Module 17

Hacking Mobile Platforms

Learning Objectives

01 Explain Mobile Platform Attack Vectors

02 Explain Various Android OS Threats and Attacks

03 Explain Various iOS Threats and Attacks

04 Summarize Mobile Device Management (MDM) Concepts

05 Present Mobile Security Guidelines and Tools

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

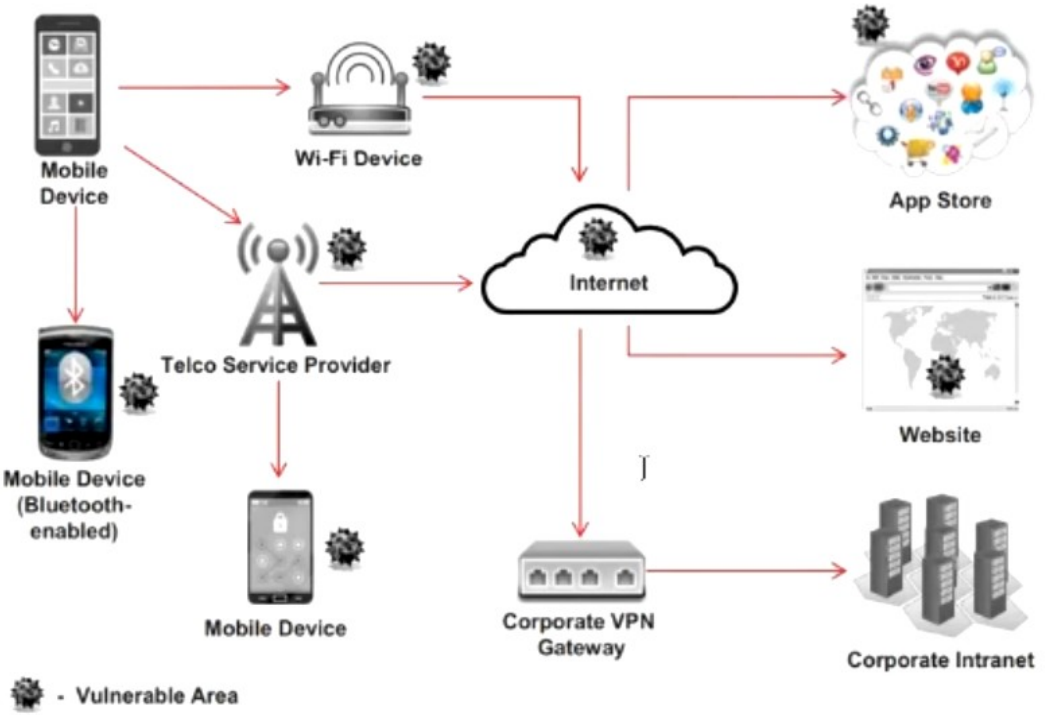
Objective 01

Explain Mobile Platform Attack Vectors

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Vulnerable Areas in Mobile Business Environment

- Smartphones offer **broad Internet** and **network connectivity** via different channels, such as 3G/4G/5G, Bluetooth, Wi-Fi, and wired computer connections
- Security threats may arise in different places along these channels during **data transmission**



https://www.ibm.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

OWASP Top 10 Mobile Risks – 2024

- M1 Improper Credential Usage
- M2 Inadequate Supply Chain Security
- M3 Insecure Authentication/Authorization
- M4 Insufficient Input/Output Validation
- M5 Insecure Communication
- M6 Inadequate Privacy Controls
- M7 Insufficient Binary Protections
- M8 Security Misconfiguration
- M9 Insecure Data Storage
- M 10 Insufficient Cryptography

https://owasp.org

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Anatomy of a Mobile Attack

Point 01 – THE DEVICE

BROWSER

- Phishing
- Framing
- Clickjacking
- Man-in-the-Mobile
- Buffer Overflow
- Data Caching

PHONE/SMS

- Baseband Attacks
- SMiShing

APPS

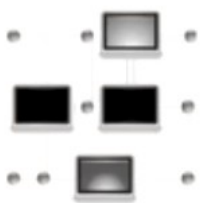
- Sensitive Data Storage
- No encryption/Weak encryption
- Improper SSL Validation
- Configuration Manipulation
- Dynamic Runtime Injection
- Unintended Permissions
- Escalated Privileges
- Access to device and User Info
- Third-party Code
- Intent Hijacking
- Zip Directory Traversal
- Side Channel Attack

MALWARE

Point 02 – THE NETWORK

THE NETWORK

- Wi-Fi (no encryption/weak encryption)
- Rogue Access Point
- Packet Sniffing
- Man-in-the-Middle (MITM)
- Session Hijacking
- DNS Poisoning
- SSLStrip
- Fake SSL Certificate
- BGP Hijacking
- HTTP Proxies



Point 03 – THE DATA CENTER / CLOUD

INTERNET

WEB SERVER

- Platform Vulnerabilities
- Server Misconfiguration
- Cross-site Scripting (XSS)
- Cross-site Request Forgery (XSRF)
- Weak Input Validation
- Brute Force Attacks
- Cross Origin Resource Sharing
- Side Channel Attack
- Hypervisor Attack

DATABASE

- SQL Injection
- Privilege Escalation
- Data Dumping
- OS Command Execution

https://www.nowsecure.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Security Issues Arising from App Stores

01 Insufficient or **no vetting of apps** leads to malicious and fake apps entering the app marketplace

02 App stores are common target for attackers to **distribute malware and malicious apps**

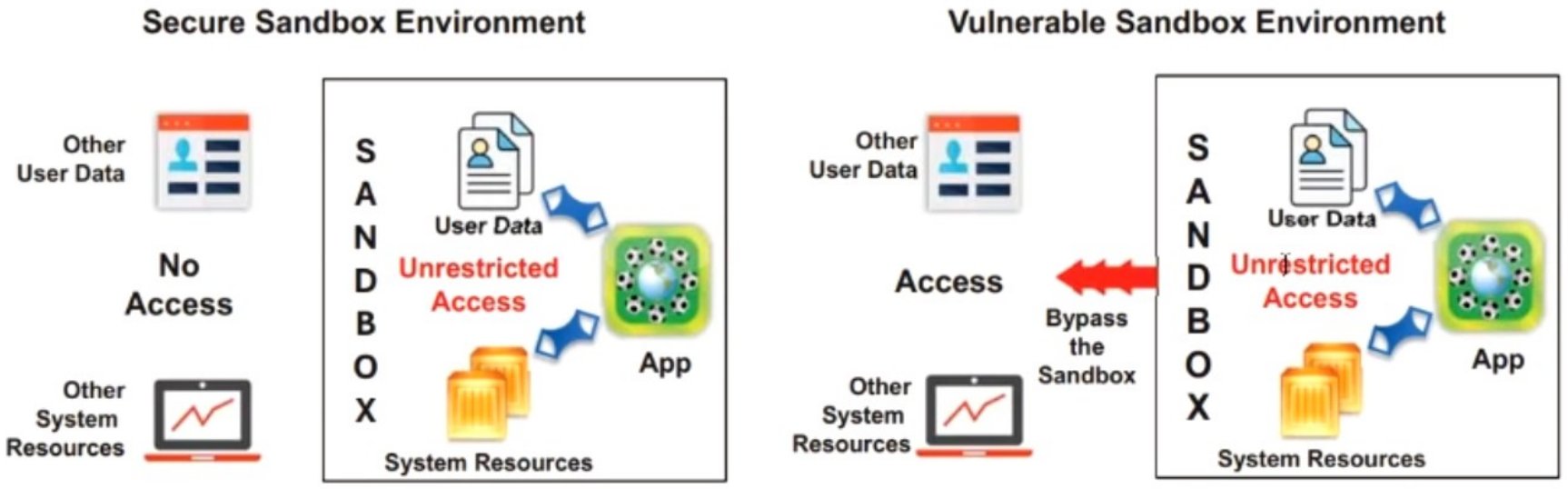
03 Attackers can also use **social engineer users** to download and run apps outside of official app stores

04 Malicious apps can **damage other applications** and data, and send your sensitive data to attackers

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

App Sandboxing Issues

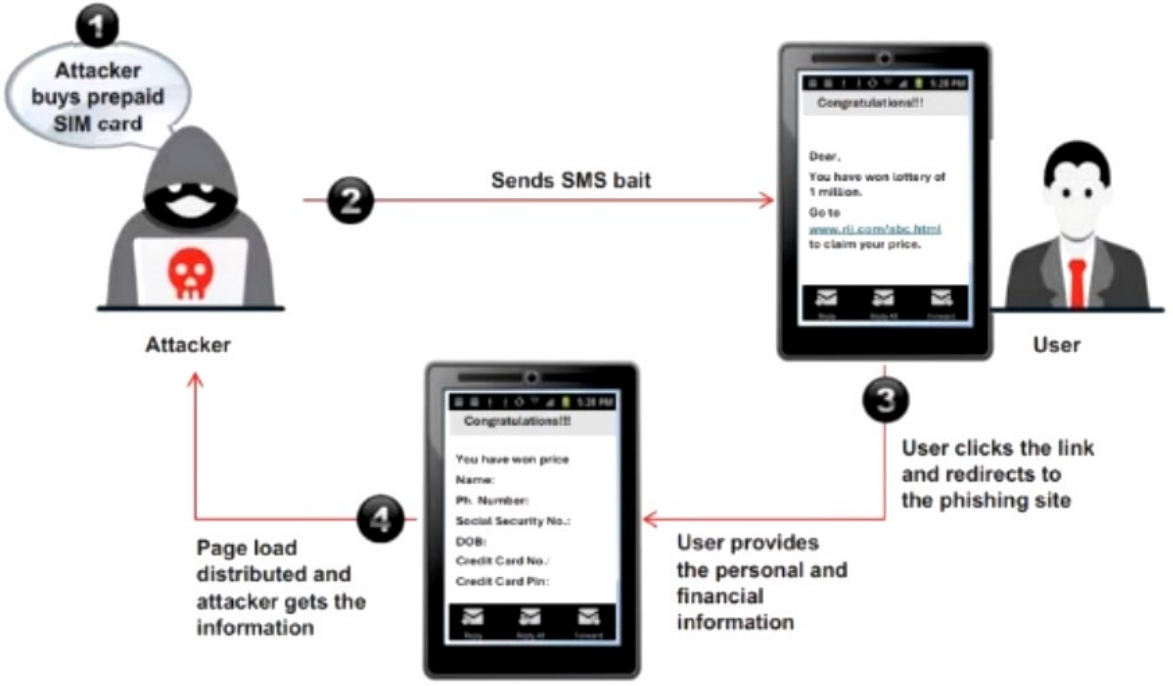
Sandboxing helps **protect systems and users** by limiting the resources the app can access to the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

- SMS Phishing is the act of trying to **acquire personal and financial information by sending SMSs** (Instant Messages or IMs) containing deceptive links



Why is SMS Phishing Effective?

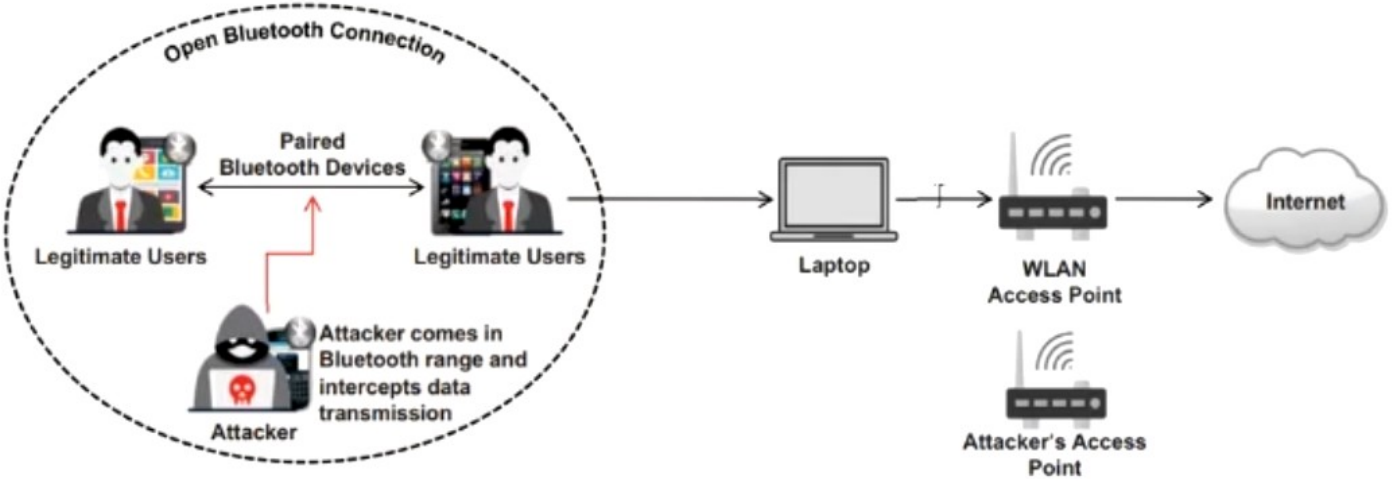
- High open rates
- Trust in SMS
- Limited space for links and content
- Lack of security awareness
- Mobile device usage
- Ease of impersonation
- Urgency and action
- Direct links and download prompts
- Prevalence of shortened URLs
- Lack of anti-phishing features

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

- Mobile **device pairing on open connections** (public Wi-Fi/unencrypted Wi-Fi routers) allows attackers to **eavesdrop** and **intercept data transmission** using techniques such as;
  - Bluesnarfing (stealing information via Bluetooth)
  - Bluebugging (gaining control over the device via Bluetooth)
- Sharing **data from malicious devices** can infect/breach data on the recipient device

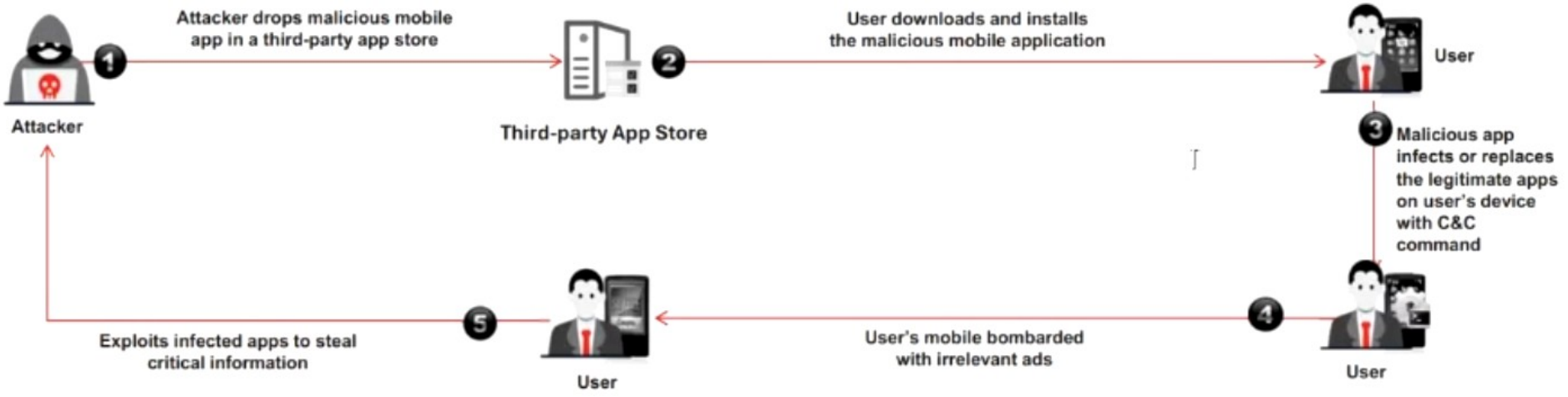
Bluebugging Attack



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Agent Smith Attack

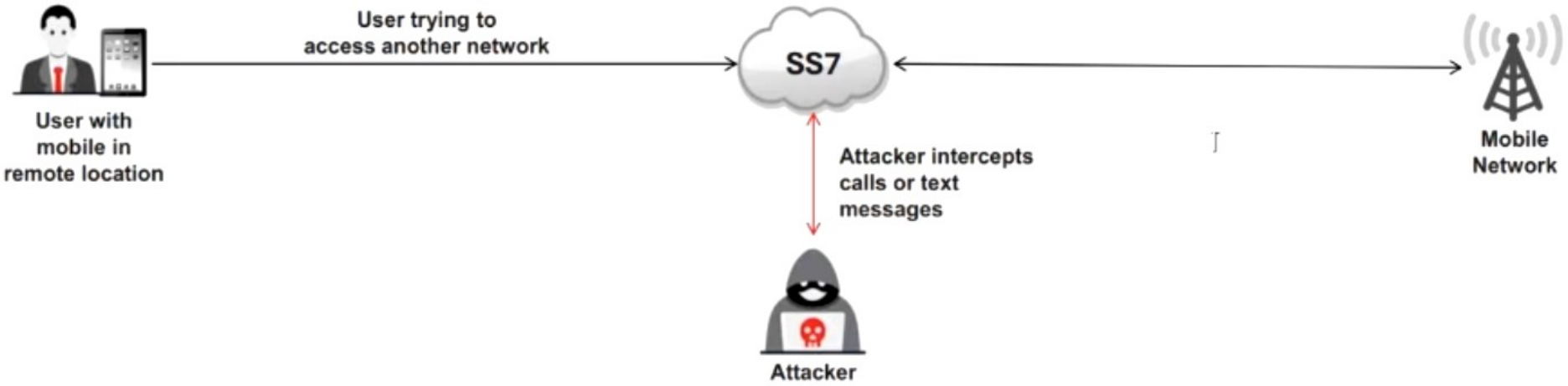
- An Agent smith attack is carried out by persuading the victim to install a malicious app designed and published by an attacker
- The malicious app **replaces legitimate apps**, such as WhatsApp, SHAREit, and MX Player
- The attacker produces **a huge volume of advertisements** on the victim's device through the infected app for financial gains



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Exploiting SS7 Vulnerability

- Signaling System 7 (SS7) is a **communication protocol** that allows mobile users to exchange communication through another cellular network
- SS7 is operated depending on **mutual trust between operators** without any authentication
- Attackers can exploit this vulnerability to perform a **man-in-the-middle attack**, impeding the texts and calls between communicating devices



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Simjacker: SIM Card Attack

- Simjacker is a vulnerability associated with a **SIM card's S@T browser**, a pre-installed software on SIM cards that is designed to provide a set of instructions
- Attackers exploit Simjacker to perform various malicious activities, such as capturing the locations of devices, monitoring calls, forcing device browsers to connect to malicious websites, and **performing DoS attacks**

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Call Spoofing

- Call spoofing is a technique used by attackers to **manipulate the caller ID** information displayed on the recipient's phone when they receive a call
- Attackers use this technique to **disguise** their phone number **as a trusted source**, tricking individuals into sharing sensitive information or paying for unnecessary services

SpoofCard

SpoofCard allows attackers to use a **virtual number** to make calls and send texts while concealing their personal information, regardless of location

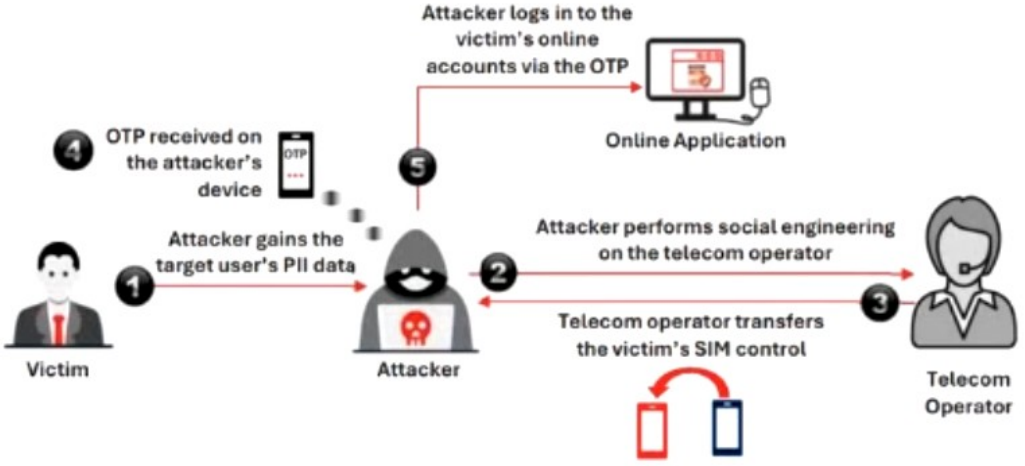
Other Call Spoofing Tools

- Fake Call (*https://play.google.com*)
- SpoofTel (*https://www.spooftel.com*)
- Fake Call and SMS (*https://play.google.com*)
- Fake Caller ID (*https://fakecallerid.io*)
- Phone Id - Fake Caller Buster (*https://play.google.com*)

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

OTP Hijacking/Two-Factor Authentication Hijacking

- Attackers hijack OTPs and redirect them to their personal devices using different techniques such as **social engineering** and **SMS jacking**
- Attackers succeed in OTP hijacking by initially **stealing the victim's PII data** by bribing or tricking the mobile store sellers or exploiting the reuse of the same number for different customers
- Attackers can also use **SIM jacking attacks** to infect the target device's SIM using malware, through which they can intercept and read OTPs



OTP Hijacking Tools

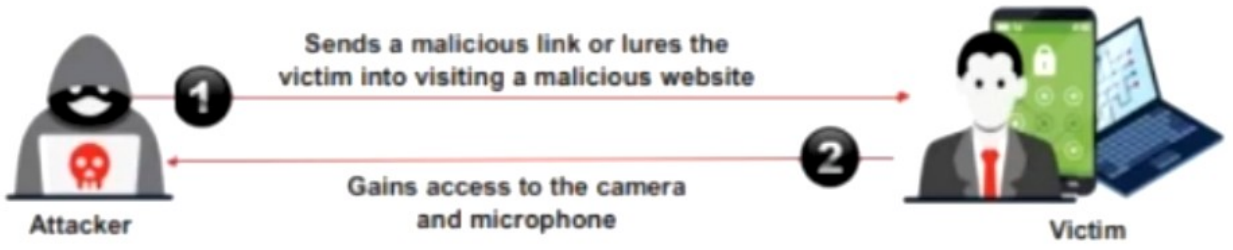
AdvPhishing	AdvPhishing is a social media phishing tool that assists attackers in **bypassing two-factor** or **OTP authentication**

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Camera/Microphone Capture Attacks

Camfecting Attack

- A camfecting attack is a **webcam capturing attack** that is performed to gain access to the camera of a target's computer or mobile device
- An attacker infects the target device with a **remote access Trojan** (RAT) and compromises it to access the victim's camera and microphone
- Using this method, the attacker can obtain sensitive data such as **personal photos**, **recorded videos**, and the **location** of the user

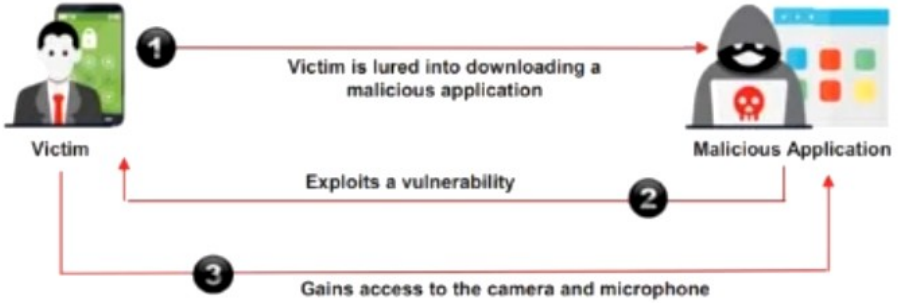


Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Camera/Microphone Capture Attacks (Cont'd)

Android Camera Hijack Attack

- Attackers exploit **Android's multiple security bypass vulnerabilities** to circumvent the required permissions and gain access to the victim's camera and microphone
- Android camera applications generally require storage permissions such as `android.permission.CAMERA`, `android.permission.RECORD_AUDIO`, and `android.permission.ACCESS_COARSE_LOCATION` to store photos and videos
- Such storage permissions provide **unrestricted access** to the entire internal storage and allows attackers to perform various activities such as capturing photos; recording videos and voice calls; and accessing stored photos



Camera/Microphone Hijacking Tools

Stormbreaker

StormBreaker can access a device's location, **webcam**, and **microphone** without explicitly **requesting any permissions**

https://www.github.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Objective 02

Explain Various Android OS Threats and Attacks

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

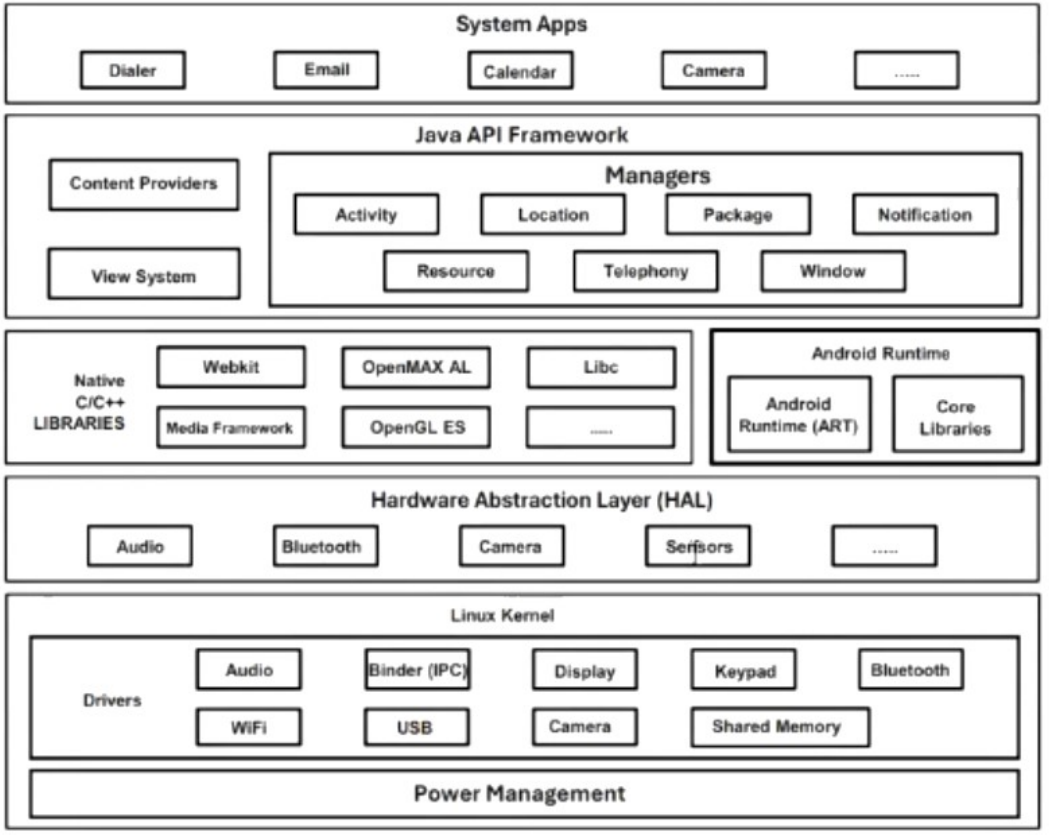
Android OS

- Android is a software environment developed by **Google for mobile devices**. It includes an operating system, middleware, and key applications

Features

- Application framework **enabling the reuse** and **replacement** of components
- Provides a variety of **pre-built** UI components
- Integrated browser based on the **open source Blink and WebKit engine**
- **Media support** for common audio, video, and still image formats (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)
- **Rich development environment** including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the **Eclipse IDE**

https://developer.android.com



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Android Device Administration API

- The Device Administration API provides **device administration features** at the system level
- This API allows developers to create **security-aware applications** that are useful in enterprise settings, where IT professionals require strong control over employee devices

Policies Supported by the Device Administration API

- Password enabled
- Minimum password length
- Alphanumeric password required
- Complex password required
- Minimum letters required in password
- Minimum lowercase letters required in password
- Minimum non-letter characters required in password
- Minimum numerical digits required in password
- Minimum symbols required in password
- Minimum uppercase letters required in password
- Password expiration timeout
- Password history restriction
- Maximum failed password attempts
- Maximum inactivity time lock
- Storage encryption required
- Camera disabled
- Prompt user to set a new password
- Device immediately locked
- Wiping of the device's data

https://developer.android.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Android Rooting

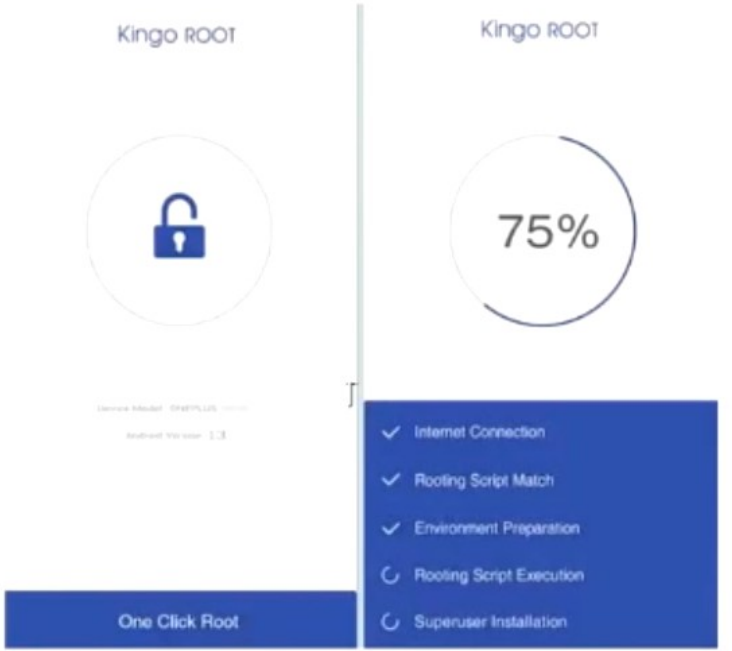
- Rooting allows Android users to **attain privileged control** (known as "root access") within Android's subsystem
- Rooting process involves exploiting security vulnerabilities in the **device firmware** and copying the SU binary to a location in the current process's PATH (e.g., /system/xbin/su) and granting it executable permissions with the **chmod command**

Android Rooting With PC using KingoRoot

- Download **KingoRoot Android (PC Version)** and install it on your desktop
- Run the tool and **connect the device** to the computer with USB cable
- Enable USB debugging mode on Android device
- Now the tool will install the **latest drivers** on your PC. You will see a new screen on your desktop with your device name and the "**ROOT**" button
- Click on **ROOT** to root your device

Android Rooting Without PC using KingoRoot

- Enable installation from **unknown sources** on Android device
- Download **KingoRoot.apk** on your Android device from play store
- Install and launch KingoRoot
- Press "**One Click Root**" on the main interface of the app. Wait a few seconds until "**root result**" appears on the display
- Attempt multiple times rooting or try PC version in case of failed



https://www.kingoapp.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

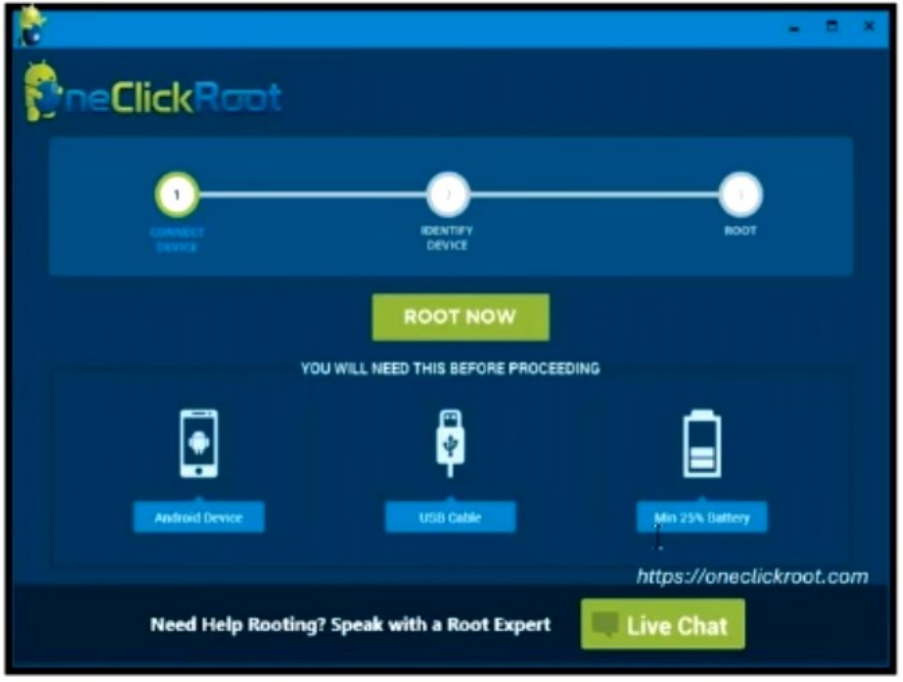
Android Rooting Tools

OneClickRoot

One Click Root is an **Android rooting software** that allows rooting of an Android smartphone and provides access to additional features such as gaining access to more apps, **installing apps on SD cards**, **accessing blocked features**, etc.

Steps to Perform Rooting are:

- Download **One Click Root (PC Version)** and install it on your desktop
- **Connect the device** to the computer with USB cable
- Enable USB debugging mode on Android device
- Run the tool One Click Root in PC and click on **ROOT** to root your device



Other Android rooting tools:

- **TunesGo** *https://tunesgo.wondershare.com*
- **RootMaster** *https://root-master.com*
- **Magisk Manager** *https://magiskmanager.com*
- **KingRoot** *https://kingrootapp.net*
- **iRoot** *https://www.iroot.com*

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Identifying Attack Surfaces Using drozer

Attackers use the drozer tool to **discover various vulnerabilities and attack surfaces** on Android devices and apps

Steps to Identify Attack Surfaces

- **Fetching Package Information**
  - `dz> run app.package.list`

    - Displays list of all packages
  - `dz> run app.package.list -f <string_name>`

    - Retrieves the package name from the list
  - `dz> run app.package.info -a <package_name>`

    - Retrieves basic details about a specific package
- **Identifying Attack Surface**
  - `dz> run app.package.attacksurface <package_name>`

    - Lists out various exported activities
  - `dz> run app.activity.info -a <package_name>`

    - Displays details of the exported activities
- **Launching Activities**
  - `dz> run app.activity.start --component <package_name> <activity_name>`

    - Displays critical information used to evade the authentication

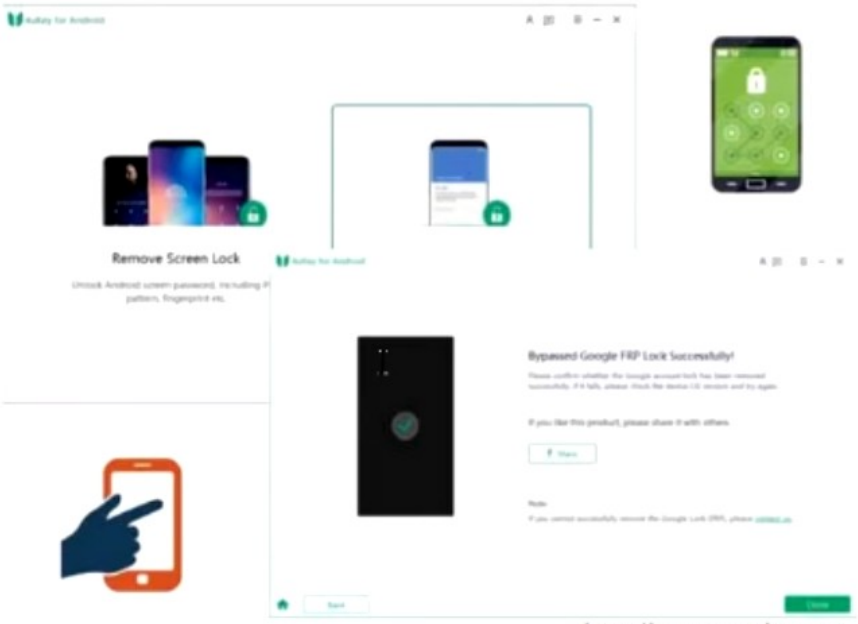
Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Bypassing FRP on Android Phones Using 4ukey

- Factory Reset Protection (FRP) is a security feature in Android devices designed to **prevent unauthorized access** to lost or stolen devices
- Attackers can bypass FRP by using specialized tools such as **4ukey** and **Octoplus FRP**

Steps to Bypass FRP on Android Phones

- **Step 1:** Launch 4uKey and connect the locked Android device to the computer → Click on the "**Remove Google Lock (FRP)**" option
- **Step 2:** Select the correct operating system (OS) version of the Android device
- **Step 3:** Click on "**Start**" button to initiate the process of removing the Google Account Lock (FRP)
- **Step 4:** Now follow the on-screen instructions to bypass FRP on Android device
- **Step 5:** Upon successful completion, you will receive a notification window displaying the message "**Bypassed Google FRP Lock Successfully**"



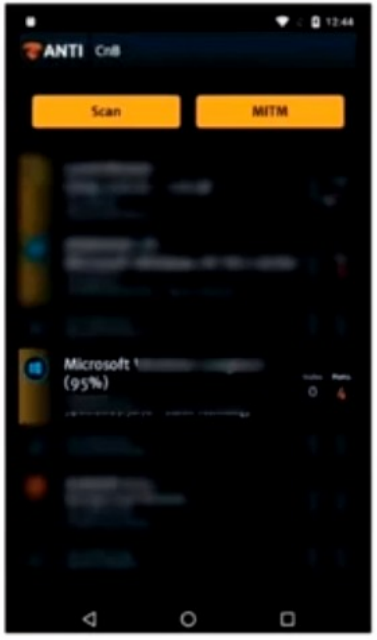
https://www.tenorshare.net

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Hacking with zANTI and Kali NetHunter

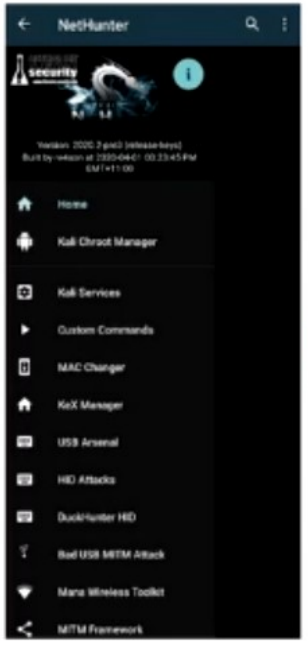
zANTI

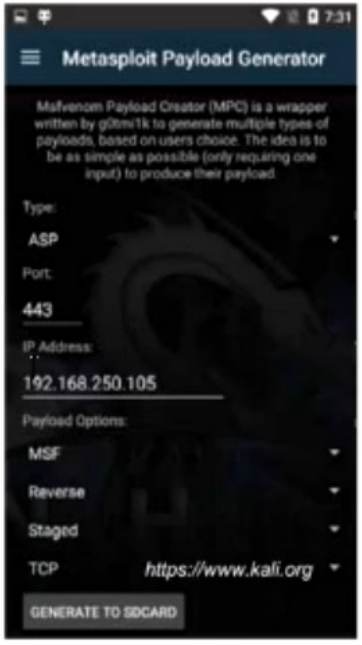
zANTI is an Android application that allows you to perform attacks, such as **spoof MAC address**, creating a malicious Wi-Fi hotspot, and **hijack session**



Kali NetHunter

Kali NetHunter provides a comprehensive suite of tools that helps attackers to conduct various attacks such as Human Interface Device (**HID) keyboard attacks**, **BadUSB attacks**, etc.

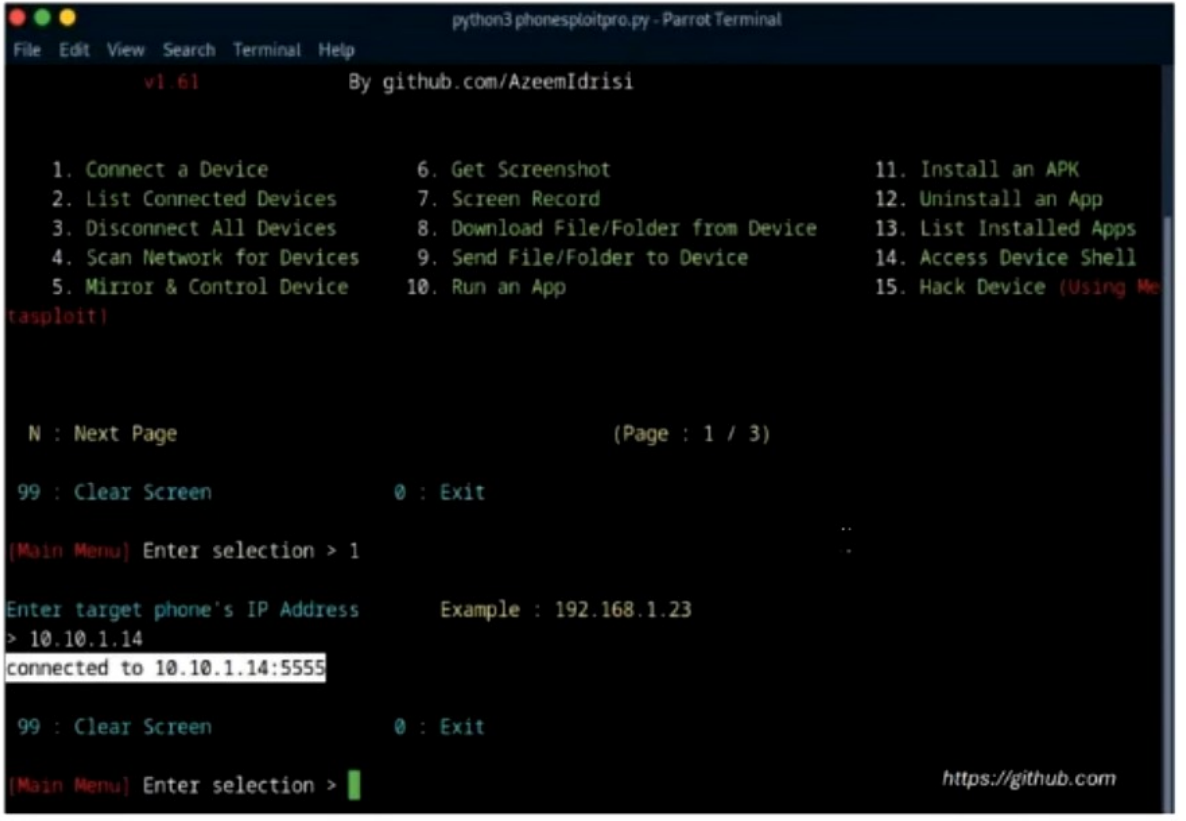




Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Exploiting Android Device through ADB Using PhoneSploit Pro

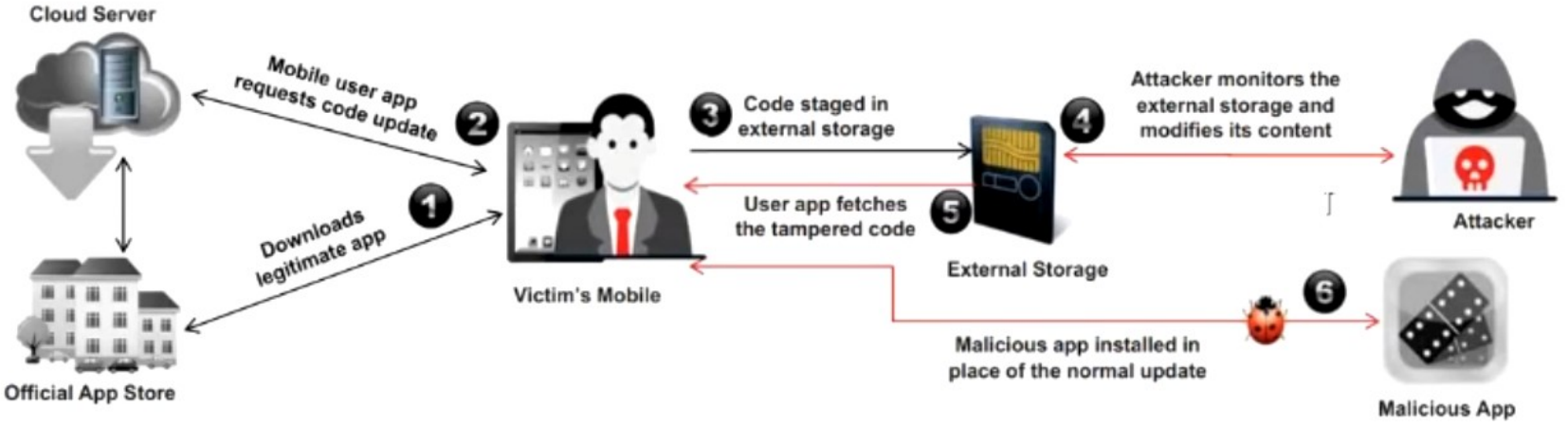
- Android Debug Bridge (ADB) is a **command-line tool** that allows attackers to communicate with the target Android device
- If the target Android device has TCP debugging enabled on **port 5555**, attackers can use tools such as PhoneSploit Pro to perform various malicious activities on the target device, such as **screen capturing**, dumping system info, viewing running applications, **port forwarding**, installing/uninstalling any application, and turning Wi-Fi on/off



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Launching Man-in-the-Disk Attack

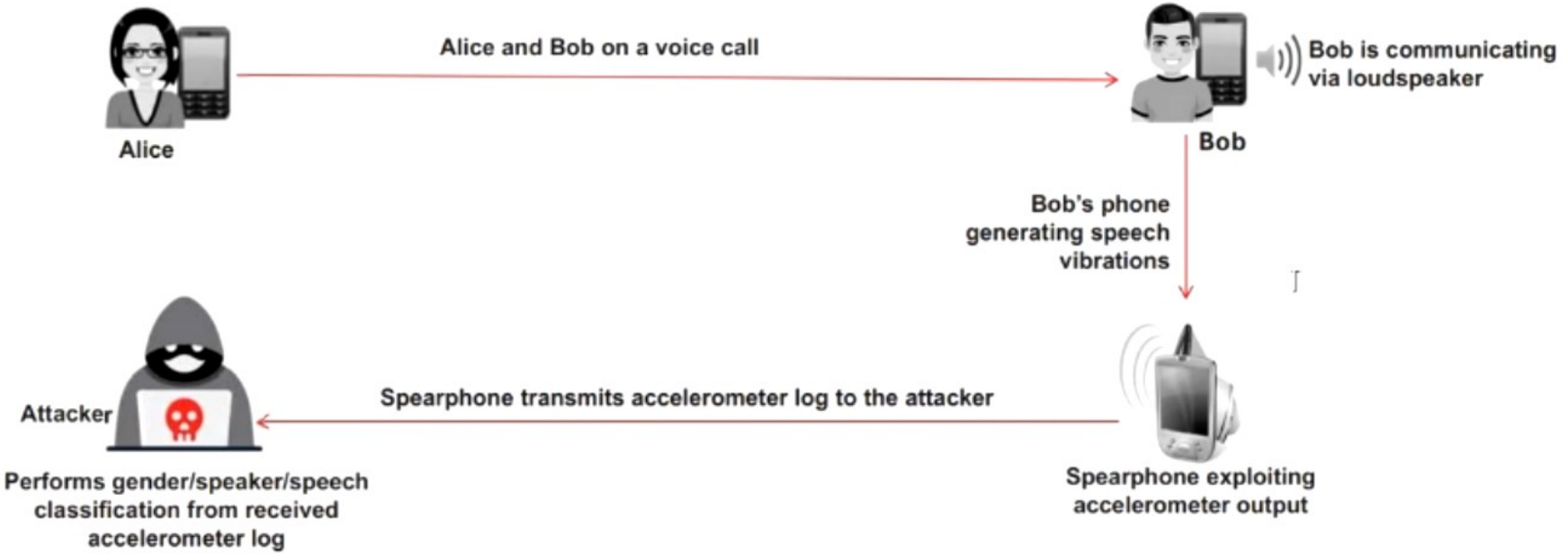
- Attackers perform man-in-the-disk (MITD) attacks when applications do not incorporate proper security measures against usage of the device's external storage
- This vulnerability leads to the **installation of potentially malicious apps** to the user's devices, thereby blocking access to legitimate apps



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Launching Spearphone Attack

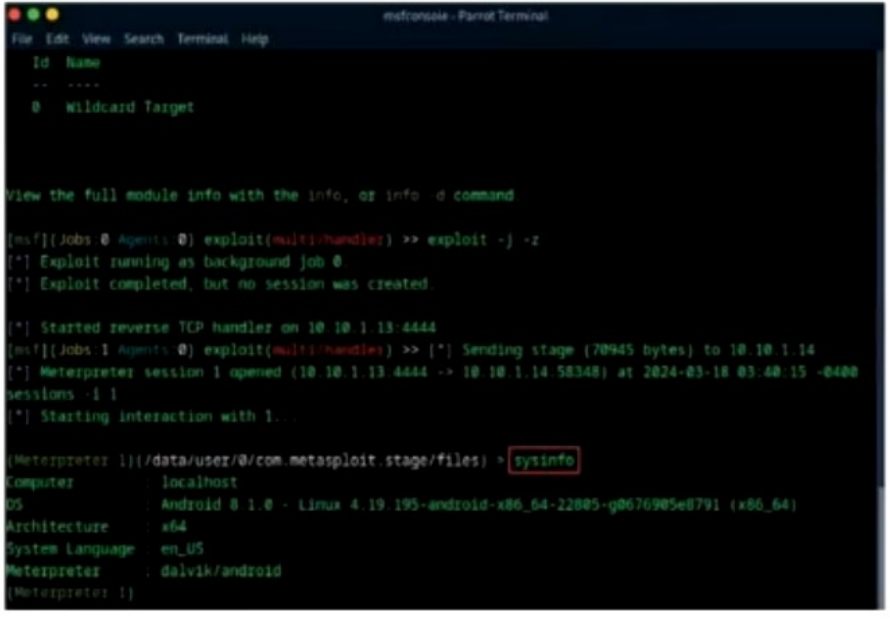
- A Spearphone attack allows Android apps to **record loudspeaker data** without any privileges
- Attackers can **eavesdrop on loudspeaker voice** conversation between remote mobile users by exploiting hardware-based motion sensor, i.e. accelerometers

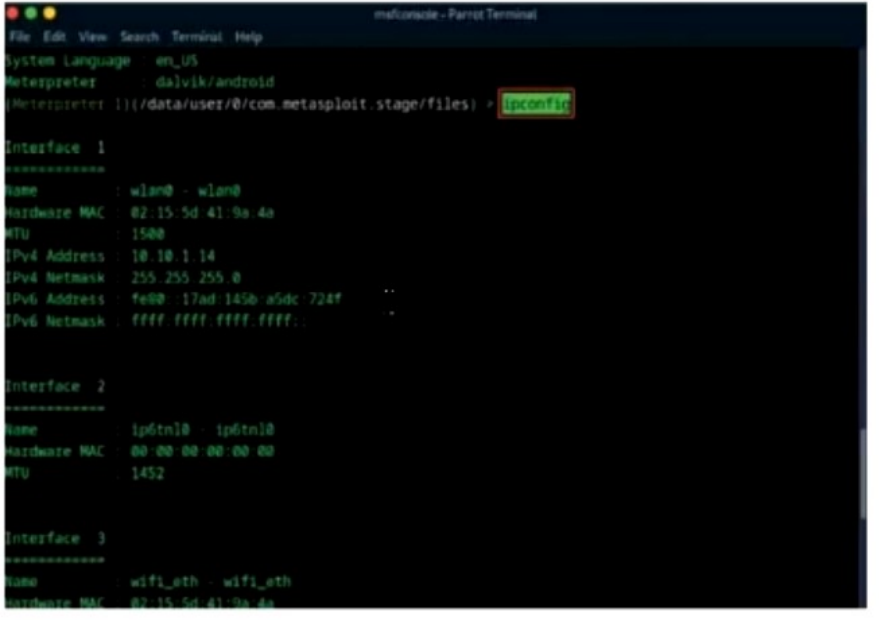


Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Exploiting Android Devices Using Metasploit

- The Metasploit Framework allows attackers to use **custom** or **in-built exploits** and payloads for exploiting the target Android device and obtain sensitive information
- After establishing a meterpreter session using Metasploit, attackers use commands such as **sysinfo**, **ipconfig**, **pwd**, **ps**, and **dump_sms** to gather sensitive data from the target Android device





Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Analyzing Android Devices

Analyzing Android devices involves examining the system to gather information, understand behavior, or identify vulnerabilities for various purposes

Some of the tasks an attacker can perform while analyzing the connected Android device:

Technique	Description
Accessing the Android Device through Shell	This technique involves the attacker connecting to an Android device over Wi-Fi instead of using a USB cable. This approach requires both the attacker's machine and the target Android device to be on the same Wi-Fi network
Enumerate the List of Installed Applications	Run the following command to list only the third-party applications: **$ adb shell pm list packages -3 –f**
Disassemble the Targeted App Package	Run the following apktool command with the proper app package name: **$ apktool d <App_package>.apk**
List Out the Open Files	Run the following command on the connected Android device to list the open files based the running process ID: **# lsof -p <pid>**
Signing and Installing Malicious APK	▪ Create a custom debug.keystore code-signing certificate by running the following command: **keytool -genkey -v -keystore ~/.android/debug.keystore -alias signkey -keyalg RSA -keysize 2048 -validity 20000** ▪ Run the following command to sign the malicious APK file with the custom code-signing certificate: **apksigner sign --ks ~/.android/debug.keystore --ks-key-alias signkey <malicious file>.apk**

https://mas.owasp.org

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Other Techniques for Hacking Android Devices

Advanced SMS Phishing

- Attackers use any **low-priced USB modem** and trick the victim into accepting the malicious settings in the mobile, which results in redirecting all the victim's data to the attacker

Bypass SSL Pinning

- Attackers can exploit SSL pinning using techniques such as **reverse engineering** and **hooking**
- Attackers modify the source code of the application to bypass SSL pinning and further perform man-in-the-middle attacks

Tap 'n Ghost Attack

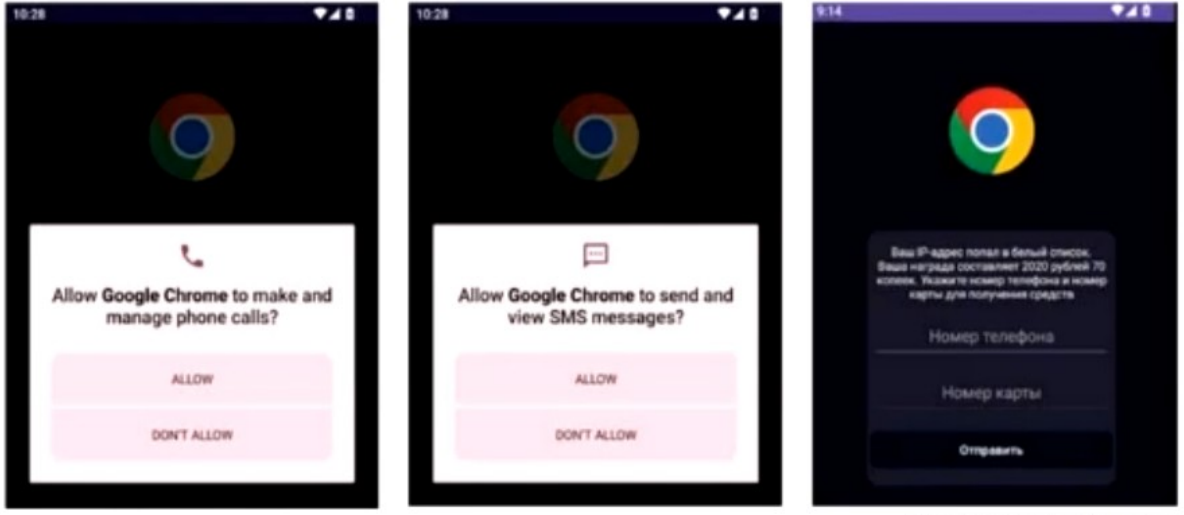
- This attack targets **NFC technology** and **RX electrodes** used in capacitive touchscreens of mobile devices
- Tap 'n Ghost is based on two attack techniques: Tag-based Adaptive Ploy (TAP) and Ghost Touch Generator

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Android Malware

Mamont

- Mamont is an Android banking Trojan that masquerades as the **Chrome browser application**, aiming to deceive users into unwittingly downloading and installing the Trojan
- Upon installation, the Trojan prompts the user to **grant permissions** such as sending and receiving phone calls and SMS messages
- The malware tricks the user to input personal information such as **phone numbers and credit card details** using a **fake cash prize claim**



https://www.gdatasoftware.com

Other Android Malware

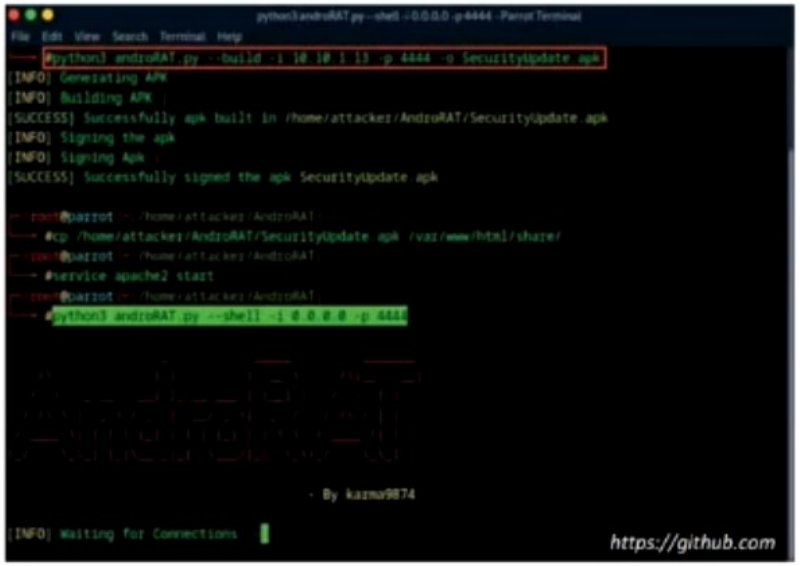
- SecuriDropper
- Dwphon
- DogeRAT
- Tambir
- SoumniBot

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Android Hacking Tools

AndroRAT

AndroRAT provides a **full persistent backdoor** to the target device as the app starts automatically on device boot up



Ghost Framework

Ghost framework is an **Android post-exploitation** tool that leverages the Android Debug Bridge (ADB) to gain **remote access** to Android devices

Other Android hacking tools:

- **hxp_photo_eye** *https://github.com*
- **Gallery Eye** *https://github.com*
- **mSpy** *https://www.mspy.com*
- **Hackingtoolkit** *https://github.com*
- **Social-Engineer Toolkit (SET)** *https://github.com*

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Securing Android Devices

- **Enable screen locks** for your Android phone for it to be more secure
- Do not directly download **Android package (APK) files**
- Never **root** your Android device
- Regularly update the **operating system**
- Download apps only from the **official Android market**
- Use **free protector Android apps** where you can assign passwords to text messages, mail accounts, etc.
- Keep your device updated with **Android antivirus software such as Kaspersky Antivirus**
- Enable **encryption** in your Android device to enhance its security

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Android Device Tracking Tools: Google Find My Device

- Google's Find My Device helps you easily **locate a lost Android device** and keeps your information on the missing device safe while you look for it

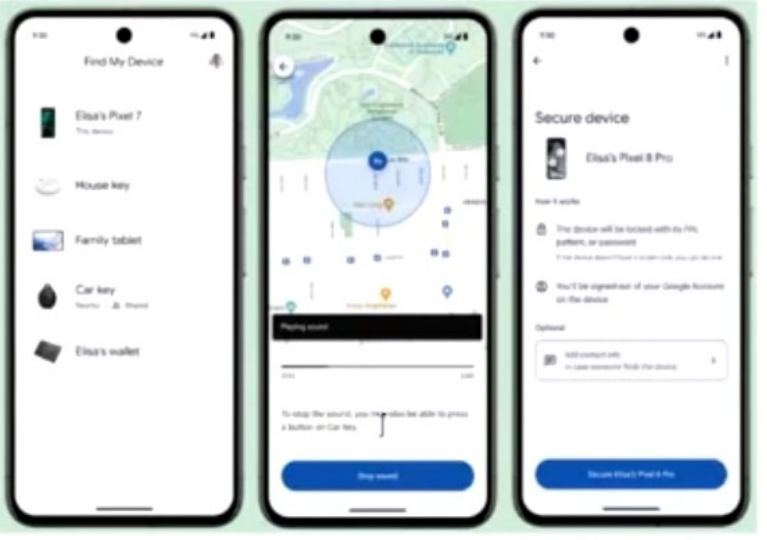
To find, lock, or erase a lost or stolen device:

- Go to **https://www.google.com/android/find** and sign in to your Google Account
- If you have more than one device, click **"Lost device"** at the top of the screen
- The device gets a **notification**
- Locate the device on the map
- Pick what you want to do

  Play sound: Rings your device at full volume for 5 minutes

  Secure Device: Locks your device with your PIN, pattern, or password

  Factory Reset Device: Permanently deletes all data on your device



https://www.google.com

Other Android Device Tracking Tools:

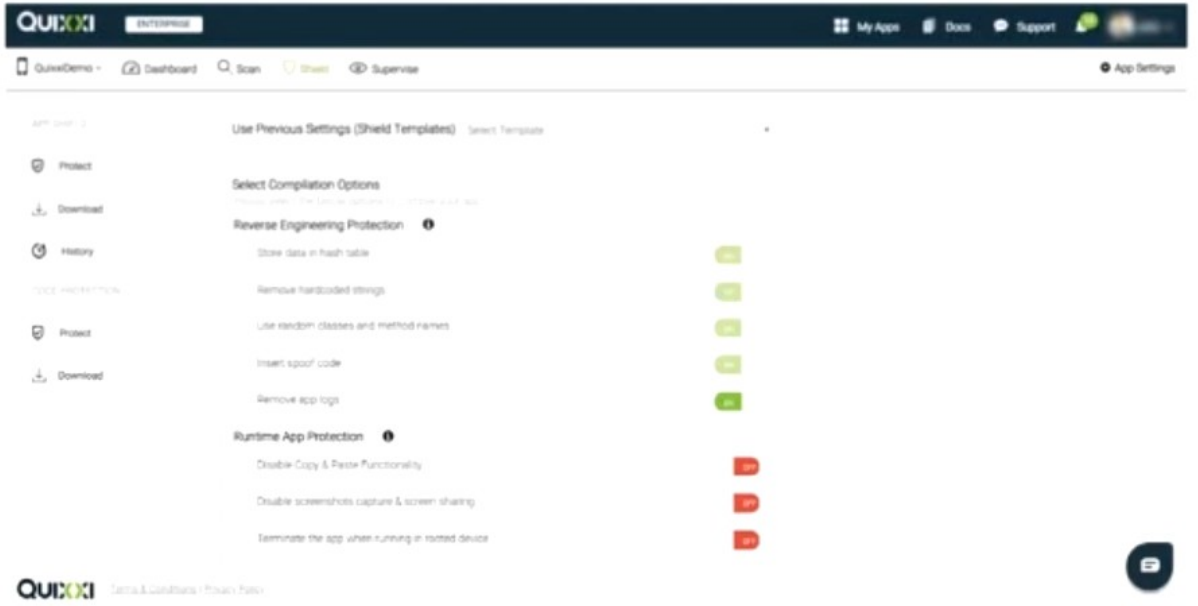
Find My Phone	Where's My Droid	Prey: Find My Phone & Security	Phone Tracker and GPS Location
https://play.google.com	*https://wheresmydroid.com*	*https://play.google.com*	*https://play.google.com*

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Android Vulnerability Scanners

Quixxi App Shield

Quixxi App Shield can be used by enterprises and mobile app developers to secure their mobile apps from piracy, revenue loss, **intellectual property (IP) theft**, **loss of user data**, **hacking**, and **cracking**



https://quixxi.com

Android Exploits
https://play.google.com

ImmuniWeb® MobileSuite
https://www.immuniweb.com

Yaazhini
https://www.vegabird.com

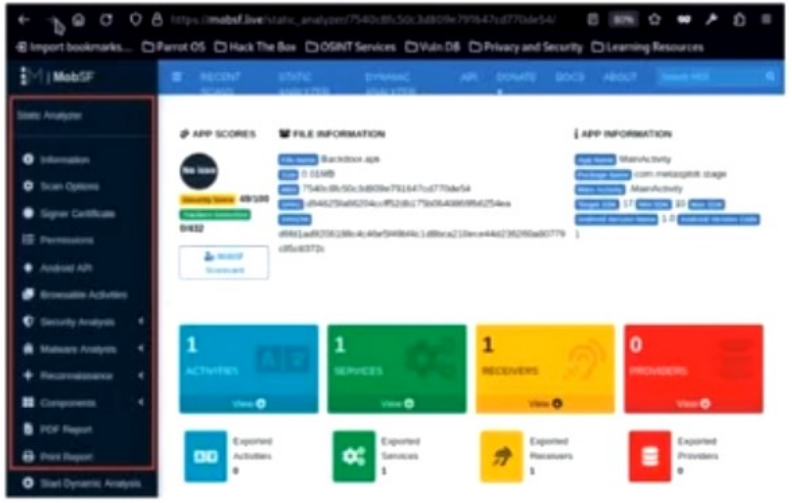
Vulners Scanner
https://play.google.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Static Analysis of Android APK

- Security analysts perform static analysis on malicious Android APKs to **examine the code** without executing the app
- This method helps in identifying harmful features or vulnerabilities in the application, or to compare the suspected APK code against **malware signatures** to identify known malware variants

MobSF



https://github.com

Sixo Online APK Analyzer

https://sisik.eu

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

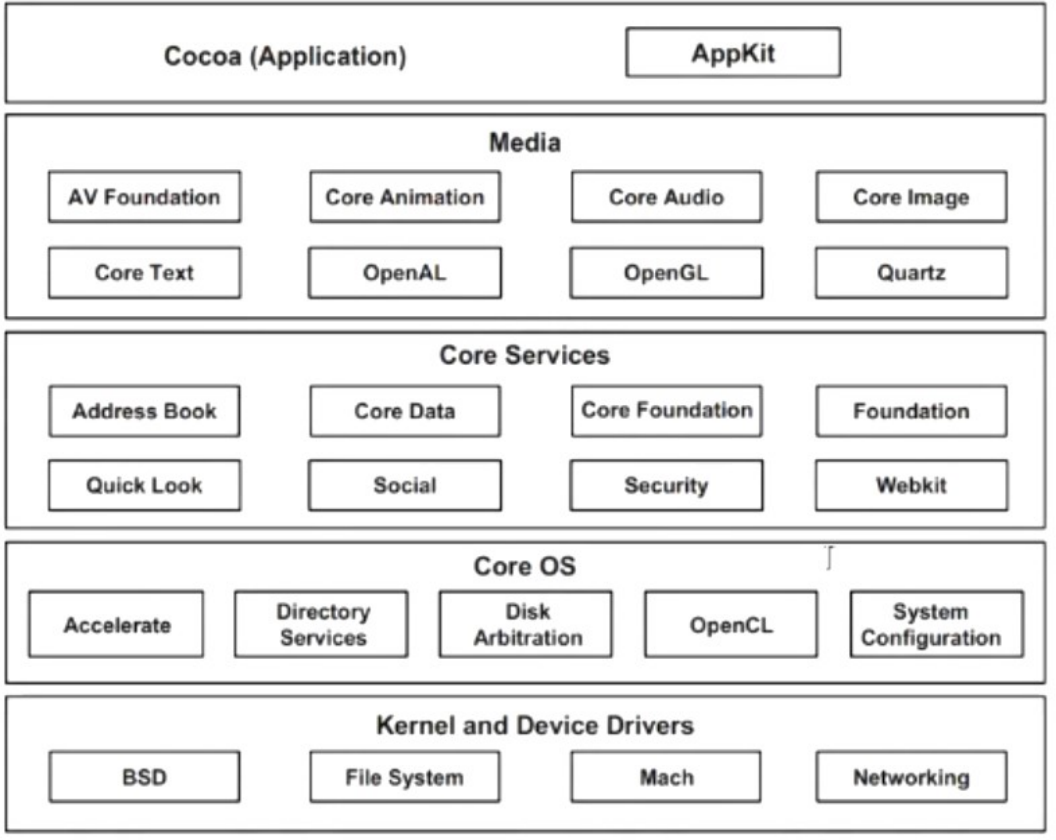
Objective 03

Explain Various iOS Threats and Attacks

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Apple iOS

- iOS is **Apple's mobile operating system**; it supports Apple devices such as iPhone, iPod touch, iPad, and Apple TV
- The user interface is based on the concept of **direct manipulation**, with **multi-touch** gestures



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Jailbreaking iOS

- Jailbreaking is defined as the process of **installing a modified set of kernel patches** that allows users to run third-party applications not signed by the OS vendor
- Jailbreaking provides **root access to the operating system** and permits downloading of third-party applications, themes, and extensions on iOS devices
- Jailbreaking **removes sandbox restrictions**, which enables malicious apps to access restricted mobile resources and information

Jailbreaking, like rooting, also comes with many security and other risks to your device, which include the following:

1. **Voiding your phone's warranty**
2. **Poor performance**
3. **Malware infection**
4. **"Bricking" the device**

Types of Jailbreaking

- **Userland Exploit**

A userland jailbreak **allows user-level access** but does not allow iboot-level access

- **iBoot Exploit**

An iboot jailbreak allows both **user-level access** and **iboot-level access**

- **Bootrom Exploit**

A bootrom jailbreak allows both **user-level access** and **iboot-level access**

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Jailbreaking Techniques

Untethered Jailbreaking

- An untethered jailbreak has the property that if the user turns the device off and back on, the device will completely start up, and the **kernel will be patched** without the help of a computer; in other words, it will be jailbroken after each reboot

Semi-tethered Jailbreaking

- A semi-tethered jailbreak has the property that if the user turns the device off and back on, the device will completely start up and will **no longer have a patched kernel**, but it will still be **usable for normal functions**. To use jailbroken addons, the user need to start the device with the help of a **jailbreaking tool**

Tethered Jailbreaking

- With a tethered jailbreak, if the device starts back up on its own, it will **no longer have a patched kernel**, and it may get stuck in a partially started state; for it to completely start up with a patched kernel, it must be "re-jailbroken" with a computer (using the "boot tethered" feature of a jailbreaking tool) each time it is turned on

Semi-untethered Jailbreaking

- A semi-untethered jailbreak is similar to a semi-tethered jailbreak. In this type of a jailbreak, when the device reboots, the kernel is not patched, but the kernel can still be patched without using a computer. This is done using an app installed on the device

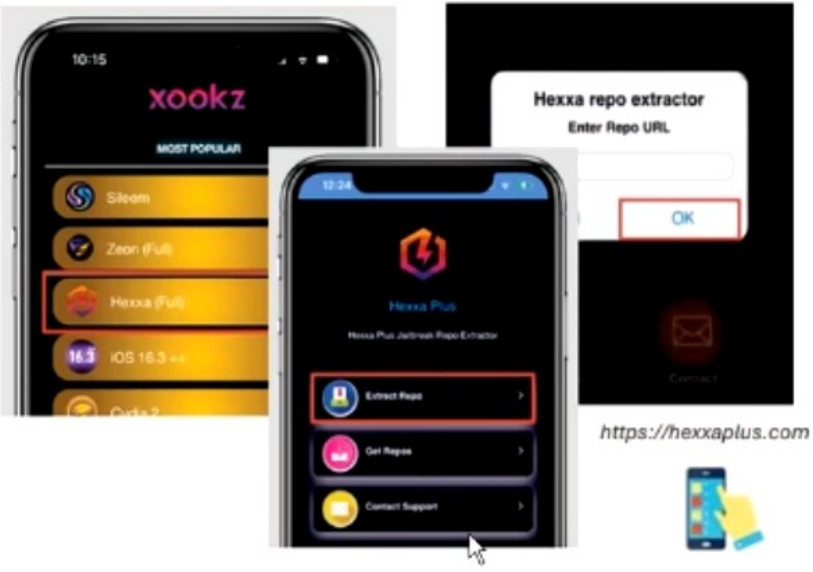
Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Jailbreaking iOS Using Hexxa Plus

- Hexxa Plus is a **jailbreak repo extractor** for the latest iOS, which allows the user to install themes, tweaks, and apps
- Using Hexxa Plus, the user can install the **latest iOS jailbreak** apps by extracting repos

Steps to jailbreak iOS

- Go to Xookz App Store → click on **Hexxa (Full)**
- On the upper right corner, click on **Install** button to receive the configuration profile onto your device
- Navigate to **Settings** → click the profile downloaded from the above step → click on **Install** button
- Enter screen password → click **Install** again
- The Hexxa Plus Repo Extractor icon will appear on the home screen
- Open the **Hexxa Plus** Repo Extractor → click on **Get Repos**
- Choose a desired jailbreaker's repo → copy its URL from the given categories
- Open the **Extract Repo** option → paste the copied URL
- Extract the jailbreaker's repo by clicking the **OK** button



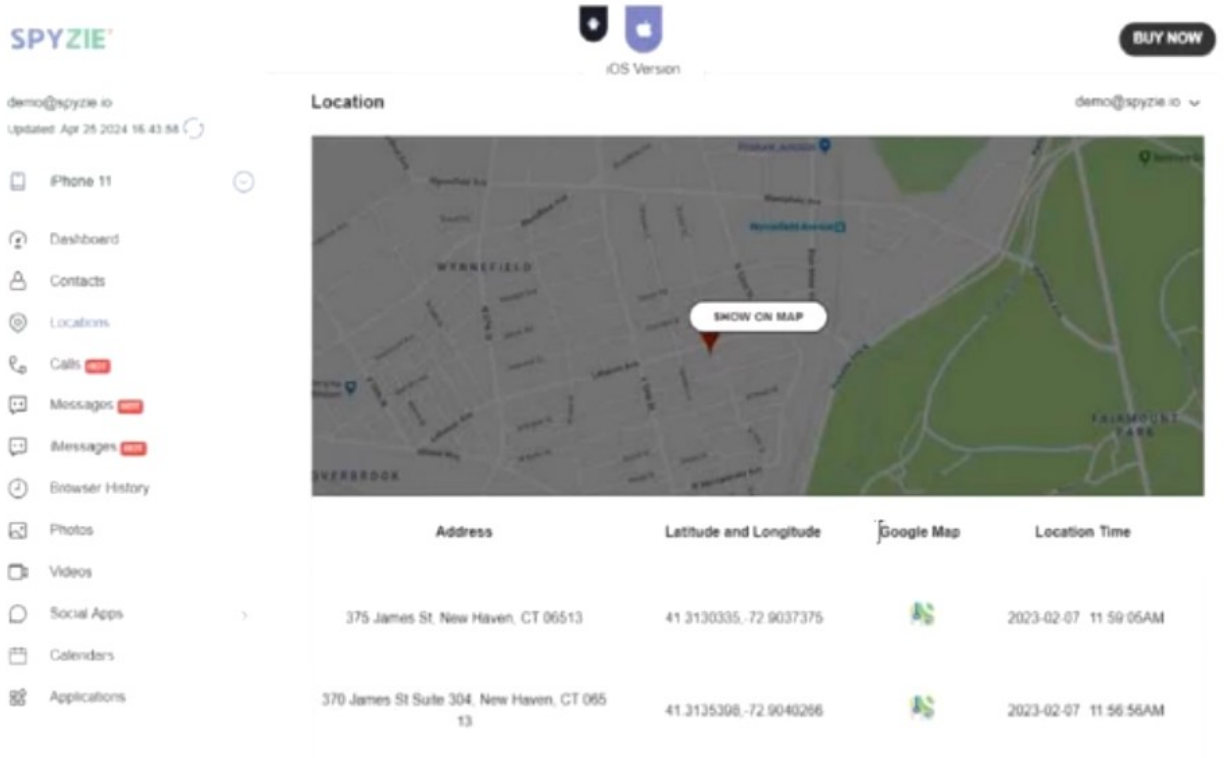
Other Jailbreaking Tools:

Redensa *https://pangu8.com*	**palera1n** *https://palera.in*	**Sileo** *https://en.sileem.com*
checkra1n *https://checkra.in*	**Zeon** *https://zeon-app.com*	**Cydia** *https://www.cydiafree.com*

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Hacking using Spyzie

- Spyzie allows attackers to **hack SMSs**, **call logs**, **app chats**, **GPS**, etc.
- This tool is compatible with all types of iOS devices, including iPhone, iPad, and iPod
- Attackers hack the target device remotely in an **invisible mode** without even jailbreaking the device

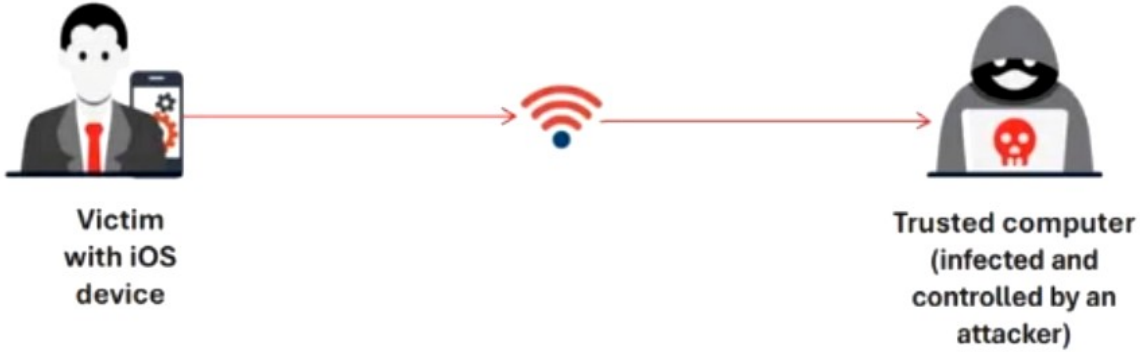


https://spyzie.io

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

iOS Trustjacking

- iOS Trustjacking is a vulnerability that can be exploited by an attacker to read messages and emails and **capture sensitive information** from a remote location without the victim's knowledge
- This vulnerability exploits the "**iTunes Wi-Fi Sync**" feature, where the victim connects their phone to any trusted computer that is already infected by an attacker



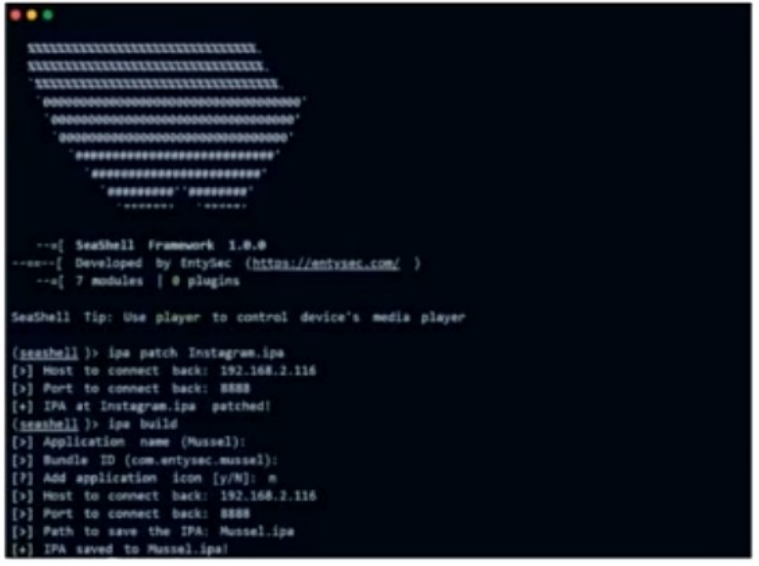
https://www.broadcom.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Post-exploitation on iOS Devices Using SeaShell Framework

SeaShell Framework

SeaShell Framework is an iOS post-exploitation framework that allow attackers to **remotely access**, **control**, and **extract sensitive information** from compromised devices



https://github.com

SeaShell Framework Commands for Post-exploitation

1. Run the following command to patch an **IPA file** and provide IP address and port number to **establish a connection**:
   - **ipa patch Instagram.ipa**
2. Now, run the following command to start a **listener** on host and port added to the patched IPA.:
   - **listener on <IP address> <Port no>**
3. Run the following command to **interact** with the **compromised device** by implementing **Pwny**:
   - **devices -i <id>**
4. Once the remote interaction is successfully established, run the following command to access web browsing history:
   - **safari_history**

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Analyzing and Manipulating iOS Applications

Manipulating an iOS Application Using Cycript

- Cycript is a **runtime manipulation tool** used by attackers to exploit the vulnerabilities in source code and modify the functionality during application runtime
- Cycript is a JavaScript (JS) interpreter that can understand Objective-C, Objective-C++, and JS commands
- Using Cycript, attackers can perform various activities such as **method swizzling**, **authentication bypass**, and **jailbreak detection bypass**

```
cy# var a = [2, 4, 6]
[2,4,6]
cy# [a objectAtIndex:0]
@2
cy# [a setObject:"hello" atIndex:2]; a
[2,4,@"hello"]
cy# var o = {field: 4}
{field:4}
cy# [o setObject:a forKey:"value"]; o
{field:4,value:[2,4,@"hello"]}
```

http://www.cycript.org

iOS Method Swizzling

- Method swizzling, also known as **monkey patching**, is a technique that involves modifying the existing methods or **adding new functionality** at runtime
- Objective-C runtime enables the switching of the method functionality from an existing functionality to a customized one
- Attackers use this technique to perform logging, **JavaScript injections**, **detection bypass**, and **authentication bypass**

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

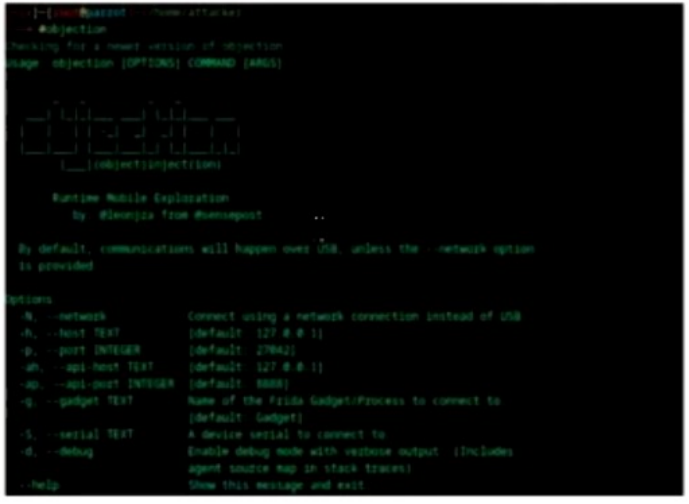
Analyzing and Manipulating iOS Applications (Cont'd)

Extracting Secrets Using Keychain Dumper

- iOS devices contain an **encrypted storage system** called a keychain that stores secrets such as passwords, certificates, and encryption keys
- Attackers use tools such as **Keychain Dumper** to extract keychains from the target iOS device

Analyzing an iOS Application Using objection

- Attackers use the objection tool to perform **method hooking**, **bypass SSL pinning**, and **bypass jailbreak detection** on the target iOS device



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Analyzing iOS Devices

Analyzing iOS devices allows attackers to understand the system's **architecture**, uncover **vulnerabilities**, and identify **exploitable weaknesses**

Techniques	Descriptions
Accessing the Device Shell	• Install the OpenSSH package in the iOS device and connect both iOS device and the host computer to the same Wi-Fi network • Run the **root@<device_ip_address>** command to access the remote device's shell
Listing installed apps	• Use tools such as Frida and run the **frida-ps –Uai** command to list all the apps currently installed on the device
Network sniffing	• Run the **rvictl -s <UDID of the iOS device>** command in the Terminal to start the device with **rvi0** interface • Start the Wireshark tool and choose the interface as "**rvi0**" • Filter the traffic using capture filters for specific monitoring **ip.addr == 192.168.2.4 && http**
Obtain open connections	• Run the **lsof -i** command to obtain a list of open network ports for all active processes on the device
Process exploration	• Use tools such as **r2frida** along with a target app such as **iGoat-Swift**. After establishing an **r2frida** session, run the **:dm** command to retrieve the app's memory maps

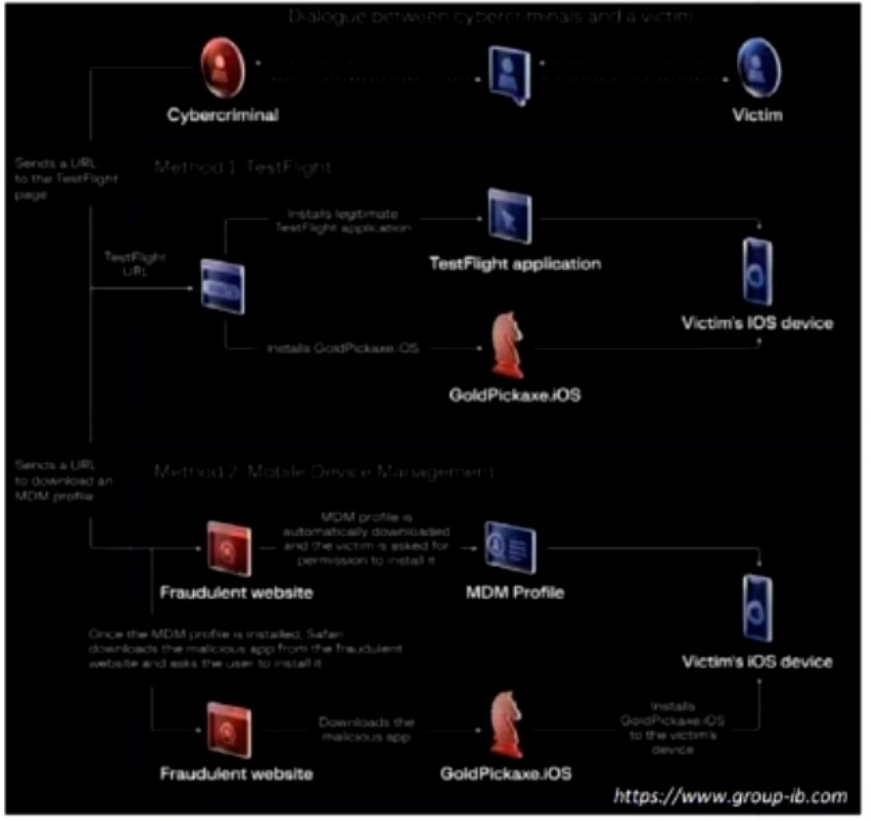
https://mas.owasp.org

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

iOS Malware

GoldPickaxe

- GoldPickaxe Trojan allows attackers to trick victims into **scanning their faces** including their **identification documents**
- The attackers ask the victims to install a masked form of **MDM profile** that allows them remotely configure the target iOS devices by sending **profiles** and **commands**



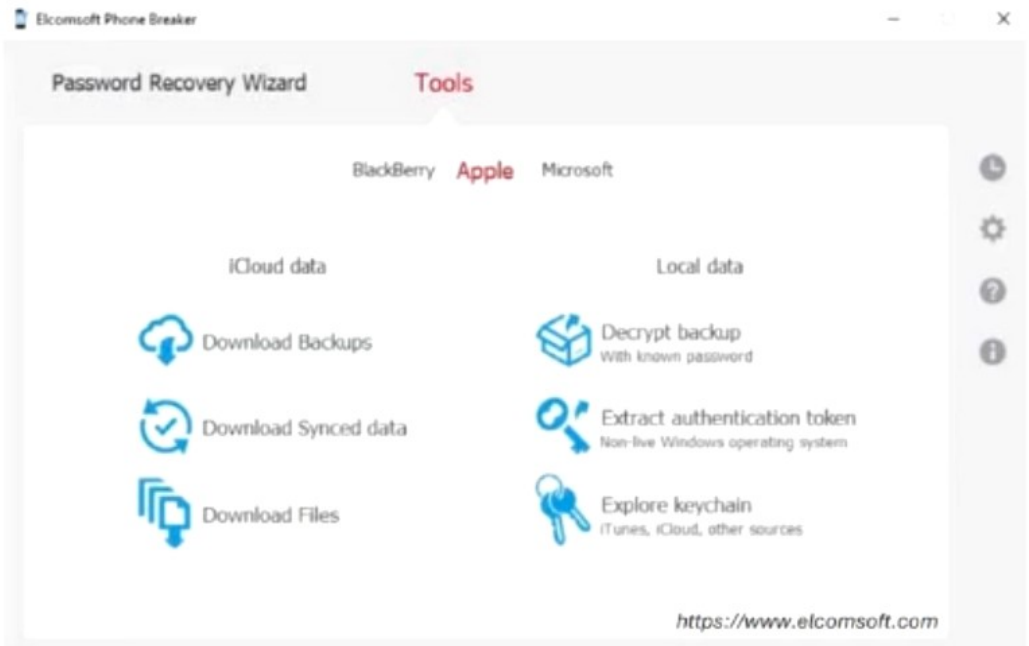
- SpectralBlur
- Mercenary Spyware
- LightSpy
- KingsPawn
- Pegasus

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

iOS Hacking Tools

Elcomsoft Phone Breaker

Elcomsoft Phone Breaker allows attackers to **perform logical and over-the-air acquisition of iOS devices**, break into encrypted backups, and obtain and analyze backups, synchronized data, and passwords from Apple iCloud



Enzyme
https://github.com

Network Analyzer: net tools
https://apps.apple.com

iOS Binary Security Analyzer
https://github.com

iWepPRO
https://apps.apple.com

Frida
https://frida.re

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Securing iOS Devices

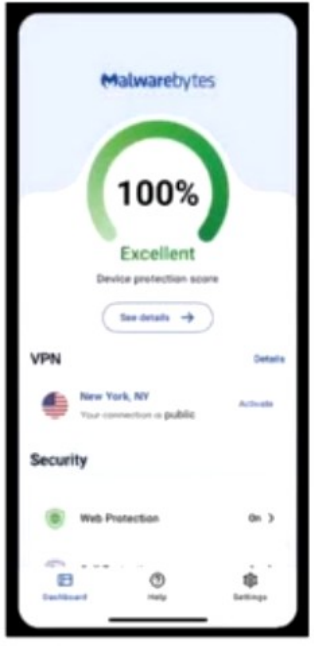
1. Use **passcode lock** feature for locking iPhone
2. Only use iOS devices on **secured** and **protected** Wi-Fi networks
3. Do not access web services on a **compromised network**
4. Deploy only **trusted** third-party **applications** on iOS devices
5. Disable **Javascript** and **add-ons** from web browser
6. Do not store sensitive data on **client-side database**
7. Do not open **links** or **attachments** from unknown sources
8. Change default password of iPhone's **root password** from **alpine**
9. **Do not jailbreak** or **root your device** if used within enterprise environments
10. Configure **Find My iPhone** and utilize it to wipe a lost or stolen device
11. **Enable Jailbreak detection** and also protect access to **iTunes AppleID** and **Google accounts**, which are tied to sensitive data
12. Regularly update your device OS with **security patches** released by Apple

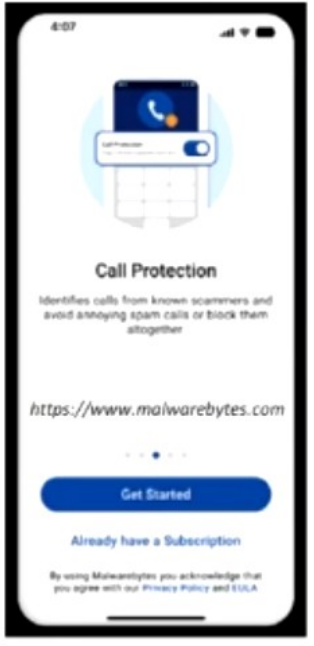
Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

iOS Device Security Tools

Malwarebytes Mobile Security

Malwarebytes Mobile Security tool **filters text messages**, **blocks** intrusive **ads**, fraudulent **calls**, **phishing sites**, and malicious content, and offers a **VPN service** that encrypts connections





- **Norton Mobile Security for iOS**
  https://us.norton.com
- **McAfee Mobile Security**
  https://www.mcafee.com
- **Trend Micro™ Mobile Security for iOS**
  https://www.trendmicro.com
- **AVG Mobile Security**
  https://www.avg.com
- **Kaspersky Standard**
  https://www.kaspersky.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

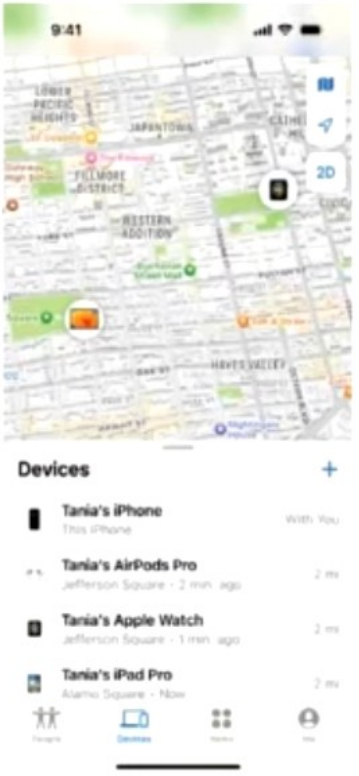
iOS Device Tracking Tools

Find My

- Find My iPhone helps **locate and protect Apple devices** that are lost or stolen
- It helps **locate a missing device on a map**, **remotely lock it**, play a sound, display a message, and remotely erase all data on it

How to Setup Find My for iPhone, iPad, or iPod Touch

- Open the **Settings** app
- Tap **Settings → [your name] → Find My**
- Tap **Find My [device]** and then turn on **Find My [device]**
- To view the device even when it is offline, **turn on Find My network**



https://support.apple.com

mSpy
https://www.mspy.com

Prey Find My Phone & Security
https://apps.apple.com

Mobile Phone Tracker Pro - SIM
https://apps.apple.com

FollowMee GPS Location Tracker
https://apps.apple.com

Phone Tracker: GPS Location
https://apps.apple.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

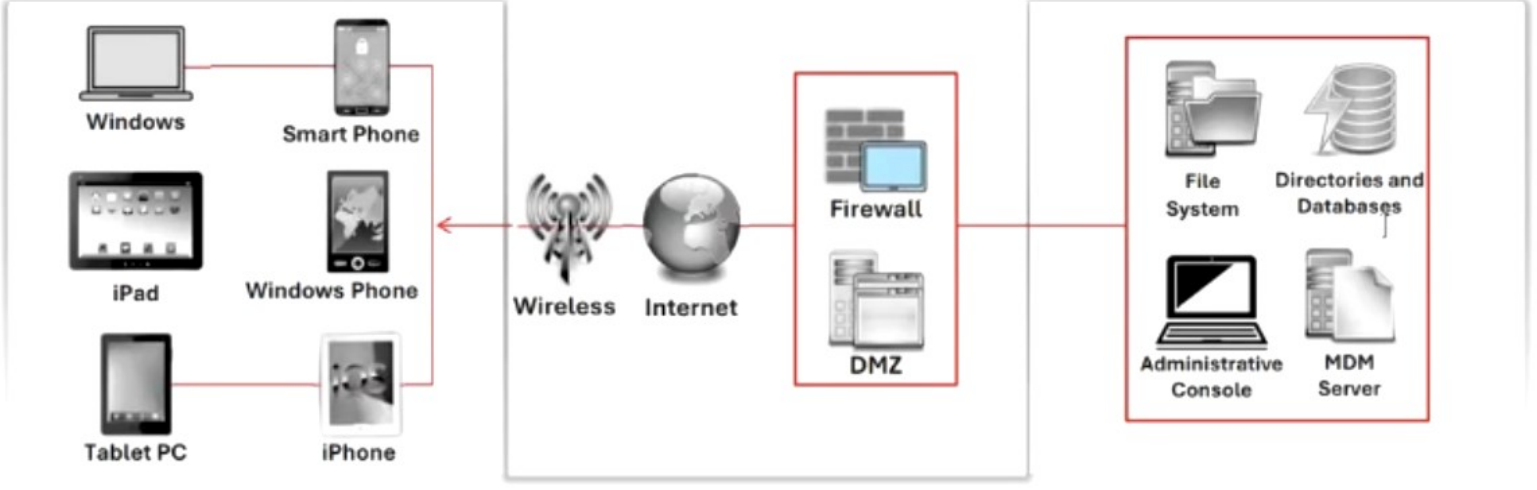
Objective 04

Summarize Mobile Device Management (MDM) Concepts

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Mobile Device Management (MDM)

- Mobile Device Management (MDM) provides platforms for **over-the-air or wired distribution of applications** and data and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablet computers
- MDM helps in implementing **enterprise-wide policies** to reduce support costs, business discontinuity, and security risks
- It helps system administrators to **deploy and manage software applications** across all enterprise mobile devices to secure, monitor, manage, and support mobile devices

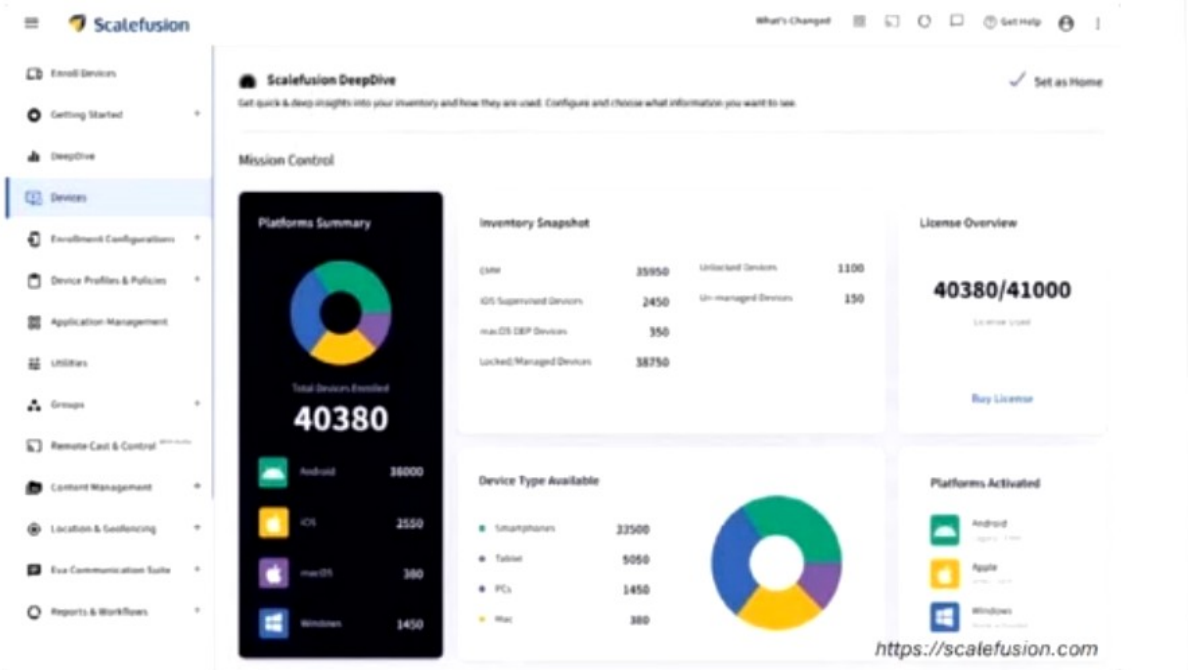


Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Mobile Device Management Solutions

Scalefusion MDM

Scalefusion MDM Software provides comprehensive **visibility** across the network for IT teams and gives control required to **secure**, **manage** and **monitor** any corporate or employee-owned devices



ManageEngine Mobile Device Manager Plus
https://www.manageengine.com

Microsoft Intune
https://www.microsoft.com

SOTI MobiControl
https://soti.net

AppTec360
https://www.apptec360.com

Jamf Pro
https://www.jamf.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Bring Your Own Device (BYOD)

- Bring your own device (BYOD) refers to a policy that allows an employee to bring their **personal devices**, such as laptops, smartphones, and tablets, to their **workplace** and use them to access the organization's resources by following the access privileges
- The BYOD policy allows employees to use the devices that they are **comfortable with** and **best fits their preferences** and work purposes

BYOD Risks

01 Sharing **confidential data** on unsecured networks

02 Data leakage and **endpoint security issues**

03 Improperly **disposing of devices**

04 Support for many **different devices**

05 Mixing personal and **private data**

06 Lost or **stolen devices**

07 Lack of awareness

08 Ability to bypass organization's **network policies**

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

BYOD Security Guidelines

For the Administrator

- Secure organization's data centers with **multi-layered protection systems**
- **Educate your employees** about the BYOD policy
- Make it clear who owns which apps and data
- Use **encrypted channel** for data transfer
- Make it clear which apps will be allowed or banned
- **Control access** based on need-to-know
- Do not allow jailbroken and **rooted devices**
- Apply **session authentication** and **timeout policy** on access gateways

For the Employee

- Use **encryption mechanism** to store data
- Maintain a **clear separation** between business and personal data
- Register devices with a **remote location** and wipe facility if **company policy permits**
- Regularly update your device with **latest OS** and **patches**
- Use **anti-virus** and **data loss prevention** (DLP) solutions
- Set a **strong passcode** on the device and change it relatively often
- Set **passwords for apps** to restrict others from accessing them

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Objective 05

Present Mobile Security Guidelines and Tools

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

OWASP Top 10 Mobile Risks and Solutions

Risks	Solutions
Improper Credential Usage	▪ Avoid using hardcoded credentials ▪ Encrypt credentials during transmission
Inadequate Supply Chain Security	▪ Ensure secure app signing and distribution processes ▪ Use only trusted and validated third-party libraries or components
Insecure Authentication/Authorization Usage	▪ Avoid weak authentication design patterns ▪ Reinforce server-side authentication
Insufficient Input/Output Validation	▪ Implement strict input and output validation techniques ▪ Use data integrity checks and follow secure coding practices
Insecure Communication	▪ Use certificates signed by a trusted CA provider ▪ Ensure that certificates are valid and fail closed

Risks	Solutions
Inadequate Privacy Controls	▪ Protect access must be protected with proper authentication and authorization ▪ Use static and dynamic security checking tools
Insufficient Binary Protections	▪ Use code obfuscation and anti-tampering techniques ▪ Use local security checks, backend enforcement, and integrity checks
Security Misconfiguration	▪ Refrain from using hardcoded default credentials ▪ Disable debugging features in the production version of the app
Insecure Data Storage	▪ Store sensitive data in secure, restricted-access storage locations ▪ Regularly update and patch all libraries, frameworks, and third-party dependencies
Insufficient Cryptography	▪ Use strong encryption algorithms having sufficient key length ▪ Use strong hash functions such as SHA-256 or bcrypt

https://owasp.org

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

General Guidelines for Mobile Platform Security

1. Do not load too many **applications** and avoid auto-upload of photos to **social networks**
2. Perform a **Security Assessment** of the Application **Architecture**
3. Maintain **configuration** control and **management**
4. **Install** applications from trusted application **stores**
5. Securely **wipe or delete** the data when disposing of the device
6. Do not share information within **GPS-enabled apps** unless necessary
7. Disable wireless access, such as **Wi-Fi** and **Bluetooth**, if not in use
8. Never connect two separate networks, such as **Wi-Fi** and **Bluetooth**, simultaneously

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

General Guidelines for Mobile Platform Security (Cont'd)

- Use passcode
- Update OS and Apps
- Enable remote management and use remote wipe services
- Do not allow Rooting or Jailbreaking
- Encrypt storage
- Perform periodic backup and synchronization
- Filter e-mail-forwarding barriers
- Configure Application certification rules
- Harden browser permission rules
- Design and implement mobile device policies

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Mobile Device Security Guidelines for the Administrator

1. Publish an **enterprise policy** that specifies the acceptable usage of consumer grade devices and bring-your-own devices in the enterprise
2. Publish an enterprise policy for the **cloud**
3. Enable **security measures** such as antivirus to protect data in the datacenter
4. Implement policy that specifies what levels of **application and data access** are allowable on consumer-grade devices and which are prohibited
5. Specify a **session timeout** through **Access Gateway**
6. Specify whether the **domain password** can be cached on the device or whether users must enter it every time they request access
7. Determine the allowed **Access Gateway authentication methods** from the following:

- No authentication
- Domain only
- SMS authentication
- RSA SecurID only
- Domain + RSA SecurID

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

SMS Phishing Countermeasures

1. Never reply to a **suspicious SMS** without verifying the source
2. Do not click on any **links** included in an SMS
3. Never reply to an SMS that requests **personal and financial information** from you
4. Review your **bank's policy** on sending SMSs
5. Enable the "**block texts from the internet**" feature from your provider
6. Never reply to an SMS which urging you to **act or respond quickly**
7. **Never call a number** left in an SMS







Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Critical Data Storage in Android and iOS: KeyStore and Keychain Recommendations

Android

- Employ authentication mechanisms such as patterns, **PINs**, passwords, and **fingerprints** to safeguard the keys in Android KeyStore
- Employ a **hardware-backed Android KeyStore** to ensure the security of the data stored
- Use **encryption methods** to store data in a non-readable format
- Implement **authorization techniques** to create and import keys
- Ensure that the keys stored in the server can be accessed only after proper authentication

iOS

- Employ authentication mechanisms such as **Touch ID**, **Face ID**, passcodes, or passwords to safeguard the keychain
- Employ **hardware-backed 256-bit AES** encryption to store critical data
- Use **access-control lists (ACLs)** to specify accessibility to the keychain by applications
- Store only small **chunks of data** directly in the keychain
- Specify **AccessControlFlags** to authenticate the key

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Reverse Engineering Mobile Applications

- Reverse engineering is the process of **analyzing and extracting** the source code of a software or application, and if needed, regenerating it with required modifications
- Reverse engineering is used to **disassemble a mobile application** to analyze its design flaws and fix any bugs that are residing in it

Reverse engineering is used to:

- Read and understand the source code
- Detect underlying vulnerabilities
- Scan for sensitive information embedded in the source code
- Conduct malware analysis
- Regenerate the application after some modifications

Why is reverse engineering effective?

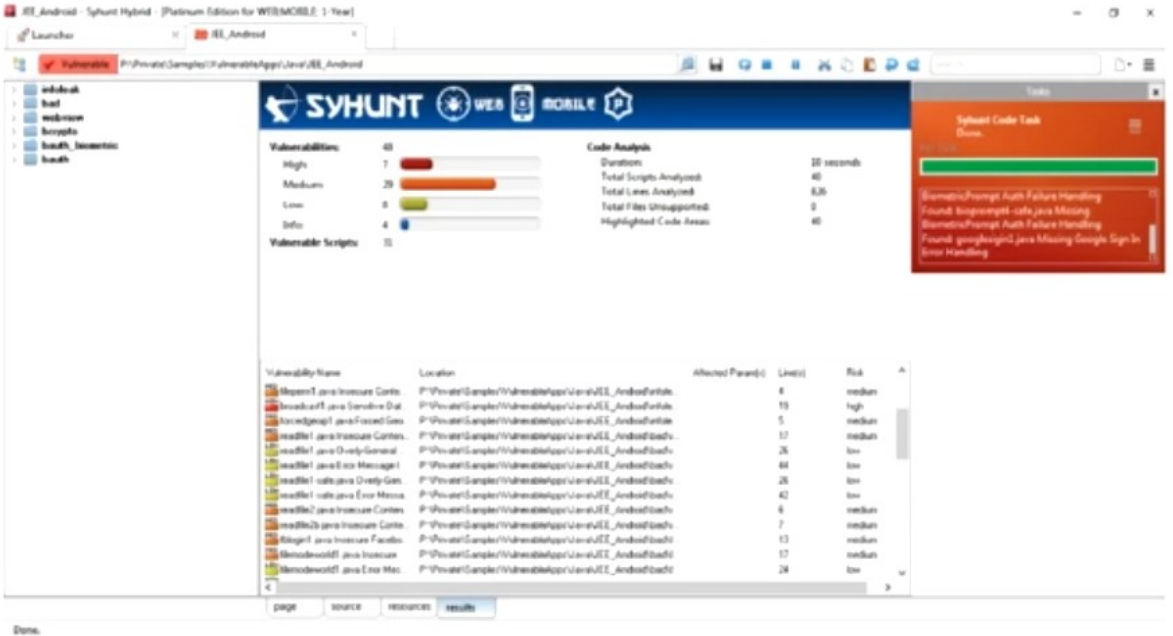
- Initiates security analysis
- Initiates black-box testing on mobiles apps
- Improves static analysis in black-box testing
- Performs resilience assessment
- Performs compliance and auditing

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Source Code Analysis Tools

Syhunt Mobile

Syhunt Mobile analyzes the **source code** of mobile applications and performs over 350 vulnerability checks for Java and **Android**, and 240 vulnerability checks for **iOS**



https://www.syhunt.com

Android lint
https://www.android.com

Zimperium's z3A
https://www.zimperium.com

Appium
https://appium.io

Selendroid
https://selendroid.io

Infer
https://fbinfer.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Reverse Engineering Tools

Apktool | Apktool is **used for reverse engineering third-party**, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications

```
$ apktool d test.apk
I: Using Apktool 2.9.3 on test.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: 1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
$ apktool b test
I: Using Apktool 2.9.3 on test
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

https://apktool.org

Androguard
https://github.com

Frida
https://www.frida.re

JEB
https://www.pnfsoftware.com

APK Editor Studio
https://github.com

Bytecode Viewer
https://github.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

App Repackaging Detectors

Appdome

- Appdome provides defenses against **app tampering**, **reverse engineering**, **method hooking**, and **unauthorized repackaging**
- The **mobile app integrity and checksum validation** feature verifies the integrity of the app by creating checksums for its binary data and structure, preventing **unauthorized modifications** and **fake apps**

https://www.appdome.com

freeRASP for Android/iOS
https://github.com

wultra
https://www.wultra.com

iXGuard
https://www.guardsquare.com

AndroCompare
https://github.com

FSquaDRA 2
https://github.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Mobile Protection and Anti-Spyware Tools

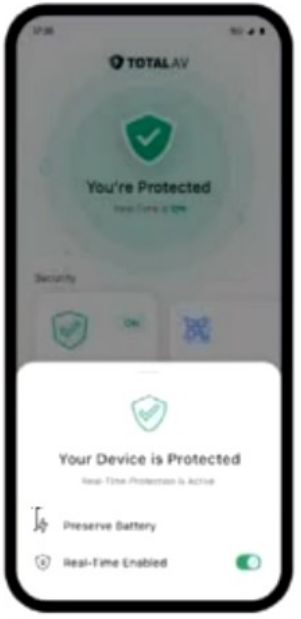
Avast Antivirus & Security

- Avast Antivirus & Security helps users in **scanning** and **securing their devices** against viruses and other malware components, strengthening privacy, and experiencing faster performance
- The tool performs automated scans to **detect threats** and **vulnerabilities**, and blocks malicious apps before getting installed

https://play.google.com

TotalAV

- TotalAV is a comprehensive security tool designed to **detect** and **halt** various forms of **spyware** that aim to snoop on and exploit users' data for financial gain



https://www.totalav.com

Other Mobile Protection Tools:

- **Comodo Mobile Security** — *https://www.comodo.com*
- **AVG Mobile Security** — *https://github.com*
- **Norton Mobile Security for iOS** — *https://us.norton.com*
- **Certo: Anti Spyware & Security** — *https://play.google.com*

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Mobile Pen Testing Toolkits

ImmuniWeb® MobileSuite

ImmuniWeb® MobileSuite leverages machine learning technology to augment and accelerate **manual mobile penetration testing** of iOS and Android mobile applications

https://www.immuniweb.com

Codified Security
https://codifiedsecurity.com

Astra Security
https://www.getastra.com

Appknox
https://www.appknox.com

Data Theorem's Mobile Secure
https://www.datatheorem.com

MobSF
https://mobsf.live

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Module Summary

In this module, we discussed the following:

- Various mobile platform attack vectors and attacks
- Various techniques and tools for hacking Android devices in detail
- How to secure Android devices along with Android security tools in detail
- Various techniques and tools for hacking iOS devices
- How to secure iOS devices along with iOS security tools in detail
- Importance of mobile device management
- Various countermeasures that can be employed to prevent mobile devices from hacking attempts by threat actors
- How to secure mobile devices using mobile security tools

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform IoT and OT hacking to compromise IoT and OT devices

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org