Mobile Ethical Hacking

Mobile Application and Device Security workshop

Mobile hacking is an emerging threat targeting many end users and enterprises. Cyber criminals launch many mobile attacks including mobile phishing attacks since they can take advantage of certain limitations of the mobile platform. This Course will prepare you to effectively evaluate the security of mobile devices, assess and identify flaws in mobile applications, and conduct a mobile device penetration test - all critical skills required to protect and defend mobile device deployments. You will learn basic principles, mobile network architecture, mobile app development, policy and enforcement rules, mobile code analysis, penetration testing and mobile ethical hacking. for better defend your organization against the onslaught of mobile device attacks

You must know!

Duration:

40 Hours

Who should attend?

Students should have familiarity with network penetration testing concepts

Main Topics:

- Device Architecture and Application Interaction
- The Stolen Device Threat and Mobile Malware
- Static Application Analysis
- Dynamic Mobile Application Analysis and Manipulation
- Mobile Penetration Testing

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים
וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

Course Modules

Module 1 –Device Architecture and Application Interaction

Mobile Problems and Opportunities

- Challenges and opportunities for secure mobile phone deployments
- Weaknesses in mobile devices
- Exploiting weaknesses in mobile apps: Bank account hijacking exercise

Mobile Device Platform Analysis

- iOS and Android permission management models
- Code signing weaknesses on Android
- Android app execution: Android Runtime vs. Android Dalvik virtual machine
- Latest Android and iOS security enhancements

Mobile Application Interaction

- Android application interaction through activities, intents, services, and broadcasts
- iOS application interaction through schemes and universal links
- Protection of application components through permissions and signatures

Mobile Device Lab Analysis Tools

- Using iOS and Android emulators
- Android mobile application analysis with Android Debug Bridge (ADB) tools
- Uploading, downloading, and installing applications with ADB
- Interacting with applications through Activity Manager

Module 2 – The Stolen Device Threat and Mobile Malware

Unlocking, Rooting, and Jailbreaking Mobile Devices

- Legal issues with rooting and jailbreaking
- Jailbreaking iOS
- Android root access through unlocked bootloaders
- Root exploits for Android
- Using a rooted or jailbroken device effectively: Tools you must have!

Mobile Phone Data Storage and File System Architecture

- Data stored on mobile devices
- Mobile device file system structure
- Decoding sensitive data from database files on iOS and Android
- Extracting data from Android backups

Mobile Device Malware Threats

- Trends and popularity of mobile device malware
- Mobile malware command-and-control architecture
- Efficiency of Android ransomware malware threats
- Analysis of iOS malware targeting non-jailbroken devices
- Hands-on analysis of Android malware
- Mobile malware defenses: What works and what doesn't

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים
וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

Module 3 - Static Application Analysis

Reverse-Engineering Obfuscated Applications

- Identifying obfuscation techniques
- Decompiling obfuscated applications
- Effectively annotating reconstructed code with Android Studio
- Decrypting obfuscated content with Simplify

Static Application Analysis

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

Third-Party Application Frameworks

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

Module 4 - Dynamic Mobile Application Analysis and Manipulation

Manipulating and Analyzing iOS Applications

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

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

Application Report Cards

- Step-by-step recommendations for application analysis
- Tools and techniques for mobile platform vulnerability identification and evaluation
- Recommended libraries and code examples for developers
- Detailed recommendations for jailbreak detection, certificate pinning, and application integrity verification
- Android and iOS critical data storage: Keychain and key store recommendations

Module 5 - Mobile Penetration Testing

Network Manipulation Attacks

- Using man-in-the-middle tools against mobile devices
- Sniffing, modifying, and dropping packets as a man-in-the-middle
- Mobile application data injection attacks

SSL/TLS Attacks

- Exploiting HTTPS transactions with man-in-the-middle attacks
- Core pen test technique: TLS impersonation against iOS Mail.app for password harvesting
- Integrating man-in-the-middle tools with Burp Suite for effective HTTP manipulation attacks
- Bypassing Android's NetworkSecurityConfig and Apple's Transport Security

Web Framework Attacks

- Site impersonation attacks
- Application cross-site scripting exploits
- Remote browser manipulation and control
- Data leakage detection and analysis
- Hands-on attacks: Mobile banking app transaction manipulation

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

Module 6 - Hands-on Lab

In this hands-on exercise, you will examine multiple applications and forensic images to identify weaknesses and sources of sensitive information disclosure, and analyze obfuscated malware samples to understand how they work. During this mobile security event you will put into practice the skills you have learned in order to evaluate systems and defend against attackers

INT

המרכז הבינלאומי
ללימודי הייטק וחדשנות

מתקדמים
לקריירה בהייטק

*6377

CISCO
Networking Academy

Microsoft Partner
Gold Learning

GLOBAL UNIVERSITY SYSTEMS

ibat COLLEGE DUBLIN

HiGHQ
מכינים אותך לעולם האמיתי

ARDEN UNIVERSITY

The University of Law

London School of Business & Finance

HTK

TORONTO SCHOOL OF MANAGEMENT

קמפוסים בפריסה ארצית:

תל אביב
ראול ולנברג 36
קריית עתידים

רחובות
רחוב אופנהיימר 5
פארק המדע

ירושלים
רחוב יפו 34

באר שבע
רחוב האנרגיה 77
פארק ההייטק