◇ EASY (Q1–Q10)

Q1. IDS stands for:
A. Internet Detection System
B. Intrusion Detection System
C. Integrated Defense System
D. Internal Detection Service

Q2. IPS differs from IDS primarily because IPS can:
A. Only log events
B. Detect malware
C. Actively block malicious traffic
D. Replace firewalls

Q3. Which IDS type monitors network traffic?
A. HIDS
B. NIDS
C. WAF
D. SIEM

Q4. A security event is best defined as:
A. A confirmed breach
B. Any observable occurrence in a system
C. A vulnerability report
D. A malware signature

Q5. Which attack targets system availability?
A. Phishing
B. SQL injection
C. DoS
D. Eavesdropping

Q6. Honeypots are mainly used to:
A. Block attackers
B. Attract and study attackers
C. Encrypt traffic
D. Replace IDS

Q7. tcpdump is primarily used for:
A. Log correlation
B. Packet capture and analysis
C. Vulnerability scanning
D. Malware removal

Q8. Which attack involves deceptive emails to steal credentials?
A. Brute force
B. Phishing
C. DDoS
D. Sniffing

Q9. Which component is most affected by buffer overflow attacks?
A. Network bandwidth
B. Application memory
C. Encryption keys
D. Disk space

Q10. Which IDS deployment monitors a single host?
A. NIDS
B. DIDS
C. HIDS
D. IPS

◇ MEDIUM (Q11–Q25)

Q11. Which IDS placement is best for detecting perimeter attacks?
A. Internal LAN
B. Host OS
C. Network gateway
D. Database server

Q12. Which attack exploits poor input validation?
A. DDoS
B. SQL injection
C. ARP spoofing
D. SYN flood

Q13. Which security event should be escalated first?
A. Successful login
B. Multiple failed logins
C. System shutdown
D. Software update

Q14. Why IPS is considered riskier than IDS?
A. Generates fewer alerts
B. Can block legitimate traffic
C. Requires signatures
D. Works only at Layer 7

Q15. Which attack category includes port scanning?
A. Reconnaissance
B. Exploitation
C. Privilege escalation
D. Persistence

Q16. Which design issue increases attack surface?
A. Least privilege
B. Input validation
C. Unnecessary open services
D. Network segmentation

Q17. Which IDS detection method uses known attack patterns?
A. Anomaly-based
B. Heuristic
C. Signature-based
D. Behavioral

Q18. Which type of honeypot provides limited interaction?
A. High-interaction
B. Medium-interaction
C. Low-interaction
D. Research honeypot

Q19. Which tcpdump option displays packet contents in ASCII?
A. -i
B. -c
C. -X
D. -w

Q20. Which security event indicates possible brute-force attack?
A. Single login failure
B. Multiple login failures from same IP
C. Password change
D. System reboot

Q21. Which vulnerability type arises from poor software design?
A. Zero-day
B. Configuration vulnerability
C. Design vulnerability
D. Environmental vulnerability

Q22. Which IDS output is most useful for forensic analysis?
A. Real-time alerts only
B. Packet captures and logs

C. CPU usage
D. Routing tables

Q23. Why honeypots should be isolated from production networks?
A. To increase performance
B. To avoid attacker pivoting
C. To improve encryption
D. To reduce logging

Q24. Which attack manipulates trust relationships in LANs?
A. Phishing
B. ARP spoofing
C. SQL injection
D. Brute force

Q25. Which tcpdump filter captures only ICMP traffic?
A. tcp
B. udp
C. icmp
D. port 80

△ HARD (Q26–Q40)

Q26. Which IDS evasion technique targets signature-based IDS?
A. Anomaly flooding
B. Payload obfuscation
C. Rate limiting
D. Blacklisting

Q27. Why false positives are a major challenge in IDS?
A. Lack of encryption
B. Excessive logging
C. Alert fatigue and ignored real threats
D. High bandwidth usage

Q28. Which attack phase is hardest for IDS to detect?
A. Reconnaissance
B. Exploitation
C. Lateral movement
D. Data exfiltration

Q29. Which honeypot type is most suitable for attacker behavior research?
A. Low-interaction

B. Medium-interaction
C. High-interaction
D. Production honeypot

Q30. Why tcpdump is often used alongside IDS tools?
A. IDS replaces packet capture
B. Provides raw packet-level evidence
C. Encrypts traffic
D. Correlates logs

Q31. Which IPS deployment mode drops packets inline?
A. Passive mode
B. Tap mode
C. Inline mode
D. Monitor mode

Q32. Which vulnerability results from insecure coding practices?
A. Physical vulnerability
B. Configuration vulnerability
C. Implementation vulnerability
D. Environmental vulnerability

Q33. Why signature-based IDS struggles with zero-day attacks?
A. Requires too much memory
B. No known attack patterns
C. Slower processing
D. Encrypted traffic only

Q34. Which security event correlation suggests a compromised host?
A. Single port scan
B. Malware alert followed by outbound C2 traffic
C. Login success
D. System backup

Q35. Which IDS limitation is mitigated by combining with SIEM?
A. Packet capture
B. Event correlation across sources
C. Rule matching
D. Traffic encryption

Q36. Which tcpdump feature allows capturing traffic to a file?
A. -r
B. -i
C. -w
D. -n

Q37. Which attack targets confidentiality most directly?
A. DoS
B. Phishing
C. Eavesdropping
D. SYN flood

Q38. Why IPS tuning is critical in production environments?
A. Reduce encryption
B. Prevent service disruption
C. Increase alerts
D. Improve routing

Q39. Which vulnerability is hardest to fix without redesign?
A. Misconfiguration
B. Weak password
C. Design flaw
D. Missing patch

Q40. Which layered approach provides strongest intrusion detection?
A. IDS only
B. IPS only
C. IDS + honeypots + SIEM
D. Firewall only