Mobile App Device Security and Penetration Testing

Duration:
5 Days

What is the course about?
In this course you will learn how to find mobile device vulnerabilities and exploit them. You will learn how to setup a mobile penetration testing and forensics environment for Android and iOS mobile devices. You will learn how to extract data and recover data from Android and iOS devices. You will et accustomed with using wide array of tools to achieve the different tasks to exploit the device.The course is based on the OWASP Top 10 Mobile Risks for both Android and iOS. You will use the risks to profile the applications and also secure them.

Duration
The course is 5 days full time.

Programming Experience
No programming experience is required but to create your own scripts and also create Malware, programming in Python, or Ruby and Java is required. You can take the course without a programming background but you will not be able perform advanced techniques or do code analysis and debugging.

Technical Skill
Programming and computer security is required. This course is suitable for security specialists and programmers. You will need to be either proficient in developing iOS or Android mobile apps or be in the security field to benefit from this course. The course is highly hands on with minimal theory. You will need a good grasp of the command line as we will primarily use Linux and Mac OS X. A Macbook is required for working on iOS apps.

Private Training
The course is only offered privately to a group, team or company. We can schedule the course on your premises or our premises. A minimum of 4 delegates is required to schedule the course. The course price is R12 599 on your premises and R17 500 on our premises. There is no fixed date to run the course; we will work with you to find a date that meets your needs. The course can also be customized to fit your team requirements.

Benefits to You
By the end of the course you will have a solid understanding of the myriad attack vectors on mobile platforms, know how to perform assessment and provide informed decisions to management, clients and developers.

Course Topics

Mobile App Ecosystem Overview
Android
iPhone
Other mobile platforms

Mobile Devices Attack Vectors
Network - Interception of data over the air
Hardware - Baseband layer attacks
OS - Defects in kernel code or vendor supplied system
Application - Apps with vulnerabilities and malicious code have access to your data and device sensors.

Setting Up Android Development Environment
Installing and configuring the Android SDK and platform tools
Setting up Android Emulators
Enabling USB Debugging on Your Android Phone

Android Fundamentals
Android History
Android Components
Activities
Services
System Services
Content Providers
Broadcast Receiver
AndroidManifest File
Android Permission System

Android Security Model
Android Security Model & Linux Kernel
Android File System
Android File Hierarchy
App Sandboxing
Secure Inter process Communication
Application Signing
App Permissions

Android Forensic Security Tools
Cellebrite
MOBILedit
AutoSpy
Apktool
dex2jar
JD-GUI

Android Data Extraction
Imaging an Android Phone
Data Extraction Techniques
Data Recovery

Security Assessments of Android Apps – OWASP TOP 10

M2 Insecure Data Storage
Share Preferences
SQlite Databases

M3 Insufficient Transport layer protection
Introduction and HTTP traffic interception
Intercepting HTTPS traffic
Passive analysis with tcpdump & Wireshark

M4 Unintended Data Leakage
Reading the clipboard
Logging

M5 Poor Authorization and Authentication
M6 Broken Cryptography

M7 Client Side Attack
SQL Injection at Client Side
Frame injection in WebViews

M8 Security Decisions via untrusted inputs
Intent Spoofing

M9 – Improper Session Handling

M10 Lack of binary protection
Reversing android apps with APKTOOL
Reversing android apps with dex2jar & JD-GUI
Finding Content Provider URIs using APKTOOL

Setting Up iOS Development

Installing and configuring the Xcode for iOS Development
Setting up iOS Simulator
Deploying iOS apps to the device

Setting Up iOS PenTesting Lab

ElcomSoft iOS Forensic Toolkit
Oxygen Forensic Suite
Prawn iRecovery Stick
iFunBox
iExplorer
iBackupBot
Cycript
Snoop-IT

Hacking iOS

Understanding the Architecture
Understanding the Device
Application Security
Jailbreaking

iOS Internals Overview
iPhone models
iPhone hardware
iPad models
iPad Hardware
File system
The HFS file System
Disk Layout
iPhone Operating System

Data Acquisition from iOS Devices
Physical acquisition
iTunes backup
iCloud backup
Acquisition via jailbreaking

iOS Data Analysis and Recovery
Timestamps
SQLite Databases
Property Lists
Recovering Deleted Records

Penetration Testing iOS Apps – Insecure Local Data Storage
iOS App Directory Structure
SQLite Data
plist files
NSUserDefaults
Core Data
KeyChain Access

Penetration Testing iOS Apps – Unintended Data Leakage
Logging
App Backgrounding
Keyboard Cache

Traffic Analysis for iOS Apps
Intercepting HTTP Traffic
Intercepting HTTP'S' Traffic
Monitoring network traffic(TCP/IP)
Runtime Analysis
Dumping class information of preinstalled apps
Dumping class information of apps installed from App Store
Cycript Basics

Runtime Code Injection Using Cycript
Accessing and modifying variables using Cycript
Exploiting authentication using Cycript
Method Swizzling using Cycript
Bypassing Jailbreak detection using Cycript
Method Swizzling using Snoop-it
App Monitering Using SNOOP-IT

Runtime analysis with GDB
Runtime Analysis with SNOOP-IT

Mobile Malware

iOS Malware
More iOS Malware
Android Malware

Network Attacks

Cydia Default password exploitation with Metasploit
Cracking OpenSSH passwords using Hydra
Metasploit bind shell on iDevices
Metasploit Reverse shell on iDevices