⍰ EASY (Q1–Q10)

Q1. Web-based attacks on Android primarily target:
A. Hardware components
B. Mobile browsers and WebViews
C. Kernel drivers
D. SIM cards

Q2. A drive-by download occurs when:
A. User installs apps from Play Store
B. Malware downloads automatically from a malicious webpage
C. User enables encryption
D. TLS is enforced

Q3. WebView vulnerabilities are dangerous because:
A. They block JavaScript
B. They bridge web content with native app code
C. They encrypt traffic
D. They prevent attacks

Q4. MITM attacks compromise which security objective first?
A. Availability
B. Confidentiality
C. Performance
D. Usability

Q5. Rogue Wi-Fi access points are also called:
A. Secure APs
B. Evil Twin access points
C. Private hotspots
D. Trusted networks

Q6. SSL stripping attacks downgrade:
A. HTTP to HTTPS
B. HTTPS to HTTP
C. TLS to IPSec
D. VPN to TLS

Q7. Packet sniffing is easiest on:
A. Wired networks
B. Encrypted networks
C. Open Wi-Fi networks
D. Cellular networks

Q8. Phishing attacks mainly exploit:
A. Cryptographic flaws
B. Human trust
C. Kernel bugs
D. Hardware failures

Q9. Smishing attacks use:
A. Email
B. SMS
C. Voice calls
D. Bluetooth

Q10. Vishing attacks are conducted via:
A. SMS
B. Email
C. Voice calls
D. Social media only

□ MEDIUM (Q11–Q25)

Q11. Mobile browsers are vulnerable because they:
A. Lack sandboxing
B. Process untrusted web content
C. Use strong encryption
D. Block scripts

Q12. Malicious web pages may exploit:
A. JavaScript and browser vulnerabilities
B. Secure APIs
C. SELinux
D. Verified Boot

Q13. WebView attacks often occur due to:
A. Disabled JavaScript
B. Exposed JavaScript interfaces
C. TLS enforcement
D. Certificate pinning

Q14. MITM attacks on mobile networks often use:
A. Encrypted VPNs
B. Rogue access points
C. Secure routers
D. IDS systems

Q15. SSL stripping is successful when:
A. Certificate pinning is used
B. Users ignore HTTPS warnings
C. TLS is enforced
D. VPN is active

Q16. Packet sniffing on wireless networks can expose:
A. Encrypted passwords
B. Plaintext credentials
C. Kernel memory
D. Hardware IDs only

Q17. Network-based mobile attacks increase when users:
A. Use VPNs
B. Connect to public Wi-Fi
C. Enable firewall
D. Disable Bluetooth

Q18. Social engineering attacks succeed because:
A. Encryption fails
B. Humans are predictable
C. Networks are slow
D. IDS fails

Q19. Malicious app deception involves:
A. Secure app updates
B. Fake apps mimicking legitimate ones
C. OS patching
D. Certificate pinning

Q20. Smishing attacks are more effective on mobile because:
A. Small screen size
B. Users trust SMS more
C. TLS is absent
D. Firewalls block emails

Q21. Attack kill chain includes:
A. Detection only
B. Reconnaissance to exploitation
C. Encryption only
D. Patch management

Q22. Behavioral analysis helps detect:
A. Known signatures only
B. Abnormal app or user behavior
C. Hardware faults
D. Network speed

Q23. Network monitoring detects:
A. UI bugs
B. Suspicious traffic patterns
C. App layouts
D. Battery usage

Q24. User awareness indicators include:
A. IDS alerts
B. Unexpected messages and links
C. Kernel logs
D. CPU usage

Q25. Mobile OS updates help prevent attacks by:
A. Increasing UI features
B. Patching known vulnerabilities
C. Removing apps
D. Disabling Wi-Fi

● HARD (Q26–Q40)

Q26. Drive-by downloads are dangerous because they:
A. Require user consent
B. Execute without user awareness
C. Use encryption
D. Need root access

Q27. WebView vulnerabilities combined with JavaScript bridges can lead to:
A. Secure IPC
B. Remote code execution
C. Network slowdown
D. App crashes only

Q28. MITM attacks are harder to detect on mobile because:
A. Strong encryption
B. Users rely on untrusted networks
C. IDS is built-in
D. VPN is default

Q29. Rogue Wi-Fi APs exploit which weakness?
A. Kernel bugs
B. Trust in network names (SSIDs)
C. Encryption algorithms
D. Hardware drivers

Q30. SSL stripping attacks fail when apps implement:
A. HTTP only
B. Certificate pinning
C. Plaintext credentials
D. Open APIs

Q31. Packet sniffing combined with MITM enables attackers to:
A. Only view traffic
B. Modify and inject data
C. Improve performance
D. Patch systems

Q32. Social engineering attacks bypass technical controls by targeting:
A. Encryption
B. Human psychology
C. Firewalls
D. IDS signatures

Q33. Smishing combined with malicious apps leads to:
A. Secure downloads
B. Credential harvesting
C. OS patching
D. App store protection

Q34. Mobile phishing differs from desktop phishing because:
A. Mobile lacks browsers
B. Limited UI hides URL details
C. TLS is stronger
D. Firewalls block it

Q35. Detection of MITM on mobile includes:
A. UI testing
B. Certificate validation failures
C. Screen resolution checks
D. Battery monitoring

Q36. Network-level defenses for mobile include:
A. App obfuscation
B. VPNs and secure Wi-Fi
C. Code signing
D. Root detection

Q37. Behavioral analysis limitations include:
A. No logs
B. False positives
C. No runtime data
D. No detection

Q38. Social engineering attacks are difficult to mitigate because:
A. No tools exist
B. Human behavior varies
C. Encryption fails
D. OS is weak

Q39. Mobile security requires layered defense due to:
A. One attack vector
B. Multiple threat vectors
C. No users
D. No networks

Q40. Effective defense against mobile threats requires:
A. Antivirus only
B. Secure OS + apps + user awareness
C. Root access
D. Disabling internet