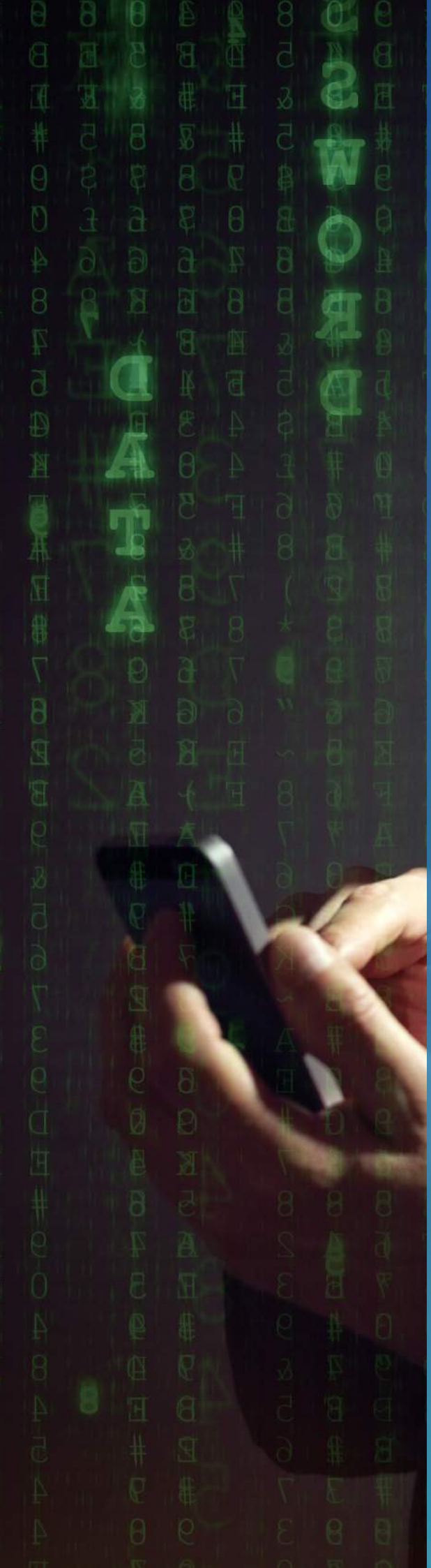

HACKERU
Experience Makes Experts

Mobile Application Penetration Testing

Index: RT400

56
Hours

Mobile Application Penetration Testing

Description

The Mobile Application Penetration Testing course is the head-start for penetration testers who wish to learn the fundamentals of Android and iOS app-security and exploitation. During this course, participants will study Android and iOS internals and understand how applications on those platforms operate. Relying on this knowledge, they will gain various methods and techniques to exploit mobile-app vulnerabilities and practice them hands-on. By the end of the course, students will have practiced different ways of exploiting mobile applications to take control of the mobile device, and will be able to test applications for their level of security.

Target Audience

The course targets participants with a foundation knowledge in information security and ethical hacking, who wish to understand the world of mobile security and penetration testing. Primarily:

- Ethical hackers
- Penetration testers
- Red Team members
- Technical cyber security personnel
- Experienced mobile developers

Prerequisites

- Good knowledge of computer networking and background in information security.
- Basic knowledge in ethical hacking, infrastructure hacking, and preferably web application hacking.
- Familiarization with Android and iOS development is an advantage.
- CEH provides a solid foundation of preliminary knowledge required for this course.

Objectives

- Understanding the mobile interface and learning how to analyze traffic on mobile devices.
- Mastering methods of penetration testing on Android devices.
- Learning how to penetrate and exploit iOS vulnerabilities.
- Learning the different ways to control a mobile device, see its traffic, listen to phone conversations, alter data and more.

Course Outline

01

Introduction to Smartphones

4 Hours

The first module will introduce participants to the fundamentals of smart-phone technology, architecture and different components. Students will also study the aspect of security for each part of the mobile platform in order to prepare them for later exploitation of the vulnerabilities engulfed in them.

- The mobile landscape
- Models of mobile security
- The differences between iOS and Android
- The risks of trusting apps to run on the device
- Overview of the attack vectors in mobile devices
- Smartphone components:
  - SIM card
  - SD card

02

Mobile Network Analysis

16 Hours

During this module participants will learn about different mobile-app security weaknesses and exploit them. They will examine both server and client-side vulnerabilities, and study authentication types, cryptographic weaknesses, traffic layers and more. By the end of the module, students will have a broad understanding of how mobile applications are vulnerable to penetration, preparing them for implementing the knowledge on each operating system specifically.

- Weak server-side APIs
  - Web service hardening
  - Secure configuration
  - API authentication
  - Defenses against injection
- Improper session-handling
  - Session expiration
  - Session fixation
  - Weak session tokens
- Protection on the OSI Transport Layer
  - Intercepting traffic
  - Secure TLS configuration
  - Certificate validation
  - Certificate pinning
- Device data leakage
  - 3rd party keyboards
  - URL caching
  - Application screenshots
  - Clipboard caching
  - Insecure logging
- Authentication & authorization
  - Mobile form factor
  - Offline authentication
  - Password management
- Broken cryptography
  - Weak cryptographic algorithms
  - Secure random-number-generation
  - Secure secret management
  - Android Keystore System
  - iOS Keychain Services

03

Android

20 Hours

This module opens with a deep coverage of the Android structure, permission, applications and components. Students will learn how to extract data and parse through large quantities of it in order to pinpoint the desired object. They will set-up virtual practice simulation-labs to exercise real-time traffic monitoring, Android hacking, exploiting client-side and server-side of Android apps, and the usage of advanced tools. By the end of this sessions, participants will be able to hack Android apps in variety of methods.

- Principals of android devices
- Android architecture
  - Permissions
  - Applications
  - Components
- Android file system
  - Defining data structure layout
    - Physical
    - File system
    - Logical
  - Data storage formats
  - Parsing and carving data
  - Physical and logical keyword searches
- Setting up your practice lab
  - Android Studio
  - AVD Installing and configuring
  - ADB
- Android SDK - main android framework
- JSON
- Signed APK trojans and exploits
  - Spade
  - FatRat
- Android Debug Bridge (adb)
- Traffic analysis
- Rooting
  - Rooting explained
  - Boot loaders
    - Locked
    - Unlocked
  - The process of rooting & installing custom ROM
- Basics of Android apps
  - Android-app components
  - Building DEX files from the command line
  - DEX analysis

- Attacking Android apps
  - The app attack-surface
  - Client-side threats
  - Backend threats
  - Testing and securing android apps
  - Automation tools
- Client-side attacks
  - Static analysis
    - App components
    - Static analysis using QARK
  - Dynamic analysis
    - Drozer
- Introduction to Drozer
- Advanced use of Drozer
- Drozer scripting
    - Introspy – Monitoring and analysis
    - Hooking using Xposed Framework
- Android malware
  - Writing Android malware
  - Registering permissions
  - Android Malware analysis
  - Android application reversing
  - Automation analysis
- Exploiting Android devices
  - MiTM attacks
  - Identifying dangerous apps
  - Using exploits
  - Extracting data from memory cards

04

iOS

16 Hours

Different to Android, the iOS operating system is considered more secure and less exposed to penetration. Yet, it is not impregnable. This module will teach participants the various known ways of penetrating into iOS. Students will cover the different components and features of the operating system, and of iOS devices.

- iOS introduction
  - iOS devices
  - iOS file system (HFS+)
  - iOS partitions
  - iOS applications
  - ARM Processor
  - iOS security mechanisms
- Penetrating iOS
  - Jailbreaking
  - Creating the penetration platform
  - SQLite databases
  - Plist files
- iOS analysis
  - Cycript runtime analysis
  - Decrypting applications
  - Hacking into iOS using GDB
- iOS Security
  - Data storage
  - Sqlite data files
  - Core data services
  - Keychain services
  - Monitoring iOS traffic
  - Intercepting SSL
- iOS forensics
  - Basics of iOS forensics
  - iOS tools for data protection
  - “Brute-forcing” the passcode
  - iTunes backup
- iOS exploitation
  - iOS malware
  - Metasploit on iOS
    - Bind shell
    - Reverse TCP
  - Backdoors
- iOS device acquisition
  - Phone identification
  - Operating modes
    - Normal
    - Recovery
  - Breaking passcodes
  - Acquisition
    - Direct
    - Logical
    - Physical
- iOS Analysis
  - Data structure and artifacts
    - Default applications
    - Popular applications
    - File carving
  - Analysis tools
- iOS backup
  - iTunes backup acquisition
  - Unencrypted backup
  - Encrypted backup
  - iCloud backup