

Mobile Pentesting: OWASP, Frida & iOS/Android

4 Days

DURATION

41

TOPICS

14

HANDS-ON ACTIVITIES

LEARNING OBJECTIVES

- Explain the OWASP Mobile Top 10 and mobile architecture threats
- Identify weaknesses in mobile device deployments
- Apply jailbreaking and rooting techniques to iOS and Android devices
- Analyse root detection techniques and bypass methods using Magisk
- Exploit Android ADB misconfigurations with PhoneSploit
- Perform static analysis and decompile iOS and Android applications
- Bypass SSL and certificate pinning using Frida and Objection
- Assess applications against the Mobile App Security Verification Standard

41 Topics

DAY 1 Introduction to Mobile Security

TOPICS

5 Activities

- Introduction to Mobile Security
- Mobile Problems and Opportunities
- Challenges and Opportunities for Secure Mobile Phone Deployments
- Weaknesses in Mobile Devices
- OWASP Mobile Top 10
- Mobile Architecture & Threats

DAY 2 iOS & Android Security Fundamentals

TOPICS

2 Hands-On Labs

iOS Architecture · Jailbreaking iOS Devices · iOS Data Storage and File System Architecture · iOS Application Interaction · iOS Malware Threats · Android Architecture · Rooting Android Devices

Root Detection Techniques and Bypass Methods

TOPICS

- **Approaches:** Signature Checks, Binary Checks, System Property Checks
- **Methodologies:** Static/Runtime Checks, Root Cloaking
- Android Data Storage and File System Architecture
- Android Application Interaction
- Android Malware Threats
- Android Platform Analysis
- Root Detection and Bypass using Magisk

Exploiting Android ADB with PhoneSploit

TOPICS

- Understanding Android Debug Bridge (ADB) and Its Security Risks
- Exploiting ADB Misconfigurations with PhoneSploit
- Identifying Weaknesses and Securing ADB Against Attacks

Static Application Analysis

4 Hands-On Labs

TOPICS

- Retrieving iOS and Android Apps for Reverse Engineering Analysis
- Decompiling Android Applications
- Circumventing iOS App Encryption
- Header Analysis and Objective-C Disassembly

Reverse-Engineering Obfuscated Applications

TOPICS

Identifying Obfuscation Techniques · Decompiling Obfuscated Applications

Analyzing SSL Pinning and Certificate Pinning

TOPICS

- **Approaches:** Manual Code Review, Hooking Methods
- **Techniques:** Patching, Runtime Hooking

Certificate Pinning and SSL Pinning Deep Dive

TOPICS

- **Methodologies:** TrustManager Validation, Network Security Config

Mobile Application Security Verification Standard

3 Hands-On Labs

TOPICS

- Step-by-Step Recommendations for Application Analysis
- Taking a Methodical Approach to Application Security Verification
- Common Pitfalls While Assessing Applications
- Detailed Recommendations for Jailbreak Detection, Certificate Pinning, and Application Integrity Verification
- **Android and iOS Critical Data Storage:** Keychain and Keystore Recommendations

Application Integrity Verification

TOPICS

- **Approaches:** Checksum Validation, Signature Verification

Securing Mobile Devices with Antivirus & Security Tools

TOPICS

- Overview of Mobile Security Solutions
- Scanning and Detecting Malware on Mobile Devices
- Best Practices for Securing Android and iOS Devices

HANDS-ON ACTIVITIES

Practise What You Learn

MODULE	ACTIVITY
Introduction to Mobile Security	HANDS-ON LAB: MOBILE DEVICE FOOTPRINTING & SCANNING ■ Gathering Information on Mobile Devices (OS, Apps, Network) ■ Identifying Open Ports & Services Running on a Mobile Device (Nmap) ■ Using Reconnaissance Tools to Map Mobile Attack Surface ■ Intercepting TLS Traffic ■ Man-in-the-Middle Troubleshooting
iOS & Android Security Fundamentals	HANDS-ON LAB ■ MDM - jump cloud ■ Threat Modelling Tool - Microsoft
Static Analysis & Reverse Engineering	HANDS-ON LAB ■ AndroRAT - Android Remote access ■ Apktool - static analysis ■ MOBSF - Static analysis report ■ Frida / Objection Lab - Bypassing SSL Pinning on Android
Mobile Penetration Testing	HANDS-ON LAB ■ Drozer - Exploit with Drozer Agent ■ Demo with Sieve Apk ■ Application Integrity Check Bypass on Android - Apktool, objection

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com