◇ EASY (Q1–Q10)

Q1. Sudden spike in CPU usage on a server may indicate:
A. Normal operation
B. Backup activity
C. Possible attack
D. System update

Q2. Which attack primarily targets system availability?
A. Phishing
B. SQL injection
C. DoS
D. Spoofing

Q3. A Network-based IDS sensor monitors:
A. System calls
B. File integrity
C. Network traffic
D. User behavior

Q4. Which sensor type runs directly on a host system?
A. NIDS
B. HIDS
C. DIDS
D. IPS

Q5. DDoS attacks typically use:
A. Single attacker
B. Insider access
C. Multiple compromised systems
D. Misconfigured firewall

Q6. Which symptom most strongly suggests a DDoS attack?
A. Unauthorized login
B. Service unavailability
C. File corruption
D. Password change

Q7. IDS agents primarily:
A. Correlate events
B. Capture and report data
C. Generate policies
D. Block traffic

Q8. Which component manages and correlates IDS alerts?
A. Sensor

B. Agent
C. IDS Manager
D. Firewall

Q9. Rate limiting helps mitigate:
A. Phishing
B. Malware infection
C. DoS attacks
D. Insider threats

Q10. Blacklisting blocks traffic based on:
A. Encryption level
B. Application type
C. IP or source identity
D. Packet size

◇ MEDIUM (Q11–Q25)

Q11. Which attack symptom indicates reconnaissance activity?
A. Service crash
B. Repeated port scans
C. Data deletion
D. CPU exhaustion

Q12. Tiered IDS architecture improves security by:
A. Eliminating sensors
B. Centralizing all traffic
C. Separating detection and management layers
D. Disabling alerts

Q13. Where should NIDS sensors be placed to detect external attacks?
A. On end-user machines
B. At network perimeter
C. On database servers
D. Inside backup network

Q14. Host-based sensors are most effective for detecting:
A. Network floods
B. Insider misuse
C. Routing attacks
D. Bandwidth exhaustion

Q15. Which DoS attack exploits protocol weaknesses?
A. Phishing

B. SYN flood
C. Trojan
D. Keylogging

Q16. Which metric increases significantly during DDoS attacks?
A. Disk space
B. CPU and bandwidth usage
C. Encryption strength
D. Authentication success

Q17. Which IDS component aggregates alerts from multiple agents?
A. Sensor
B. Agent
C. Manager
D. Firewall

Q18. Why sensor placement inside the internal network is important?
A. Detect lateral movement
B. Increase latency
C. Replace firewalls
D. Reduce logs

Q19. Which DoS mitigation technique limits connection attempts per IP?
A. Encryption
B. Rate limiting
C. Blackholing
D. Logging

Q20. Which IDS agent function is most critical?
A. Policy creation
B. Event collection
C. Alert correlation
D. Traffic blocking

Q21. Which DDoS defense involves dropping traffic at upstream providers?
A. Rate limiting
B. Blacklisting
C. Traffic scrubbing
D. Local firewall

Q22. Which tier typically performs correlation in IDS architecture?
A. Sensor tier
B. Collection tier
C. Management tier
D. Access tier

Q23. Which symptom may indicate application-layer DoS?
A. Network link down
B. Excessive HTTP requests
C. ICMP flooding
D. ARP poisoning

Q24. Which approach minimizes false positives in DoS detection?
A. Static thresholds
B. Behavior baselining
C. IP blocking only
D. Manual monitoring

Q25. Why IDS agents should be lightweight?
A. To replace IPS
B. To avoid impacting host performance
C. To block traffic faster
D. To encrypt logs

△ HARD (Q26–Q40)

Q26. Which sensor placement best detects east-west traffic attacks?
A. Internet gateway
B. DMZ only
C. Internal network segments
D. External router

Q27. Why DDoS attacks are difficult to mitigate completely?
A. Use weak encryption
B. Originate from distributed sources
C. Target only one protocol
D. Require insider access

Q28. Which DoS mitigation technique dynamically adapts to traffic patterns?
A. Static ACLs
B. Rate limiting with thresholds
C. Blacklisting only
D. Manual blocking

Q29. Which IDS architecture scales best for large enterprises?
A. Standalone IDS
B. Centralized IDS
C. Distributed tiered IDS
D. Host-only IDS

Q30. Which IDS agent communication must be secured to prevent tampering?
A. Agent to kernel
B. Sensor to network
C. Agent to manager
D. Manager to SOC

Q31. Which attack symptom most strongly suggests slow-rate DoS?
A. Sudden bandwidth spike
B. Gradual resource exhaustion
C. Immediate service crash
D. Packet loss only

Q32. Why blacklisting alone is insufficient for DDoS defense?
A. Requires encryption
B. Attackers rotate IP addresses
C. Increases CPU usage
D. Reduces logging

Q33. Which IDS design helps reduce single point of failure?
A. Single manager
B. Distributed managers
C. Standalone sensors
D. Host-only IDS

Q34. Which DoS attack targets application resources rather than bandwidth?
A. UDP flood
B. ICMP flood
C. HTTP GET flood
D. Smurf attack

Q35. Why sensor tuning is critical in DoS detection?
A. Reduce encryption
B. Balance detection accuracy and false positives
C. Increase alerts
D. Disable logging

Q36. Which IDS manager task is most critical during an attack?
A. Log archival
B. Alert correlation and escalation
C. Signature update
D. Sensor installation

Q37. Which DoS mitigation technique protects backend servers transparently?
A. Rate limiting
B. Reverse proxy/load balancer

C. Blacklisting
D. Firewall ACL

Q38. Which attack symptom indicates IDS evasion attempt?
A. Normal traffic pattern
B. Fragmented or malformed packets
C. Clean logs
D. Low CPU usage

Q39. Which layered approach best mitigates DoS attacks?
A. Firewall only
B. IDS only
C. Rate limiting + load balancing + IDS
D. Antivirus only

Q40. Which combination provides strongest enterprise-level DoS resilience?
A. Static firewall rules
B. Blacklisting only
C. Tiered IDS + traffic scrubbing + rate limiting
D. Host-based IDS only