Android Malware

Comprehensive guide — architecture, analysis, techniques, and practical exercises

01 Introduction to Android Malware

Scope, threat models, and landscape — why Android is targeted and common attacker goals.

02 Android Architecture & Security

Key platform layers (Linux kernel, ART, apps, SELinux, permissions) and built-in defenses.

03 📁 Android Folder Structure

Filesystem layout on devices and emulators — where apps, logs, and artifacts live for analysis.

04 📦 APK Internals - Deep Structure

Breakdown of APKs: manifest, classes (DEX), resources, native libs, signing and packing tricks.

05 📄 XML in Android - Complete Analysis

Parsing manifests and resource XML: intents, permissions, exported components and malicious indicators.

06 Development Environment Setup

Tooling and safe lab setup: Android SDK, ADB, emulators, virtual devices and containment best practices.

07 🛠️ Advanced Practical Tools

Hands-on tools for reversing and inspection: jadx, apktool, frida, drozer, and network interceptors.

08 Android App Components

Activities, Services, BroadcastReceivers, ContentProviders — how components are abused by malware.

Core Techniques

09 1. Data Exfiltration

Methods for stealing contacts, SMS, files, and credentials; local vs. network exfil strategies.

10 2. Persistence Mechanisms

Techniques to remain resident: autostart receivers, scheduled jobs, abusing accessibility services.

11 3. Privilege Escalation

Local escalation paths, exploit primitives, and misuse of system APIs or misconfigurations.

12 4. Anti-Analysis Techniques

Emulator detection, sandbox checks, runtime checks, and conditional payload activation.

13 5. Network Communication

C2 patterns, covert channels, encryption, domain fronting and bulletproof hosting considerations.

14 6. Obfuscation Methods

String/flow obfuscation, native loaders, packing and multi-stage loaders used to evade detection.

15 7. Emulator Detection

Checks targeting emulator artifacts, sensor absence and behavior-based heuristics to avoid analysis.

16 8. Dynamic Analysis Evasion

Anti-frida, anti-debug, and runtime packing strategies to foil dynamic instrumentation.

Analysis & Detection

17 Reverse Engineering

Static reversing workflows, DEX analysis, deobfuscation steps and useful heuristics for analysts.

18 Dynamic Analysis

Runtime monitoring, hooking, behavioral tracing and building reproducible analysis labs.

19 🔍 Mobile Forensics - Artifact Analysis

Key artifacts to collect from devices and emulators, timeline reconstruction and evidence handling.

20 Detection Methods

YARA rules, indicators, ML features and practical detection strategies for defenders.

21 Real-World Case Studies

Dissection of notable Android campaigns — techniques used, indicators and lessons learned.

22 Practical Exercises

Hands-on labs and challenges: reversing, instrumentation, sandboxing and building detection rules.

23 Conclusions & Resources

Summary, defensive recommendations and curated resources for further study.