



Comprehensive iOS Penetration Testing Syllabus

Module 1: Getting Started with iOS Pentesting **2 Hours - 7 Topics**

- **Introduction to iOS (Day 1)**
- **iOS security model (Day 1)**
- **What makes iOS security different? (Day 1)**
- **App Signing & iOS Sandboxing (Day 1)**
- **iOS File System isolation (Day 1)**
- **OWASP Top 10 Mobile (Day 1)**
- **Intro to Objective-C and Swift (Day 1)**

Module 2: Setting up the pentesting environment **4 Hours - 6 Topics**

- **Lab Setup overview (Day 2)**
- **Basics of Jailbreaking (Day 2)**
- **Device Setup (Day 2)**
- **Jailbreaking your iOS device (Day 3)**
- **Cydia, Mobile Substrate (Day 3)**
- **Testing through iOS (Day 3)**

Module 3: Application Static Analysis **2 Hours - 6 Topics**

- **The need for Static Analysis (Day 4)**
- **Sources for Static Analysis (Day 4)**
- **The IPA file package (Day 4)**
- **Investigating Binaries (Day 4)**
- **The Code Resources file (Day 4)**
- **Hands-on Lab: Binary Static Analysis manual and automated (Day 4)**

Module 4: Application Storage Analysis **2 Hours - 4 Topics**

- **Application Storage Analysis (Day 5)**
- **File System access security (Day 5)**
- **Different Insecure local data storage (Day 5)**
- **Hands-on Lab: Binary Static Analysis manual and automated (Day 5)**

Module 5: Tools and Techniques for iOS Reverse Engineering **4 Hours - 5 Topics**

- **Basics of iOS reverse engineering (Day 6)**
- **Introduction to Hopper (Day 6)**
- **Disassembling methods (Day 6)**
- **Modifying assembly instructions (Day 7)**
- **Hands-on-Lab: iOS reverse engineering (Day 7)**



Module 6: IOS Client-Side Injections **2 Hours - 3 Topics**

- **Different types of client-side attacks (Day 8)**
- **How to use burp suit in IOS (Day 8)**
- **Hands-on-Lab: IOS client-side injections (Day 8)**

Module 7: IOS Network Analysis **4 Hours - 6 Topics**

- **Common Vulnerabilities related to traffic (Day 9)**
- **Traffic Analysis and Manipulation (Day 9)**
- **Common Architecture (Day 9)**
- **Bad Session Management (Day 10)**
- **Importing SSL certificates & trusted CA's (Day 10)**
- **Hands-on-Lab: IOS Network Analysis (Day 10)**

Module 8: Run Time Analysis **4 Hours - 7 Topics**

- **Temporary Runtime Manipulation (Day 11)**
- **Persistent Runtime Manipulation (Day 11)**
- **Runtime manipulation with Cycrypt (Day 11)**
- **Hands-on Lab: Run Time Analysis (Day 11)**
- **Method Swizzling using Cycrypt (Day 12)**
- **Method Swizzling different techniques (Day 12)**
- **Hands-on-Lab: Run Time Analysis (Day 12)**

Module 9: Unintended Data Leakage **4 Hours - 2 Topics**

- **Types of Data Leakage (Day 13)**
- **Hands-on-Lab: Data Leakage (Day 14)**

Module 10: Mobile OWASP TOP 10 **8 Hours - 2 Topics**

- **IOS OWASP Top 10 (Day 15 & 16)**
- **Hands-on-Lab: OWASP Top 10 (Day 17 & 18)**

Module 11: Techniques for IOS Security Testing **8 Hours - 2 Topics**

- **Industries best practices for IOS & checklist (Day 19 & 20)**
- **Hands-on-Labs: Automated method for IOS Pentesting (Day 21 & 22)**

Module 12: Securing iOS Apps **2 Hours - 4 Topics**

- **Securing iOS applications (Day 23)**
- **Code obfuscation techniques (Day 23)**
- **Piracy/Jailbreak checks (Day 23)**
- **Where to look for vulnerabilities in code? (Day 23)**

Module 13: Fundamental of IOS forensics **2 Hours - 1 Topic**

- **Basic IOS Forensic (Day 24)**



Module 14: Reporting techniques

2 Hours - 1 Topic

- **IOS application penetration testing report (Day 25)**

