? EASY (Q1–Q10)

Q1. Ethical hacking is performed to:
A. Steal confidential data
B. Test and improve security
C. Damage systems
D. Bypass laws

Q2. A security evaluation plan defines:
A. Coding standards
B. Scope and rules of engagement
C. Malware payloads
D. Network speed

Q3. White-box testing provides:
A. No system knowledge
B. Partial system knowledge
C. Full system and code knowledge
D. Only network access

Q4. Foot-printing is the phase of:
A. Exploitation
B. Information gathering
C. Maintaining access
D. Covering tracks

Q5. Passive foot-printing involves:
A. Direct interaction with target
B. Exploiting vulnerabilities
C. Collecting publicly available information
D. Port scanning

Q6. Social engineering primarily exploits:
A. Encryption flaws
B. Human trust
C. Network latency
D. Hardware errors

Q7. Traceroute is used to:
A. Scan ports
B. Discover network path
C. Crack passwords
D. Encrypt traffic

Q8. Port scanning helps identify:
A. Physical devices
B. Open services and ports
C. User behavior
D. Encryption keys

Q9. Vulnerability scanning focuses on:
A. Finding misconfigurations and known flaws
B. Stealing credentials
C. Crashing systems
D. Modifying code

Q10. SYN scan is also known as:
A. Full connect scan
B. Stealth scan
C. UDP scan
D. Xmas scan

□ MEDIUM (Q11–Q25)

Q11. Rules of engagement in ethical hacking ensure:
A. Unlimited access
B. Legal and ethical boundaries
C. Faster scanning
D. Exploit success

Q12. Black-box testing simulates:
A. Insider testing
B. Real external attacker
C. Developer testing
D. Source-code review

Q13. Active foot-printing differs from passive because it:
A. Uses public sources only
B. Interacts directly with target systems
C. Avoids detection
D. Requires no tools

Q14. Social engineering attacks can be:
A. Human-based
B. Technology-based
C. Hybrid
D. All of the above

Q15. Traceroute identifies:
A. MAC addresses only
B. Intermediate network hops
C. Encryption algorithms
D. User credentials

Q16. Network scanning identifies:
A. Live hosts
B. Network topology
C. IP ranges
D. All of the above

Q17. Banner grabbing reveals:
A. Password hashes
B. Service and version information
C. User roles
D. Encryption keys

Q18. Vulnerability scanners rely on:
A. Exploit development
B. Known vulnerability databases
C. Social engineering
D. Hardware access

Q19. TCP-based scanning includes:
A. SYN scan
B. FIN scan
C. NULL scan
D. All of the above

Q20. IDLE scan hides attacker identity by using:
A. Proxy servers
B. Zombie hosts
C. VPN tunnels
D. Firewalls

Q21. UDP scanning is challenging because:
A. UDP is encrypted
B. No response indicates ambiguity
C. It is slower than TCP always
D. It requires authentication

Q22. OS detection attempts to identify:
A. User privileges
B. Operating system and version
C. Database schema
D. Application logic

Q23. Stealth scanning aims to:
A. Generate alerts
B. Avoid detection
C. Crash services
D. Encrypt packets

Q24. Scanning too aggressively may:
A. Improve stealth
B. Trigger IDS/IPS alerts
C. Reduce bandwidth usage
D. Encrypt traffic

Q25. Vulnerability scanning output should be:
A. Ignored
B. Used for exploitation only
C. Analyzed and prioritized
D. Deleted

🔴 HARD (Q26–Q40)

Q26. Ethical hacking without authorization is:
A. Legal
B. Ethical
C. Illegal
D. Recommended

Q27. Grey-box testing provides:
A. No knowledge
B. Partial internal knowledge
C. Full internal knowledge
D. Only network diagrams

Q28. Passive foot-printing is preferred when:
A. Exploitation is required
B. Avoiding detection is critical
C. Full access is allowed
D. Scanning is blocked

Q29. Social engineering attacks are dangerous because they:
A. Require malware
B. Bypass technical controls
C. Are easily detected
D. Need admin access

Q30. Traceroute output can reveal:
A. Firewall rules
B. Network architecture
C. User credentials
D. Encryption keys

Q31. Excessive scanning traffic may lead to:
A. Better results
B. Detection and blocking
C. Faster exploitation
D. Encryption failure

Q32. Vulnerability scanning should be followed by:
A. Immediate exploitation
B. Risk assessment
C. Covering tracks
D. Ignoring findings

Q33. FIN, NULL, and XMAS scans exploit:
A. Application bugs
B. TCP flag behavior
C. UDP protocol
D. Encryption weakness

Q34. IDLE scanning is effective only when:
A. Zombie host is predictable
B. Firewall is disabled
C. Target is offline
D. IDS is absent

Q35. Ethical hackers must always:
A. Avoid documentation
B. Report findings responsibly
C. Hide vulnerabilities
D. Publish exploits

Q36. OS fingerprinting accuracy depends on:
A. Application code
B. Network responses and timing
C. User behavior
D. Database content

Q37. Scanning methodologies should balance:
A. Speed and noise
B. Security and usability
C. Cost and encryption
D. Hardware and software

Q38. Advanced scans evade detection by:
A. Flooding traffic
B. Mimicking normal packets
C. Crashing IDS
D. Disabling firewalls

Q39. Foot-printing and scanning primarily help attackers by:
A. Encrypting data
B. Reducing uncertainty
C. Crashing servers
D. Increasing bandwidth

Q40. Ethical scanning success is measured by:
A. Number of alerts
B. Quality of discovered risks
C. System downtime
D. Packet loss