Mobile Penetration Tester (MPT)

Mobile penetration testing (MPT) is the best path for those willing to learn Android and iOS pen-testing. It may be a hobbyist who is doing it for fun, or a professional looking to progress at their work. It's a fantastic way to get into the world of cybersecurity.

The convenience of using mobile phones has increased, and so has the urge to use them for information. Every day, the attackers get more subtle and stronger at their approach. Almost 5.20 billion people are using mobile devices across the globe. It reflects the large number of needs it represents.

Unsecure cell phones or reckless users may be an entry point to a cybercrime. It is believed that android devices are easier to penetrate than iPhone. Apple is known for its security, penetrating iPhone is rare but not unheard of. Some cell phones are infiltrated for getting information about the company the individual works in, or his bank details resulting in an intruder receiving a wide range of sensitive information. Learn more…

❖ WHO IS THIS COURSE FOR?

MPT will benefit all who want to choose their career as a Penetration Tester and want to add Mobile Pentesting to their skill-set

- Ethical Hacker
- Penetration Testers
- Mobile Application Developers
- Security professionals interested in Mobile App Security
- Anyone interested in ethical hacking
- Anyone interested in information security concepts

❖ PREREQUISITES

- Basic concepts of Networking
- Penetration Testing Engagement Basics
- Students should have familiarity with network penetration testing concepts.
- Should know how Web Protocols works
- Proficient in Linux Basics
- Must have a clear understanding of fundamentals of Assembly Language
- Should know how Web Protocols works
- Clear concepts of TCP/IP Protocol Suite

❖ SYSTEM REQUIREMENT

- CPU: 64-bit Intel i5/i7 with 4th generation + (2.0 GHz)
- 8 GB of RAM or higher
- 300 GB free space
- Administrator Access
- Wi-Fi 802.11 capability
- Windows 10 Pro, Linux or macOS (Latest updated)

NOTE: All other software and configuration requirement will be provided and guided.

❖ COURSE DURATION

- 45 Hours

❖ PRICING

MPT training + course material + exam certification free.

800 USD | 59,000/- INR

❖ MPT COURSE SYLLABUS

Module 1 - Brief Introduction to Android and digging deeper into Android.

Module 2 - Sandboxing and permission model.

Module 3 - Application Signing and Android Start-up process.

Module 4 - Setting up “Penetration Testing Lab” for Android.

Module 5 - Installation process of Burpsuite for Android Security Assessment.

Module 6 - APKtool for Android Security Assessment.

Module 7 - Brief Introduction to Android Mobile Security Framework.

Module 8 - Reversing Android Application and android application teardown.

Module 9 - Auditing Android Application.

Module 10 - OWASP TOP 10 vulnerability for Mobile.

Module 11 - Insecure File Storage (Path Transversal and LFI).

Module 12 - HTTPS Proxy Interception for Android Security Assessment.

Module 13 - Android Traffic Analysis

Module 14 - Identifying and exploiting the vulnerability

Module 15 - Cross-Application Scripting in Android

Module 16 - Android ARM Exploitation

Module 17 - 7 Real-time Lab for Android Penetration Testing and case studies

Module 18 - Writing a Pentest Report

Module19- Brief Introduction to IOS Mobile Penetration Testing

Module 20- Brief Introduction to IOS Application

Module 21- MVC and Event-Driven Architecture

Module 22- ARM Processor

Module 23- IOS Security Mechanism

Module 24- Brief Introduction of Jailbreaking

Module 25- Lab Setup of Jailbreaking

Module 26- Setup up Pentest Platform

Module 27- SQLite Database

Module 28- Plist Files

Module 29- Class-DUMP-Z

Module 30-Runtime Analysis with Cycript

Module 31- Cycript and Class DUMP-Z

Module 32- Decrypting Application

Module 33- Runtime Analysis with GDB

Module 34- Installing Challenge Apps

Module 35- Data Storage and Security

Module 36- NSUSERS Default

Module 37- SQLite Data Files

Module 38- Core Data Services

Module 39- Keychain

Module 40- Cached copy and Monitoring Network Communication

Module 41- Intercepting SSL Traffic

Module 42- IOS Attack, Anti-Piracy, and Anti-Anti-Piracy with GDB

Module 43- Anti-Anti-Piracy with GDB level 2

Module 44- Mobile Substrate

Module 45- IOS forensics Basic

Module 46- IPHONE Data Protection Tools

Module 47- Exploring the DUMPED Image

Module 48- Brute forcing the Passcode

Module 49- Interesting Files and Analyzing iTunes Backup.

Module 50- IOS Malware

Module 51- Metasploit Bind Shell on IOS

Module 53- Metasploit Reverse TCP on IOS

Module 54- Brief Introduction of Daemon and Backdoor

Module 55- Addendum IOS 8.1 Jailbreak

Module 56- Addendum- Installing Apps from Cydia on IOS 8