# 40 multiple-choice questions and 10 fill-in-the-blank sample questions for CSI4139/CEG4399 Design of Secure Computer Systems and SEC5100 Fundamentals of Cybersecurity Fall 2024

**Multiple Choice Questions:**

1. **Which of the following best describes an "asset" in information security?**
   a) A process used to secure data
   b) A tangible or intangible resource of value
   c) A method for detecting threats
   d) A security breach
   **Answer:** b) A tangible or intangible resource of value

2. **In which phase of the software lifecycle are vulnerabilities identified and analyzed?**
   a) Implementation
   b) Monitoring
   c) Testing
   d) Design
   **Answer:** c) Testing

3. **What is the purpose of the 'Monitoring' phase in security?**
   a) To implement new security technologies
   b) To continuously assess and track security threats
   c) To install patches
   d) To create new cryptographic algorithms
   **Answer:** b) To continuously assess and track security threats

4. **Which model categorizes information security risks based on confidentiality, integrity, and availability?**
   a) STRIDE
   b) CIA Triad
   c) DREAD
   d) Bell-LaPadula
   **Answer:** b) CIA Triad

5. **What is the most significant advantage of encryption in information security?**
   a) Ensuring data integrity
   b) Securing physical assets
   c) Protecting confidentiality of data

d) Detecting intrusions
**Answer:** c) Protecting confidentiality of data

6. **A system vulnerability is defined as:**
   a) A tool to combat threats
   b) A weakness in the system that can be exploited by a threat actor
   c) A method for patching software
   d) A form of physical attack on hardware
   **Answer:** b) A weakness in the system that can be exploited by a threat actor

7. **Which of the following is considered a physical security measure?**
   a) Firewalls
   b) Biometrics
   c) Encryption algorithms
   d) Anti-virus software
   **Answer:** b) Biometrics

8. **A Denial of Service (DoS) attack is designed to:**
   a) Access confidential information
   b) Prevent access to a service
   c) Modify system files
   d) Steal user credentials
   **Answer:** b) Prevent access to a service

9. **Which of the following is a key characteristic of the STRIDE model?**
   a) It focuses on the encryption of data
   b) It categorizes threats into six distinct areas
   c) It is used to create firewalls
   d) It prevents all external attacks
   **Answer:** b) It categorizes threats into six distinct areas

10. **Which of the following is a social engineering attack?**
    a) SQL injection
    b) Phishing
    c) Buffer overflow
    d) Man-in-the-middle
    **Answer:** b) Phishing

11. **Which type of attack attempts to exhaust the resources of a network?**
    a) SQL Injection
    b) Phishing
    c) Denial of Service

d) Cross-Site Scripting
**Answer:** c) Denial of Service

12. **Which cryptographic technique uses two keys: one for encryption and another for decryption?**
    a) Symmetric encryption
    b) Hashing
    c) Asymmetric encryption
    d) Steganography
    **Answer:** c) Asymmetric encryption

13. **The primary goal of access control is to:**
    a) Encrypt user passwords
    b) Grant and restrict permissions to resources
    c) Prevent hardware failures
    d) Detect external attacks
    **Answer:** b) Grant and restrict permissions to resources

14. **Which type of malware replicates itself and spreads to other systems without user intervention?**
    a) Virus
    b) Worm
    c) Trojan
    d) Ransomware
    **Answer:** b) Worm

15. **What is the primary focus of the testing phase in software development?**
    a) Fixing software bugs
    b) Identifying security vulnerabilities
    c) Writing code
    d) Designing the interface
    **Answer:** b) Identifying security vulnerabilities

16. **In a public-key infrastructure (PKI), the responsibility of issuing and verifying certificates is managed by:**
    a) Firewalls
    b) Access control systems
    c) Certificate Authorities (CAs)
    d) Antivirus programs
    **Answer:** c) Certificate Authorities (CAs)

17. **Which of the following is a key feature of Multi-Factor Authentication (MFA)?**

a) Requires two or more methods of verification
b) Requires one-time passwords
c) Only uses biometrics
d) Uses one password for multiple services
**Answer:** a) Requires two or more methods of verification

18. **The main purpose of a firewall is to:**
a) Encrypt sensitive data
b) Monitor and control incoming and outgoing network traffic
c) Patch system vulnerabilities
d) Authenticate users
**Answer:** b) Monitor and control incoming and outgoing network traffic

19. **A zero-day vulnerability refers to:**
a) A vulnerability that has been patched
b) A vulnerability that is actively being exploited but has no patch available
c) A vulnerability only discovered by ethical hackers
d) A vulnerability in cryptographic algorithms
**Answer:** b) A vulnerability that is actively being exploited but has no patch available

20. **What type of malware is designed to demand payment after infecting a system?**
a) Trojan
b) Worm
c) Ransomware
d) Spyware
**Answer:** c) Ransomware

21. **Which phase in SDLC focuses on implementing security measures after designing the system?**
a) Planning
b) Testing
c) Implementation
d) Design
**Answer:** c) Implementation

22. **Which threat model is widely used to assess system security?**
a) STRIDE
b) DREAD
c) NIST
d) MITRE
**Answer:** a) STRIDE

23. **When dealing with identity management, which method combines multiple attributes to validate a user?**
    a) Single sign-on
    b) Multi-factor authentication
    c) Role-based access control
    d) Attribute-based access control
    **Answer:** d) Attribute-based access control

24. **The principle of 'least privilege' states that:**
    a) Users should have full access to all data
    b) Users should only have the minimum level of access required
    c) Privileges should be revoked after 30 days
    d) Systems should grant access based on seniority
    **Answer:** b) Users should only have the minimum level of access required

25. **Which protocol ensures secure communication over a computer network by encrypting data?**
    a) HTTP
    b) FTP
    c) TLS
    d) SSH
    **Answer:** c) TLS

26. **An attack that takes advantage of improper input validation is known as:**
    a) Cross-site scripting (XSS)
    b) SQL Injection
    c) Buffer Overflow
    d) Social engineering
    **Answer:** b) SQL Injection

27. **Which of the following is an example of a phishing attack?**
    a) An attacker impersonates a legitimate website to steal user information
    b) A system is overwhelmed with requests, causing a crash
    c) A hacker exploits a software vulnerability
    d) A malicious script is embedded into a web page
    **Answer:** a) An attacker impersonates a legitimate website to steal user information

28. **The goal of incident response is to:**
    a) Prevent future attacks
    b) Detect and mitigate attacks as they occur
    c) Execute denial-of-service attacks

d) Monitor network traffic
**Answer:** b) Detect and mitigate attacks as they occur

29. **Which of the following attacks exploits a vulnerability in cryptographic algorithms?**
    a) SQL injection
    b) Man-in-the-middle attack
    c) Denial of service
    d) Cryptographic brute force attack
    **Answer:** d) Cryptographic brute force attack

30. **The process of reviewing logs to identify any suspicious activity is known as:**
    a) Data mining
    b) Log analysis
    c) Vulnerability scanning
    d) Patch management
    **Answer:** b) Log analysis

31. **What is the purpose of a firewall in a network security setup?**
    a) To authenticate users accessing the network
    b) To block unauthorized access while permitting authorized communications
    c) To encrypt data transmitted over the network
    d) To detect and remove malware from systems
    **Answer:** b) To block unauthorized access while permitting authorized communications
32. **In terms of cybersecurity, what does the term "vulnerability" refer to?**
    a) A method used to defend against cyberattacks
    b) A weakness in a system that can be exploited by a threat
    c) A secure encryption algorithm
    d) A system's backup process
    **Answer:** b) A weakness in a system that can be exploited by a threat
33. **Which of the following is the primary function of antivirus software?**
    a) Prevent network traffic from being intercepted
    b) Detect and remove malicious software from computers
    c) Encrypt files stored on a hard drive
    d) Monitor user behavior on websites
    **Answer:** b) Detect and remove malicious software from computers
34. **What is the key advantage of asymmetric encryption over symmetric encryption?**
    a) It is faster to encrypt data
    b) It uses two different keys, one for encryption and one for decryption
    c) It does not require a private key
    d) It ensures that encryption keys never expire
    **Answer:** b) It uses two different keys, one for encryption and one for decryption

35. **Which attack involves intercepting communication between two systems to steal or alter information?**
    a) Phishing
    b) Man-in-the-middle attack
    c) Brute force attack
    d) Denial of service attack
    **Answer:** b) Man-in-the-middle attack
36. **A primary function of the "Monitoring" phase in cybersecurity is to:**
    a) Conduct system backups
    b) Continuously track system vulnerabilities
    c) Install new software updates
    d) Analyze data encryption methods
    **Answer:** b) Continuously track system vulnerabilities
37. **Which term refers to the method of disguising data to prevent unauthorized access while it is transmitted across a network?**
    a) Authentication
    b) Encryption
    c) Hashing
    d) Steganography
    **Answer:** b) Encryption
38. **Which of the following is an example of a social engineering attack?**
    a) Using malware to damage a system
    b) Manipulating users into providing confidential information
    c) Exploiting a software vulnerability to gain unauthorized access
    d) Flooding a server with traffic to overload it
    **Answer:** b) Manipulating users into providing confidential information
39. **Which principle in security states that users should only have access to the data and resources they need to perform their tasks?**
    a) Full access
    b) Role-based access control
    c) Least privilege
    d) Multi-factor authentication
    **Answer:** c) Least privilege
40. **A cryptographic hash function is used to:**
    a) Generate public and private key pairs
    b) Encrypt large amounts of data
    c) Verify the integrity of data by producing a fixed-length output
    d) Decrypt messages
    **Answer:** c) Verify the integrity of data by producing a fixed-length output

**10 Fill-in-the-Blank Questions:**

41. _____ encryption uses the same key for both encryption and decryption.
    **Answer:** Symmetric

42. A Denial-of-Service (DoS) attack attempts to overwhelm a _____ to make it unavailable.
**Answer:** Network/server

43. In information security, the acronym CIA stands for confidentiality, integrity, and _____.
**Answer:** Availability

44. _____ is a security measure that requires two or more methods of authentication.
**Answer:** Multi-factor authentication

45. The _____ phase in the software development lifecycle is responsible for identifying security vulnerabilities before release.
**Answer:** Testing

46. A _____ is a type of malware that demands payment to regain access to a system.
**Answer:** Ransomware

47. The _____ is a security model used to classify system threats.
**Answer:** STRIDE

48. An attacker attempting to steal login credentials by tricking users with fraudulent emails is performing a _____ attack.
**Answer:** Phishing

49. _____ ensures that a user can only access the resources necessary for their role.
**Answer:** Least privilege

50. _____ attacks exploit software vulnerabilities by injecting malicious code.
**Answer:** SQL injection