? EASY (Q1–Q10)

Q1. Android Debug Bridge (ADB) is primarily used to:
A. Encrypt Android apps
B. Communicate with Android devices
C. Scan networks
D. Crack passwords

Q2. ADB follows a:
A. Peer-to-peer architecture
B. Client–server architecture
C. Master–slave architecture
D. Distributed architecture

Q3. The ADB client runs on:
A. Android device
B. Android kernel
C. Developer machine
D. Cloud server

Q4. The ADB daemon (adbd) runs on:
A. Developer system
B. Android device
C. Router
D. Database server

Q5. ADB server listens on which default port?
A. 80
B. 443
C. 5037
D. 8080

Q6. The command `adb devices` is used to:
A. Install APK
B. List connected devices
C. Access shell
D. View logs

Q7. ADB can connect over:
A. USB only
B. TCP/IP only
C. USB and TCP/IP
D. Bluetooth only

Q8. `adb install` **is used to:**
A. Remove apps
B. Install APK files
C. View permissions
D. Debug kernel

Q9. Logcat is used to:
A. Encrypt logs
B. View system and app logs
C. Scan ports
D. Capture packets

Q10. ADB shell provides:
A. GUI access
B. Command-line access to device
C. Network scanning
D. File encryption

□ MEDIUM (Q11–Q25)

Q11. ADB enables penetration testers to:
A. Patch Android OS
B. Interact deeply with app and system
C. Replace kernel
D. Disable SELinux permanently

Q12. Debuggable apps are risky because they:
A. Are faster
B. Allow runtime inspection
C. Improve security
D. Block reverse engineering

Q13. `adb pull` **command is used to:**
A. Upload files to device
B. Download files from device
C. Delete files
D. Encrypt files

Q14. `adb push` **allows testers to:**
A. Pull logs
B. Copy files to device
C. Reboot device
D. Scan ports

Q15. ADB over network is dangerous because:
A. Uses encryption
B. Can allow remote unauthorized access
C. Improves debugging
D. Requires VPN

Q16. Android emulator testing is preferred because it:
A. Is illegal
B. Is isolated and safe
C. Is slower
D. Requires rooting

Q17. Static analysis tools for Android analyze:
A. Runtime memory
B. APK without execution
C. Network traffic
D. Kernel modules

Q18. Dynamic analysis tools require:
A. Source code
B. App execution
C. APK signing
D. Root always

Q19. Network traffic analysis tools focus on:
A. UI elements
B. App communication
C. File permissions
D. Code obfuscation

Q20. Android pentesting frameworks provide:
A. OS updates
B. Integrated testing capabilities
C. Antivirus engines
D. Encryption services

Q21. ADB misuse can compromise:
A. Device confidentiality
B. Device integrity
C. Device availability
D. All of the above

Q22. `adb logcat` **helps identify:**
A. Hardware failures
B. Sensitive data leakage in logs
C. Disk errors
D. Network routing

Q23. ADB access bypasses which security layer?
A. Network firewall
B. App sandbox (partially)
C. Encryption
D. SELinux fully

Q24. USB debugging should be:
A. Always enabled
B. Disabled in production devices
C. Enabled for all users
D. Ignored

Q25. Android pentesting tools are mainly used to:
A. Create malware
B. Identify security weaknesses
C. Patch OS
D. Block traffic

🟢 HARD (Q26–Q40)

Q26. ADB architecture improves flexibility by separating:
A. UI and logic
B. Client, server, and daemon
C. Kernel and apps
D. Storage and memory

Q27. Unauthorized ADB access is most dangerous when:
A. Device is locked
B. Device is unlocked with debugging enabled
C. SELinux is enforcing
D. Network is secure

Q28. Debuggable flag in AndroidManifest.xml allows:
A. Production execution
B. Runtime inspection and debugging
C. Encryption
D. Permission escalation

Q29. ADB shell commands can be abused to:
A. Only read logs
B. Access sensitive files
C. Improve performance
D. Encrypt data

Q30. Emulator-based testing differs from physical devices because:
A. Emulator has no security
B. Emulator provides controlled environment
C. Emulator cannot run apps
D. Emulator uses real hardware

Q31. Network traffic interception in Android testing helps detect:
A. UI flaws
B. Insecure communication
C. Kernel bugs
D. Hardware issues

Q32. Dynamic analysis combined with ADB enables:
A. Static code review only
B. Runtime behavior observation
C. OS replacement
D. Encryption removal

Q33. ADB over TCP/IP should be restricted because:
A. It improves performance
B. It exposes remote attack surface
C. It encrypts traffic
D. It requires authentication

Q34. Android pentesting tools often require rooted devices to:
A. Break encryption
B. Access protected areas
C. Improve UI
D. Disable kernel

Q35. Detection of ADB misuse involves monitoring:
A. Screen resolution
B. USB and network debugging events
C. File size
D. App updates

Q36. ADB compromises confidentiality when attackers:
A. Reboot device
B. Extract sensitive app data
C. View UI
D. Enable airplane mode

Q37. ADB compromises integrity when attackers:
A. Read logs
B. Modify system or app files
C. List devices
D. Check version

Q38. Android pentesting tools limitations include:
A. Perfect detection
B. False positives and device dependency
C. No reports
D. No learning curve

Q39. Secure SDLC recommends ADB usage:
A. In production always
B. Only during development/testing
C. Never
D. For end users

Q40. The safest practice regarding ADB is:
A. Enable permanently
B. Enable only when required and disable later
C. Share access
D. Ignore security warnings