◇ EASY (Q1–Q10)

Q1. Snort is primarily classified as a:
A. Host-based firewall
B. Network Intrusion Detection System
C. SIEM tool
D. Log analyzer

Q2. Which library does Snort use for packet capture on Linux?
A. WinPcap
B. libnet
C. libpcap
D. tcpdump

Q3. Which Snort mode is used only to display packets on the screen?
A. IDS mode
B. Packet logger mode
C. Sniffer mode
D. Inline mode

Q4. Which tool is required to run Snort on Windows?
A. Sysmon
B. WinPcap/Npcap
C. Wireshark
D. PowerShell

Q5. IDS systems are considered which type of control?
A. Preventive
B. Detective
C. Corrective
D. Deterrent

Q6. Which Nagios component performs actual system checks?
A. Core daemon
B. Plugins
C. Web UI
D. Event handler

Q7. Which IDS deployment places sensors at multiple locations?
A. Standalone IDS
B. Centralized IDS
C. Distributed IDS
D. Host-only IDS

Q8. Which Nagios feature notifies administrators of failures?
A. Dashboard

B. Alerting mechanism
C. Plugin API
D. Log rotation

Q9. IDS evasion aims to:
A. Strengthen detection
B. Avoid triggering alerts
C. Encrypt packets
D. Replace IPS

Q10. Which system aspect is mainly monitored by Nagios?
A. Intrusions
B. Availability and performance
C. Malware signatures
D. Packet payloads

◇ MEDIUM (Q11–Q25)

Q11. Which Snort component matches traffic against rules?
A. Packet decoder
B. Preprocessor
C. Detection engine
D. Output module

Q12. Why is Snort preferred on Linux for production use?
A. Better GUI
B. Native kernel access and performance
C. Easier installation
D. Fewer rules

Q13. Which IDS architecture component correlates alerts?
A. Sensor
B. Agent
C. Manager / Console
D. Packet decoder

Q14. Which IDS evasion technique splits malicious payloads?
A. Encoding
B. Flooding
C. Fragmentation
D. Spoofing

Q15. Which IDS evasion technique spreads attack traffic over time?
A. Flooding

B. Encoding
C. Low-and-slow attack
D. Fragment overlap

Q16. Why encrypted traffic reduces IDS effectiveness?
A. Larger packets
B. Payload inspection is not possible
C. Routing is disabled
D. Headers are removed

Q17. Which Nagios protocol enables monitoring of remote Linux hosts?
A. SNMP
B. NRPE
C. Syslog
D. NetFlow

Q18. In Nagios, alerts are triggered when:
A. Plugins run
B. Host is registered
C. Thresholds are violated
D. Logs are rotated

Q19. Which IDS evasion uses different data representations?
A. Flooding
B. Encoding/obfuscation
C. Spoofing
D. Replay

Q20. Which IDS architecture scales best in enterprises?
A. Standalone
B. Host-only
C. Distributed
D. Inline-only

Q21. Which Nagios object defines what is monitored?
A. Command
B. Time period
C. Host/Service
D. Contact

Q22. Why preprocessors are critical in Snort?
A. Encrypt traffic
B. Normalize and prepare traffic
C. Store logs
D. Send alerts

Q23. Which monitoring metric may indicate a DoS attack?
A. Disk space usage
B. CPU and latency spike
C. File permission change
D. User login count

Q24. Which IDS evasion exploits protocol ambiguities?
A. Encoding
B. Flooding
C. Protocol manipulation
D. Low-and-slow

Q25. Which tool confirms service impact during attacks?
A. Snort
B. Wireshark
C. Nagios
D. tcpdump

△ HARD (Q26–Q40)

Q26. Which IDS evasion exploits differences between IDS and OS TCP stacks?
A. Flooding
B. Encoding
C. Protocol normalization mismatch
D. Timing attack

Q27. Why protocol normalization reduces IDS evasion?
A. Blocks encrypted traffic
B. Enforces consistent protocol interpretation
C. Drops packets
D. Increases bandwidth

Q28. Which Snort mode can actively drop packets?
A. Sniffer
B. Packet logger
C. IDS
D. Inline

Q29. Which operational risk arises from aggressive IPS/IDS tuning?
A. False negatives
B. False positives blocking legitimate traffic
C. Lack of alerts
D. No logging

Q30. In distributed IDS, what is the main role of central manager?
A. Packet capture
B. Rule creation only
C. Event correlation and control
D. Traffic routing

Q31. Which IDS evasion is most effective against signature-based IDS?
A. Behavioral profiling
B. Payload obfuscation
C. Rate limiting
D. Blacklisting

Q32. How does Nagios complement IDS in SOC operations?
A. Blocks attacks
B. Correlates logs
C. Confirms service availability impact
D. Decrypts traffic

Q33. Which scenario best represents IDS evasion?
A. Immediate detection
B. Attack below alert thresholds
C. Firewall block
D. Antivirus quarantine

Q34. Why Snort preprocessors are vital against evasion?
A. Faster routing
B. Traffic reassembly and normalization
C. Encryption
D. Logging

Q35. Which Nagios component schedules checks?
A. Plugin
B. NRPE
C. Core daemon
D. Web UI

Q36. Which limitation differentiates IDS from IPS?
A. Scalability
B. Detection accuracy
C. Lack of prevention
D. Lack of logs

Q37. Which IDS evasion manipulates TCP sequence handling?
A. Flooding
B. Encoding

C. Sequence number manipulation
D. Timing

Q38. Best sensor placement to detect lateral movement is:
A. Internet gateway only
B. DMZ only
C. Internal network segments
D. External router

Q39. Why Nagios is not an IDS?
A. Cannot alert
B. Does not detect intrusions directly
C. Lacks plugins
D. Cannot monitor hosts

Q40. Which integrated approach offers strongest detection & response?
A. IDS only
B. Monitoring only
C. IDS + Nagios + SIEM
D. Firewall only