? EASY (Q1–Q10)

Q1. The CIA triad in information security stands for:
A. Control, Integrity, Availability
B. Confidentiality, Integrity, Availability
C. Confidentiality, Inspection, Access
D. Control, Inspection, Authorization

Q2. OWASP Top 10 focuses primarily on:
A. Network vulnerabilities
B. Web application security risks
C. Hardware attacks
D. Physical security

Q3. SQL Injection is an example of:
A. Network attack
B. Injection attack
C. Cryptographic attack
D. Physical attack

Q4. Android applications are packaged as:
A. EXE
B. IPA
C. APK
D. JAR

Q5. A Denial-of-Service (DoS) attack targets:
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q6. A firewall primarily works at which level?
A. Application only
B. Network and transport layers
C. Physical layer
D. User interface

Q7. Malware that encrypts files and demands payment is:
A. Worm
B. Trojan
C. Ransomware
D. Spyware

Q8. Footprinting is part of which hacking phase?
A. Maintaining access
B. Reconnaissance
C. Covering tracks
D. Exploitation

Q9. Packet sniffing is easiest on:
A. Encrypted VPN
B. Open Wi-Fi networks
C. Cellular networks
D. Fiber networks

Q10. Ethical hacking must always require:
A. Root access
B. Written authorization
C. Internet access
D. Zero defenses

□ MEDIUM (Q11–Q25)

Q11. Blind SQL Injection differs from error-based SQL injection because it:
A. Uses syntax errors
B. Relies on application responses without errors
C. Requires source code
D. Is faster

Q12. Stored XSS is more dangerous than reflected XSS because it:
A. Requires user input
B. Executes automatically for multiple users
C. Uses GET method
D. Needs no browser

Q13. Buffer overflow vulnerabilities occur mainly due to:
A. Encryption failures
B. Improper bounds checking
C. Network latency
D. Poor UI design

Q14. RBAC access control assigns permissions based on:
A. Identity
B. Roles
C. Attributes
D. Location

Q15. A botnet is best described as:
A. A secured network
B. A group of compromised machines under attacker control
C. A firewall cluster
D. IDS network

Q16. In Android, application sandboxing is enforced using:
A. Antivirus
B. Linux UID and process isolation
C. Firewall rules
D. VPN

Q17. Static Application Security Testing (SAST) analyzes:
A. Runtime traffic
B. Source code or binaries
C. Network packets
D. User behavior

Q18. Dynamic Application Security Testing (DAST) is performed:
A. During coding
B. On running applications
C. On source code only
D. After deployment only

Q19. A Man-in-the-Middle (MITM) attack mainly compromises:
A. Availability
B. Confidentiality and Integrity
C. Authentication only
D. Physical security

Q20. ARP poisoning allows attackers to:
A. Encrypt traffic
B. Intercept network communication
C. Improve routing
D. Patch ARP tables

Q21. Enumeration in hacking aims to:
A. Scan vulnerabilities
B. Extract detailed system information
C. Crack passwords
D. Install malware

Q22. SMB relay attacks exploit weakness in:
A. Encryption algorithms
B. Authentication without signing
C. DNS resolution
D. HTTP headers

Q23. Malware that hides its presence deeply in OS is:
A. Worm
B. Rootkit
C. Adware
D. Spyware

Q24. Reverse engineering an APK primarily threatens:
A. Network security
B. Intellectual property and secrets
C. Hardware
D. Physical access

Q25. IDS differs from IPS because IDS:
A. Blocks traffic automatically
B. Only detects and alerts
C. Encrypts traffic
D. Controls access

🔴 HARD (Q26–Q40)

Q26. Time-based blind SQL injection exploits:
A. Error messages
B. Database response delays
C. Stored procedures
D. Network congestion

Q27. Chained vulnerabilities are dangerous because they:
A. Affect only UI
B. Combine multiple flaws for higher impact
C. Reduce attack surface
D. Require admin access initially

Q28. Certificate pinning prevents which attack effectively?
A. XSS
B. MITM
C. SQL Injection
D. CSRF

Q29. IDLE scan in Nmap is stealthy because it:
A. Uses UDP
B. Uses a zombie host
C. Sends SYN floods
D. Uses ICMP only

Q30. Fileless malware is difficult to detect mainly because it:
A. Is slow
B. Resides in memory
C. Uses signatures
D. Requires reboot

Q31. Behavioral malware detection is strongest against:
A. Known malware only
B. Zero-day threats
C. Signed apps
D. Static binaries

Q32. Android rooting breaks security primarily by:
A. Encrypting storage
B. Breaking sandbox isolation
C. Enabling SELinux
D. Improving updates

Q33. WebView vulnerabilities combined with JavaScript bridges may lead to:
A. UI crash
B. Remote code execution
C. Network slowdown
D. App signing failure

Q34. Session hijacking is possible when:
A. Sessions are encrypted
B. Session IDs are predictable or exposed
C. MFA is enabled
D. HTTPS is enforced

Q35. Smishing attacks are more effective on mobile because:
A. Users ignore SMS
B. SMS appears more trustworthy
C. Firewalls block SMS
D. TLS is mandatory

Q36. Advanced Persistent Threats (APTs) focus on:
A. Speed
B. Stealth and long-term access
C. Random scanning
D. Script automation

Q37. System file integrity verification relies mainly on:
A. Encryption
B. Hash comparison
C. Access control
D. IDS alerts

Q38. Honeypots are primarily deployed to:
A. Block attacks
B. Detect and study attackers
C. Encrypt traffic
D. Replace firewalls

Q39. Mobile malware abusing Accessibility Services can:
A. Improve UX
B. Automate malicious actions
C. Patch vulnerabilities
D. Disable apps

Q40. A secure cybersecurity strategy must integrate:
A. Tools only
B. Technology, processes, and people
C. Antivirus only
D. Firewalls only