◇ EASY (Q1–Q10)

Q1. Which model defines Confidentiality, Integrity, and Availability?
A. OSI model
B. CIA triad
C. TCP/IP model
D. AAA model

Q2. A firewall primarily provides which security control?
A. Corrective
B. Detective
C. Preventive
D. Compensating

Q3. Which tool is used for packet capture and protocol analysis?
A. OpenVAS
B. Wireshark
C. Nagios
D. Snort

Q4. A vulnerability is best described as:
A. A malicious act
B. A system weakness
C. An attacker
D. A security policy

Q5. Which firewall inspects only packet headers?
A. Proxy firewall
B. NGFW
C. Packet filtering firewall
D. WAF

Q6. VPNs primarily secure data over:
A. Private leased lines
B. Public networks
C. LAN only
D. Offline networks

Q7. IDS systems mainly perform which function?
A. Blocking attacks
B. Detecting attacks
C. Encrypting traffic
D. Load balancing

Q8. Nagios is mainly used to monitor:
A. Intrusions
B. Availability and performance
C. Malware signatures
D. Encryption strength

Q9. Syslog traditionally uses which UDP port?
A. 22
B. 80
C. 443
D. 514

Q10. DoS attacks mainly impact which security goal?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

◇ MEDIUM (Q11–Q25)

Q11. Risk is best expressed as:
A. Threat + Asset
B. Vulnerability + Control
C. Threat × Vulnerability × Impact
D. Asset − Control

Q12. Which firewall architecture places public servers between two firewalls?
A. Screened host
B. DMZ with dual firewall
C. Packet filter only
D. Proxy-only

Q13. Which iptables chain processes packets destined for the local host?
A. OUTPUT
B. FORWARD
C. INPUT
D. PREROUTING

Q14. Which VPN protocol provides network-layer security?
A. SSL
B. PPTP
C. IPsec
D. HTTPS

Q15. Which IDS type monitors a single host?
A. NIDS
B. HIDS
C. DIDS
D. IPS

Q16. Which attack phase includes port scanning?
A. Exploitation
B. Privilege escalation
C. Reconnaissance
D. Persistence

Q17. Which log source best detects brute-force attacks?
A. DNS logs
B. Authentication logs
C. Proxy logs
D. Application logs

Q18. Which DoS mitigation limits connections per IP?
A. Encryption
B. Rate limiting
C. Load balancing
D. Logging

Q19. Which IDS detection method uses known attack patterns?
A. Anomaly-based
B. Behavioral
C. Signature-based
D. Heuristic

Q20. Which Nagios component performs system checks?
A. Core daemon
B. Plugin
C. Web UI
D. Event handler

Q21. Which IPsec protocol manages key exchange?
A. AH
B. ESP
C. IKE
D. HMAC

Q22. Why SIEM correlation is important?
A. Reduces storage
B. Detects multi-stage attacks

C. Encrypts logs
D. Replaces IDS

Q23. Which IDS architecture scales best in enterprises?
A. Standalone IDS
B. Host-only IDS
C. Distributed IDS
D. Inline IDS

Q24. Which tool visualizes Snort alerts via web interface?
A. Kibana
B. BASE
C. Nagios
D. OpenVAS

Q25. Which VPN type connects branch offices?
A. Remote access VPN
B. Mobile VPN
C. Site-to-site VPN
D. Personal VPN

△ HARD (Q26–Q40)

Q26. Which risk treatment accepts potential loss?
A. Avoidance
B. Mitigation
C. Transfer
D. Acceptance

Q27. Why stateful firewalls are more secure than stateless ones?
A. Faster routing
B. Track connection state
C. Use encryption
D. Perform NAT

Q28. Which IDS evasion technique splits payloads?
A. Encoding
B. Flooding
C. Fragmentation
D. Spoofing

Q29. Which IPsec mode encrypts the entire original IP packet?
A. Transport mode

B. Tunnel mode
C. Split tunnel
D. Hybrid mode

Q30. Why split tunneling increases risk?
A. Higher latency
B. Data leakage
C. CPU overhead
D. Routing loops

Q31. Which DoS attack targets application resources?
A. ICMP flood
B. SYN flood
C. HTTP GET flood
D. UDP flood

Q32. Which IDS placement best detects lateral movement?
A. Internet gateway
B. DMZ only
C. Internal network segments
D. External router

Q33. Why encrypted traffic reduces IDS visibility?
A. Headers are hidden
B. Payload inspection is not possible
C. Routing fails
D. Logs are disabled

Q34. Which SIEM component performs correlation?
A. Log collector
B. Storage layer
C. Correlation engine
D. Dashboard

Q35. Which IDS evasion exploits protocol ambiguities?
A. Encoding
B. Flooding
C. Protocol manipulation
D. Timing attack

Q36. Which Nagios observation may indicate DDoS?
A. File deletion
B. Sudden CPU and latency spike
C. Password change
D. Log rotation

Q37. Why insider threats are difficult to detect?
A. Use malware
B. Appear as legitimate users
C. Use DDoS
D. Disable IDS

Q38. Which IPsec feature prevents replay attacks?
A. Encryption
B. Sequence numbers
C. NAT traversal
D. Key lifetime

Q39. Which combined approach gives strongest SOC visibility?
A. Firewall only
B. IDS only
C. IDS + SIEM + Monitoring
D. Antivirus only

Q40. Why defence-in-depth is effective?
A. Eliminates all threats
B. Single strong firewall
C. Multiple layered controls
D. Reduces encryption cost