iOS Applications Hacking

3-Days Hands-on

Course Syllabus

AppSec Labs Ltd.

info@appsec-labs.com | https://appsec-labs.com | 23 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

iOS Application Hacking
3-day hands on course

Course description

This course will focus on the techniques and tools for testing the security of iOS mobile applications. During this course, the students will learn about important topics such as the iOS Security model, how to perform static analysis, traffic manipulation, and dynamic analysis. By taking this course, you will be able to perform penetration testing on iOS mobile applications and expose potential vulnerabilities in the tested application.

The objectives of the course are:

- Understand the iOS application threat landscape
- Perform penetration testing on iOS mobile apps
- Identify vulnerabilities and exploit them
- Operate AppSec Labs' unique ***AppUse*** customized VM for android pen-testing (https://appsec-labs.com/appuse)
- Operate AppSec Labs' unique ***iNalyzer*** app for iOS pen-testing (https://appsec-labs.com/inalyzer/)

Target audience

Members of the security / software development team:

- Security penetration testers
- Mobile developers
- Advanced QA teams

Prerequisites

Before attending this course, students should be familiar with:

- Common security concepts
- Basic knowledge of the Linux OS
- Advantage: C / C++ background and basic knowledge of the iOS development platform

Hardware/Software requirements

Please make sure that each machine has:

- At least 4GB of RAM (6GB is highly recommended)
- 30GB of free HD space
- VMware player (free) or VMware workstation (commercial)
- Wireless connectivity in the class – a dedicated router accessible from the class' network
- **Must:** Participants must bring iPhone/IPad devices with iOS 8.x or iOS 9.x to the course. The devices have to be jailbroken.

Course topics

Day 1

Introduction to iOS Security

- Introduction to iOS
- What makes mobile security different?
- OWASP Top 10 Mobile
- iOS Device Architecture
- iOS Security Model
- iOS File System isolation
- Application Sandbox
- The iOS Pen-Testing Environment
- Lab Setup overview
- Device Setup
- Jailbreaking iOS
- Cydia Installations
- AppSec Labs iNalyzer
- **Hands-on Lab: Setting-up and Exploring the iOS environment**

Application Static Analysis

- The need for Static Analysis
- Sources for Static Analysis
- The IPA file package
- IPA file deployment on device
- IPA manual file installation
- The CodeResources file
- Anti-tampering configuration
- Tampering with IPA Content
- Investigating View Controllers
- Investigating Info.plist file
- Listing all CFUR types on a device
- Investigating Binaries
- iOS Binary Application Structure Encryption
- Decrypting Binaries
- Investigating binary content
- Reversing Interfaces
- Using iNalyzer for static analysis
- **Hands-on Lab: Binary Static Analysis manual and automated**

Day 2

Application Storage Analysis

- Application Storage Analysis
- File System access security
- File System Data Protection Class
- File System access
- Application storages
- Property list files (.plist)
- Tampering with Property list files (.plist)
- Investigating Plist files – plutil.
- Database files (.db/.sqlite)
- Snapshots Storage
- Persistent Cookies
- Investigating Logs
- Keyboard Cache
- Cryptographic failures
- Keychain access
- iNalyzer Storage Snapshot

Traffic Manipulation

- Traffic Analysis and Manipulation
- Common architecture
- Bad Session Management
- Phone identifiers used in authentication
- Credentials leakage
- Client information sent to advertisement/analytics server
- Server side vulnerabilities
- Sniffing Traffic
- Traffic interception
- SSL obstacles
- Importing SSL certificates & trusted CA's
- Bypassing server certificate validations
- **Hands-on Lab: Catch and manipulate application's traffic**

Day 3

Temporary runtime manipulation

- Temporary Runtime Manipulation
- Why do we need temporary runtime manipulation?
- Temporary runtime manipulation tools
- Objective C class interposing
- Runtime manipulation with Cycript
- Cycript as a tampering tool
- Runtime manipulation with iNalyzer Dashboard
- **Hands-on Lab: Objective C and runtime manipulation using iNalyzer and cycript**

Persistent runtime manipulation

- Persistent Runtime Manipulation
- Means of persistent manipulation
- Persistent runtime manipulation technique
- Persistent runtime manipulation - backstage
- Persistent runtime manipulation frameworks
- Theos Injection Framework
- iNalyzer header dump
- iNalyzer class dump reference
- Reversing iOS Binary
- Remote debugging with GDB
- Summary
- **Hands-on Lab: Persistent runtime manipulation using Theos**