

MOBILE APPLICATION SECURITY TESTING

TABLE OF CONTENT

Duration – 5 Days

Day 1: Introduction to Mobile Security

- 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

- iOS Architecture
- Jailbreaking iOS Devices
- iOS Data Storage and File System Architecture
- iOS Application Interaction
- iOS Malware Threats
- Android Architecture
- Rooting Android Devices
- Android Data Storage and File System Architecture
- Android Application Interaction
- Android Malware Threats
- Android Platform Analysis

Day 3: Static Analysis & Reverse Engineering

- Hands-On Lab: Mobile Device Footprinting & Scanning
 - Gathering Information on Mobile Devices (OS, Apps, Network)
 - o Identifying Open Ports & Services Running on a Mobile Device
 - Using Reconnaissance Tools to Map Mobile Attack Surface
- Static Application Analysis



- o 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
 - o Identifying Obfuscation Techniques
 - Decompiling Obfuscated Applications

Day 4: Mobile Penetration Testing

- Mobile Application Security Verification Standard
 - Step-by-Step Recommendations for Application Analysis
 - o Taking a Methodical Approach to Application Security Verification
 - o 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
- Penetration Testing with Lab
 - Intercepting TLS Traffic
 - Man-in-the-Middle Troubleshooting
- Hands-On Lab: Exploiting Android ADB with PhoneSploit
 - o Understanding Android Debug Bridge (ADB) and Its Security Risks
 - Exploiting ADB Misconfigurations with PhoneSploit
 - o Identifying Weaknesses and Securing ADB Against Attacks

Day 5: API Security & Mobile Device Protection

- API Security Audit Testing
 - Introduction to API Security
 - Basics of API Fundamentals
 - Common Vulnerabilities and Attack Vectors in APIs (OWASP Top 10 API Security Risks)
 - o API Authentication, Authorization, and Data Integrity
 - Tools and Methodologies for API Security Testing



- Assessing the Resilience of APIs to Various Types of Attacks
- Penetration Testing Techniques for APIs
- Hands-On Lab: Securing Mobile Devices with Antivirus & Security Tools
 - Overview of Mobile Security Solutions
 - Scanning and Detecting Malware on Mobile Devices
 - Best Practices for Securing Android and iOS Devices
- API Security Tools & Best Practices
 - Real-World Case Studies
 - $\circ \quad \text{API Security Tools Overview} \\$
 - Securing APIs Best Practices