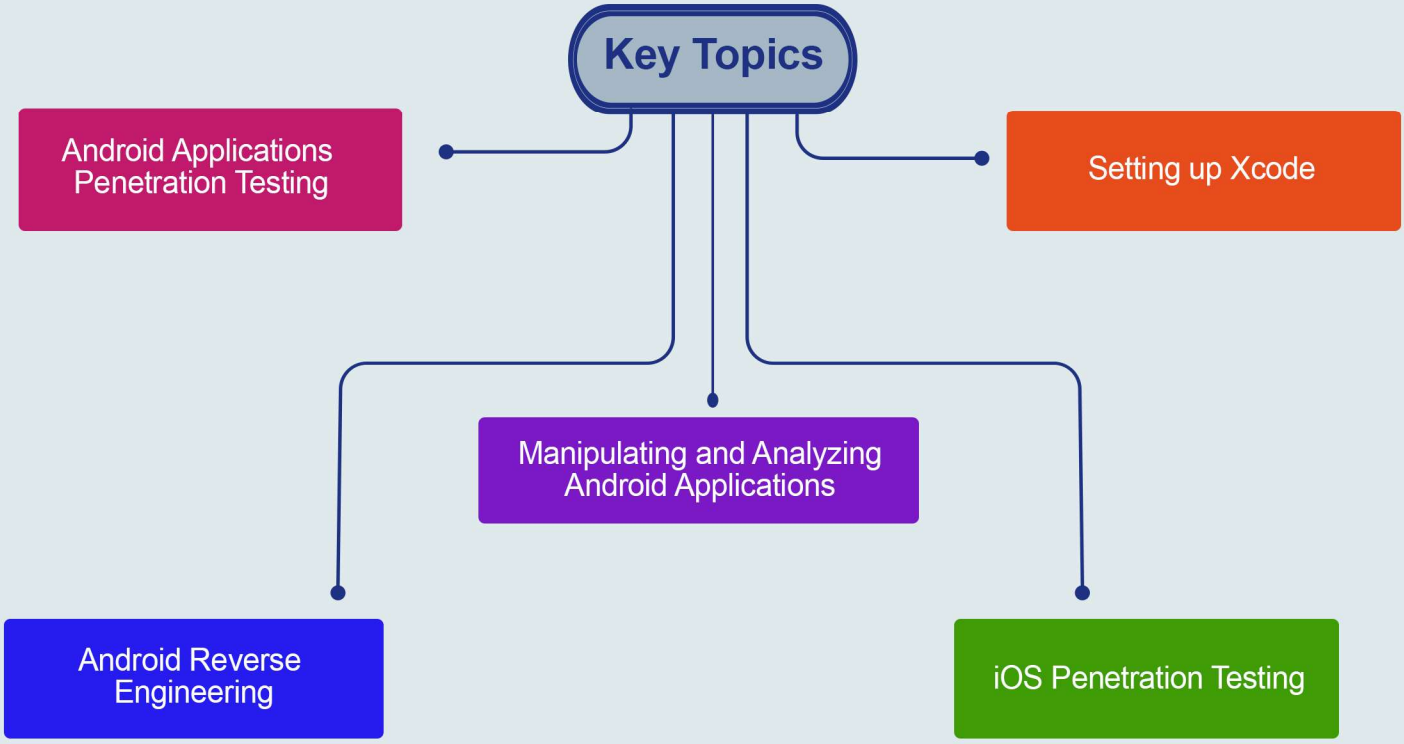
About the Course

Mobile devices introduce new threats to organizations through untrusted applications. Therefore, it has become a mandate to evaluate and identify flaws regularly and conduct penetration tests to avoid any mishaps and losses. We are going to start from scratch in this course and aim to learn all the details related to Ethical Hacking for Mobile Applications & Mobile Devices. Without any need of prior knowledge you will understand how hackers attack mobile applications & devices and protect yourself against these attacks. You will build your own hacking lab on your computer so that you can practice all the things that we are going to learn in this course.

Learning Objectives

Key Topics



Pre Requisites

- Ethical Hacking & Penetration Testing Concepts Course
- Ethical Hacking & Penetration Testing Tools Course
- Mobile Application Security Course

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Mobile Ethical Hacking & Penetration Testing eBook

Who Should Attend

- PenTesters
- CISOs
- Security Analysts
- Mobile App Developers

Syllabus

Android Applications Penetration Testing

- Introduction to Android Application Penetration Testing
- Android Application Penetration Testing Ecosystem
- Overview of Automated Android Application Penetration Testing Tools
- Meeting Android Penetration Testing Challenges
- Auditing Android Application for OWASP Mobile Top 10 Vulnerabilities

Android Reverse Engineering

- Introduction to Reverse Engineering
- Android Reverse Engineering Introduction
- Reverse Engineering Tools
- Identifying obfuscation techniques
- Decompiling obfuscated applications
- Effectively annotating reconstructed code with Android Studio
- Decrypting obfuscated content with Simplify
- Infecting Legitimate Android Application with Malwares
- Exploiting Android apps using backup techniques
- Hello World App
- Creating APK
- Dalvik Bytecode
- App Manipulation
- Signing
- Jadx Usage
- ProGuard Usage
- Obfuscated APK Decryption
- Game Hacking Practice
- Word Game Codes
- Reverse Engineering Advanced
- Method Manipulation
- Hacking the Game

Syllabus

Manipulating and Analyzing Android Applications

- Android application manipulation with Apktool
- Reading and modifying Dalvik bytecode
- Adding Android application functionality, from Java to Dalvik bytecode
- Android application interaction and intent manipulation with Drozer
- Method hooking with Frida and Objection

iOS Penetration Testing

- Basic Requirements
- Application Penetration Testing Ecosystem
- Overview of Automated iOS Application Penetration Testing Tools
- Introduction to Snoop-it
- Traffic analysis with Snoop-it
- Analyzing keychain with Snoop-it
- Runtime Analysis with Snoop-it
- Jailbreaking

Setting up Xcode

- Installing Xcode
- Introduction to Objective-C
- Building iOS Application
- Understanding Application Structure in Xcode
- Adding functionality to “HelloWorld” application

iOS Application Penetration Testing

- Introduction to iOS Application Penetration Testing
- Meeting iOS Application Penetration Testing Challenges
- Auditing iOS Application for OWASP Mobile Top 10 Vulnerabilities

Syllabus

iOS Reverse Engineering

- o iOS Reverse Engineering Introduction
- o Jailbreak Detection
- o Assembly
- o Hexadecimal
- o Cycript
- o Manipulating App in Runtime
- o Swift Challenges
- o Hopper

Static Application Analysis

- o Retrieving iOS and Android apps for reverse engineering analysis
- o Decompiling Android applications
- o Circumventing iOS app encryption
- o Header analysis and Objective-C disassembly
- o Accelerating iOS disassembly: Hopper and IDA Pro
- o Swift iOS apps and reverse-engineering tools
- o Effective Android application analysis with MobSF

Third-Party Application Frameworks

- o Examining .NET-based Xamarin applications
- o Examining HTML5-based PhoneGap applications

Manipulating and Analyzing iOS Applications

- o Runtime iOS application manipulation with Cycript and Frida
- o iOS method swizzling
- o iOS application vulnerability analysis with Objection
- o Tracing iOS application behavior and API use
- o Extracting secrets with KeychainDumper
- o Method hooking with Frida and Objection

Syllabus

Mobile Application Security Verification Standard

- 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
- Android and iOS critical data storage

CTF: Banking App Hacking

- CTF Introduction
- CTF Practice
- Installing Genymotion
- Genymotion Settings
- Server Setup (Windows)
- Server Setup (Mac)
- Running App
- Bypassing Root Detection
- Activity Manipulation
- Simple Admin Flaw
- Admin Vulnerability
- Cryptology Hacking
- Hacking Content Providers

Using Mobile Device Remote Access Trojans

- Building RAT tools for mobile device attacks
- Hiding RATs in legitimate Android apps
- Customizing RATs to evade anti-virus tools
- Integrating the Metasploit Framework into your mobile pen test
- Effective deployment tactics for mobile device Phishing attacks

Hands-on Training

- Lab 1 - Hack an Android Device
- Lab 2 - Harvest User Credentials
- Lab 3 - Launch a DoS Attack
- Lab 4 - Exploit the Android Platform
- Lab 5 - Analyze a Malicious App
- Lab 6 - Secure Android Devices from Malicious App