⍰ EASY (Q1–Q10)

Q1. Packet sniffing is the process of:
A. Encrypting network traffic
B. Capturing and analyzing network packets
C. Blocking network connections
D. Authenticating users

Q2. Which protocol sends data in plaintext and is vulnerable to sniffing?
A. HTTPS
B. FTP
C. SSH
D. SFTP

Q3. Passive sniffing involves:
A. Injecting packets
B. Only listening to network traffic
C. Modifying packets
D. Flooding the network

Q4. Active sniffing usually requires:
A. Encryption
B. Network manipulation
C. Secure protocols
D. Offline access

Q5. ARP poisoning targets which protocol?
A. TCP
B. UDP
C. ARP
D. ICMP

Q6. MAC flooding attacks exploit:
A. DNS cache
B. CAM table overflow
C. Routing tables
D. Firewall rules

Q7. DNS spoofing aims to:
A. Encrypt DNS responses
B. Redirect users to malicious sites
C. Block DNS servers
D. Improve resolution speed

Q8. Wireshark is primarily used for:
A. Malware creation
B. Packet capture and analysis
C. Port scanning
D. Password cracking

Q9. Capture filters in Wireshark are applied:
A. After packet capture
B. Before packet capture
C. During packet analysis only
D. At OS boot

Q10. Display filters in Wireshark are used to:
A. Reduce captured data
B. Filter displayed packets
C. Encrypt packets
D. Modify traffic

□ MEDIUM (Q11–Q25)

Q11. Active sniffing differs from passive sniffing because it:
A. Uses encrypted traffic
B. Alters network behavior
C. Requires no interaction
D. Is undetectable

Q12. ARP poisoning enables attackers to perform:
A. DoS only
B. Man-in-the-Middle attacks
C. Encryption
D. Firewall bypass only

Q13. MAC flooding forces a switch to behave like:
A. Router
B. Hub
C. Firewall
D. Proxy

Q14. DNS cache poisoning attacks:
A. Web servers
B. DNS resolvers
C. Email servers
D. Clients only

Q15. Protocols vulnerable to sniffing include:
A. HTTPS and SSH
B. Telnet and FTP
C. IPsec and SSL
D. SFTP and SCP

Q16. ARP spoofing is dangerous because it:
A. Encrypts traffic
B. Redirects traffic through attacker
C. Blocks all packets
D. Resets connections

Q17. Wireshark capture filters use which syntax?
A. Wireshark display syntax
B. Berkeley Packet Filter (BPF)
C. Regex
D. SQL

Q18. DNS spoofing may lead to:
A. Credential theft
B. Phishing attacks
C. Malware downloads
D. All of the above

Q19. Passive sniffing is difficult on switched networks because:
A. Traffic is encrypted
B. Switches isolate traffic
C. Firewalls block packets
D. IDS prevents sniffing

Q20. ARP poisoning typically affects:
A. Network layer
B. Transport layer
C. Data link layer
D. Application layer

Q21. MAC flooding is mitigated by:
A. Encryption
B. Port security on switches
C. Firewalls
D. VPNs

Q22. DNS hacking can involve:
A. Zone transfers
B. Cache poisoning
C. DNS spoofing
D. All of the above

Q23. Wireshark display filters are evaluated:
A. During capture
B. After capture
C. Before capture
D. At OS boot

Q24. Sniffing attacks mainly compromise:
A. Availability
B. Confidentiality
C. Integrity
D. Authentication

Q25. Secure protocols mitigate sniffing by using:
A. Obfuscation
B. Encryption
C. Compression
D. Fragmentation

● HARD (Q26–Q40)

Q26. ARP poisoning works because ARP:
A. Is encrypted
B. Is stateless and unauthenticated
C. Uses TCP
D. Uses digital signatures

Q27. DNS spoofing detection is difficult because:
A. DNS uses TCP only
B. Responses appear legitimate
C. Traffic is encrypted
D. DNS is authenticated

Q28. MAC flooding attacks are effective when:
A. Switch CAM table size is limited
B. Encryption is enabled
C. Port security is active
D. VLANs are configured

Q29. Capture filters improve performance by:
A. Filtering packets after capture
B. Limiting packets captured
C. Encrypting traffic
D. Analyzing packets faster

Q30. Active sniffing is detectable due to:
A. Network anomalies
B. Increased ARP traffic
C. Duplicate MAC entries
D. All of the above

Q31. DNS cache poisoning increases risk by:
A. Slowing DNS resolution
B. Redirecting legitimate traffic
C. Blocking DNS servers
D. Encrypting queries

Q32. ARP poisoning countermeasures include:
A. Static ARP entries
B. ARP inspection
C. Encryption
D. All of the above

Q33. Wireshark is unsuitable for:
A. Protocol analysis
B. Traffic troubleshooting
C. Malware creation
D. Network forensics

Q34. Passive sniffing is most effective on:
A. Switched Ethernet
B. Wireless networks
C. Encrypted tunnels
D. VLANs

Q35. DNSSEC mitigates:
A. MAC flooding
B. DNS spoofing
C. ARP poisoning
D. Sniffing

Q36. Sniffing countermeasures focus on:
A. Blocking traffic
B. Encrypting sensitive data
C. Increasing bandwidth
D. Removing switches

Q37. Wireshark analysis helps defenders by:
A. Encrypting packets
B. Detecting anomalies and attacks
C. Blocking traffic
D. Authenticating users

Q38. ARP spoofing often precedes:
A. DDoS
B. Man-in-the-middle attacks
C. SQL injection
D. Buffer overflow

Q39. DNS hacking impacts users by:
A. Improving performance
B. Redirecting to malicious servers
C. Blocking internet access only
D. Encrypting DNS traffic

Q40. Defense against sniffing requires:
A. One control only
B. Defense-in-depth
C. Disabling switches
D. Removing routers