organization.

Job rotation is an important part of many organizations' security strategies, particularly in financial institutions and other sectors handling sensitive information.

Question 233:

C) Fiber-Optic (Correct Answer)

Explanation: Fiber-optic cabling is the type of network cabling that transmits light instead of electrical signals. This technology uses thin strands of glass or plastic (optical fibers) to transmit data as pulses of light. Fiber-optic cables offer several advantages over traditional copper cables:

Higher bandwidth and faster data transmission speeds over longer distances.

Immunity to electromagnetic interference and radio-frequency interference.

Lower signal attenuation, allowing for longer cable runs without the need for signal boosters.

Enhanced security, as it's more difficult to tap into fiber-optic cables without detection.

Thinner and lighter cables, making installation easier in some environments.

These characteristics make fiber-optic cabling ideal for high-speed, long-distance data transmission in various networking applications, from telecommunications to enterprise networks.

Question 234:

B) Set up a one-way non-transitive trust (Correct Answer)

Explanation: Frank Castle should set up a one-way non-transitive trust to meet his requirements. Here's why:

One-way trust: This allows the partner organization's Active Directory forest (B) to access Frank's domain's forest resources, but not vice versa. Users in Frank's domain won't be able to access B's resources.

Non-transitive: This ensures that the trust doesn't flow upward through the domain tree as it is formed. It limits the trust relationship to only the directly involved domains, preventing unintended access to other domains in the forest.

This configuration provides the necessary access for the partner organization while maintaining strict control over the trust relationship, enhancing security by limiting the scope of the trust to only what is required.

Question 235:

D) Authentication (Correct Answer)

Explanation: In Information Systems Security, the process used when a traveler presents their ticket and driver's license at the airport to check bags and receive a boarding pass is Authentication. This process involves verifying the identity of an individual by comparing the provided credentials (in this case, the ticket and driver's license) with known, trusted information. Authentication is a crucial security measure that ensures only authorized individuals are granted access to specific resources or services. In the airport scenario:

1. The ticket confirms the traveler's reservation.
2. The driver's license serves as a government-issued photo ID to verify the traveler's identity.
3. Together, these documents authenticate that the person presenting them is indeed the authorized traveler.

This multi-factor authentication approach (something you have - the ticket, and something you are - photo ID) increases the security of the process by requiring multiple forms of verification.

Question 236:

D) MOD (Correct Answer)

Explanation: The mathematical operation that makes all the given equations correct is MOD (modulus). The modulus operation returns the remainder after division of one number by another. Let's verify each equation:

1. 8 MOD 6 = 2 (8 divided by 6 leaves a remainder of 2)
2. 8 MOD 4 = 0 (8 divided by 4 leaves no remainder)
3. 10 MOD 3 = 1 (10 divided by 3 leaves a remainder of 1)
4. 10 MOD 2 = 0 (10 divided by 2 leaves no remainder)

The modulus operation is widely used in computer science and cryptography for various purposes, including generating pseudo-random numbers, hashing, and ensuring values fall within a specific range.

Question 237:

D) Hoax (Correct Answer)

Explanation: A hoax is a form of social engineering attack that uses the threat of malicious code to trick users into damaging their own system. Unlike a Trojan, which is actual

malicious software, a hoax relies purely on deception and manipulation of the user. Characteristics of a hoax include:

- False warnings about non-existent viruses or security threats.
- Instructions to delete certain files or modify system settings, claiming it will protect the system.
- Urgency to share the warning with others, spreading the hoax further.
- Often spread through email chains or social media.

The danger of hoaxes lies in their ability to cause users to take harmful actions voluntarily, potentially disrupting systems or deleting important files. Educating users about these tactics is crucial for preventing such attacks.

Question 238:

C) Access aggregation (Correct Answer)

Explanation: Access aggregation refers to the practice of gathering multiple pieces of non-sensitive information and combining or aggregating them to obtain sensitive information, often used in reconnaissance attacks. This technique is particularly dangerous because:

1. Each piece of information on its own may seem harmless and not raise security concerns.
2. When combined, these pieces can reveal a comprehensive picture that was not intended to be disclosed.
3. It can bypass security measures designed to protect individual pieces of sensitive data.
4. It's often difficult to detect as the collection of information may occur over time and from various sources.

Attackers might use access aggregation to build detailed profiles of targets, understand organizational structures, or

identify vulnerabilities in systems. To counter this threat, organizations need to implement robust information classification and access control policies, and be aware of how seemingly innocuous data could be combined to reveal sensitive information.

Question 239:

D) Security Control (Correct Answer)

Explanation: In Information Systems Security, a Security Control is any security mechanism, tool, or practice that can deter and mitigate undesirable actions or events. This is a broad term that encompasses various types of controls, including:

- Preventative controls: Designed to stop unwanted events from occurring.
- Detective controls: Aimed at identifying and characterizing incidents in progress.
- Corrective controls: Used to reduce the impact of an incident.
- Deterrent controls: Intended to discourage potential attackers.

Security controls can be technical (e.g., firewalls, encryption), administrative (e.g., policies, procedures), or physical (e.g., locks, security guards). The term "Security Control" is more comprehensive than the other options, as it includes all types of measures used to protect information assets and mitigate risks.

Question 240:

D) API keys (Correct Answer)

Explanation: To ensure that third-party users of his services' API can be tracked to prevent abuse, Hannibal King should implement API keys. API keys are unique identifiers that are used to authenticate a user, developer, or calling program

to an API. They offer several benefits for tracking and preventing abuse:

1. Authentication: Each API key is unique to a specific user or application, allowing for identification of who is making the API calls.
2. Usage Tracking: API keys enable monitoring of how often and in what way each user is accessing the API.
3. Rate Limiting: They allow for the implementation of rate limiting to prevent overuse or abuse of the API.
4. Access Control: Different API keys can be given different levels of access, allowing for fine-grained control over what each user can do.
5. Revocation: If abuse is detected, the specific API key can be revoked without affecting other users.

By implementing API keys, Hannibal King can effectively track usage, identify potential abusers, and take action to prevent misuse of his services' API.

Question 241:

B) TGS (Correct Answer)

Explanation: In the Kerberos authentication system, the Ticket Granting Service (TGS) is responsible for generating new tickets and session keys and sending them to the client. The Kerberos authentication process involves several steps:

1. The client requests a Ticket Granting Ticket (TGT) from the Authentication Server (AS).
2. The AS verifies the client's credentials and issues a TGT.
3. The client uses the TGT to request a service ticket from the TGS.
4. The TGS generates a new ticket and session keys for the requested service and sends them to the

client.
5. The client uses this ticket to access the desired service.

The TGS plays a crucial role in the Kerberos system by issuing service-specific tickets, allowing clients to access various services without repeatedly authenticating with their long-term secret key.

Question 242:

B) Sanitization (Correct Answer)

Explanation: The removal of a hard drive from a PC before it is retired and sold as surplus is an example of sanitization. Sanitization is the process of removing sensitive data from storage devices to prevent unauthorized access to that data. This process can involve several methods:

1. Physical removal of storage media (as in this case).
2. Overwriting data with random patterns.
3. Degaussing (for magnetic media).
4. Encryption (with subsequent destruction of the encryption key).

Sanitization is crucial when disposing of or repurposing IT equipment to ensure that no sensitive data can be recovered by the next user or through forensic analysis. It's an important part of data lifecycle management and helps organizations comply with data protection regulations and maintain information security.

Question 243:

C) Nondisclosure Agreement (NDA) (Correct Answer)

Explanation: A Nondisclosure Agreement (NDA) is the document used to protect confidential information within an organization from being exposed by a former employee or other person with privileged information. Key aspects of an NDA include:

- Definition of confidential information: Specifies what information is considered confidential.
- Obligations of the recipient: Outlines how the confidential information should be protected and used.
- Duration: Specifies how long the agreement remains in effect.
- Consequences of breach: Details the penalties for violating the agreement.

NDAs are crucial for protecting trade secrets, proprietary information, and other sensitive data. They create a legal obligation for the signer to maintain confidentiality, providing organizations with legal recourse if the agreement is violated. NDAs are commonly used with employees, contractors, business partners, and in merger and acquisition discussions.

Question 244:

A) High-Level Data Link Control (HDLC) (Correct Answer)

Explanation: High-Level Data Link Control (HDLC) is a layer 2 protocol used to transmit data over synchronous communication lines. It has several key features:

1. Supports full-duplex communications: Allows simultaneous two-way communication.
2. Enables both point-to-point and multipoint connections: Can be used in various network topologies.
3. Offers flow control: Manages the rate of data transmission to prevent overwhelming the receiver.
4. Includes error detection and correction: Ensures data integrity during transmission.
5. Uses synchronous communication: Provides efficient, continuous data transfer.

HDLC is a bit-oriented protocol, meaning it can transfer any bit pattern without conflicting with data-link control information. It's widely used in WAN environments and serves as the basis for other protocols like PPP (Point-to-Point Protocol). HDLC's versatility and reliability make it a fundamental protocol in data communications.

Question 245:

C) Privacy Act of 1974 (Correct Answer)

Explanation: The Privacy Act of 1974 is the US law that mandates government agencies to maintain only necessary records for conducting their business, destroy those records when no longer needed, and provides a formal procedure for individuals to access and request amendments to their records. Key provisions of this act include:

1. Restricting disclosure of personally identifiable information.
2. Granting individuals the right to access records about themselves.
3. Allowing individuals to request corrections to their records.
4. Requiring agencies to establish appropriate administrative, technical, and physical safeguards for records.
5. Limiting the collection, maintenance, use, and dissemination of personal information to what is relevant and necessary.

This act is fundamental to protecting individual privacy in the context of government record-keeping and serves as a cornerstone of US privacy law.

Question 246:

C) Physical (Correct Answer)

Explanation: In the OSI (Open Systems Interconnection) model, data is sent as bits at the Physical layer. This is Layer 1, the lowest layer of the OSI model. Key characteristics of the Physical layer include:

- Deals with the actual physical connection between devices.
- Defines the electrical and physical specifications of the data connection.
- Responsible for transmission and reception of raw bit streams over a physical medium.
- Handles aspects like voltage levels, data rates, maximum transmission distances, and physical connectors.
- Converts the digital bits into electrical, radio, or optical signals.

Understanding the Physical layer is crucial for network engineers and technicians as it forms the foundation upon which all higher-level network functions are built.

Question 247:

B) Prepare data for use by the Application Layer (Correct Answer)

Explanation: The primary function of the Presentation Layer in the OSI model is to prepare data for use by the Application Layer. This layer, also known as Layer 6, acts as a translator between the Application Layer and the lower layers. Key functions of the Presentation Layer include:

1. Data formatting: Ensures that data from the application layer of one system can be read by the application layer of another system.
2. Data encryption and decryption: Provides security by encrypting data before transmission and decrypting it upon receipt.

3. Data compression: Reduces the size of data for more efficient transmission.
4. Character code translation: Converts between different character and data representations (e.g., ASCII to EBCDIC).
5. Data serialization: Converts complex data structures or objects into a format that can be transmitted over the network.
6. Protocol conversion: Translates between different data formats or protocols if necessary.

By performing these functions, the Presentation Layer ensures that data from the Application Layer is in a format that can be understood by the receiving system, regardless of differences in data representation between the sender and receiver. This layer plays a crucial role in maintaining data integrity and compatibility across different systems in a network.

Conclusion: Exam Preparation Strategies

Preparing for the CISSP exam requires a comprehensive approach that goes beyond simply memorizing facts. Effective exam preparation involves managing anxiety, employing mnemonic techniques to aid recall, and following a structured checklist to ensure all key areas are covered. By addressing the psychological aspects of exam-taking alongside content mastery, candidates can maximize their chances of success.

Managing exam anxiety is crucial, as even the most knowledgeable professionals can underperform if overwhelmed by stress. Practical steps for reducing stress and relaxation techniques can help candidates maintain focus and clarity during the exam. These strategies, when practiced regularly, can significantly improve performance under pressure.

Mnemonic techniques tailored to the CISSP domains provide powerful tools for organizing and recalling vast amounts of information. By creating memorable associations and acronyms, candidates can more easily retain and access critical concepts across all eight domains of the Common Body of Knowledge (CBK).

Finally, a comprehensive exam preparation checklist serves as a roadmap, ensuring that no crucial areas are overlooked in the lead-up to the exam. This structured approach helps candidates systematically review all necessary material, identify areas needing additional focus, and enter the exam with confidence.

By integrating these strategies - anxiety management, mnemonic techniques, and a thorough preparation checklist - CISSP candidates can approach the exam with a well-rounded, confident mindset, ready to demonstrate their expertise in information security.

Managing Exam Anxiety

Exam anxiety is a common challenge faced by many CISSP candidates, regardless of their level of preparation or expertise. The high stakes and comprehensive nature of the CISSP exam can trigger stress responses that may interfere with performance. Understanding and managing this anxiety is crucial for success.

Recognizing Exam Anxiety

Exam anxiety manifests in various ways, both physically and mentally. Physical symptoms may include:

- Rapid heartbeat
- Sweating
- Nausea
- Trembling
- Shortness of breath

Mental symptoms often include:

- Racing thoughts
- Difficulty concentrating
- Blanking out on familiar material
- Negative self-talk
- Catastrophizing potential outcomes

Recognizing these symptoms is the first step in managing exam anxiety. It's important to understand that some level

of anxiety is normal and can even be beneficial, as it keeps you alert and focused. However, excessive anxiety can impair performance and needs to be addressed.

Practical Steps for Reducing Stress

1. **Thorough Preparation**: The most effective way to reduce exam anxiety is to be well-prepared. Create a study schedule well in advance of the exam date and stick to it consistently. Cover all domains of the CBK thoroughly, and use practice exams to identify areas needing additional focus.
2. **Simulate Exam Conditions**: Regularly practice under conditions similar to the actual exam. This includes timing yourself, using similar question formats, and even dressing as you would for the exam. This familiarity can significantly reduce anxiety on exam day.
3. **Maintain Physical Health**: Regular exercise, a balanced diet, and adequate sleep are crucial for managing stress and maintaining mental clarity. In the weeks leading up to the exam, prioritize these aspects of your health.
4. **Visualization Techniques**: Spend time visualizing yourself successfully completing the exam. This positive mental rehearsal can boost confidence and reduce anxiety.
5. **Arrive Early**: On exam day, arrive at the testing center well before the scheduled time. This allows you to familiarize yourself with the surroundings and settle your nerves without feeling rushed.
6. **Positive Self-Talk**: Replace negative thoughts with positive, affirming statements. Remind yourself of your preparation and capabilities.

7. **Break Down the Exam**: During the exam, focus on one question at a time rather than becoming overwhelmed by the entire test. Remember that you don't need to answer every question correctly to pass.
8. **Use Anxiety Management Techniques**: Employ techniques like deep breathing or progressive muscle relaxation during the exam if you feel anxiety rising.

Relaxation Techniques

1. **Deep Breathing**: Practice deep, diaphragmatic breathing. Inhale slowly through your nose for a count of four, hold for a count of four, then exhale slowly through your mouth for a count of four. Repeat this several times to calm your nervous system.
2. **Progressive Muscle Relaxation**: Systematically tense and then relax different muscle groups in your body. Start with your toes and work your way up to your head. This technique helps release physical tension and promotes a sense of calm.
3. **Mindfulness Meditation**: Practice focusing your attention on the present moment without judgment. This can help clear your mind of anxious thoughts and improve concentration.
4. **Guided Imagery**: Use your imagination to visualize a peaceful, calming scene. This can help distract from anxious thoughts and promote relaxation.
5. **5-4-3-2-1 Grounding Technique**: Use your senses to ground yourself in the present moment. Identify 5 things you can see, 4 things you can touch, 3 things you can hear, 2 things you can smell, and 1 thing you can taste.

Long-Term Anxiety Management

While these techniques are valuable for managing anxiety during the exam, it's also important to develop long-term strategies for stress management. Consider the following:

- Regular mindfulness or meditation practice
- Yoga or tai chi
- Journaling
- Seeking support from a study group or mentor
- Professional counseling if anxiety is severe or persistent

Remember, experiencing some anxiety is normal and can even enhance performance by keeping you alert and focused. The goal is not to eliminate anxiety entirely, but to manage it effectively so that it doesn't interfere with your ability to demonstrate your knowledge and skills during the exam.

By implementing these practical steps and relaxation techniques, CISSP candidates can approach the exam with greater confidence and composure, allowing their preparation and expertise to shine through.

Mnemonic Techniques for CISSP Domains

Mnemonic techniques are powerful tools for memorizing and recalling complex information, making them particularly useful for mastering the extensive content covered in the CISSP exam. Here are various mnemonic devices tailored to each of the eight CISSP domains:

1. Security and Risk Management

- **SPARC**: Security, Privacy, Availability, Risk, Compliance
- Covers key areas within this domain
- **GAPP**: Governance, Asset management, Personnel security, Policies
- Outlines critical components of security management
- **RITO**: Risk, Issues, Threats, Opportunities
- Reminds of key factors in risk assessment
- **PAIN**: Policy, Awareness, Implementation, Necessity
- Steps for effective security policy management

2. Asset Security

- **CIANA**: Confidentiality, Integrity, Availability, Non-repudiation, Authentication
- Core principles of information security
- **CLASS**: Classification, Labeling, Accounting, Storage, Sanitization
- Key aspects of data lifecycle management
- **DRIP**: Data Retention, Information classification, Privacy, Protection controls
- Essential elements of asset security

3. Security Architecture and Engineering

- **STRIDE**: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
- Common types of security threats
- **PASTA**: Process for Attack Simulation and Threat Analysis

- A methodology for threat modeling
- **SABSA**: Sherwood Applied Business Security Architecture
- Framework for enterprise security architecture

4. Communication and Network Security

- **OSI**: Open Systems Interconnection model
- Please Do Not Throw Sausage Pizza Away
- Physical, Data Link, Network, Transport, Session, Presentation, Application
- **TCP/IP**: Transmission Control Protocol/Internet Protocol
- Please Do Not Take Sales People's Advice
- Physical, Data Link, Network, Transport, Session, Presentation, Application
- **SSID**: Service Set Identifier
- Some Security Is Desirable (for wireless networks)

5. Identity and Access Management (IAM)

- **AAA**: Authentication, Authorization, Accounting
- Core components of access control
- **RBAC**: Role-Based Access Control
- Remember: Bosses Assign Capabilities
- **ABAC**: Attribute-Based Access Control
- Always Be Assessing Characteristics
- **DAC**: Discretionary Access Control
- Decisions Are Customizable
- **MAC**: Mandatory Access Control
- Mandates Are Compulsory

6. Security Assessment and Testing

- **OWASP**: Open Web Application Security Project
- Only Web Apps Should Pass
- **NIST**: National Institute of Standards and Technology
- Never Ignore Security Testing
- **CVSS**: Common Vulnerability Scoring System
- Calculate Vulnerabilities' Severity Systematically

7. Security Operations

- **ITIL**: Information Technology Infrastructure Library
- Improve The Infrastructure Lifecycle
- **SIEM**: Security Information and Event Management
- See Important Events Meticulously
- **SOC**: Security Operations Center
- Supervise, Observe, Control

8. Software Development Security

- **SDLC**: Software Development Life Cycle
- Specify, Design, Leverage, Construct
- **SAST**: Static Application Security Testing
- Scan And Secure Thoroughly
- **DAST**: Dynamic Application Security Testing
- Detect And Stop Threats

Additional General CISSP Mnemonics:

- **AIC**: Availability, Integrity, Confidentiality

- Core principles of information security (alternative to CIA)
- **NIST RMF**: National Institute of Standards and Technology Risk Management Framework
- Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor
- **OCTAVE**: Operationally Critical Threat, Asset, and Vulnerability Evaluation
- Organize, Collect, Train, Analyze, Validate, Evaluate
- **COBIT**: Control Objectives for Information and Related Technologies
- Control Operations By Implementing Technology
- **COSO**: Committee of Sponsoring Organizations
- Control Operations, Secure Organization
- **BCP**: Business Continuity Planning
- Be Continuously Prepared
- **DRP**: Disaster Recovery Planning
- Develop Recovery Procedures
- **BIA**: Business Impact Analysis
- Breakdown Important Assets
- **SLE**: Single Loss Expectancy
- Specific Loss Estimate
- **ALE**: Annual Loss Expectancy
- Annual Loss Estimate
- **ARO**: Annual Rate of Occurrence
- Annual Risk Occurrence
- **MTBF**: Mean Time Between Failures
- Measure Time Before Faults
- **MTTR**: Mean Time To Repair

- Measure Time To Restore
- **RPO**: Recovery Point Objective
- Restore Previous Operations
- **RTO**: Recovery Time Objective
- Restore Timely Operations
- **ISO/IEC 27001**: Information Security Management System
- Implement Security Operations/Manage Effectively
- **GDPR**: General Data Protection Regulation
- Guard Data, Protect Rights
- **HIPAA**: Health Insurance Portability and Accountability Act
- Health Information Privacy And Accountability
- **PCI DSS**: Payment Card Industry Data Security Standard
- Protect Card Information, Demonstrate Security Standards
- **SOX**: Sarbanes-Oxley Act
- Secure Organizational eXpenditures
- **GLBA**: Gramm-Leach-Bliley Act
- Guard Legally Banking Assets
- **FERPA**: Family Educational Rights and Privacy Act
- Families Expect Records Protected Always
- **FISMA**: Federal Information Security Management Act
- Federal Information Should Maintain Assurance
- **COPPA**: Children's Online Privacy Protection Act
- Children's Online Privacy Protected Always
- **BYOD**: Bring Your Own Device

- Bring Your Own Danger
- **IoT**: Internet of Things
- Insecure objects Threatening
- **VPN**: Virtual Private Network
- Virtually Protected Network
- **IDS**: Intrusion Detection System
- Identify Dangerous Situations
- **IPS**: Intrusion Prevention System
- Interrupt Potential Security-breaches
- **WAF**: Web Application Firewall
- Watch And Filter
- **DLP**: Data Loss Prevention
- Don't Leak Private-information
- **EDR**: Endpoint Detection and Response
- Examine Device Risks
- **CASB**: Cloud Access Security Broker
- Control Access, Secure Boundaries
- **SOAR**: Security Orchestration, Automation and Response
- Streamline Operations, Automate Responses
- **ZTA**: Zero Trust Architecture
- Zero Trust Always
- **DevSecOps**: Development, Security, and Operations
- Develop Securely, Operate Prudently
- **CSIRT**: Computer Security Incident Response Team
- Coordinate Security Incident Response Thoroughly
- **CIRT**: Computer Incident Response Team

- Coordinate Incident Response Team
- **CERT**: Computer Emergency Response Team
- Computer Emergencies Require Teamwork
- **APT**: Advanced Persistent Threat
- Always Persistent Trouble
- **RAT**: Remote Access Trojan
- Remote Access Trouble
- **XSS**: Cross-Site Scripting
- X-tra Sneaky Scripts
- **CSRF**: Cross-Site Request Forgery
- Crafty Site Requests Forgery
- **SQL Injection**: Structured Query Language Injection
- Sneaky Queries Leaking Information
- **DoS**: Denial of Service
- Deny or Slow
- **DDoS**: Distributed Denial of Service
- Distributed Deny or Slow
- **MFA**: Multi-Factor Authentication
- Multiple Factors Authenticate
- **2FA**: Two-Factor Authentication
- Two Factors Authenticate
- **SSO**: Single Sign-On
- Simple Sign-On
- **PKI**: Public Key Infrastructure
- Public Keys Implemented
- **CA**: Certificate Authority
- Certify Authenticity

- **RA**: Registration Authority
- Register Applicants
- **CRL**: Certificate Revocation List
- Certificates Revoked List
- **OCSP**: Online Certificate Status Protocol
- Online Certificates Status Protocol
- **HSM**: Hardware Security Module
- Hardware Secures Material
- **TPM**: Trusted Platform Module
- Trusted Platform Mechanism
- **SELinux**: Security-Enhanced Linux
- Secure Every Linux
- **AppArmor**: Application Armor
- Applications Armored

These mnemonics cover a wide range of topics within the CISSP domains and related areas. They can be used as quick memory aids during study and even during the exam itself. Remember, the key to effective use of mnemonics is regular practice and association with the full concepts they represent.

Final Exam Preparation Checklist

A comprehensive final exam preparation checklist is crucial for ensuring that CISSP candidates are fully prepared and confident on exam day. This checklist covers all aspects of exam readiness, from content review to logistical preparations.

Content Review

1. **Domain Mastery**:

- Review all eight CISSP domains thoroughly
- Focus extra attention on areas identified as weaknesses during practice exams
- Use the Official (ISC)² CISSP Study Guide as a primary reference

2. **Practice Exams**:
   - Complete at least 3-5 full-length practice exams under timed conditions
   - Analyze results to identify areas needing additional study
   - Aim for a consistent score of 80% or higher before attempting the real exam
3. **Concept Application**:
   - Practice applying concepts to real-world scenarios
   - Review case studies and example situations provided in study materials
4. **Mnemonic Review**:
   - Review and practice all mnemonic devices created during study
   - Ensure you can expand on each mnemonic with detailed explanations

Exam Strategies

1. **Time Management**:
   - Practice pacing strategies to ensure completion of all questions within the allotted time
   - Develop a strategy for handling difficult questions (e.g., marking for review and returning later)
2. **Question Analysis**:

- Review techniques for breaking down complex questions
- Practice identifying key words and eliminating incorrect answer choices

3. **Stress Management**:
    - Review and practice relaxation techniques
    - Prepare positive self-talk statements for use during the exam

Logistical Preparation

1. **Exam Registration**:
    - Confirm exam date, time, and location
    - Review all rules and requirements provided by (ISC)²
2. **Travel Plans**:
    - Plan route to testing center, accounting for potential traffic or delays
    - If traveling long distance, confirm accommodation arrangements
3. **Required Documents**:
    - Prepare two forms of valid identification as required by (ISC)²
    - Print and bring exam confirmation email
4. **Personal Items**:
    - Prepare comfortable, layered clothing for exam day
    - Pack any permitted items (e.g., clear water bottle)

4. **Mental Preparation**:
    - Review key concepts and mnemonics one final time

- Get a good night's sleep before the exam
- Eat a healthy meal before the exam
- Practice relaxation techniques to manage exam anxiety

5. **Time Management**:
    - Plan to arrive at the testing center at least 30 minutes early
    - Review your time management strategy for the exam
6. **Post-Exam Plan**:
    - Have a plan for after the exam, regardless of the outcome
    - Consider scheduling a relaxing activity to decompress
7. **Final Review**:
    - Go through this checklist one last time to ensure nothing is overlooked

By following this comprehensive checklist, CISSP candidates can ensure they are fully prepared for exam day, both logistically and mentally. This thorough preparation can significantly reduce exam-day stress and increase the likelihood of success.

E-Learning Course Video Bonus Access

Thank you for purchasing the ISC2 CISSP Study Guide 2025-2026. We truly appreciate your business and trust in our comprehensive exam preparation materials.

To access your **9 Hours Premium E-Learning Course**, please scan the QR code below:

We hope this additional resource enhances your exam preparation and helps you achieve CISSP certification.

If you have any questions or need assistance, please don't hesitate to contact our support team.

Best of luck with your studies!

Sincerely,

NewGrade Publication
Newgradepublication@gmail.com