# ? EASY (Q1–Q10)

**Q1. Android is primarily based on which kernel?**
A. Windows kernel
B. Linux kernel
C. UNIX kernel
D. BSD kernel

**Q2. The topmost layer of Android architecture is:**
A. Linux Kernel
B. Native Libraries
C. Application Layer
D. Android Runtime

**Q3. Android applications are primarily written in:**
A. C only
B. Java / Kotlin
C. Python
D. Swift

**Q4. An Android application package is known as:**
A. JAR
B. APK
C. EXE
D. IPA

**Q5. Each Android app runs in:**
A. Shared memory space
B. Its own sandbox
C. Kernel space
D. BIOS layer

**Q6. Android permissions are declared in:**
A. build.gradle
B. AndroidManifest.xml
C. classes.dex
D. resources.arsc

**Q7. Android Runtime (ART) is responsible for:**
A. Network routing
B. App execution
C. UI rendering
D. File storage

**Q8. The /data directory mainly stores:**
A. System files
B. User application data
C. Kernel modules
D. Boot files

**Q9. SELinux in Android enforces:**
A. Optional security
B. Mandatory Access Control
C. Discretionary Access Control
D. Role-based control

**Q10. Rooting an Android device gives:**
A. Guest access
B. Superuser privileges
C. Network isolation
D. Encryption

---

# □ MEDIUM (Q11–Q25)

**Q11. Android sandboxing improves security by:**
A. Sharing resources
B. Isolating applications
C. Allowing root access
D. Removing permissions

**Q12. The Application Framework provides:**
A. Hardware drivers
B. High-level system services
C. Kernel scheduling
D. Encryption keys

**Q13. Dalvik VM was replaced by ART to improve:**
A. Network security
B. App performance and efficiency
C. UI design
D. Permission handling

**Q14. classes.dex contains:**
A. UI layouts
B. Compiled bytecode
C. App permissions
D. Resources

**Q15. Android UID is used to:**
A. Encrypt apps
B. Identify applications uniquely
C. Manage networks
D. Track devices

**Q16. Verified Boot ensures:**
A. Faster startup
B. Device integrity at boot time
C. App encryption
D. Network security

**Q17. The /system partition is usually:**
A. Writable by users
B. Read-only
C. Temporary
D. Encrypted per app

**Q18. Content Providers are used to:**
A. Play media
B. Share data between apps securely
C. Execute services
D. Render UI

**Q19. Intent filters allow Android to:**
A. Encrypt intents
B. Resolve app components
C. Block apps
D. Log traffic

**Q20. Rooting increases attack surface because it:**
A. Reduces permissions
B. Breaks sandbox isolation
C. Improves updates
D. Enables encryption

**Q21. Exploit-based rooting uses:**
A. User approval
B. Vulnerabilities in OS or kernel
C. Google Play services
D. App permissions

**Q22. Android app signing ensures:**
A. Confidentiality
B. App authenticity and integrity
C. Network security
D. Faster installation

**Q23. /sdcard storage is considered:**
A. Secure internal storage
B. Publicly accessible storage
C. Kernel storage
D. Encrypted partition

**Q24. Android permissions prior to version 6 were:**
A. Runtime-based
B. Install-time only
C. Dynamic
D. Optional

**Q25. Root detection mechanisms aim to:**
A. Improve performance
B. Detect compromised devices
C. Encrypt storage
D. Block updates

---

# 🟥 HARD (Q26–Q40)

**Q26. Android security model relies heavily on:**
A. Antivirus software
B. Linux user isolation and sandboxing
C. Firewalls
D. IDS

**Q27. Improper permission configuration may lead to:**
A. DoS attacks
B. Privilege escalation
C. Hardware failure
D. Network outage

**Q28. Rooted devices are risky because attackers can:**
A. Only read logs
B. Modify system binaries
C. Disable screen lock
D. Improve performance

**Q29. SELinux enforcing mode:**
A. Logs violations only
B. Blocks policy violations
C. Allows all actions
D. Is disabled by default

**Q30. Insecure file permissions can expose:**
A. Kernel code only
B. Sensitive app data
C. Network routes
D. BIOS data

**Q31. Android application sandboxing fails if:**
A. App uses intents
B. Device is rooted
C. App is signed
D. SELinux is enabled

**Q32. ART improves security by:**
A. Removing sandbox
B. Ahead-of-Time (AOT) compilation
C. Using interpreted code
D. Allowing root

**Q33. Android build process security includes:**
A. Obfuscation only
B. Signing and verification
C. Root access
D. Debug flags

**Q34. Privilege escalation on Android often targets:**
A. UI components
B. Kernel vulnerabilities
C. App resources
D. Layout files

**Q35. Misconfigured Content Providers can lead to:**
A. Secure data sharing
B. Data leakage
C. Encryption
D. App crashes only

**Q36. Verified Boot failure indicates:**
A. App corruption
B. System integrity compromise
C. Network attack
D. Storage full

**Q37. Rooting detection is critical for:**
A. Games only
B. Banking and enterprise apps
C. Media apps
D. UI apps

**Q38. Android security differs from desktop OS because:**
A. No kernel
B. App-level sandboxing by default
C. No permissions
D. No updates

**Q39. Insecure IPC mechanisms can cause:**
A. Hardware failure
B. Inter-app attacks
C. Network outage
D. Disk corruption

**Q40. Defense against Android attacks requires:**
A. Root access
B. Secure coding + platform security
C. Antivirus only
D. User ignorance