ZERO TO HERO ANDROID

Android Security Awareness & Red-Team Concepts (Ethical Use Only)

Part 1: Foundations & Lab Setup

What is this: Core concepts for Android security learning and safe lab creation.

How it works: Covers Linux basics, environment setup on mobile/PC, and installing essential tools in an isolated lab.

Tools/Topics: Linux basics, virtualization/emulators, mobile labs, Windows/Linux tools

Part 2: Tooling Overview

What is this: Survey of common Android testing tools and categories.

How it works: Explains what botnets/RATs/payload frameworks are conceptually and where they fit in assessments.

Tools/Topics: Framework categories, cloud instances, device selection

Part 3: Persistence (Concepts)

What is this: Understanding persistence techniques at a high level.

How it works: Explains why persistence exists, how systems resist it, and how to detect/remove it.

Tools/Topics: Android app lifecycle, permissions, system protections

Part 4: Advanced Attack Patterns (Overview)

What is this: High-level look at modern attack chains affecting Android.

How it works: Breaks down stages (delivery, execution, C2) without operational detail; focuses on recognition.

Tools/Topics: Threat modeling, kill chain concepts

Part 5: Packaging & Delivery Concepts

What is this: How attackers disguise or deliver malicious apps (conceptually).

How it works: Covers risks of repackaging, sideloading, and update abuse; emphasizes user safeguards.

Tools/Topics: APK structure, signing, app distribution risks

Part 6: Network & IP-Based Risks

What is this: Risks related to exposed services and network interactions.

How it works: Explains how misconfigurations can expose devices and how to secure them.

Tools/Topics: Ports, firewalls, NAT, secure configs

Part 7: Obfuscation & Evasion (Awareness)

What is this: Why malware uses obfuscation and how defenders respond.

How it works: Covers detection basics, signatures vs behavior, and safe analysis approaches.

Tools/Topics: Static/dynamic analysis concepts

Part 8: Cloud & Performance Setup

What is this: Using cloud resources for testing labs.

How it works: Explains resource allocation and safe usage for analysis environments.

Tools/Topics: Cloud VMs, resource planning

Part 9: Ransomware (Awareness)

What is this: How ransomware operates at a high level on mobile.

How it works: Focus on indicators of compromise and prevention strategies.

Tools/Topics: Backup strategies, permissions hygiene

Part 10: Safety, Evasion Awareness & Hygiene

What is this: Recognizing risky behaviors and protecting devices.

How it works: Covers safe browsing, app vetting, permissions, and incident response basics.

Tools/Topics: Play Protect, updates, backups, MFA

Part 11: Social Engineering (Awareness)

What is this: Human factors in mobile attacks.

How it works: How attackers exploit trust and how users can identify red flags.

Tools/Topics: Phishing awareness, messaging risks

Part 12: Defense & Best Practices

What is this: Practical steps to secure Android devices and labs.

How it works: Hardening devices, monitoring, and response playbooks.

Tools/Topics: Security checklists, updates, backups