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
   Answer: b

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
   Answer: c

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
   Answer: b

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
   Answer: c

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

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

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
Answer: c

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
   Answer: c

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

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
    Answer: b

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

---

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
   Answer: b

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
   Answer: c

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

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

5. **What is the key feature of one-time pad encryption?**
   a) Reusable keys
   b) Perfect secrecy

c) Symmetric key generation
d) Complex implementation
Answer: b

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

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

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

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

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

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

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
   Answer: b

2. **Which phase of the SDLC focuses on defining security needs and sensitivity assessments?**
   a) Disposal
   b) Development/Acquisition
   c) Initiation
   d) Implementation
   Answer: c

3. **Which NIST publication provides guidelines for integrating security into the SDLC?**
   a) 800-128
   b) 800-14
   c) 800-53
   d) 800-37
   Answer: b

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
   Answer: b

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
   Answer: b

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

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
   Answer: b

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

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

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
Answer: c

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

---

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
Answer: b

2. **What does "authentication" verify in access control?**
   a) The resource type
   b) User permissions
   c) User identity
   d) Resource location
   Answer: c

3. **Which access control model allows resource owners to manage permissions?**
   a) MAC
   b) RBAC
   c) DAC
   d) ABAC
   Answer: c

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
   Answer: b

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

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
   Answer: b

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
   Answer: b

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

d) RBAC
Answer: c

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
Answer: c

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

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

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
   Answer: c

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
   Answer: c

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

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

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
   Answer: b

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
   Answer: c

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
   Answer: b

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

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

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

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

---

50 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
   Answer: b

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
   Answer: b

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
   Answer: b

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

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

c) SQL Injection
d) Phishing
Answer: b

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
Answer: a

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

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
Answer: b

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

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

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

---

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
Answer: b

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
Answer: b

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

d) Sideloading
Answer: b

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
Answer: a

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
Answer: b

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

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

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

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
Answer: b

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
Answer: b

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

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
   Answer: b

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
   Answer: b

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
   Answer: b

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
   Answer: b

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
   Answer: b

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

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
   Answer: b

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
Answer: b

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

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
Answer: c

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

---

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
   Answer: b

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
   Answer: b

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
   Answer: c

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
   Answer: b

5. **Which type of detection involves tools like SIEM and IDS?**
   a) User reporting
   b) Threat hunting
   c) Automated monitoring
   d) Manual analysis
   Answer: c

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
Answer: c

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
   Answer: b

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
   Answer: c

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

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
    Answer: b

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