Chapter 1 of *Computer Security: Principles and Practice* (MCQs)

1. What is the primary goal of computer security?

A) To ensure data is destroyed
B) To protect confidentiality, integrity, and availability of information
C) To grant access to unauthorized users
D) To store large amounts of data
Answer: B

2. Which term refers to the preservation of restrictions on information access and disclosure?

A) Privacy
B) Data confidentiality
C) System integrity
D) Availability
Answer: B

3. What does privacy assure in terms of information collection and storage?

A) Data confidentiality
B) That individuals control what information is collected and by whom
C) Unrestricted access to all data
D) Availability
Answer: B

4. What is meant by 'data integrity'?

A) Ensuring that data is always available
B) Preserving unauthorized data access
C) Information is changed only in authorized ways
D) Ensuring that all data is stored in the cloud
Answer: C

5. What does system integrity ensure?

A) The system performs its intended function in an unimpaired manner
B) Data is corrupted
C) Unauthorized access is allowed
D) The system is available to all users
Answer: A

6. What is meant by 'availability' in computer security?

A) Limiting access to data
B) Ensuring timely and reliable access to information
C) Modifying system data
D) Creating backups of data
Answer: B

7. Which term refers to verifying the authenticity of users and the validity of messages?

A) Privacy
B) Integrity
C) Authenticity
D) Accountability
Answer: C

8. What does accountability in security support?

A) Data corruption
B) Prevention of all security measures
C) Nonrepudiation and fault isolation
D) Data deletion
Answer: C

9. What is the impact level if a security breach causes minor financial loss or harm?

A) Low
B) Moderate
C) High
D) Severe
Answer: A

10. What is an example of a high-impact security breach?

A) Minor damage to organizational assets
B) Temporary data loss
C) Severe damage to organizational operations and major financial loss
D) A brief system malfunction
Answer: C

11. Which type of attack involves an entity inside the security perimeter?

A) Insider attack
B) Outsider attack
C) Passive attack
D) Active attack
Answer: A

12. What type of security breach impacts system availability?

A) Unauthorized disclosure
B) System failure
C) Denial of service
D) Falsification
Answer: C

13. What does a passive attack attempt to do?

A) Destroy system resources
B) Modify data
C) Eavesdrop on transmissions without altering system resources
D) Disable security measures
Answer: C

14. Which of the following is NOT an example of a countermeasure?

A) Prevent
B) Recover
C) Attack
D) Detect
Answer: C

15. Which category of vulnerability involves a loss of confidentiality?

A) Corrupted
B) Leaky
C) Unavailable
D) Secured
Answer: B

16. What is an example of a network attack surface vulnerability?

A) Open ports on outward-facing servers
B) Backup failures
C) Weak encryption in local databases
D) Hardware damage
Answer: A

17. What security requirement limits access to authorized users only?

A) Availability
B) Access control
C) Confidentiality
D) Usurpation
Answer: B

18. What is the role of awareness and training in security?

A) To prevent external attacks
B) To monitor network traffic
C) To educate users on security risks and policies
D) To modify system programs
Answer: C

19. What is a masquerade attack?

A) Direct access to data
B) Intercepting a message
C) An unauthorized entity posing as an authorized user
D) Modifying a data packet
Answer: C

20. What is meant by 'defense in depth'?

A) A single layer of defense
B) Multiple layers of security controls
C) No security at all
D) Using a simple password
Answer: B

21. What is the purpose of audit and accountability in security?

A) To keep logs for network errors
B) To track and report unlawful system activities
C) To manage user passwords
D) To block all external traffic
Answer: B

22. What is the principle of 'least privilege'?

A) Allowing maximum access
B) Limiting access to the minimum level required for tasks
C) Granting all users administrative privileges
D) Disabling all security controls
Answer: B

23. Which term defines a situation where an unauthorized entity gains access to sensitive data?

A) Usurpation
B) Interception
C) Intrusion
D) Deception
Answer: C

24. What is the goal of risk assessment in security?

A) Preventing all risks
B) Evaluating and mitigating risks
C) Recovering lost data
D) Monitoring user activity
Answer: B

25. What is encapsulation in security design?

A) Exposing sensitive data
B) Hiding data and functions within a module
C) Sharing data across the network
D) Encrypting all communications
Answer: B

26. What is the role of a security policy?

A) Allow unrestricted data access
B) Provide guidelines for security rules and practices
C) Erase all system logs
D) Disable system firewalls
Answer: B

27. What does 'assurance' mean in a security context?

A) Guaranteeing unauthorized access
B) Confidence in the system's ability to enforce security policies
C) Complete vulnerability
D) Disabling encryption
Answer: B

28. What is the importance of configuration management in security?

A) Tracking network traffic
B) Managing system resources during attacks
C) Establishing secure configurations of information systems
D) Storing sensitive data
Answer: C

29. Which of the following is an example of physical and environmental protection in security?

A) Encrypting email
B) Limiting physical access to systems
C) Installing anti-virus software
D) Backing up data on the cloud
Answer: B

30. What is a common human attack surface vulnerability?

A) Hardware failure
B) Social engineering
C) Network congestion
D) Memory leaks
Answer: B

31. What is a denial-of-service (DoS) attack?

A) An attack that steals user credentials
B) An attack that prevents legitimate users from accessing a service
C) An attack that modifies email content
D) An attack that redirects web traffic
Answer: B

32. Which type of attack involves capturing and retransmitting messages?

A) Replay attack
B) Passive attack
C) Traffic analysis
D) Insider attack
Answer: A

33. Which of the following describes 'usurpation' in security?

A) Preventing unauthorized access
B) Controlling system resources by unauthorized entities
C) Modifying system configurations
D) Logging unauthorized attempts
Answer: B

34. What does 'falsification' mean in the context of security threats?

A) Encrypting sensitive data
B) Preventing attacks from insiders
C) Providing false data to deceive authorized entities
D) Blocking malicious websites
Answer: C

35. What is an 'attack tree' used for in security?

A) Monitoring system performance
B) Analyzing the various ways a system can be attacked
C) Storing backup data
D) Detecting malware
Answer: B

36. What does the 'least astonishment' design principle refer to?

A) Making security features complex
B) Ensuring security measures are intuitive and user-friendly
C) Removing all security controls
D) Disabling encryption for easy access
Answer: B

37. What is the purpose of system and communications protection?

A) To allow free access to all data
B) To control and monitor organizational communications
C) To block all internet traffic
D) To disable firewall rules
Answer: B

38. What is an example of a software attack surface vulnerability?

A) Poor ventilation in server rooms
B) Unpatched web server software
C) USB ports left open
D) Encrypted communication lines
Answer: B

39. Which of the following is an example of a threat action categorized under 'disruption'?

A) Unauthorized data access
B) Incapacitating system components
C) Data encryption
D) System auditing
Answer: B

40. What is the primary focus of the National Institute of Standards and Technology (NIST) in terms of security?

A) To promote global trade
B) To develop standards related to security in the U.S. government and private sector
C) To provide internet access
D) To track global security breaches
Answer: B

41. What is the difference between passive and active attacks?

A) Passive attacks alter data; active attacks do not
B) Passive attacks eavesdrop without altering data; active attacks modify data
C) Active attacks are internal; passive attacks are external
D) Active attacks only occur in software systems
Answer: B

42. Which of the following principles focuses on minimizing security-related surprises to users?

A) Open design
B) Psychological acceptability
C) Layering
D) Modularity
Answer: B

43. What is a human attack surface?

A) Vulnerabilities in software code
B) Vulnerabilities created by human factors, such as social engineering or insider threats
C) Weaknesses in firewall design
D) Problems with system encryption
Answer: B

44. What is the function of incident response in computer security?

A) Disabling system audits
B) Handling security breaches, including preparation and recovery
C) Preventing external access to systems
D) Monitoring web traffic
Answer: B

45. What does 'nonrepudiation' ensure in computer security?

A) That an action cannot be denied by its originator
B) That all actions are reversible
C) That data is confidential
D) That a system is always available
Answer: A

46. What is the role of 'access control' in security?

A) To encrypt all communications
B) To allow only authorized users access to information and systems
C) To monitor the internal network
D) To perform regular data backups
Answer: B

47. What does 'residual vulnerability' refer to in the context of countermeasures?

A) The complete elimination of risk
B) Vulnerabilities that remain after security measures are applied
C) Temporary system failures
D) The ability to recover data from a breach
Answer: B

48. What does 'economy of mechanism' refer to in security design principles?

A) Using complex security mechanisms
B) Keeping security mechanisms as simple as possible
C) Reducing encryption keys
D) Limiting system access
Answer: B

49. Which of the following is a primary component of a 'computer security strategy'?

A) Random security updates
B) Security policy, implementation, assurance, and evaluation
C) Providing free access to users
D) Disabling access to the internet
Answer: B

50. What does 'modularity' refer to in fundamental security design principles?

A) Combining multiple functions into one large unit
B) Breaking systems into small, independent components
C) Using a single method for all security measures
D) Encrypting all data at rest
Answer: B

51. What is a 'countermeasure' in the context of security?

A) A technique to launch attacks on a system
B) A method to prevent, detect, or recover from security breaches
C) A type of malicious software
D) A network vulnerability
Answer: B

52. What type of attack seeks to alter system resources or disrupt their operation?

A) Passive attack
B) Active attack
C) Insider attack
D) Interception attack
Answer: B

53. Which of the following is a type of security breach that results in false data being accepted as true?

A) Exposure
B) Masquerade
C) Falsification
D) Interception
Answer: C

54. Which of the following is an example of an 'insider attack'?

A) A hacker from another country accessing a system
B) An employee stealing company data
C) An external entity altering communication channels
D) A network crash due to a power outage
Answer: B

55. What is the goal of 'nonrepudiation' in computer security?

A) Prevent unauthorized access
B) Ensure that a sender cannot deny sending a message
C) Ensure that data is not modified
D) Provide a backup for data
Answer: B

56. What does 'least common mechanism' refer to in security design?

A) Reducing the number of mechanisms shared by multiple users
B) Allowing all users to share one security mechanism
C) Using a single security policy for all systems
D) Simplifying user interfaces
Answer: A

57. Which of the following attacks would be categorized as an 'unauthorized disclosure'?

A) Interference with system functions
B) An attacker gaining access to sensitive information
C) Modification of system files
D) Preventing users from accessing a website
Answer: B

58. What is an 'attack surface' in computer security?

A) The total number of authorized users of a system
B) The set of exploitable vulnerabilities in a system
C) The geographical location of a data center
D) The encryption level of a system's data
Answer: B

59. What is meant by 'complete mediation' in security design?

A) All access to resources must be checked for proper authorization
B) Users should not have access to any system resources
C) Only privileged users can access resources
D) Resources should be freely available to all users
Answer: A

60. What is 'layering' in the context of security design principles?

A) Combining security functions into a single layer
B) Using multiple layers of defense to protect a system
C) Reducing the number of security controls
D) Granting full access to users
Answer: B

61. What is the goal of 'separation of privilege' in security design?

A) Limiting access based on user roles
B) Preventing administrators from accessing user data
C) Giving all users the same privileges
D) Combining multiple security layers into one
Answer: A

62. Which attack type involves sending a large number of requests to a system to overwhelm it?

A) Denial of service
B) Masquerade
C) Replay attack
D) Eavesdropping
Answer: A

63. What does 'psychological acceptability' focus on in security design?

A) Making security mechanisms user-friendly and easy to understand
B) Ensuring security systems are invisible to users
C) Prioritizing security over usability
D) Requiring complex passwords from all users
Answer: A

64. What is an example of a 'replay attack'?

A) Sending a legitimate message repeatedly to disrupt a service
B) Reading a message without altering it
C) Accessing a system using another user's credentials
D) Blocking messages from reaching their destination
Answer: A

65. What is a 'traffic analysis' attack?

A) Eavesdropping on a system's messages without modifying them
B) Modifying the content of messages
C) Observing patterns in network communications to gather information
D) Blocking messages from being sent
Answer: C

66. What is meant by 'fail-safe defaults' in security design principles?

A) If a security mechanism fails, the system defaults to granting access
B) If a security mechanism fails, the system defaults to denying access
C) The system shuts down in case of any security failure
D) The system automatically repairs vulnerabilities
Answer: B

67. Which type of attack aims to make services unavailable by overwhelming the system?

A) Usurpation
B) Eavesdropping
C) Denial of service
D) Falsification
Answer: C

68. What is the function of 'isolation' in security design principles?

A) Separating sensitive data and functions from less secure areas
B) Combining all system resources into one unit
C) Allowing open access to secure areas
D) Hiding the existence of security measures
Answer: A

69. What does 'misuse' refer to in terms of threat consequences?

A) Allowing unauthorized users access to secure data
B) An entity using a system component to perform unauthorized actions
C) Accessing a system with proper credentials
D) Correctly following security protocols
Answer: B

70. What is a key characteristic of a 'social engineering' attack?

A) It involves malware disguised as legitimate software
B) It exploits human behavior to gain unauthorized access
C) It requires sophisticated technical knowledge
D) It targets network vulnerabilities directly
Answer: B