◇ EASY (Q1–Q10)

Q1. Which attack originates from a single source system?
A. Distributed attack
B. Traditional attack
C. Botnet attack
D. Amplification attack

Q2. A DDoS attack primarily affects which security objective?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q3. Which intruder type is an authorized user misusing privileges?
A. External intruder
B. Script kiddie
C. Insider
D. Hacktivist

Q4. Which IDS type analyzes traffic on a network segment?
A. HIDS
B. NIDS
C. DIDS
D. WAF

Q5. IPS differs from IDS because IPS can:
A. Only detect attacks
B. Only log events
C. Actively prevent attacks
D. Replace SIEM

Q6. Defence in Depth refers to:
A. Using a single strong firewall
B. Layered security controls
C. Only endpoint security
D. Only network security

Q7. Which detection method relies on known attack signatures?
A. Anomaly-based
B. Heuristic-based
C. Signature-based
D. Behavior-based

Q8. Snort is best classified as a:
A. HIDS

B. NIDS
C. SIEM
D. Firewall

Q9. Which tool is primarily used for host-based intrusion detection?
A. Snort
B. Suricata
C. OSSEC
D. Zeek

Q10. ELK stack stands for:
A. Elastic, Logstash, Kibana
B. Event, Log, Kernel
C. Elastic, Linux, Kubernetes
D. Event, Log, Knowledge

◇ MEDIUM (Q11–Q25)

Q11. Which attack type uses multiple compromised systems?
A. Traditional attack
B. Insider attack
C. Distributed attack
D. Privilege escalation

Q12. Which intruder type is most difficult to detect?
A. External attacker
B. Insider
C. Script kiddie
D. Hacktivist

Q13. Which IDS deployment is best for monitoring critical servers?
A. NIDS
B. HIDS
C. DIDS
D. Perimeter IDS

Q14. Which IPS category operates inline with network traffic?
A. Passive IPS
B. Host-based IPS
C. Network-based IPS
D. Log-based IPS

Q15. Which layer is NOT part of defence in depth?
A. Network security

B. Application security
C. Physical security
D. Single perimeter firewall only

Q16. Which detection method establishes a baseline of normal behavior?
A. Signature-based
B. Anomaly-based
C. Rule-based
D. Pattern-based

Q17. Which IDS/IPS challenge results from anomaly detection?
A. False negatives
B. False positives
C. No alerts
D. Encrypted traffic

Q18. Which Snort component applies detection rules?
A. Packet decoder
B. Preprocessor
C. Detection engine
D. Output module

Q19. Which Suricata feature differentiates it from Snort?
A. Single-threaded design
B. Multi-threading support
C. Lack of rule support
D. Host-based monitoring

Q20. Which OSSEC feature supports log analysis?
A. Packet sniffing
B. File integrity monitoring
C. Active response
D. Log-based analysis

Q21. In threat hunting, what is the first step?
A. Automated blocking
B. Hypothesis creation
C. Incident response
D. Alert tuning

Q22. Which ELK component is responsible for log ingestion and parsing?
A. Elasticsearch
B. Logstash
C. Kibana
D. Beats

Q23. Which attack is best detected using anomaly-based IDS?
A. Known malware
B. Zero-day attack
C. Signature attack
D. Replay attack

Q24. Which IDS architecture aggregates alerts from multiple sensors?
A. Standalone IDS
B. Distributed IDS
C. Host-only IDS
D. Inline IDS

Q25. Which threat hunting outcome confirms malicious activity?
A. Hypothesis invalidation
B. Indicator of compromise
C. Baseline creation
D. Noise reduction

△ HARD (Q26–Q40)

Q26. Why distributed attacks are harder to mitigate than traditional attacks?
A. Use weak protocols
B. Originate from multiple sources
C. Lack encryption
D. Target only applications

Q27. Which intruder motivation aligns with hacktivism?
A. Financial gain
B. Political or ideological goals
C. Skill development
D. Insider revenge

Q28. Which IDS type best detects insider misuse?
A. NIDS
B. Perimeter IDS
C. HIDS
D. Inline IPS

Q29. Why defence in depth reduces overall risk?
A. Eliminates vulnerabilities
B. Provides multiple detection and prevention layers
C. Reduces costs
D. Prevents all attacks

Q30. Which detection methodology is least effective against encrypted traffic?
A. Signature-based
B. Anomaly-based
C. Behavioral
D. Metadata analysis

Q31. Which scenario best demonstrates threat hunting?
A. Responding to an alert
B. Proactively searching for hidden attackers
C. Blocking traffic automatically
D. Updating firewall rules

Q32. Why ELK is valuable for threat hunting?
A. Packet capture
B. Centralized log correlation and visualization
C. Inline blocking
D. Malware removal

Q33. Which Snort limitation is addressed by SIEM integration?
A. Packet decoding
B. Event correlation across sources
C. Rule matching
D. Traffic capture

Q34. Which IPS risk must be carefully managed in production?
A. False negatives
B. False positives causing service disruption
C. Lack of encryption
D. Lack of logs

Q35. Which comparison is correct?
A. Snort is HIDS, OSSEC is NIDS
B. Suricata supports multi-threading, Snort traditionally does not
C. OSSEC analyzes network packets only
D. Snort replaces SIEM

Q36. Which IDS/IPS tuning goal improves SOC efficiency?
A. Increase alerts
B. Reduce false positives
C. Disable anomaly detection
D. Ignore low-severity events

Q37. Which threat hunting data source is most valuable?
A. Single firewall log
B. Correlated logs across endpoints, network, and applications

C. Only IDS alerts
D. System uptime metrics

Q38. Which attack pattern best evades signature-based IDS?
A. Known exploit
B. Obfuscated or polymorphic attack
C. Static malware
D. Fixed port scan

Q39. Why insider threats require different detection strategies?
A. Use encrypted traffic
B. Appear as legitimate users
C. Operate externally
D. Are easy to block

Q40. Which layered approach best strengthens detection and response?
A. IDS only
B. IPS only
C. IDS + IPS + SIEM + Threat Hunting
D. Firewall only