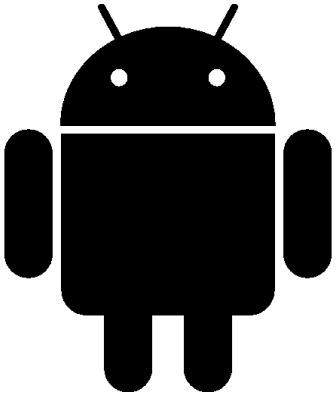
Intellectual POINT
EXCELLENCE THROUGH EDUCATION

POLITO INC
Masterful Cyber Security

Hacking the Android APK Training



Description:

This cross-discipline, hands-on training will walk participants through Android application testing and APK reversing basics. The tools and techniques imparted in this training will help guide APK analysis, mobile threat research, and mobile application penetration testing. Free and open source tools will be emphasized, while recognizing the potential role of commercial tools in static and dynamic analysis of APKs. The training will conclude with a CTF-style competition requiring participants to use their new skills to dissect actual Android applications including malicious APKs, intentionally vulnerable APKs, and custom APKs. An entry-level Android device will be provided to each participant to use during the class and CTF depending on class size.

Average Salary

$121,622/year

Level

Beginner/Intermediate

Pre-Requisites

Previous mobile development or general pen testing experience is helpful, but not required.

Course Breakdown:

Introduction to Android and Mobile Security Fundamentals

- OWASP Mobile Top 10
- Compare/contrast Android and iOS security

Into to Android Applications and the APK

- Play store
- Developer versions
- Where else to obtain APKs

Android Application Hacking Use Cases

- Mobile Application Security / Mobile Penetration Testing
- Bug Bounties
- Mobile Malware/Adware Research
- Mobile APT Research
- Mobile Forensics

Setting Up Your Android Test Environment

- VM
- Android Studio and adb tools
- Open source and free APK tools for static and dynamic analysis (apktool, JadX, etc.)
- Emulators
- Physical devices
  - Unlocking bootloaders and rooting test devices

Static Analysis

- Obtaining the APK
- APK structure and file contents
- Decoding and analyzing AndroidManifest.xml
  - API levels and compatibility
  - Permissions
  - App components and intents
- Certificates
- Decoding and Reversing DEX
  - Java source code triage techniques (no mobile coding experience required)

Course Breakdown contd:

Dynamic Analysis

- Proxy Options (Burp Suite, other proxy tools and techniques)
- Using dynamic test frameworks on device (e.g., Drozer, Frida/Brida)
- Logs, debug logs, and crash reports

Forensic Analysis

- App locations and local directory structure (rooted vs. un-rooted)
- Logical vs. physical Android acquisitions
- Obtaining and reviewing SQLite databases

Intermediate and Advanced Topics

- Bypassing Certificate Pinning
- Modifying and re-signing APKs
- De-obfuscating source code
- Identifying and understanding mobile app traffic, APIs, and server infrastructure
- Mobile malware/adware techniques and detection methodologies

Example APK Analysis Walkthroughs

- Malicious APK teardown and mobile threat research
- Banking APK and healthcare APK penetration tests

Capstone: Hacking the Android APK CTF Tournament

Required Materials

Students will need to bring their own Windows/Linux/macOS laptop with 8+ GB RAM, WiFi, USB, and VirtualBox or VMware installed. A VM will be made available to attendees for download before class, as well as available on USB flash drives at the start of class. Physical, rooted Android test devices will be available for use by students for the duration of the training (depending on class size).

About the Instructor:

Ben brings a diverse background in cybersecurity, IT, law, and law enforcement to Polito. After earning his JD from William & Mary School of Law in 2010 and providing IT and e-discovery support to law firms, Ben joined Booz Allen Hamilton as a cyber security consultant in 2012. While a member of Advanced Persistent Threat (APT) hunt teams assigned to commercial and federal clients, Ben sharpened his network security monitoring, forensics, incident response, malware analysis, cyber threat intelligence, and security architecture skills. He has earned the CISSP, GIAC Certified Forensic Analyst (GCFA), GIAC Web Application Penetration Tester (GWAPT), and Splunk Certified Power User certifications. Ben is a member of the Maryland bar and volunteers at a pro bono legal clinic.

POLITO INC
Masterful Cyber Security