CEH v12 Lesson 10 :

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Hacking Android and iOS
- Exercise 2 — Mobile Device Management (MDM)
- Exercise 3 — Preventing Mobile Device Exploitation

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

- Mobile Platform Attack Vectors
- Hacking Android OS
- Mobile Platform Attack Vectors
- Hacking Android OS
- Jailbreaking and Rooting Mobile Devices
- iOS Hacking Tools
- Securing iOS Devices
- Mobile Device Management
- Mobile Security Guidelines and Tools
- Application Management
- Content Management
- Remote Wipe
- Geofencing
- Geolocation
- Screen Locks
- Push Notifications

- Passwords and Pins
- Biometrics
- Context-aware Authentication
- Containerization
- Storage Segmentation
- Full Device Encryption
- Mobile Security Guidelines
- Mobile Security Tools

Lab Duration

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

Exercise 1 — Hacking Android and iOS

iOS is the mobile operating system used on Apple mobile devices, such as iPhones and iPads. There can be various design flaws in iOS or its applications, leading to various attacks. For example, some advanced users jailbreak iOS to get root access, potentially allowing an attacker to gain administrative control and modify the underlying iOS.

In this exercise, you will learn about hacking iOS.

Learning Outcomes

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

- Mobile Platform Attack Vectors
- Hacking Android OS
- Jailbreaking and Rooting Mobile Devices
- iOS Hacking Tools
- Securing iOS Devices

Mobile Platform Attack Vectors

Mobile devices have become a common commodity for everyone in today's environment. Most users have their mobile devices connected to the Internet, either through mobile data plans or through wireless connectivity. However, this increases the security threats for mobile devices. The attackers use various attack vectors to attack the mobile devices. The attackers look for financial and personal information or even use the mobile devices for other purposes, such as crypto mining or bots.

The attackers can use various types of attack vectors to gain control of the mobile devices or the information stored within them.

Some key attack vectors are:

Malware

MMalware is one of the most common attack vectors in networks and mobile devices. With malware, attackers can drop viruses, trojans, rootkits, or spyware onto a target device. Malware can modify existing apps to access information or track users' activities on mobile devices or make an operating-system-level modification to gain administrative access.

App Stores Attackers create malicious mobile apps and then use the app stores to distribute them. The app store for Android is an open place. The app store for Android is not vetted, and attackers can easily create and upload a malicious app. Once a malicious app is downloaded and installed on a mobile device, an attacker can access information on or take control of the device.**Data Exfiltration**After an attacker has compromised a device, they can perform various activities. For example, they can print screens or send data to their command-and-control center. Data can be extracted from emails or copied to a USB drive.**Data Tampering**An attacker can also perform data tampering by modifying applications, rooting, or jailbreaking the device.**Data Loss**Data loss can occur if an attacker steals the mobile device or it is lost, delete the data, or exploit application vulnerabilities to steal data.

Hacking Android OS

Android is widely used on all types of mobile devices. Various mobile device vendors use Android and re-brand it to release it under their brand. For example, OnePlus, which makes mobile phones, has re-branded Android under their brand known as OxygenOS.

Android has several vulnerabilities, which the attackers target to hack into like another operating system. There are different ways to hack into Android OS. For example, the

attacker can root the device and modify the underlying kernel and system files.

An attacker can use various other tools to hack an Android device, such as the following:

- **NetCut** — Used to block wireless access on the mobile device
- **Drozer** — Discovers vulnerabilities within a mobile device and is used to discover an attack surface
- **Low Orbit Ion Cannon (LOIC)** — Used to perform DoS attacks
- **DroidSheep** — Used to perform session hijacking attacks
- **FaceNiff** — Used for sniffing and intercepting traffic over a wireless network

Rooting

A user can root the device and modify the underlying kernel and system files. When the attacker roots the Android device, it gives full administrative control to the user. A user can root the Android device using various tools, such as:

- KingoRoot
- TunesGo Root Android Tool
- One Click Root
- Z4root
- Towelroot
- RootMaster
- SuperSU Root
- Root Genius

Jailbreaking

The iOS device users do not have administrative control or root access by default. They are regular users who can install/uninstall apps, run signed apps, and modify settings. However, a root user can perform other tasks, such as modifying the underlying system.

Jailbreaking is a method of modifying the underlying kernel by patching it with custom code. When a user modifies the kernel, the user gains administrative capabilities,

allowing the user to run unsigned apps that are not available in the official Apple App Store. For example, a user has developed a malicious iOS app that he wants to test. When the user jailbreaks an iPhone, the user can execute the app, which without jailbreaking would not have been possible.

Even though some users perform jailbreaking for their benefit, it hampers the security of the iOS device. After jailbreaking an iOS device, the user may face performance deterioration and malware attacks.

Some of the applications that you can use for jailbreaking an iOS device are:

- Cydia
- Hexxa Plus
- Apricot
- Yuxigon
- Sileo
- Trimgo
- Bregxi
- Yalu

iOS Hacking Tools

Several iOS hacking tools are available. Some of the key tools are:

Malware

Malware is malicious software designed to perform an illegitimate task or activity. For example, malware may be created to steal information or simply cause performance issues. There are several iOS-specific malware that exists. Some of the key ones are:

- Clicker Trojan Malware
- Trident Malware
- Exodus
- Checkrain

- AceDeceiver Trojan
- XcodeGhost
- KeyRaider
- Pegasus

Hacking Tools

Other than using malware as a tool, some applications are available to hack iOS devices. Some of the key applications are:

- Spyzie
- Network Analyzer Pro
- Elcomsoft Phone Breaker
- Fing
- Network Analyzer Master
- Spyic
- iWebPRO
- Frida
- iOS Reverse Engineering Toolkit (iRET)
- netKillUIbeta
- Myriam iOS Security App
- iSpy
- Cycript
- Paraben DS
- Firecat
- Highster Mobile

Securing iOS Devices

You can use various methods to secure iOS devices. Here are some methods that you can use:

- Lock your phone with a password or PIN
- Avoid downloading apps from any untrusted store. Use only Apple App Store to download applications
- Avoid storing data on the local device
- Avoid adding add-ons in a Web browser
- Do NOT jailbreak the iOS device
- Install and configure Vault app to store and hide confidential and critical data
- Use VPN to encrypt your traffic
- Always use two-factor authentication
- Avoid connecting the iOS device to open public wireless networks
- Disable Bluetooth and wireless when not in use
- Enable the Reset Keyboard Dictionary feature to delete the keyboard cache
- Enable the Erase Data feature to erase data from iPhone after 10 wrong attempts to unlock it
- Always keep the iOS device updated
- Avoid clicking on any link in a message or email from an unknown sender

Exercise 2 — Mobile Device Management (MDM)

Most organizations now allow the use of mobile phones to share their data. However, there is always a risk of stolen data or compromised mobile phones. However, mobility has become a necessity for many people, and therefore, organizations often use different methods to allow the use of mobile phones.

It can be difficult to manage the devices. This is where Mobile Device Management (MDM) comes in. MDM is a feature used in an enterprise network to secure a mobile device environment. MDM can control, configure, update, and secure remote mobile devices.

Using MDM, you can block rooting, jailbreaking, or any other feature you do not want the employees to use. MDM also allows you to restrict the use of any application other than the approved applications from your app store.

MDM can enable geofencing, alerting the administrator if a user leaves the defined perimeter. Alongside this, you can also configure asset tracking. Even if the SIM is changed, you will locate the device.

An organization should also use the following methods when using MDM:

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

In this exercise, you should learn about mobile security solutions.

Learning Outcomes

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

- Application Management
- Content Management
- Remote Wipe
- Geofencing
- Geolocation
- Screen Locks
- Push Notifications
- Passwords and Pins

- Biometrics
- Context-aware Authentication
- Containerization
- Storage Segmentation
- Full Device Encryption

Exercise 3 — Preventing Mobile Device Exploitation

Mobile devices are widely used for personal and official reasons. 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. No matter the purpose of the device, its security is important. A user needs to ensure that the mobile device is safe and not hacked, stolen, or otherwise compromised. In this exercise, you will learn about some common methods to prevent mobile device exploitation.

Learning Outcomes

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

- Mobile Security Guidelines
- Mobile Security Tools

Mobile Security Guidelines

Certain methods 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 a spam
- Use screen locks with password or PIN

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

Administrators

The administrators need to control mobile usage within an enterprise environment. The administrators should perform the following tasks:

- Create and implement a mobile device policy
- Install and implement MDM to control the mobile devices
- Configure policies to secure the enterprise data on mobile devices
- Configure two-factor authentication
- Configure an app store to limit the apps to be used
- Monitor the security across all mobile devices continuously
- Keep all mobile devices and apps updated with the latest updates
- Secure all mobiles devices with the latest anti-malware

Mobile Security Tools

A user can use various mobile tools to increase the security of mobile devices. Some of the key tools are:

- **Lookout Personal**: Used for identity and theft protection
- **Zimperium's zIPS**: Works as an Intrusion Prevention System (IPS) in the mobile devices
- **BullGuard Mobile Security**: Used for malware protection and remote wipe
- **Bitdefender Mobile Security & Antivirus**: Works as an antivirus
- **Malwarebytes for Android**: Works as an anti-spyware application

Most anti-malware vendors also have mobile versions to help users protect their devices.