

**Mastering Android Penetration Testing (MAPT) — Course Content**

**Module 1 – Introduction to Android Security & Pentesting**

* Android OS architecture & security model
* App lifecycle & components (Activities, Services, Broadcast Receivers, Content Providers)
* Types of Android security threats
* Pentesting methodology for mobile apps

**Module 2 – Setting Up the Pentesting Environment**

* Installing Android Studio & SDK tools
* Setting up Android Virtual Devices (AVDs)
* Using physical devices for testing (rooted & non-rooted)
* Installing tools: ADB, Frida, MobSF, Burp Suite

**Module 3 – Android Application Fundamentals**

* APK structure & components
* AndroidManifest.xml analysis
* Understanding Dalvik/ART runtime
* Permission model & security implications

**Module 4 – Static Analysis of Android Apps**

* Decompiling APKs (apktool, JADX)
* Analyzing source code for vulnerabilities
* Finding hardcoded secrets & API keys
* Reverse engineering obfuscated code

**Module 5 – Dynamic Analysis of Android Apps**

* Monitoring app behavior in real-time
* Using Frida for runtime instrumentation
* Hooking methods to bypass security checks
* Monitoring network traffic with Burp/ZAP

**Module 6 – Android Debug Bridge (ADB) Exploitation**

* ADB basics & device communication
* Extracting data via ADB commands
* Exploiting misconfigured ADB services

**Module 7 – Insecure Data Storage**

* Exploiting SQLite databases
* Accessing SharedPreferences & internal storage
* Analyzing external storage for sensitive data
* Exploiting Android backup files

**Module 8 – Insecure Communication**

* Exploiting apps without HTTPS/TLS
* Bypassing SSL pinning
* MITM attacks on mobile apps
* Intercepting & modifying API calls

**Module 9 – Authentication & Authorization Flaws**

* Bypassing login screens & authentication flows
* Exploiting insecure session tokens
* Privilege escalation within the app

**Module 10 – WebView Exploitation**

* Exploiting insecure WebView configurations
* JavaScript injection in WebViews
* File access & local file inclusion attacks

**Module 11 – Insecure Code Practices**

* Hardcoded credentials
* Improper use of crypto APIs
* Unvalidated inputs & parameter tampering

**Module 12 – Reverse Engineering & Code Patching**

* Disassembling & modifying APKs
* Rebuilding and signing modified apps
* Bypassing root detection & jailbreak checks

**Module 13 – Exploiting Android Components**

* Attacking exported Activities & Services
* Broadcast Receiver abuse
* Content Provider exploitation

**Module 14 – Rooting & Privilege Escalation**

* Understanding Android rooting techniques
* Exploiting device vulnerabilities for root access
* Post-exploitation persistence

**Module 15 – Mobile Malware Analysis**

* Identifying malicious apps
* Analyzing malware behavior in a sandbox
* Detecting spyware & ransomware samples

**Module 16 – Exploiting Android IoT & Wearable Devices**

* Attack surface of Android-based IoT devices
* Bluetooth & NFC exploitation
* Firmware extraction & analysis

**Module 17 – Advanced Android Exploitation**

* Exploiting native code with buffer overflows
* Dynamic instrumentation with Objection & Frida
* Exploiting vulnerabilities in third-party SDKs

**Module 18 – Mobile App Security Bypass**

* Bypassing root/jailbreak detection
* Circumventing SSL pinning and emulator checks
* Defeating anti-debugging mechanisms

**Module 19 – Reporting & Documentation**

* Writing Android pentest reports
* Creating PoC videos/screenshots
* Suggesting remediation & secure coding practices

**Module 20 – Final Android Pentesting Project**

* Full-scope Android app assessment
* Chaining multiple vulnerabilities into complex exploits
* Final report & presentation to stakeholders