50 Questions for Chapter 1,2 - Overview of Security Principles and Introduction

Multiple-Choice Questions (70%)

1. **What are the three components of the CIA Triad in computer security?**
   a) Confidentiality, Accountability, Availability
   b) Confidentiality, Integrity, Availability
   c) Control, Integrity, Accessibility
   d) Confidentiality, Authentication, Availability

2. **What type of security involves safeguarding against human error and system failures?**
   a) Cybersecurity
   b) Physical security
   c) Reliability and redundancy
   d) Network security

3. **What is the primary focus of computer security?**
   a) Preventing unintentional damage
   b) Protecting systems from malicious activities
   c) Enhancing usability of networks
   d) Increasing system performance

4. **What does the NIST Computer Security Handbook define as a key objective of cybersecurity?**
   a) Detecting and correcting errors
   b) Ensuring availability and accessibility
   c) Preserving integrity, availability, and confidentiality
   d) Automating response systems

5. **What type of attack involves monitoring transmissions to obtain information?**
   a) Active attacks
   b) Eavesdropping
   c) Spoofing
   d) Denial of Service

6. **Which model is used to identify spoofing, tampering, and repudiation threats?**
   a) STRIDE
   b) DREAD
   c) OSI
   d) CIA

7. **Which type of risk assessment process ranks threats based on their risk levels?**
   a) STRIDE
   b) Threat modeling
   c) Risk prioritization
   d) Mitigation strategy

8. **What are assets in the context of threat modeling?**
   a) User passwords

b) Security vulnerabilities
c) Valuable data or system components
d) Encryption algorithms

9. **Which threat modeling technique evaluates the damage caused by a threat?**
   a) DREAD
   b) STRIDE
   c) OSI model
   d) Security risk analysis

10. **Which of the following is a human vulnerability in security systems?**
    a) Unpatched software
    b) Social engineering attacks
    c) Configuration vulnerabilities
    d) Buffer overflows

Fill-in-the-Blank Questions (30%)

11. The CIA Triad consists of Confidentiality, Integrity, and _____.
12. A _____ attack involves unauthorized modification of data.
13. The STRIDE model stands for Spoofing, Tampering, Repudiation, Information Disclosure, _____, and Elevation of Privilege.
14. The _____ model assigns risk levels based on damage, reproducibility, exploitability, affected users, and discoverability.
15. Risk _____ involves calculating the likelihood and impact of threats.
16. Social engineering attacks often exploit _____ vulnerabilities.
17. The goal of threat modeling is to develop targeted _____ measures.
18. Vulnerability _____ includes discovery, disclosure, patching, and testing.
19. A _____ attack occurs when an adversary denies involvement in an action.
20. The NIST framework emphasizes _____ management as a key step in mitigating risks.

50 Questions for Chapter 3 - Review of Cryptography

Multiple-Choice Questions (70%)

1. **What is the primary goal of encryption?**
   a) Increase system efficiency
   b) Encode messages to obscure their meaning
   c) Enhance file compression
   d) Secure physical access to systems

2. **Which cipher shifts letters by a fixed number of places in the alphabet?**
   a) Substitution cipher
   b) Atbash cipher
   c) Caesar cipher
   d) Vigenère cipher

3. **Which encryption method uses the same key for encryption and decryption?**
   a) Symmetric encryption
   b) Asymmetric encryption
   c) Hashing
   d) Digital signatures

4. **What is the primary weakness of the Caesar cipher?**
   a) Lack of scalability
   b) Short keys
   c) Predictable patterns
   d) High computational complexity

5. **What is the key feature of one-time pad encryption?**
   a) Reusable keys
   b) Perfect secrecy
   c) Symmetric key generation
   d) Complex implementation

6. **Which cryptography technique involves reordering characters in plaintext?**
   a) Substitution
   b) Transposition
   c) Hashing
   d) Encoding

7. **What is the primary function of a cryptanalyst?**
   a) Encrypting messages
   b) Deciphering ciphertext
   c) Managing keys
   d) Distributing certificates

8. **Which algorithm is widely used for public-key encryption?**
   a) DES
   b) AES
   c) RSA
   d) Caesar

9. **What is the process of converting ciphertext back to plaintext?**
   a) Encryption
   b) Hashing
   c) Decryption
   d) Encoding

10. **What does DES primarily rely on for encryption?**
    a) Key expansion
    b) Substitution and transposition
    c) Hash functions
    d) Random number generators

Fill-in-the-Blank Questions (30%)

11. The two main types of encryption are symmetric and _____.
12. A cryptosystem must ensure that plaintext is equal to _____ of the ciphertext.
13. The Caesar cipher achieves encryption by _____ the alphabet.
14. Transposition techniques achieve encryption through character _____.
15. Perfect secrecy is achieved with a _____ cipher.
16. The RSA algorithm is an example of _____ encryption.
17. Shannon's theory of good ciphers emphasizes _____ and diffusion.
18. Cryptanalysis involves analyzing _____ to decipher encoded messages.
19. The primary goal of _____ is to spread plaintext information across ciphertext.
20. A secure cipher must resist brute-force attacks and statistical _____.
11.

---

50 Questions for Chapter 4 - Security in the Software Development Life Cycle

Multiple-Choice Questions (70%)

1. **What is the primary goal of secure software development?**
    a) To enhance system efficiency
    b) To prevent vulnerabilities and resist attacks
    c) To reduce development time
    d) To simplify the coding process
2. **Which phase of the SDLC focuses on defining security needs and sensitivity assessments?**
    a) Disposal
    b) Development/Acquisition
    c) Initiation
    d) Implementation
3. **Which NIST publication provides guidelines for integrating security into the SDLC?**
    a) 800-128
    b) 800-14

c) 800-53
d) 800-37

4. **What is the purpose of a Configuration Management Plan (CMP)?**
   a) To manage system disposal
   b) To track and control changes to the system
   c) To prevent security breaches during maintenance
   d) To reduce software development costs

5. **What does "containerization" in storage segmentation aim to achieve?**
   a) Faster system processing
   b) Separating business and personal data
   c) Encrypting sensitive information
   d) Automating backup processes

6. **Which SDLC phase involves implementing security testing and accreditation?**
   a) Initiation
   b) Development/Acquisition
   c) Implementation
   d) Operation/Maintenance

7. **What is the role of the Configuration Control Board (CCB)?**
   a) To enforce encryption policies
   b) To approve and monitor changes
   c) To archive outdated configurations
   d) To manage licensing agreements

8. **Which model of software development allows overlapping phases?**
   a) Waterfall
   b) Spiral
   c) Modified Waterfall
   d) Sashimi

9. **Which is a common software vulnerability?**
   a) Encryption
   b) Buffer overflow
   c) Two-factor authentication
   d) Regular expressions

10. **What is the main benefit of using automated tools in secure software development?**
    a) Reduced costs
    b) Faster bug resolution
    c) Early identification of vulnerabilities
    d) Enhanced user experience

Fill-in-the-Blank Questions (30%)

11. The _____ phase is responsible for sensitivity assessments in the SDLC.
12. Storage _____ separates corporate data from personal data in mobile devices.
13. The purpose of a Configuration Management Plan is to manage system _____ and updates.
14. NIST Special Publication _____ guides secure system configuration management.
15. Software vulnerabilities such as _____ injection can be mitigated with prepared statements.
16. The _____ model is a one-way software development framework.
17. Regular backups and secure storage help protect against data _____.
18. A security _____ outlines actions to mitigate risks during system operations.
19. The _____ phase of SDLC involves archiving and media sanitization.
20. NIST recommends integrating security into every phase of the _____.

50 Questions for Chapter 5 - Access Control and Management

Multiple-Choice Questions (70%)

1. **What is the primary purpose of access control?**
   a) To speed up system processes
   b) To restrict unauthorized access
   c) To enhance encryption capabilities
   d) To automate backups
2. **What does "authentication" verify in access control?**
   a) The resource type
   b) User permissions
   c) User identity
   d) Resource location
3. **Which access control model allows resource owners to manage permissions?**
   a) MAC
   b) RBAC
   c) DAC
   d) ABAC
4. **What is a common weakness of Discretionary Access Control (DAC)?**
   a) Requires complex algorithms
   b) Heavily reliant on user discretion
   c) Cannot be used in operating systems
   d) Incompatible with role-based access control

5. **Which role is responsible for overseeing compliance with data privacy policies?**
   a) Owner
   b) Custodian
   c) Privacy Officer
   d) End User

6. **In Mandatory Access Control (MAC), what dictates access permissions?**
   a) User discretion
   b) Organizational policies and classification labels
   c) Network administrators
   d) Encryption algorithms

7. **What does the Attribute-Based Access Control (ABAC) model consider?**
   a) User permissions only
   b) Environmental and object attributes
   c) Hardware configurations
   d) Role hierarchies

8. **What is the least restrictive access control model?**
   a) MAC
   b) ABAC
   c) DAC
   d) RBAC

9. **What is the purpose of geofencing in access control?**
   a) Tracking mobile devices
   b) Encrypting user data
   c) Restricting access based on location
   d) Managing resource ownership

10. **Which access control phase involves maintaining logs of user actions?**
    a) Authentication
    b) Authorization
    c) Accounting
    d) Identification

Fill-in-the-Blank Questions (30%)

11. The access control model that assigns permissions based on roles is _____.
12. In the MAC model, access is determined by _____ labels.
13. Geofencing uses _____ data to define physical boundaries for device operation.
14. The _____ is responsible for implementing access control policies.
15. The Attribute-Based Access Control (ABAC) model uses _____ rules for decision-making.

16. A _____ identifies a resource that a subject interacts with in access control.
17. The _____ phase involves verifying user credentials during access control.
18. Discretionary Access Control (DAC) is commonly implemented in _____ systems.
19. An organization's _____ policies help enforce consistent access control measures.
20. User Access Control (UAC) is a feature used in _____ to manage privileges.

---

50 Questions for Chapter 6 - Security in the Network and Internet

Multiple-Choice Questions (70%)

1. **What distinguishes a network from a stand-alone device?**
   a) Physical portability
   b) Complexity of operations
   c) Exposure to external environments
   d) Speed of processing

2. **What layer in the OSI model manages end-to-end communication and error correction?**
   a) Network Layer
   b) Session Layer
   c) Transport Layer
   d) Data Link Layer

3. **Which protocol is widely used for web traffic?**
   a) SMTP
   b) Telnet
   c) HTTP
   d) SNMP

4. **What is a major vulnerability of networks?**
   a) Unknown routing paths
   b) Standardized encryption protocols
   c) Enclosed communication boundaries
   d) Predictable node behavior

5. **What is the primary purpose of a firewall in network security?**
   a) Encrypt data
   b) Block unauthorized access
   c) Analyze network packets
   d) Automate routing decisions

6. **Which type of attack involves intercepting and modifying communications between two parties?**
   a) Spoofing
   b) Denial of Service

c) Man-in-the-Middle
d) Buffer Overflow

7. **What is the primary function of a port scan in a network attack?**
   a) To encrypt communications
   b) To gather information about open services
   c) To establish secure connections
   d) To block unauthorized access

8. **Which type of network covers a large geographic area?**
   a) LAN
   b) WAN
   c) PAN
   d) MAN

9. **What does TCP/IP ensure in a network communication?**
   a) User authentication
   b) Correct packet sequencing
   c) Encrypted payload delivery
   d) Hardware compatibility

10. **Which is a characteristic of internetworks?**
    a) Single-point ownership
    b) Heterogeneous structure
    c) Centralized access control
    d) Minimal user connectivity

Fill-in-the-Blank Questions (30%)

11. The _____ layer of the OSI model is responsible for routing packets.
12. TCP/IP uses _____ numbers to designate specific applications.
13. A _____ attack floods a target with SYN requests without completing the handshake.
14. _____ is a technique used to define geographical boundaries for device operation.
15. The primary goal of a _____ is to inspect and control incoming and outgoing traffic.
16. A _____ attack exploits a vulnerability to gain control of a remote system.
17. A _____ is a network of networks, often managed by different entities.
18. The process of breaking data into smaller units for transmission is called _____.
19. Network _____ refers to the lack of control over unknown paths.
20. A _____ is a tool that monitors and alerts administrators about network threats.

0 Questions for Chapter 7 - Cloud Security

Multiple-Choice Questions (70%)

1. **What is the top reported cloud security challenge?**
   a) Insecure APIs
   b) Data loss and leakage
   c) Lack of scalability
   d) Compliance issues

2. **Which is a common cause of cloud security breaches?**
   a) Insufficient server backups
   b) Misconfiguration of cloud platforms
   c) Excessive encryption
   d) Weak hardware infrastructure

3. **What is a significant benefit of cloud-based security solutions?**
   a) Increased local storage
   b) Better scalability and flexibility
   c) Limited automation options
   d) Reduced encryption overhead

4. **What percentage of organizations report a lack of confidence in their cloud security posture?**
   a) 50%
   b) 72%
   c) 85%
   d) 96%

5. **Which attack is on the rise in cloud environments?**
   a) Man-in-the-Middle
   b) Cryptojacking
   c) SQL Injection
   d) Phishing

6. **What does DLP in cloud security stand for?**
   a) Data Loss Prevention
   b) Distributed Log Processing
   c) Dynamic Layer Protection
   d) Data Link Protocol

7. **Which tool helps detect and prevent cloud misconfigurations?**
   a) API Gateway
   b) SIEM solutions
   c) Cloud automation scripts
   d) DLP tools

8. **What is a barrier to cloud-based security adoption?**
   a) Increased speed of deployment
   b) Lack of expertise/training

c) Enhanced cost efficiency
d) Integration with existing systems

9. **What method protects sensitive data in cloud environments?**
   a) Default settings
   b) Strong encryption
   c) Public cloud interfaces
   d) Simplified authentication

10. **What is the primary concern with insecure APIs?**
    a) Slower communication
    b) Vulnerability to attacks
    c) Lack of user management
    d) Reduced scalability

Fill-in-the-Blank Questions (30%)

11. The _____ report highlights the latest cloud security challenges.
12. Misconfigurations in cloud platforms often expose _____ data.
13. Cloud cryptojacking involves attackers using resources to mine _____.
14. _____ tools help prevent unauthorized data transfers in cloud environments.
15. Cloud-based security solutions offer better _____ than on-premises tools.
16. The process of managing multiple cloud environments is called _____ cloud management.
17. A _____ response tool helps mitigate cloud threats faster.
18. Regular _____ can help prevent ransomware risks in the cloud.
19. Cloud providers offer _____ encryption solutions to secure data.
20. Organizations face challenges securing _____ in cloud environments.

---

50 Questions for Chapter 8 - Mobile and Embedded Device Security

Multiple-Choice Questions (70%)

1. **What is a feature phone?**
   a) A phone with only SMS capabilities
   b) A traditional phone with limited features
   c) A smartphone with advanced encryption
   d) A device primarily for gaming

2. **What risk does GPS tagging pose to mobile devices?**
   a) Loss of performance

b) Increased exposure to targeted attacks
c) Reduced battery life
d) Inconsistent connectivity

3. **Which technique separates corporate and personal data on mobile devices?**
   a) Encryption
   b) Containerization
   c) Geo-fencing
   d) Sideloading

4. **What is the primary goal of mobile device management (MDM)?**
   a) Managing updates and encryption
   b) Reducing device size
   c) Enhancing app performance
   d) Preventing malware

5. **What is a sideloading risk in mobile devices?**
   a) Improved app performance
   b) Access to malicious applications
   c) Enhanced app compatibility
   d) Reduced encryption needs

6. **Which embedded system is often part of IoT devices?**
   a) Mainframes
   b) Smart thermostats
   c) Supercomputers
   d) Gaming consoles

7. **What is the main risk of using QR codes?**
   a) Shortened URLs
   b) Malware injection
   c) Reduced performance
   d) Lack of encryption

8. **What percentage of laptop thefts occur in unattended cars?**
   a) 20%
   b) 25%
   c) 15%
   d) 30%

9. **Which of the following helps reduce mobile device theft risks?**
   a) Using white headphone cords
   b) Keeping devices out of sight in high-risk areas
   c) Disabling encryption settings
   d) Using feature phones instead of smartphones

10. **What is a common feature of wearable technology?**
    a) Replaceable batteries

b) Connectivity to smartphones
c) Built-in GPS tagging
d) Ability to run desktop applications

Fill-in-the-Blank Questions (30%)

11. A _____ is a type of portable computing device without a keyboard.
12. GPS tagging adds _____ data to media files.
13. The risk of _____ increases when mobile devices access untrusted content.
14. Mobile device theft often occurs in _____ locations.
15. The process of bypassing built-in mobile security limitations is called _____.
16. Smartphones are considered _____ personal computers.
17. Mobile management tools enforce _____ settings on devices.
18. _____ codes are vulnerable to redirection to malicious sites.
19. Storage segmentation creates separate _____ for corporate and personal data.
20. Mobile device management uses _____ updates for remote configuration.

50 Questions for Chapter 9 - Operating System Security

Multiple-Choice Questions (70%)

1. **What is the primary function of an operating system?**
   a) Encrypting data
   b) Managing hardware and software resources
   c) Monitoring network activity
   d) Detecting malware
2. **What are the three components of an operating system security environment?**
   a) Processes, Kernels, and Memory
   b) Memory, Services, and Files
   c) Authentication, Authorization, and Auditing
   d) Processes, Services, and Encryption
3. **What is the purpose of a BIOS password?**
   a) Prevent access to the hard drive
   b) Block unauthorized changes during booting
   c) Encrypt the boot sequence
   d) Log all boot events
4. **Which of the following helps prevent dictionary attacks on passwords?**
   a) Using encryption algorithms

b) Implementing salt with passwords
c) Storing passwords in plain text
d) Using multiple user accounts

5. **What is the primary concern with FTP in file transfers?**
   a) Speed of transfer
   b) Lack of encryption for credentials
   c) Compatibility issues
   d) Difficult configuration

6. **Which component is used for storing and retrieving sensitive data in an OS?**
   a) Services
   b) Memory
   c) Files
   d) Networking protocols

7. **What is a chroot jail used for?**
   a) Encrypting files on the server
   b) Restricting server's view of the file system
   c) Logging unauthorized access
   d) Improving application performance

8. **Which of the following is an operating system vulnerability?**
   a) Frequent patching
   b) Internet Information Services (IIS)
   c) Mandatory access control
   d) Layered encryption

9. **Which technique ensures virtual machines are isolated from each other?**
   a) File permissions
   b) Hypervisor monitoring
   c) BIOS configuration
   d) Memory segregation

10. **What does a security hardening guide recommend for operating systems?**
    a) Installing default software configurations
    b) Enabling all services by default
    c) Disabling unnecessary applications
    d) Using local rather than remote administration

Fill-in-the-Blank Questions (30%)

11. The primary role of _____ is to manage system resources and provide services to users.

12. A _____ attack guesses passwords by hashing dictionary words and comparing them with stored hashes.

13. FTP transmits usernames and passwords in _____.
14. Virtual machines are managed by software known as the _____.
15. The use of _____ with passwords makes brute-force attacks more difficult.
16. _____ tools help monitor and analyze logging information for suspicious behavior.
17. The process of loading an OS into memory from a powered-off state is called _____.
18. Operating system security is improved by removing _____ services and applications.
19. A _____ provides multi-layer security by restricting access to specific parts of a file system.
20. To ensure system security, organizations should enforce _____ for sensitive operations.

---

50 Questions for Chapter 10 - Computer Security Incident Handling

Multiple-Choice Questions (70%)

1. **What is the purpose of incident response?**
   a) To ensure systems are patched
   b) To minimize the impact of security incidents
   c) To automate data backups
   d) To improve system performance
2. **What is the first phase of the Incident Response Life Cycle?**
   a) Detection and Analysis
   b) Preparation
   c) Containment, Eradication, and Recovery
   d) Post-Incident Activity
3. **Which team model is ideal for small organizations with centralized IT operations?**
   a) Coordinating Team Model
   b) Distributed Model
   c) Centralized Model
   d) Ad hoc Model
4. **What is the goal of the containment phase in incident handling?**
   a) Recover deleted data
   b) Stop the spread of the incident
   c) Identify all vulnerabilities
   d) Document the root cause
5. **Which type of detection involves tools like SIEM and IDS?**
   a) User reporting
   b) Threat hunting
   c) Automated monitoring
   d) Manual analysis

6. **What is the purpose of a Lessons Learned Meeting?**
   a) Coordinate with external agencies
   b) Share security tools
   c) Improve future incident responses
   d) Notify employees about threats

7. **What does IOC stand for in incident analysis?**
   a) Indicators of Containment
   b) Indicators of Compromise
   c) Incident Operational Criteria
   d) Incident Of Concern

8. **What activity is part of the Post-Incident phase?**
   a) Isolating affected systems
   b) Erasing malicious data
   c) Conducting a metrics review
   d) Analyzing threats in real-time

9. **Which strategy ensures evidence integrity during incident handling?**
   a) Manual tracking
   b) Digital signatures
   c) Automated backups
   d) Root cause analysis

10. **What is the main challenge in sharing incident-related data?**
    a) Lack of storage capacity
    b) Privacy concerns
    c) Manual tracking
    d) Slow system speeds

Fill-in-the-Blank Questions (30%)

11. The _____ phase involves developing policies and acquiring tools for incident handling.
12. During the _____ phase, organizations isolate threats and restore systems.
13. The process of identifying abnormal behavior in systems is called _____.
14. Indicators of Compromise (IOCs) include IP addresses and _____ hashes.
15. A Lessons Learned Meeting focuses on documenting insights to improve _____ strategies.
16. Incident response plans must include protocols for notifying _____.
17. Threat intelligence feeds help identify _____ threats.
18. Restoring data from backups is part of the _____ phase.
19. Incident response teams use _____ tools to track and manage incidents.

20. Analyzing metrics such as response time is part of the _____ phase.

Chapter 11 - AI's Role in Cybersecurity Threats and Defenses

Multiple-Choice Questions (70%)

1. **What is the primary role of AI in threat detection systems?**
   a) Encrypting communication channels
   b) Automating threat identification and response
   c) Reducing system processing time
   d) Enhancing user interface design

2. **Which of the following is an example of AI-powered cybersecurity threats?**
   a) Malware analysis
   b) Automated threat detection
   c) AI-enhanced phishing attacks
   d) Endpoint monitoring

3. **What is a key application of predictive threat modeling using AI?**
   a) Analyzing past cyber incidents
   b) Predicting potential attack vectors
   c) Encrypting sensitive files
   d) Training cybersecurity staff

4. **How does AI enhance vulnerability management?**
   a) By automating compliance reporting
   b) By identifying and prioritizing vulnerabilities
   c) By blocking all potential threats
   d) By replacing traditional security teams

5. **What type of cybersecurity risk is addressed by AI in endpoint security?**
   a) Predictable data traffic
   b) Unauthorized device access
   c) System performance optimization
   d) Public key distribution

6. **Which AI application is used in fraud detection?**
   a) Behavioral biometrics
   b) Endpoint monitoring
   c) Data exfiltration detection
   d) Smart city monitoring

7. **What is AI-driven threat hunting?**
   a) The use of AI to identify vulnerabilities in other AI systems
   b) The proactive search for potential cyber threats using AI
   c) Automating compliance audits
   d) Training staff on security protocols

8. **How does AI support security operations centers (SOCs)?**
   a) By eliminating manual incident response
   b) By automating log analysis and threat prioritization
   c) By redesigning network architecture
   d) By improving password complexity

9. **What is a significant benefit of using AI in detecting DDoS attacks?**
   a) Encrypting network traffic
   b) Identifying patterns in traffic anomalies
   c) Reducing the bandwidth of malicious traffic
   d) Automating user authentication

10. **How is AI used in cybersecurity training?**
    a) To create realistic threat simulations
    b) To replace traditional training programs
    c) To manage access control
    d) To perform compliance monitoring

Fill-in-the-Blank Questions (30%)

11. AI enhances phishing prevention by detecting _____ patterns in emails.
12. _____ systems use AI to detect insider threats based on user behavior.
13. AI in fraud detection relies on _____ biometrics to identify anomalies.
14. Predictive analytics in cybersecurity uses _____ models to anticipate attacks.
15. AI-powered incident response automates _____ to minimize response times.
16. In endpoint security, AI monitors _____ traffic to detect anomalies.
17. AI enhances IoT security by identifying vulnerabilities in _____ devices.
18. Threat intelligence gathering with AI relies on _____ data feeds for analysis.
19. AI helps secure e-commerce platforms by detecting _____ attempts during transactions.
20. AI-powered DLP solutions protect against _____ data breaches.

RESPONSES

Chapter 1,2 - Overview of Security Principles and Introduction

Choice Questions (70%)

1. What are the three components of the CIA Triad in computer security?
   Answer: b) Confidentiality, Integrity, Availability
2. What type of security involves safeguarding against human error and system failures?
   Answer: c) Reliability and redundancy
3. What is the primary focus of computer security?
   Answer: b) Protecting systems from malicious activities
4. What does the NIST Computer Security Handbook define as a key objective of cybersecurity?
   Answer: c) Preserving integrity, availability, and confidentiality
5. What type of attack involves monitoring transmissions to obtain information?
   Answer: b) Eavesdropping
6. Which model is used to identify spoofing, tampering, and repudiation threats?
   Answer: a) STRIDE
7. Which type of risk assessment process ranks threats based on their risk levels?
   Answer: c) Risk prioritization
8. What are assets in the context of threat modeling?
   Answer: c) Valuable data or system components
9. Which threat modeling technique evaluates the damage caused by a threat?
   Answer: a) DREAD
10. Which of the following is a human vulnerability in security systems?
    Answer: b) Social engineering attacks

Fill-in-the-Blank Questions (30%)

11. The CIA Triad consists of Confidentiality, Integrity, and _____.
    Answer: Availability
12. A _____ attack involves unauthorized modification of data.
    Answer: Tampering
13. The STRIDE model stands for Spoofing, Tampering, Repudiation, Information Disclosure, _____, and Elevation of Privilege.
    Answer: Denial of Service

14. The _____ model assigns risk levels based on damage, reproducibility, exploitability, affected users, and discoverability.
    Answer: DREAD
15. Risk _____ involves calculating the likelihood and impact of threats.
    Answer: Assessment
16. Social engineering attacks often exploit _____ vulnerabilities.
    Answer: Human
17. The goal of threat modeling is to develop targeted _____ measures.
    Answer: Security
18. Vulnerability _____ includes discovery, disclosure, patching, and testing.
    Answer: Lifecycle
19. A _____ attack occurs when an adversary denies involvement in an action.
    Answer: Repudiation
20. The NIST framework emphasizes _____ management as a key step in mitigating risks.
    Answer: Proactive

Chapter 3 - Review of Cryptography

Choice Questions (70%)

1. What is the primary goal of encryption?
   Answer: b) Encode messages to obscure their meaning
2. Which cipher shifts letters by a fixed number of places in the alphabet?
   Answer: c) Caesar cipher
3. Which encryption method uses the same key for encryption and decryption?
   Answer: a) Symmetric encryption
4. What is the primary weakness of the Caesar cipher?
   Answer: c) Predictable patterns
5. What is the key feature of one-time pad encryption?
   Answer: b) Perfect secrecy
6. Which cryptography technique involves reordering characters in plaintext?
   Answer: b) Transposition
7. What is the primary function of a cryptanalyst?
   Answer: b) Deciphering ciphertext
8. Which algorithm is widely used for public-key encryption?
   Answer: c) RSA

9. What is the process of converting ciphertext back to plaintext?
   Answer: c) Decryption

10. What does DES primarily rely on for encryption?
    Answer: b) Substitution and transposition

Fill-in-the-Blank Questions (30%)

11. The two main types of encryption are symmetric and _____.
    Answer: Asymmetric

12. A cryptosystem must ensure that plaintext is equal to _____ of the ciphertext.
    Answer: Decryption

13. The Caesar cipher achieves encryption by _____ the alphabet.
    Answer: Shifting

14. Transposition techniques achieve encryption through character _____.
    Answer: Reordering

15. Perfect secrecy is achieved with a _____ cipher.
    Answer: One-time pad

16. The RSA algorithm is an example of _____ encryption.
    Answer: Public-key

17. Shannon's theory of good ciphers emphasizes _____ and diffusion.
    Answer: Confusion

18. Cryptanalysis involves analyzing _____ to decipher encoded messages.
    Answer: Ciphertext

19. The primary goal of _____ is to spread plaintext information across ciphertext.
    Answer: Diffusion

20. A secure cipher must resist brute-force attacks and statistical _____.
    Answer: Analysis

Chapter 4 - Security in the Software Development Life Cycle

Choice Questions (70%)

1. What is the primary goal of secure software development?
   Answer: b) To prevent vulnerabilities and resist attacks

2. Which phase of the SDLC focuses on defining security needs and sensitivity assessments?
   Answer: c) Initiation

3. Which NIST publication provides guidelines for integrating security into the SDLC?
   Answer: b) 800-14

4. What is the purpose of a Configuration Management Plan (CMP)?
   Answer: b) To track and control changes to the system
5. What does "containerization" in storage segmentation aim to achieve?
   Answer: b) Separating business and personal data
6. Which SDLC phase involves implementing security testing and accreditation?
   Answer: c) Implementation
7. What is the role of the Configuration Control Board (CCB)?
   Answer: b) To approve and monitor changes
8. Which model of software development allows overlapping phases?
   Answer: d) Sashimi
9. Which is a common software vulnerability?
   Answer: b) Buffer overflow
10. What is the main benefit of using automated tools in secure software development?
    Answer: c) Early identification of vulnerabilities

Fill-in-the-Blank Questions (30%)

11. The _____ phase is responsible for sensitivity assessments in the SDLC.
    Answer: Initiation
12. Storage _____ separates corporate data from personal data in mobile devices.
    Answer: Segmentation
13. The purpose of a Configuration Management Plan is to manage system _____ and updates.
    Answer: Changes
14. NIST Special Publication _____ guides secure system configuration management.
    Answer: 800-128
15. Software vulnerabilities such as _____ injection can be mitigated with prepared statements.
    Answer: SQL
16. The _____ model is a one-way software development framework.
    Answer: Waterfall
17. Regular backups and secure storage help protect against data _____.
    Answer: Loss
18. A security _____ outlines actions to mitigate risks during system operations.
    Answer: Plan

19. The _____ phase of SDLC involves archiving and media sanitization.
    Answer: Disposal
20. NIST recommends integrating security into every phase of the _____.
    Answer: SDLC

Chapter 5 - Access Control and Management

Choice Questions (70%)

1. What is the primary purpose of access control?
   Answer: b) To restrict unauthorized access
2. What does "authentication" verify in access control?
   Answer: c) User identity
3. Which access control model allows resource owners to manage permissions?
   Answer: c) DAC
4. What is a common weakness of Discretionary Access Control (DAC)?
   Answer: b) Heavily reliant on user discretion
5. Which role is responsible for overseeing compliance with data privacy policies?
   Answer: c) Privacy Officer
6. In Mandatory Access Control (MAC), what dictates access permissions?
   Answer: b) Organizational policies and classification labels
7. What does the Attribute-Based Access Control (ABAC) model consider?
   Answer: b) Environmental and object attributes
8. What is the least restrictive access control model?
   Answer: c) DAC
9. What is the purpose of geofencing in access control?
   Answer: c) Restricting access based on location
10. Which access control phase involves maintaining logs of user actions?
    Answer: c) Accounting

Fill-in-the-Blank Questions (30%)

11. The access control model that assigns permissions based on roles is _____.
    Answer: RBAC
12. In the MAC model, access is determined by _____ labels.
    Answer: Classification

13. Geofencing uses _____ data to define physical boundaries for device operation.
    Answer: Location

14. The _____ is responsible for implementing access control policies.
    Answer: Custodian

15. The Attribute-Based Access Control (ABAC) model uses _____ rules for decision-making.
    Answer: Conditional

16. A _____ identifies a resource that a subject interacts with in access control.
    Answer: Object

17. The _____ phase involves verifying user credentials during access control.
    Answer: Authentication

18. Discretionary Access Control (DAC) is commonly implemented in _____ systems.
    Answer: Operating

19. An organization's _____ policies help enforce consistent access control measures.
    Answer: Security

20. User Access Control (UAC) is a feature used in _____ to manage privileges.
    Answer: Windows

Chapter 6 - Security in the Network and Internet

Choice Questions (70%)

1. What distinguishes a network from a stand-alone device?
   Answer: c) Exposure to external environments

2. What layer in the OSI model manages end-to-end communication and error correction?
   Answer: c) Transport Layer

3. Which protocol is widely used for web traffic?
   Answer: c) HTTP

4. What is a major vulnerability of networks?
   Answer: a) Unknown routing paths

5. What is the primary purpose of a firewall in network security?
   Answer: b) Block unauthorized access

6. Which type of attack involves intercepting and modifying communications between two parties?
   Answer: c) Man-in-the-Middle

7. What is the primary function of a port scan in a network attack?
   Answer: b) To gather information about open services

8. Which type of network covers a large geographic area?
   Answer: b) WAN

9. What does TCP/IP ensure in a network communication?
   Answer: b) Correct packet sequencing

10. Which is a characteristic of internetworks?
    Answer: b) Heterogeneous structure

Fill-in-the-Blank Questions (30%)

11. The _____ layer of the OSI model is responsible for routing packets.
    Answer: Network

12. TCP/IP uses _____ numbers to designate specific applications.
    Answer: Port

13. A _____ attack floods a target with SYN requests without completing the handshake.
    Answer: SYN flood

14. _____ is a technique used to define geographical boundaries for device operation.
    Answer: Geofencing

15. The primary goal of a _____ is to inspect and control incoming and outgoing traffic.
    Answer: Firewall

16. A _____ attack exploits a vulnerability to gain control of a remote system.
    Answer: Remote code execution

17. A _____ is a network of networks, often managed by different entities.
    Answer: Internetwork

18. The process of breaking data into smaller units for transmission is called _____.
    Answer: Fragmentation

19. Network _____ refers to the lack of control over unknown paths.
    Answer: Vulnerability

20. A _____ is a tool that monitors and alerts administrators about network threats.
    Answer: Intrusion Detection System

Chapter 7 - Cloud Security

Choice Questions (70%)

1. What is the top reported cloud security challenge?
   Answer: b) Data loss and leakage

2. Which is a common cause of cloud security breaches?
   Answer: b) Misconfiguration of cloud platforms

3. What is a significant benefit of cloud-based security solutions?
   Answer: b) Better scalability and flexibility
4. What percentage of organizations report a lack of confidence in their cloud security posture?
   Answer: b) 72%
5. Which attack is on the rise in cloud environments?
   Answer: b) Cryptojacking
6. What does DLP in cloud security stand for?
   Answer: a) Data Loss Prevention
7. Which tool helps detect and prevent cloud misconfigurations?
   Answer: b) SIEM solutions
8. What is a barrier to cloud-based security adoption?
   Answer: b) Lack of expertise/training
9. What method protects sensitive data in cloud environments?
   Answer: b) Strong encryption
10. What is the primary concern with insecure APIs?
    Answer: b) Vulnerability to attacks

Fill-in-the-Blank Questions (30%)

11. The _____ report highlights the latest cloud security challenges.
    Answer: Cloud Security
12. Misconfigurations in cloud platforms often expose _____ data.
    Answer: Sensitive
13. Cloud cryptojacking involves attackers using resources to mine _____.
    Answer: Cryptocurrency
14. _____ tools help prevent unauthorized data transfers in cloud environments.
    Answer: DLP
15. Cloud-based security solutions offer better _____ than on-premises tools.
    Answer: Scalability
16. The process of managing multiple cloud environments is called _____ cloud management.
    Answer: Multi
17. A _____ response tool helps mitigate cloud threats faster.
    Answer: Automated
18. Regular _____ can help prevent ransomware risks in the cloud.
    Answer: Backups

19. Cloud providers offer _____ encryption solutions to secure data.
    Answer: Built-in

20. Organizations face challenges securing _____ in cloud environments.
    Answer: APIs

Chapter 8 - Mobile and Embedded Device Security

Choice Questions (70%)

1. What is a feature phone?
   Answer: b) A traditional phone with limited features

2. What risk does GPS tagging pose to mobile devices?
   Answer: b) Increased exposure to targeted attacks

3. Which technique separates corporate and personal data on mobile devices?
   Answer: b) Containerization

4. What is the primary goal of mobile device management (MDM)?
   Answer: a) Managing updates and encryption

5. What is a sideloading risk in mobile devices?
   Answer: b) Access to malicious applications

6. Which embedded system is often part of IoT devices?
   Answer: b) Smart thermostats

7. What is the main risk of using QR codes?
   Answer: b) Malware injection

8. What percentage of laptop thefts occur in unattended cars?
   Answer: b) 25%

9. Which of the following helps reduce mobile device theft risks?
   Answer: b) Keeping devices out of sight in high-risk areas

10. What is a common feature of wearable technology?
    Answer: b) Connectivity to smartphones

Fill-in-the-Blank Questions (30%)

11. A _____ is a type of portable computing device without a keyboard.
    Answer: Tablet

12. GPS tagging adds _____ data to media files.
    Answer: Geographical

13. The risk of _____ increases when mobile devices access untrusted content.
    Answer: Malware

14. Mobile device theft often occurs in _____ locations.
    Answer: Public

15. The process of bypassing built-in mobile security limitations is called _____.
    Answer: Jailbreaking

16. Smartphones are considered _____ personal computers.
    Answer: Handheld

17. Mobile management tools enforce _____ settings on devices.
    Answer: Encryption

18. _____ codes are vulnerable to redirection to malicious sites.
    Answer: QR

19. Storage segmentation creates separate _____ for corporate and personal data.
    Answer: Containers

20. Mobile device management uses _____ updates for remote configuration.
    Answer: Over-the-air

Chapter 9 - Operating System Security

Choice Questions (70%)

1. What is the primary function of an operating system?
   Answer: b) Managing hardware and software resources

2. What are the three components of an operating system security environment?
   Answer: b) Memory, Services, and Files

3. What is the purpose of a BIOS password?
   Answer: b) Block unauthorized changes during booting

4. Which of the following helps prevent dictionary attacks on passwords?
   Answer: b) Implementing salt with passwords

5. What is the primary concern with FTP in file transfers?
   Answer: b) Lack of encryption for credentials

6. Which component is used for storing and retrieving sensitive data in an OS?
   Answer: c) Files

7. What is a chroot jail used for?
   Answer: b) Restricting server's view of the file system

8. Which of the following is an operating system vulnerability?
   Answer: b) Internet Information Services (IIS)

9. Which technique ensures virtual machines are isolated from each other?
   Answer: b) Hypervisor monitoring
10. What does a security hardening guide recommend for operating systems?
    Answer: c) Disabling unnecessary applications

Fill-in-the-Blank Questions (30%)

11. The primary role of _____ is to manage system resources and provide services to users.
    Answer: Operating systems
12. A _____ attack guesses passwords by hashing dictionary words and comparing them with stored hashes.
    Answer: Dictionary
13. FTP transmits usernames and passwords in _____.
    Answer: Plaintext
14. Virtual machines are managed by software known as the _____.
    Answer: Hypervisor
15. The use of _____ with passwords makes brute-force attacks more difficult.
    Answer: Salt
16. _____ tools help monitor and analyze logging information for suspicious behavior.
    Answer: Intrusion Detection
17. The process of loading an OS into memory from a powered-off state is called _____.
    Answer: Booting
18. Operating system security is improved by removing _____ services and applications.
    Answer: Unnecessary
19. A _____ provides multi-layer security by restricting access to specific parts of a file system.
    Answer: Chroot jail
20. To ensure system security, organizations should enforce _____ for sensitive operations.
    Answer: Password policies

Chapter 10 - Computer Security Incident Handling

Choice Questions (70%)

1. What is the purpose of incident response?
   Answer: b) To minimize the impact of security incidents
2. What is the first phase of the Incident Response Life Cycle?
   Answer: b) Preparation

3. Which team model is ideal for small organizations with centralized IT operations?
   Answer: c) Centralized Model
4. What is the goal of the containment phase in incident handling?
   Answer: b) Stop the spread of the incident
5. Which type of detection involves tools like SIEM and IDS?
   Answer: c) Automated monitoring
6. What is the purpose of a Lessons Learned Meeting?
   Answer: c) Improve future incident responses
7. What does IOC stand for in incident analysis?
   Answer: b) Indicators of Compromise
8. What activity is part of the Post-Incident phase?
   Answer: c) Conducting a metrics review
9. Which strategy ensures evidence integrity during incident handling?
   Answer: b) Digital signatures
10. What is the main challenge in sharing incident-related data?
    Answer: b) Privacy concerns

Fill-in-the-Blank Questions (30%)

11. The _____ phase involves developing policies and acquiring tools for incident handling.
    Answer: Preparation
12. During the _____ phase, organizations isolate threats and restore systems.
    Answer: Containment
13. The process of identifying abnormal behavior in systems is called _____.
    Answer: Detection
14. Indicators of Compromise (IOCs) include IP addresses and _____ hashes.
    Answer: File
15. A Lessons Learned Meeting focuses on documenting insights to improve _____ strategies.
    Answer: Response
16. Incident response plans must include protocols for notifying _____.
    Answer: Stakeholders
17. Threat intelligence feeds help identify _____ threats.
    Answer: Emerging
18. Restoring data from backups is part of the _____ phase.
    Answer: Recovery

19. Incident response teams use _____ tools to track and manage incidents.
    Answer: Monitoring

20. Analyzing metrics such as response time is part of the _____ phase.
    Answer: Post-Incident

Chapter 11 - AI's Role in Cybersecurity Threats and Defenses

Multiple-Choice Questions (70%)

1. **What is the primary role of AI in threat detection systems?**
   Answer: b) Automating threat identification and response

2. **Which of the following is an example of AI-powered cybersecurity threats?**
   Answer: c) AI-enhanced phishing attacks

3. **What is a key application of predictive threat modeling using AI?**
   Answer: b) Predicting potential attack vectors

4. **How does AI enhance vulnerability management?**
   Answer: b) By identifying and prioritizing vulnerabilities

5. **What type of cybersecurity risk is addressed by AI in endpoint security?**
   Answer: b) Unauthorized device access

6. **Which AI application is used in fraud detection?**
   Answer: a) Behavioral biometrics

7. **What is AI-driven threat hunting?**
   Answer: b) The proactive search for potential cyber threats using AI

8. **How does AI support security operations centers (SOCs)?**
   Answer: b) By automating log analysis and threat prioritization

9. **What is a significant benefit of using AI in detecting DDoS attacks?**
   Answer: b) Identifying patterns in traffic anomalies

10. **How is AI used in cybersecurity training?**
    Answer: a) To create realistic threat simulations

Fill-in-the-Blank Questions (30%)

11. AI enhances phishing prevention by detecting _____ patterns in emails.
    Answer: Behavioral

12. _____ systems use AI to detect insider threats based on user behavior.
    Answer: User and Entity Behavior Analytics (UEBA)

13. AI in fraud detection relies on _____ biometrics to identify anomalies.
    Answer: Behavioral

14. Predictive analytics in cybersecurity uses _____ models to anticipate attacks.
    Answer: Machine learning

15. AI-powered incident response automates _____ to minimize response times.
    Answer: Threat analysis

16. In endpoint security, AI monitors _____ traffic to detect anomalies.
    Answer: Network

17. AI enhances IoT security by identifying vulnerabilities in _____ devices.
    Answer: Connected

18. Threat intelligence gathering with AI relies on _____ data feeds for analysis.
    Answer: Real-time

19. AI helps secure e-commerce platforms by detecting _____ attempts during transactions.
    Answer: Fraudulent

20. AI-powered DLP solutions protect against _____ data breaches.
    Answer: Accidental