? EASY (Q1–Q10)

Q1. A Denial of Service (DoS) attack primarily affects:
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q2. Distributed Denial of Service (DDoS) differs from DoS because it:
A. Uses encryption
B. Uses multiple attacking systems
C. Targets databases only
D. Requires user interaction

Q3. A botnet consists of:
A. Firewalls
B. Compromised machines under attacker control
C. IDS sensors
D. Honeypots

Q4. Smurf attacks exploit:
A. TCP three-way handshake
B. ICMP echo requests
C. ARP protocol
D. DNS queries

Q5. SYN flooding targets which protocol mechanism?
A. DNS resolution
B. TCP connection establishment
C. UDP transmission
D. ICMP replies

Q6. Session hijacking aims to:
A. Encrypt sessions
B. Take over an active user session
C. Block network traffic
D. Scan ports

Q7. Cookies are commonly used for:
A. Encryption
B. Session management
C. Firewall rules
D. Port scanning

Q8. Spoofing involves:
A. Encrypting packets
B. Forging identity information
C. Blocking connections
D. Monitoring traffic

Q9. Hijacking differs from spoofing because hijacking:
A. Uses encryption
B. Takes over an existing session
C. Occurs only offline
D. Is always passive

Q10. Botnets are commonly controlled using:
A. BIOS
B. Command and Control (C2) servers
C. IDS
D. VPNs

□ MEDIUM (Q11–Q25)

Q11. Volumetric DDoS attacks overwhelm:
A. CPU only
B. Network bandwidth
C. Databases
D. Authentication services

Q12. Protocol-level DDoS attacks exploit:
A. Application bugs
B. Weaknesses in protocol design
C. User credentials
D. Encryption keys

Q13. Application-layer DoS attacks target:
A. Network links
B. Firewalls
C. Web applications
D. Routers

Q14. Botnet command channels may use:
A. HTTP or IRC
B. BIOS
C. FTP only
D. ICMP only

Q15. Smurf attacks are effective because:
A. ICMP broadcasts amplify traffic
B. TCP is unreliable
C. DNS is slow
D. Encryption is weak

Q16. SYN flooding causes servers to:
A. Drop packets
B. Exhaust connection resources
C. Crash instantly
D. Encrypt traffic

Q17. Session hijacking can occur due to:
A. Strong encryption
B. Weak session IDs
C. Multi-factor authentication
D. Secure cookies

Q18. HTTP session hijacking often exploits:
A. TLS
B. Unencrypted cookies
C. VPN tunnels
D. IDS rules

Q19. Network-level hijacking usually involves:
A. SQL injection
B. Man-in-the-middle attacks
C. Buffer overflow
D. XSS only

Q20. Botnets are difficult to dismantle because:
A. They use a single server
B. They are distributed globally
C. They are visible
D. They are centralized

Q21. SYN cookies mitigate SYN floods by:
A. Encrypting traffic
B. Avoiding half-open connections
C. Blocking ICMP
D. Using UDP

Q22. Session fixation attacks manipulate:
A. Passwords
B. Session identifiers
C. Encryption keys
D. Ports

Q23. DDoS detection often relies on:
A. User complaints only
B. Traffic pattern analysis
C. File integrity checks
D. OS updates

Q24. Application-layer DoS is harder to detect because:
A. Traffic looks legitimate
B. Volume is high
C. Uses ICMP
D. Uses spoofing

Q25. Secure session management includes:
A. Long-lived cookies
B. Random session IDs
C. Plaintext transmission
D. Disabled HTTPS

🟥 HARD (Q26–Q40)

Q26. Botnet resilience is increased through:
A. Single C2 server
B. Peer-to-peer control models
C. Fixed IP addresses
D. Manual updates

Q27. Reflection attacks amplify traffic by:
A. Sending direct requests
B. Using third-party servers to reply to victim
C. Blocking responses
D. Encrypting packets

Q28. Smurf attack mitigation involves:
A. Allowing broadcasts
B. Disabling ICMP broadcast replies
C. Increasing bandwidth
D. Using FTP

Q29. SYN flooding is effective because TCP:
A. Is connectionless
B. Maintains state during handshake
C. Uses encryption
D. Uses UDP

Q30. Session hijacking risk increases when:
A. HTTPS is enforced
B. Cookies lack secure flags
C. Tokens are rotated
D. MFA is enabled

Q31. Botnet-based DDoS differs from flash crowds because:
A. Traffic patterns differ
B. Both are identical
C. Flash crowds are malicious
D. Botnets are legitimate

Q32. Application-layer DDoS attacks require:
A. High bandwidth
B. Understanding of application logic
C. ICMP floods
D. ARP spoofing

Q33. TCP hijacking requires prediction of:
A. MAC addresses
B. Sequence numbers
C. IP addresses only
D. Ports only

Q34. Session hijacking via XSS occurs when:
A. Cookies are HttpOnly
B. Scripts steal session tokens
C. TLS is used
D. IDS is active

Q35. Botnet detection can leverage:
A. Signature-only analysis
B. Behavioral and traffic analysis
C. File hashing
D. User training

Q36. DDoS mitigation strategies include:
A. Rate limiting and traffic scrubbing
B. Password changes
C. OS reinstallation
D. Disk encryption

Q37. Spoofing vs hijacking difference is best described as:
A. Identity forging vs session takeover
B. Same concept
C. Encryption vs decryption
D. Passive vs active

Q38. SYN cookies reduce impact by:
A. Dropping SYN packets
B. Delaying resource allocation
C. Encrypting headers
D. Blocking ports

Q39. Session hijacking violates which security objective most directly?
A. Availability
B. Confidentiality
C. Integrity
D. Authentication

Q40. Effective defense against DDoS requires:
A. Single firewall
B. Multi-layered network defenses
C. Antivirus only
D. Password policies