Practice Labs - Ethical Hacker v10

Hacking Mobile Platforms

Introduction

Ethical Hacking
Mobile Devices
Mobile Platform
Mobile Device Management (MDM)
Hacking Methods
Exploitation
OWASP

Welcome to the **Hacking Mobile Platforms** Practice Lab. In this module, you will be provided with the information needed to develop your knowledge.

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Mobile Hacking Methods
- Exercise 2 - Preventing Mobile Device Exploitation

After completing this lab, you will have further knowledge of:

- OWASP Top 10 Mobile Threats

- Methods to prevent Mobile device exploitation
- Using Mobile Device Management (MDM)

Exam Objectives

The following exam objective is covered in this lab:

- **1.1** Network and Communication Technologies

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **30 minutes** to complete this lab.

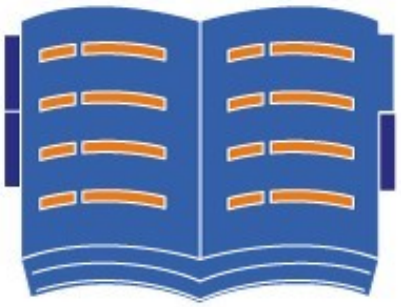
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

> Click **Next** to view the Lab topology used in this module.

Lab Topology

This lab contains supporting materials for Certified Ethical Hacker v10.



Click **Next** to proceed to the first exercise.

Exercise 1 - Mobile Hacking Methods

Mobile devices are now widely used for many different purposes, and the information being accessed is stored in many different formats. The information is retrieved through downloaded applications, which are attained using mobile connectivity.

When a user is downloading and installing an app from the data store, they are connected to the internet. Being present on the internet makes the mobile device vulnerable. Any system or mobile device connected to the internet is not safe, but you can take precautionary measures to minimize the security risks to them.

In this exercise, you will learn about the OWASP Top 10 Mobile Threats.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- OWASP Top 10 Mobile Threats

Task 1 - OWASP Top 10 Mobile Threats

The Open Web Application Security Project (OWASP) performs extensive research and has released to the Top 10 Mobile Threats in 2016.

Here is the list of Top 10 Mobile Threats:

1. Improper Platform Usage

There are certain features that may be built-in to the mobile apps that are meant only for the developers. However, if the hacker knows these features, the entire mobile app is at risk of exploitation.

2. Insecure Data Storage

Often, the developers do not efficiently handle the data in storage. For example, the hacker is able to extract data from the cache. The developer did not think about clearing the cache or encrypting the information.

3. Insecure Communication

Insecure communication relates to several vulnerabilities, such as:

- Poor handshaking
- Incorrect SSL version usage
- Weak negotiation
- Cleartext communication of sensitive information

Even though the developers may be cautious about encrypting the data at reset, they can forget to encrypt the data in transit. This means that the data is being sent in cleartext, which can be captured, read, or modified by a hacker.

4. Insecure Authentication

Most mobile apps use offline authentication, which does not require the user to authenticate with an online server. A hacker can use a custom tool to bypass the local authentication method to gain access to the data stored in the app. Insecure authentication also includes improper session management. The sessions, if not closed properly, can allow the hacker to gain access to the mobile app and its data.

5. Insufficient Cryptography

If the developer does not implement sufficient or proper cryptography, the hacker can decrypt the insufficient cryptography to gain access to the data. This problem

can arise due to poor cryptography or flawed encryption/decryption procedures implemented in the mobile app code.

6. Insecure Authorization

Insecure authorization refers to the server-side vulnerabilities in the authorization. If the permissions are not checked properly when a user accesses a feature, it can also allow the hacker access to exploit the features.

7. Client code quality

The client code quality refers to mistakes made by developers in the mobile app code. The two most common errors to the client code are buffer overflow and memory leaks. These can allow the hacker to gain control over the mobile app. This can lead to data theft and control over the mobile device.

8. Code Tempering

After a mobile app is downloaded to the device, its code is resident in the device. A hacker can perform code tempering to steal information, change the API, or access the premium features of the mobile app, which otherwise would be locked. In the worst-case scenario, a piece of malicious code could be added to the mobile app code. The modified mobile app can then be distributed through mobile app stores.

9. Reverse Engineering

Mobile apps can be reverse-engineered. A hacker may reverse engineer a mobile app to study its functionality and find vulnerabilities that may exist in the code. For example, if the developer has included user credentials as a backdoor, then it can be used by the hacker for data theft.

10. Extraneous Functionality

During the development of a mobile app, the developers often include features that can help them during the testing. However, these features are not always removed when the mobile app is released to production. One example is a backdoor, which is included to allow the developer to access the mobile app without any issues. It is a

security bypass, which if found and exploited by a hacker, can have severe implications, such as data theft

---

Exercise 2 - Preventing Mobile Device Exploitation

Mobile devices are widely used for personal and official reasons. No matter what the purpose of the device is, the security of it is important. A user needs to ensure that the mobile device is safe and not hacked, stolen, or otherwise compromised. A device for personal use could have personal data at risk, while a device for official uses could put the organization's data at risk.

In this exercise, you will learn about some of the common methods used to prevent mobile device exploitation.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Methods to prevent Mobile device exploitation
- Using Mobile Device Management (MDM)

Task 1 - Methods to Prevent Mobile Device Exploitation

There are certain methods that should be implemented to prevent the misuse of mobile devices, whether they are used for personal or official purposes.

Here is a list of methods that you can use to protect mobile devices:

- Disable services like Wi-Fi and Bluetooth when not required
- Enable GPS only when required
- Do not jailbreak or root the phone
- Perform regular backups
- Perform regular updates on the mobile device

- Restrict access to the device using an authentication method, such as a PIN, or fingerprint scan
- Avoid connecting to open networks
- Install applications from the trusted app stores only
- Encrypt the mobile device
- Scan every app being installed
- Avoid saving passwords on the mobile device
- Avoid clicking URLs received in spam

Specific to official use, in addition to the above-given methods, the organization should also use the following methods using Mobile Device Management (MDM):

- Enable Remote Location feature
- Enable Remote Wipe feature
- Enable encryption
- Enable Geofencing feature
- Allow installation of apps from your organization's app store
- Allow specific apps to be installed using blacklisting and whitelisting
- Use password enforcement
- Perform device inventory and management

Note that this is not an exhaustive list, but most of the MDM products have these features. A few features, such as integration with third-party products, may be specific to an MDM.

Developers

Developers must use caution while developing mobile app code. They should follow the key guidelines below:

- Follow proper code development guidelines
- Ensure proper data storage using encryption
- Use SSL/TLS for data in transit
- Prohibit the use of self-signing certificates and use trusted ones
- Use online authentication whenever possible
- Process authentication information on the server-side
- Perform code integrity checks on the app on the mobile device

- Use strong cryptography
- Perform user permission checks on the server-side
- Use code standards to create consistent codes and avoid vulnerabilities
- Perform a thorough test of the mobile code
- Use anti-tampering techniques
- Use root and jailbreak detection methods

Obfuscate the code to avoid reverse engineering

Task 2 - Using Mobile Device Management (MDM)

Most organizations now allow the use of mobile phones to share their data. However, there is always a risk of data being stolen or the mobile phone being compromised. Even though this can put the organization at big risk, the mobility of people has also become a necessity, and therefore, organizations often use different methods to allow the use of mobile phones. There are four methods that are used:

Bring Your Own Device (BYOD)

Organizations might allow you to bring your own device for official use. However, the organizations need to ensure that if there is any corporate data on the mobile phone, it should not be compromised. To safeguard the data, mobile phones must be encrypted.

Choose Your Own Device (CYOD)

This method provides employees the freedom to choose the device of their choice. The employee can either purchase the device from the organization or pay rent. The organization, however, has complete control over the mobile device.

Corporate-Owned, Personally Enabled (COPE)

The organization provides the mobile device to the user. However, as a user, you are only allowed to install apps that are pre-approved.

Corporate-Owned, Business Only (COBO)

The organization provides, controls, and manages the devices. The applications and the data belong to the organization.

MDM

With any of the given methods, it is difficult to manage these devices. This is where Mobile Device Management (MDM) comes in. MDM is a feature used in an enterprise network to keep a mobile device environment secure. For example, if an employee loses their mobile phone, the MDM administrator can remotely wipe out the data to prevent any misuse. Using MDM, you can block rooting, jailbreaking, or any other feature that you do not want the employees to use

With the use of MDM, you can fully control the mobile devices. For example, you will be able to restrict the use of any application other than the approved applications from your app store.

To protect the corporate data in case the mobile device is lost, you can use the Remote Wipe feature to wipe the mobile storage completely, erase sensitive data, and its configuration. You can also enable full device encryption. This will ensure that the data remains secure and confidential, even if it is stolen.

Another use of MDM is that you can enable geofencing, which alerts the administrator if a user leaves the defined perimeter. Geofencing requires the administrator to define a perimeter, then it can be configured to send an alert if the user moves outside of it.

You can also configure asset tracking. Even if the SIM is changed, you would be able to locate the device.

Review

Well done, you have completed the **Hacking Mobile Platforms** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Mobile Hacking Methods
- Exercise 2 - Preventing Mobile Device Exploitation

You should now have further knowledge of:

- OWASP Top 10 Mobile Threats
- Methods to prevent Mobile device exploitation
- Using Mobile Device Management (MDM)

Feedback