SYLLABUS

MASPT

MOBILE APPLICATION SECURITY AND PENETRATION TESTING

VERSION 2.5

A must have for any penetration tester's skill arsenal

eLearnSecurity
Forging security professionals

eLearnSecurity has been chosen by students in over 140 countries in the world and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto security to be free

COURSE DESCRIPTION

Mobile Application Security and Penetration Testing (MASPT) gives penetration testers and IT security professionals the practical skills necessary to understand the technical threats and attack vectors targeting mobile devices.

This course will walk you through the process of identifying security issues on Android and iOS applications, using a wide variety of techniques including Reverse Engineering, Static/Dynamic/Runtime and Network Analysis.

The student will expand their knowledge of how to code simple iOS and Android applications in order to build real-world POCs and exploits. These skills will be necessary to understand mobile application security fully.

Additionally, many vulnerable mobile applications included in the training course will give the student the chance to practice and learn things by actually doing them: from decrypting and disassembling applications, to writing fully working exploits and malicious applications.

WHO SHOULD TAKE THIS COURSE AND PREREQUISITES

The MASPT training course benefits the career of Penetration Testers and IT security personnel in charge of defending their organization's applications and data. We also believe this course will be interesting for developers who want to know more about security mechanisms and features implemented in mobile OSs such as Android and iOS.

Although MASPT uses and explains several snippets of iOS and Android Applications source codes, this course only requires that students possess basic Java/iOS programming skills.

NOTE: *In order to perform certain techniques explained in the iOS-related modules, physical devices such as an iPod, iPhone, or iPad might be necessary. Unlike iOS, the Android-related modules do not require an Android device: Android SDK and virtualization provides all the necessary tools for both Windows and Nix systems*.*

WHO SHOULD NOT TAKE THIS COURSE

This course is not for you if you are looking for something that:

- Teaches you mobile application programming
- Teaches you how to jailbreak or root iOS/Android devices
- Will give you a certification without any effort
- You can memorize to pass a multiple-choice test
- Will not make you think

HOW AM I GOING TO LEARN THIS?

eLearnSecurity courses are very interactive, addictive, and presents content in such a way that it appeals to all learning styles. During this training course, you will face several guided challenges that will provide you with relevant and hands-on practical application experience. Don't expect an outdated way of learning by reading pages and pages of theoretical methodologies.

NO BORING THEORIES ABOUT THE UNIVERSE HERE!

We take our learning to the next level by not only explaining how an attack works but furthering your experience by showing you how it works in practice with real examples and labs that reflect real-world application vulnerabilities.

CAN I TRACK MY LEARNING PROGRESS?

...or will I only find out during the exam if I learned something?

The answer to these questions is very simple. During the training course, you will find several labs. Together, we will solve these, explaining all the necessary concepts along the way. You are then free to practice the labs as long as you like. If you can solve the challenge, that demonstrates that you learned and properly understood the concepts.

IS THERE A FINAL EXAMINATION?

Yes. The final exam consists of a hands-on challenge in which the student has to prove the skills acquired during the training course.

The student will be provided with a real-world scenario of two Android applications to analyze and pentest.

The final deliverable will be a working and reproducible proof of concept that will be reviewed by the training course instructor.

No written report is required.

WILL I GET A CERTIFICATE?

Once you pass the final exam, you will be awarded the eMAPT "eLearnSecurity Mobile Application Penetration Tester" certification.

You can print your shiny new certificate directly or have it shipped to you.

ORGANIZATION OF CONTENTS

The student is provided with a suggested learning path to ensure the maximum success rate with core foundational topics—which means no fluff, only real concepts.

ANDROID PENTESTING

- Module 1: Android Architecture
- Module 2: Setting up a Test Environment
- Module 3: Android Build Process
- Module 4: Reversing APKs
- Module 5: Device Rooting
- Module 6: Android Application Fundamentals
- Module 7: Network Traffic
- Module 8: Device and Data Security
- Module 9: Tapjacking
- Module 10: Static Code Analysis
- Module 11: Dynamic Code Analysis

iOS PENTESTING

- Module 1: iOS Architecture
- Module 2: Device Jailbreaking
- Module 3: Setting up a Testing Environment
- Module 4: iOS Building Process
- Module 5: Reversing iOS Apps
- Module 6: iOS Application Fundamentals
- Module 7: iOS Testing Fundamentals
- Module 8: Network Traffic
- Module 9: Device Administrator
- Module 10: Dynamic Analysis

MODULE 1: ANDROID ARCHITECTURE

Before we dive into Security and Penetration Testing, we introduce you to the Android environment. There are few key concepts you should be familiar with before we get started.

The Android operating system is essentially a Linux operating system, which means, for this course, it is helpful if you are familiar with the basics of Linux, such as file permissions and navigating the filesystem.

MODULE 2: SETTING UP A TESTING ENVIRONMENT

Before diving into Android Application Security, we need to have a means to examine, build, debug, and run applications.

As such, we'll need to install the Android Studio IDE (Integrated Development Environment).

MODULE 3: ANDROID BUILD PROCESS

Understanding how Android Studio compiles code and resources into a working Android application will help you better understand how all the pieces fit together, which will also provide insight into the protection employed to guarantee the authenticity of applications and circumstances by which they can be rendered meaningless.

MODULE 4: REVERSING APKs

In this module, we will discuss the process of reversing Android applications, which is an important skill for anyone who wants to audit the security of third-party applications when the source code is unavailable.

Reversing also provides a more comprehensive view of the built applications, including all libraries and impacts of the build process.

4. Reversing APKs
- **4.1. APKTool**
- **4.2. Dex2Jar**
- **4.3. JD-GUI**
- **4.4. Smali/Backsmali**
- **4.5. Obfuscation**
- **4.6. Additional APK Contents**
- **4.7. Hardware Optimization**
- **4.8. OEM Apps**

MODULE 5: DEVICE ROOTING

Rooting is a process by which one obtains "root" or system-level access to an Android device.

In this module, you will learn why rooting can be important for our security tests but also what the implications are of rooting a device.

5. Device Rooting
- **5.1. What is Rooting**
  - 5.1.1. Su, SuperUser and SuperSU
- **5.2. Potential Issues**
- **5.3. Custom ROMs**
  - 5.3.1. OmniROM and CyanogenMod
  - 5.3.2. Google Nexus

MODULE 6: ANDROID APPLICATION FUNDAMENTALS

To perform a thorough pentest on Android applications, you must know and master all of its components.

In this module, you will study all the fundamental concepts and topics that you may encounter during your security testing tasks.

MODULE 7: NETWORK TRAFFIC

Mobile devices are unique in how they use networks, being almost exclusively wireless and often bouncing between cellular and Wi-Fi networks.

To lower cellular data traffic, some cellular carriers provide Wi-Fi hotspots for their customers. Bad guys know this and will often set up fake Wi-Fi networks, tricking the devices into connecting.

In this module, you will learn how to configure your environment in order to inspect and analyze network traffic.

MODULE 8: DEVICE AND DATA SECURITY

How secure is the data stored on mobile devices? That has become a hot topic as of late. In fact, insecure data storage is the second most common vulnerability, according to the OWASP Mobile Top Ten.

MODULE 9: TAPJACKING

If you are familiar with Clickjacking in web applications, you are already familiar with the basic concepts of Tapjacking.

In a Tapjacking attack, a malicious application is launched and positions itself atop a victim application. In this module, you will see examples of Tapjacking, as well as how to properly develop an application to not be vulnerable to this issue.

MODULE 10: STATIC CODE ANALYSIS

Static Code Analysis is the process of programmatically examining application code on the disk, rather than while it is running.

There are numerous scientifically rigorous approaches to the problems of validating that code is free of errors.

In this module, you will learn how to perform security tests on Android applications by using different static code analysis techniques.

MODULE 11: DYNAMIC CODE ANALYSIS

Dynamic Code Analysis is the process by which code is reviewed for vulnerabilities by executing some or all of the code.

This execution could occur in a normal environment, virtualized environment or a debugger.

This type of inspection also allows you to directly observe network requests, view interactions with other applications and see the results of any error conditions encountered.

MODULE 1: iOS ARCHITECTURE

To understand the iOS ecosystem, we need to realize that an iOS operating system is based on Darwin OS, which was originally written by Apple in C, C++ and Objective-C. Darwin is also at the heart of OS X, and thus OS X and iOS share a common foundation.

Unlike Android, the iOS operating system is not open source; however, it is helpful to be familiar with the UNIX fundamentals, especially file permissions and user privileges.

MODULE 2: DEVICE JAILBREAKING

Jailbreaking is the process of actively circumventing/removing such restrictions and other security controls put in place by the operating system.

This allows users to install unapproved apps (apps not signed by a certificate issued by Apple) and leverage more APIs, which are otherwise not accessible in normal situations.

While we do not show you, or tell you how to jailbreak iOS devices, we explain to you the various ways of jailbreaking and implications for both a user and a developer/pentester.

MODULE 3: SETTING UP A TESTING ENVIRONMENT

Before we proceed in the content, it is important to understand a few fundamental concepts unique to the Apple ecosystem, and more precisely related to the iOS app development process.

Apple provides simulators for different hardware and iOS versions.

MODULE 4: iOS BUILD PROCESS

In this module, you will learn how the iOS build process works and what the differences are between running an application on a device or the emulator.

MODULE 5: REVERSING iOS APPS

An attacker has incentive to examine and understand how the software works, so they can look for further weak spots or patch/manipulate the binaries to their advantage.

In this module, you will see the most common techniques and tools to successfully reverse iOS applications.

MODULE 6: iOS APPLICATION FUNDAMENTALS

In order to perform a thorough pentest on iOS applications, you must know and master all of its components.

In this module, you will learn how applications are composed and what each component is used for.

MODULE 7: iOS TESTING FUNDAMENTALS

In this module, you will run your security tests against iOS applications.

Depending on the target of your tests, you will learn different techniques and use multiple tools to reach your goal.

MODULE 8: NETWORK TRAFFIC

In this module, you will learn how to configure your environment in order to inspect and analyze network traffic.

MODULE 9: DEVICE ADMINISTRATION

Since iOS version 6, Apple has incorporated built-in support for powerful device management capability with fine grain controls that allows an organization to control corporate Apple devices and the data stored on them.

In this module, you will see the options organizations have to administer all the active devices under their control. These include ensuring that the devices are in compliance, that the software running on these devices is up-to-date, and much more.

9. Device Administration
- **9.1. Device Management**
- **9.2. Device Enrollment**
  - 9.2.1. Employee Owned
  - 9.2.2. Organization Owned
- **9.3. MDM Profiles**
  - 9.3.1. Passcode Policies
  - 9.3.2. Setting Alteration
  - 9.3.3. Data Protection
  - 9.3.4. Remote Wipe
  - 9.3.5. MDM Solutions
- **9.4. Jailbreak Detection**
  - 9.4.1. File System Changes
  - 9.4.2. Write Access
  - 9.4.3. Access to System Functions

MODULE 10: DYNAMIC ANALYSIS

There is a certain class of applications that has a significant amount of client-side logic built into it. Typical examples include word-processing software, image editors, games, utilities, etc.

In such cases, there is an incentive for attackers to examine and understand how the software works, so they can then look for weak spots in the application or bypass restrictions that are applied locally.

10. Dynamic Analysis
- **10.1. Objective-C Runtime**
- **10.2. Cycript**
  - 10.2.1. Installation
  - 10.2.2. Attach Cycript
  - 10.2.3. Cycript Usage
  - 10.2.4. Method Swizzling
- **10.3. Attack Custom Apps**
  - 10.3.1. LogMeIn
  - 10.3.2. LogMeIn2
- **10.4. Tools**
  - 10.4.1. IDB
  - 10.4.2. Snoop-it

ABOUT US

We are eLearnSecurity.

Based in Santa Clara, California, with offices in Pisa, Italy and Dubai, UAE, Caendra Inc. is a trusted source of IT security skills for IT professionals and corporations of all sizes. Caendra Inc. is the Silicon Valley-based company behind the eLearnSecurity brand.

eLearnSecurity has proven to be a leading innovator in the field of practical security training, with best of breed virtualization technology, in-house projects such as Coliseum Web Application Security Framework and Hera Network Security Lab, which has changed the way students learn and practice new skills.

Contact details:

www.elearnsecurity.com
contactus@elearnsecurity.com