HackerU

Android –
Mobile Security

CR111

05
Days

Android - Mobile Security

Outline

In this course, participants will learn about the Android operating system and how to work with Android development frameworks. The course covers operating system structures and applications. The course will also include topics about reverse engineering, application manipulation, & malware analysis. In addition, the participants will learn how to investigate malicious application, security issues and how to perform third-party manipulation.

Target Audience

Anyone who wants to understand how android, the most popular operation system, works.

- Learn the basic of android programing & (java) code.
- Investigate and explore the vulnerabilities of android applications.
- Analysis & Research of Android applications

Objectives

On completing this course, you will be able to:

- Know how Android's Internal operations work.
- Build a basic application for Android.
- Know the structure of an Android app.
- Understanding the vulnerability and issues of Android applications.
- Reverse engineer, manipulate, and investigate applications.
- Bypass SSL network security mechanisms in Android applications.
- Create malicious applications.

Hardware Requirements

- Kali Linux virtual machine
- Win7\10 virtual machine (backup)
- Android studio on host machine and kali virtual
- Java installed on all host pc & kali
- Ability to install extensions & tool with no administrator block
- Full internet access

Prerequisites

Before attending this course, students must have the following technical knowledge:

- Basic knowledge of working with Windows & Linux OSs.

Content

Day 1 — Module 01
Introduction to Android & Android Studio

❚ Introduction to Android

❚ Android file system.

❚ Android permissions

❚ Interaction with Android through ADB (android debug bridge).

❚ Android Emulation

❚ Working Android Studio

❚ Create "HELLO WORLD" first application

Day 2 — Module 02
Android programming

❚ Java programing basics

❚ Android Activities life cycle, events.

❚ Adding\Defining\Editing visual elements.

❚ Create an application with multiple Activities.

❚ Signing an application

Day 3 — Module 03
Android Reverse Engineering

❚ Reversing Android applications

▫ Decomplication

▫ Java code review

▫ Smali code review (machine code)

▫ Recompiling an app

❚ Code editing methods.

❚ Explore Reversing tools & Frameworks.

❚ Malicious Android applications

❚ Getting full control of an Android device with reverse shell.

Day 4 — Module 04
Networking & SSL pinning

❚ Network monitoring using Burp & proxy Configuration.

❚ Android traffic interception

❚ SSL verification methods.

❚ Interception with SSL pinning.

❚ Certificate – Manual obtaining and generating.

❚ Bypass Trust Managers.

Day 5 — Module 05
MobSF & Drozer

❚ Analysis methodologies

▫ Static analysis

▫ Dynamic analysis

❚ MODSF installation, Security review & Resources.

❚ Drozer Server, Sessions, Interacting with services.

❚ Android challenges & Final Exercises

Learn how to **investigate malicious application, security issues** and how to perform third-party manipulation"

The HackerU
Advantage

We have unparalleled experience in building advanced training programs for companies and organizations around the world — Talk to one of our experts and find out why.

01
Handcrafted Training Programs

02
State-Of-The-Art Learning Materials

03
Israel's Premier Training Center

04
Fueled by Industry Leading Cyber Experts

05
Over 20 Years of Proven IT-Education Success

Info@hackerupro.com

hackerupro.com