⍰ EASY (Q1–Q10)

Q1. Mobile malware is designed primarily to:
A. Improve app performance
B. Compromise mobile devices and data
C. Patch vulnerabilities
D. Optimize battery usage

Q2. Android malware commonly spreads through:
A. Official OS updates
B. Malicious applications
C. Hardware faults
D. Secure APIs

Q3. Spyware on mobile devices mainly targets:
A. Network speed
B. User data and activities
C. Hardware drivers
D. Battery health

Q4. Ransomware affects which security objective most directly?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q5. Adware primarily aims to:
A. Encrypt files
B. Display unwanted advertisements
C. Steal passwords
D. Disable antivirus

Q6. Banking malware targets:
A. Media files
B. Financial credentials
C. System logs
D. Kernel modules

Q7. Static Android app analysis does NOT require:
A. APK file
B. Source code execution
C. Permissions review
D. Manifest analysis

Q8. Dynamic analysis requires:
A. Source code
B. Runtime execution
C. Decompilation only
D. Hash comparison

Q9. Indicators of Compromise (IOCs) include:
A. App icons
B. Suspicious permissions and network traffic
C. UI themes
D. Screen resolution

Q10. Mobile malware evolution is driven by:
A. User awareness
B. Improved security controls
C. Attacker adaptation
D. OS stability

□ MEDIUM (Q11–Q25)

Q11. Android malware infection vectors include:
A. Secure Play Store apps only
B. Third-party app stores and phishing links
C. OS kernel updates
D. Encrypted storage

Q12. Trojans disguise themselves as:
A. System services
B. Legitimate applications
C. Kernel drivers
D. Bootloaders

Q13. Fileless mobile malware primarily operates in:
A. External storage
B. Memory
C. System partition
D. Cache directory

Q14. Static analysis helps identify:
A. Runtime memory usage
B. Hardcoded secrets and APIs
C. Network latency
D. CPU scheduling

Q15. Dynamic analysis reveals:
A. App permissions only
B. Actual malicious behavior during execution
C. APK structure only
D. Code obfuscation

Q16. Behavioral analysis focuses on:
A. Code syntax
B. App actions and patterns
C. UI layout
D. File compression

Q17. Android malware often abuses permissions such as:
A. INTERNET and READ_SMS
B. BLUETOOTH only
C. NFC only
D. CAMERA only

Q18. Reverse engineering mobile malware helps defenders:
A. Spread malware
B. Understand functionality and create signatures
C. Increase infection rate
D. Disable updates

Q19. Signature-based detection is limited because:
A. It detects zero-day threats
B. Malware changes signatures frequently
C. It uses heuristics
D. It analyzes behavior

Q20. Heuristic-based detection focuses on:
A. Exact hash matching
B. Suspicious code patterns
C. Network speed
D. File size

Q21. Behavioral-based detection identifies malware by:
A. Known hashes
B. Runtime actions
C. App name
D. Developer signature

Q22. MobSF is primarily used for:
A. Network routing
B. Mobile app security analysis
C. Password cracking
D. Kernel debugging

Q23. Android malware often communicates with:
A. Google servers
B. Command and Control (C2) servers
C. DNS root servers
D. App store servers

Q24. Rooted devices are more vulnerable because:
A. They are encrypted
B. Malware gains elevated privileges
C. Updates are faster
D. Permissions are reduced

Q25. Malware targeting mobile devices often exploits:
A. Hardware defects
B. User trust and app permissions
C. BIOS vulnerabilities
D. Secure boot

● HARD (Q26–Q40)

Q26. Banking malware combined with overlay attacks enables:
A. Network scanning
B. Credential theft during legitimate app usage
C. Encryption
D. IDS detection

Q27. Fileless mobile malware is harder to detect because it:
A. Uses disk files
B. Leaves minimal forensic artifacts
C. Is slower
D. Requires reboot

Q28. Android malware persistence is commonly achieved via:
A. Temporary files
B. Auto-start services and receivers
C. Screen locks
D. UI components

Q29. Reverse engineering APKs threatens security by:
A. Improving encryption
B. Exposing hardcoded secrets
C. Reducing attack surface
D. Increasing performance

Q30. Static analysis limitations include:
A. Full runtime visibility
B. Inability to observe dynamic behavior
C. No access to code
D. No permission data

Q31. Dynamic analysis limitations arise when malware:
A. Executes normally
B. Detects emulators or sandboxes
C. Uses permissions
D. Is static

Q32. Behavioral analysis is effective against:
A. Known malware only
B. Zero-day mobile malware
C. Signed apps
D. Static code

Q33. Android malware often abuses Accessibility Services to:
A. Improve UX
B. Capture user input and automate actions
C. Encrypt data
D. Patch vulnerabilities

Q34. Mobile malware targeting IoT-connected apps increases risk because:
A. IoT is isolated
B. Compromise extends beyond mobile device
C. IoT uses strong security
D. Apps are sandboxed

Q35. Network traffic analysis helps identify:
A. UI bugs
B. Malicious C2 communication
C. Layout flaws
D. App themes

Q36. Indicators of mobile malware include:
A. Improved performance
B. Unexpected permissions and battery drain
C. Faster boot time
D. Stable network

Q37. Desktop malware differs from mobile malware because mobile:
A. Has no OS security
B. Relies heavily on app permissions
C. Has no network
D. Cannot be infected

Q38. Static vs Dynamic analysis comparison shows that:
A. Static is always sufficient
B. Dynamic provides runtime insights
C. Dynamic replaces static
D. Static detects behavior

Q39. Effective mobile malware defense requires:
A. Antivirus only
B. Secure apps, OS updates, and user awareness
C. Root access
D. Disabling internet

Q40. Ethical requirement in mobile malware analysis is:
A. Speed
B. Isolation and authorization
C. Internet access
D. Public execution