◇ EASY (Q1–Q10)

Q1. The primary objective of Information Security is to ensure:
A. Speed, scalability, storage
B. Confidentiality, Integrity, Availability
C. Authentication, authorization, accounting
D. Encryption, hashing, encoding

Q2. Which component of the CIA triad is affected by a Denial-of-Service (DoS) attack?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q3. Which of the following best defines a security threat?
A. A weakness in a system
B. A potential cause of an unwanted incident
C. An actual security breach
D. A countermeasure

Q4. Which attack attempts to observe information without altering it?
A. Active attack
B. Passive attack
C. Insider attack
D. Privilege escalation

Q5. Malware that disguises itself as legitimate software is known as:
A. Worm
B. Virus
C. Trojan
D. Rootkit

Q6. Which security control category includes policies and procedures?
A. Physical
B. Technical
C. Administrative
D. Logical

Q7. Unauthorized modification of data primarily violates which CIA principle?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q8. Which of the following is an example of a physical security control?
A. Firewall

B. Encryption
C. IDS
D. Biometric access

Q9. An attacker who has legitimate access to an organization's systems is called:
A. Script kiddie
B. Hacktivist
C. Insider threat
D. Cyber terrorist

Q10. Which term refers to the path used by an attacker to gain access to a system?
A. Vulnerability
B. Exploit
C. Attack vector
D. Payload

◇ MEDIUM (Q11–Q25)

Q11. Which of the following best differentiates a threat from a vulnerability?
A. Threat is internal; vulnerability is external
B. Threat is a weakness; vulnerability is an attack
C. Threat is a potential danger; vulnerability is a weakness
D. Threat and vulnerability are identical

Q12. Traffic analysis attacks primarily compromise:
A. Integrity
B. Availability
C. Confidentiality
D. Authentication

Q13. Which attack manipulates human psychology rather than exploiting technical flaws?
A. SQL injection
B. Buffer overflow
C. Social engineering
D. ARP spoofing

Q14. Which of the following is an example of a network-based attack?
A. Shoulder surfing
B. SQL injection
C. IP spoofing
D. Logic bomb

Q15. In defense-in-depth, which layer should be considered the last line of defense?
A. Firewall

B. IDS
C. Application security
D. Data encryption

Q16. Which threat actor is most likely motivated by political or ideological goals?
A. Cyber criminal
B. Hacktivist
C. Insider
D. Script kiddie

Q17. Which attack modifies data packets during transmission?
A. Eavesdropping
B. Sniffing
C. Man-in-the-Middle
D. Traffic analysis

Q18. Malware that spreads without user interaction is classified as:
A. Virus
B. Worm
C. Trojan
D. Spyware

Q19. Which security principle ensures that users cannot deny their actions?
A. Confidentiality
B. Integrity
C. Availability
D. Non-repudiation

Q20. Which control is MOST effective against brute-force password attacks?
A. Strong hashing
B. Rate limiting
C. Encryption
D. Firewalls

Q21. A zero-day attack exploits:
A. A known vulnerability with a patch
B. A misconfigured firewall
C. An unknown vulnerability
D. Weak user passwords

Q22. Which security mechanism detects suspicious activity rather than blocking it?
A. Firewall
B. IDS
C. IPS
D. VPN

Q23. Which type of attack primarily targets availability by overwhelming resources?
A. Phishing
B. DDoS
C. SQL injection
D. Keylogging

Q24. Which of the following BEST mitigates insider threats?
A. Antivirus
B. Least privilege
C. Encryption
D. DMZ

Q25. Which attack exploits trust relationships between networked systems?
A. Replay attack
B. Spoofing
C. Dictionary attack
D. Shoulder surfing

◇ HARD (Q26–Q40)

Q26. Which CIA component is most impacted if log files are altered to hide evidence of intrusion?
A. Confidentiality
B. Availability
C. Integrity
D. Authentication

Q27. A passive attacker capturing encrypted traffic is MOST likely performing:
A. Data modification
B. Traffic analysis
C. Replay attack
D. Privilege escalation

Q28. Which security failure allowed the Equifax breach to occur?
A. Weak encryption
B. Poor authentication
C. Unpatched vulnerability
D. Insider attack

Q29. Which attack combines interception and modification of communications?
A. Sniffing
B. Spoofing
C. Man-in-the-Middle
D. Dictionary attack

Q30. Which threat model considers humans as the weakest security link?
A. Cryptographic model
B. Network model
C. Social engineering model
D. OS security model

Q31. Which attack is MOST difficult to detect in real time?
A. DoS
B. Passive eavesdropping
C. SQL injection
D. Malware infection

Q32. Which scenario BEST illustrates an integrity attack?
A. Website defacement
B. Data exfiltration
C. Service outage
D. Password guessing

Q33. A compromised admin account is MOST dangerous because it violates:
A. Least privilege
B. Defense-in-depth
C. Separation of duties
D. All of the above

Q34. Which control MOST directly prevents unauthorized data disclosure if a laptop is stolen?
A. Antivirus
B. Disk encryption
C. IDS
D. Patch management

Q35. Which attack uses previously captured authentication data to gain access?
A. Brute force
B. Replay attack
C. Dictionary attack
D. Phishing

Q36. Which threat actor typically has the highest level of resources and sophistication?
A. Script kiddie
B. Cyber criminal
C. Nation-state attacker
D. Insider

Q37. Which type of malware hides its presence by modifying the operating system?
A. Trojan
B. Worm

C. Rootkit
D. Spyware

Q38. A failure to segregate network zones MOST increases the risk of:
A. Social engineering
B. Lateral movement
C. Password reuse
D. Phishing

Q39. Which principle ensures that compromise of one control does not lead to total failure?
A. Least privilege
B. CIA triad
C. Defense-in-depth
D. Risk assessment

Q40. Which factor MOST influences the success of a targeted phishing attack?
A. Encryption algorithm
B. User awareness level
C. Firewall configuration
D. Network bandwidth