Hacking Wireless Networks

Module 16

Hacking Wireless Networks

Through radio frequency technology, Wi-Fi allows devices to access wireless networks without cables from anywhere within range of an access point.

ICON KEY

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

Lab Scenario

Wireless networking is revolutionizing the way people work and play. A wireless local area network (WLAN) is an unbounded data communication system, based on the IEEE 802.11 standard, which uses radio frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections. With the need for a physical connection or cable removed, individuals are able to use networks in new ways, and data has become ever more portable and accessible.

Although wireless networking technology is becoming increasingly popular, because of its convenience, it has many security issues, some of which do not exist in wired networks. By nature, wirelessly transferred data packets are airborne and available to anyone with the ability to intercept and decode them. For example, several reports have demonstrated the weaknesses in the Wired Equivalent Privacy (WEP) security algorithm, specified in the 802.11x standard, which is designed to encrypt wireless data.

As an ethical hacker or penetration tester (hereafter, pen tester), you must have sound knowledge of wireless concepts, wireless encryption, and related threats in order to protect your company's wireless network from unauthorized access and attacks. You should determine critical sources, risks, or vulnerabilities associated with your organization's wireless network, and then check whether the current security system is able to protect the network against all possible attacks.

Lab Objectives

The objective of the lab is to protect the target wireless network from unauthorized access. To do so, you will perform various tasks that include, but are not limited to:

- Discover Wi-Fi networks
- Capture and analyze wireless traffic
- Crack WEP, WPA, and WPA2 Wi-Fi networks

Lab Environment

Tools demonstrated in this lab are available at E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection

- Administrator privileges to run the tools

Lab Duration

Time: 125 Minutes

Overview of Wireless Networking

In wireless networks, communication takes place through radio wave transmission, which usually takes place at the physical layer of the network structure. Thanks to the wireless communication revolution, fundamental changes to data networking and telecommunication are taking place. This means that you will need to know and understand several types of wireless networks. These include:

- **Extension to a wired network**: A wired network is extended by the introduction of access points between the wired network and wireless devices
- **Multiple access points**: Multiple access points connect computers wirelessly
- **LAN-to-LAN wireless network**: All hardware APs have the ability to interconnect with other hardware access points
- **3G/4G hotspot**: A mobile device shares its cellular data wirelessly with Wi-Fi-enabled devices such as MP3 players, notebooks, tablets, cameras, PDAs, and netbooks

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack target wireless networks. The recommended labs that will assist you in learning various wireless network hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint a Wireless Network	√		
	1.1 Find Wi-Fi Networks in Range using NetSurveyor	√		
2	Perform Wireless Traffic Analysis	√		√
	2.1 Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark	√		√
3	Perform Wireless Attacks	√	√	√
	3.1 Find Hidden SSIDs using Aircrack-ng		√	
	3.2 Crack a WEP Network using Wifiphisher		√	
	3.3 Crack a WEP Network using Aircrack-ng		√	√
	3.4 Crack a WPA Network using Fern Wifi Cracker	√		

	3.5 Crack a WPA2 Network using Aircrack-ng	√		√
	3.6 Create a Rogue Access Point to Capture Data Packets using MANA-Toolkit		√	

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 CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs 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 iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Requirements

Before you begin the labs in this module, you must configure your environment, so that you can connect your machine to a wireless network. For this purpose, you will need a wireless network adaptor and an access point.

The demonstrations in this lab use a **Linksys 802.11 g WLAN** adapter and **CEH-LABS** as the access point. The **CEH-LABS** access point has been configured with WEP, WPA, and WPA2 encryption as per the lab requirements.

Note: Here, the WEP encryption key is **1234567890**. The WPA and WPA2 encryption password is **password1**.

Note: If you decide to use a different wireless adapter, the steps to set up the adapter might differ.

1. Connect your access point **CEH-LABS**.

   Note: Ensure that wireless router is plugged in to the network/Internet.

2. Turn on the **Windows 10** virtual machine, and log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Lab Prerequisites\Linksys Adapter**, right-click **setup64.exe**, and click the **Troubleshoot compatibility** option.

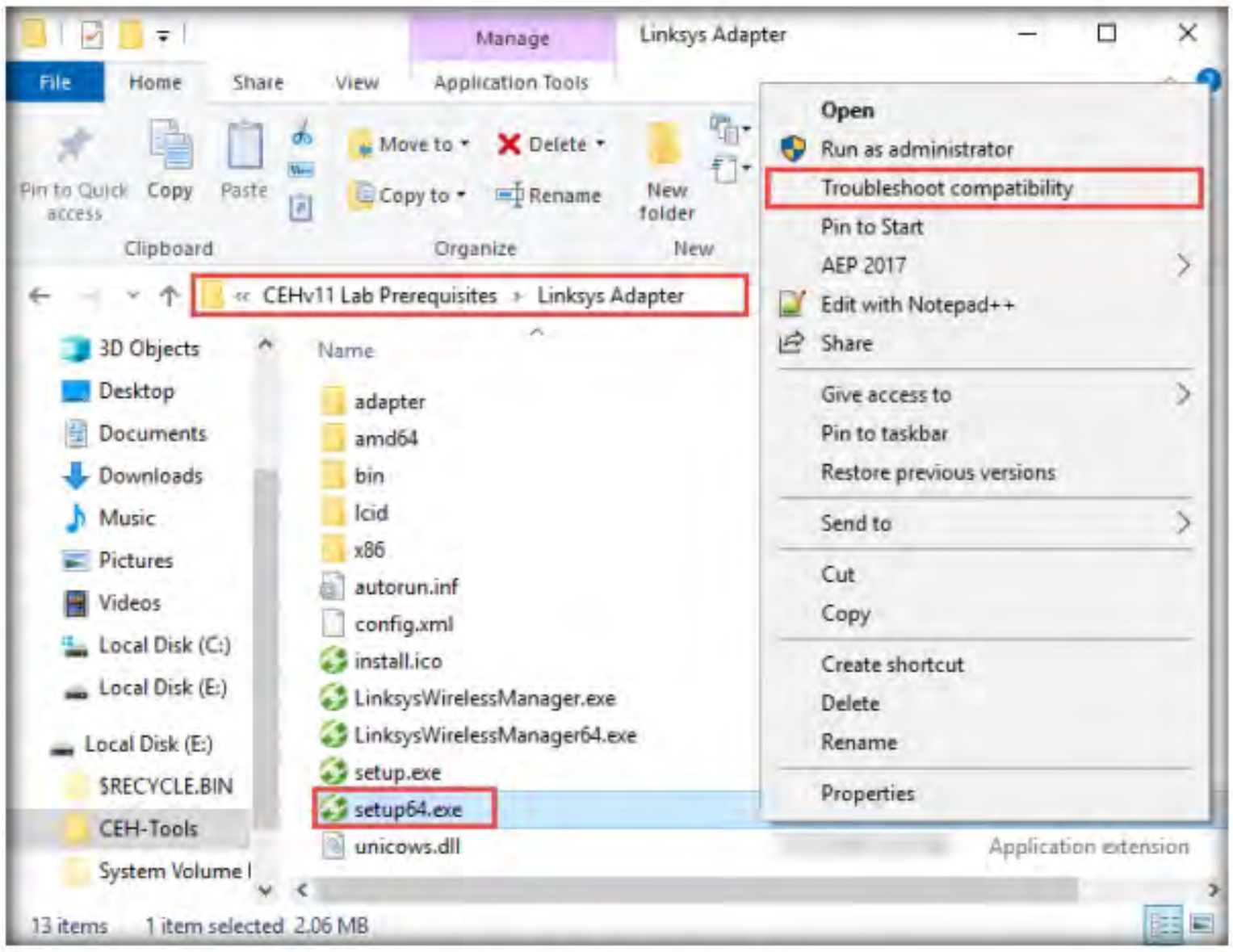

Figure 1: The Linksys Adapter Folder

4. The **Program Compatibility Troubleshooter** wizard appears and begins **Detecting issues**.
5. After the issues have been detected, the **Select troubleshooting option** wizard appears; click **Try recommended settings**.

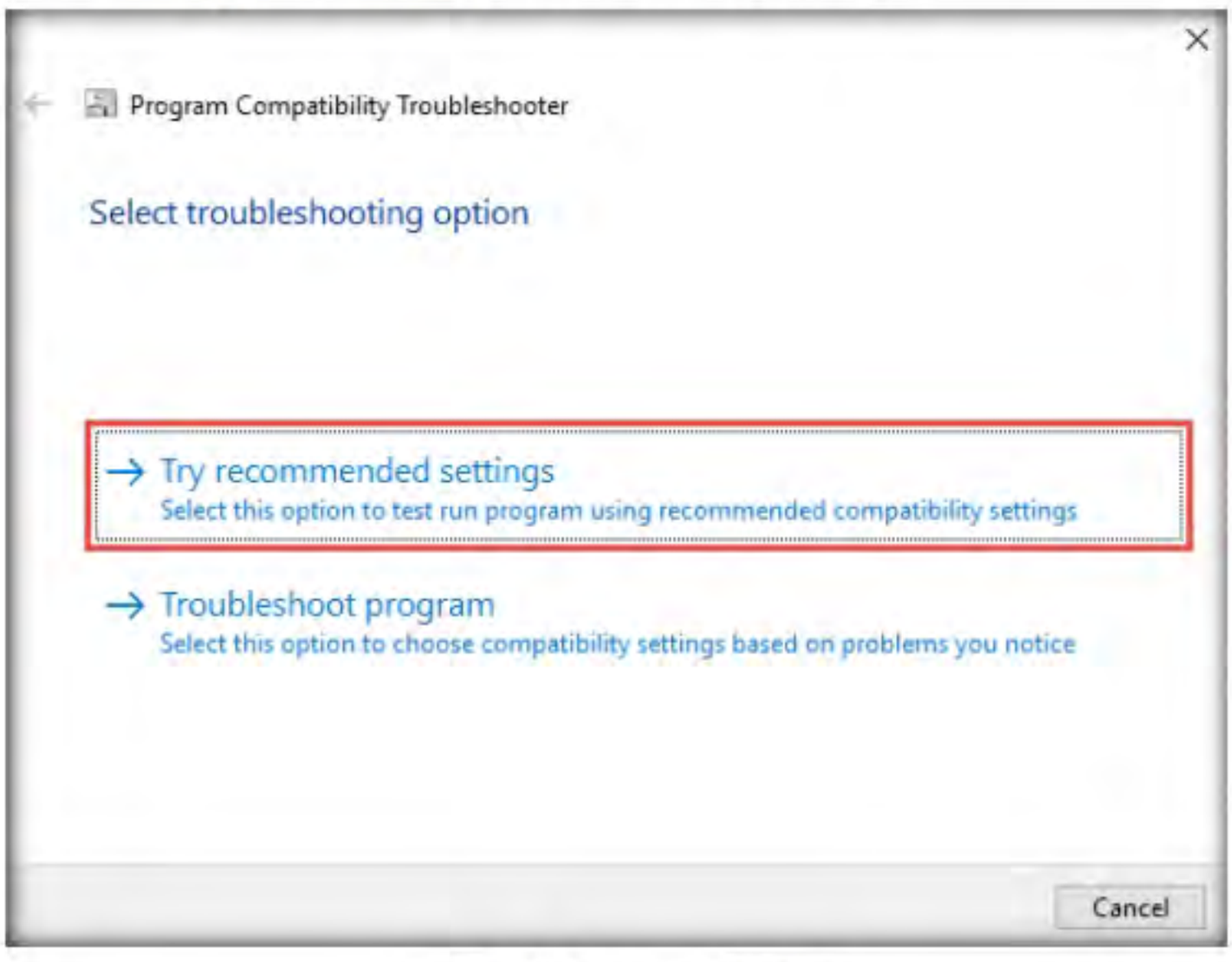

Figure 2: Click Try recommended settings

6. In the **Test compatibility settings for the program** wizard, click **Test the program...**

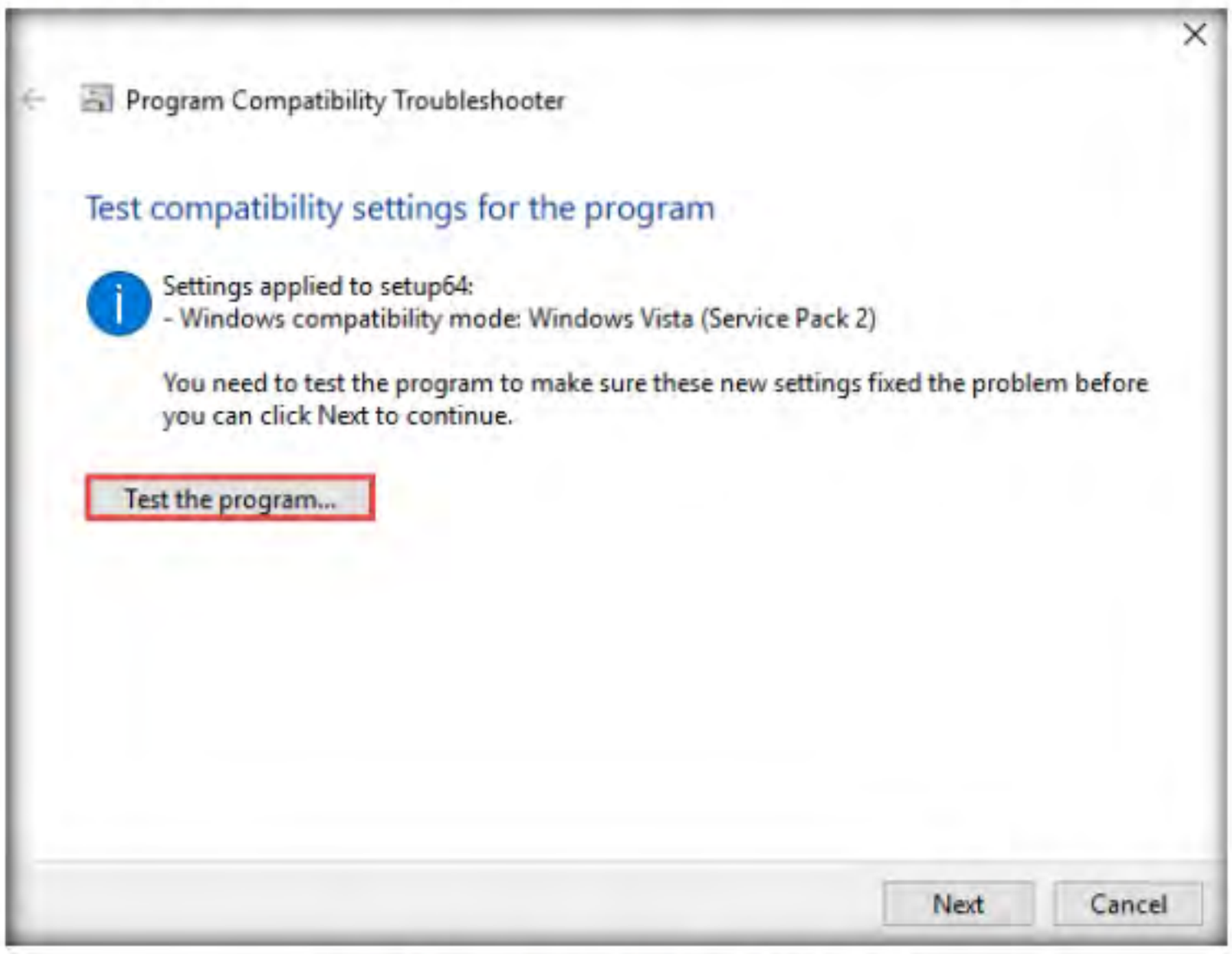

Figure 3: Program Compatibility Troubleshooter wizard

7. A **User Account Control** pop-up appears; click **Yes**.
8. The **Linksys Adapter Setup Wizard** appears; click **Next**.

Figure 4: Linksys Adapter Setup Wizard

9. In the **License Agreement** wizard, check the **I accept this agreement** checkbox and click **Next**.
10. The **Preparing System for Install** wizard appears; wait for it to complete.

Figure 5: Preparing System for Install wizard

11. The **Insert Adapter** wizard appears. Plug your **Linksys 802.11 g WLAN** adapter into an available USB port.

Figure 6: Insert Adapter wizard

12. After connecting the **Linksys 802.11 g WLAN** adapter, 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 **Windows 10**; click **OK**.

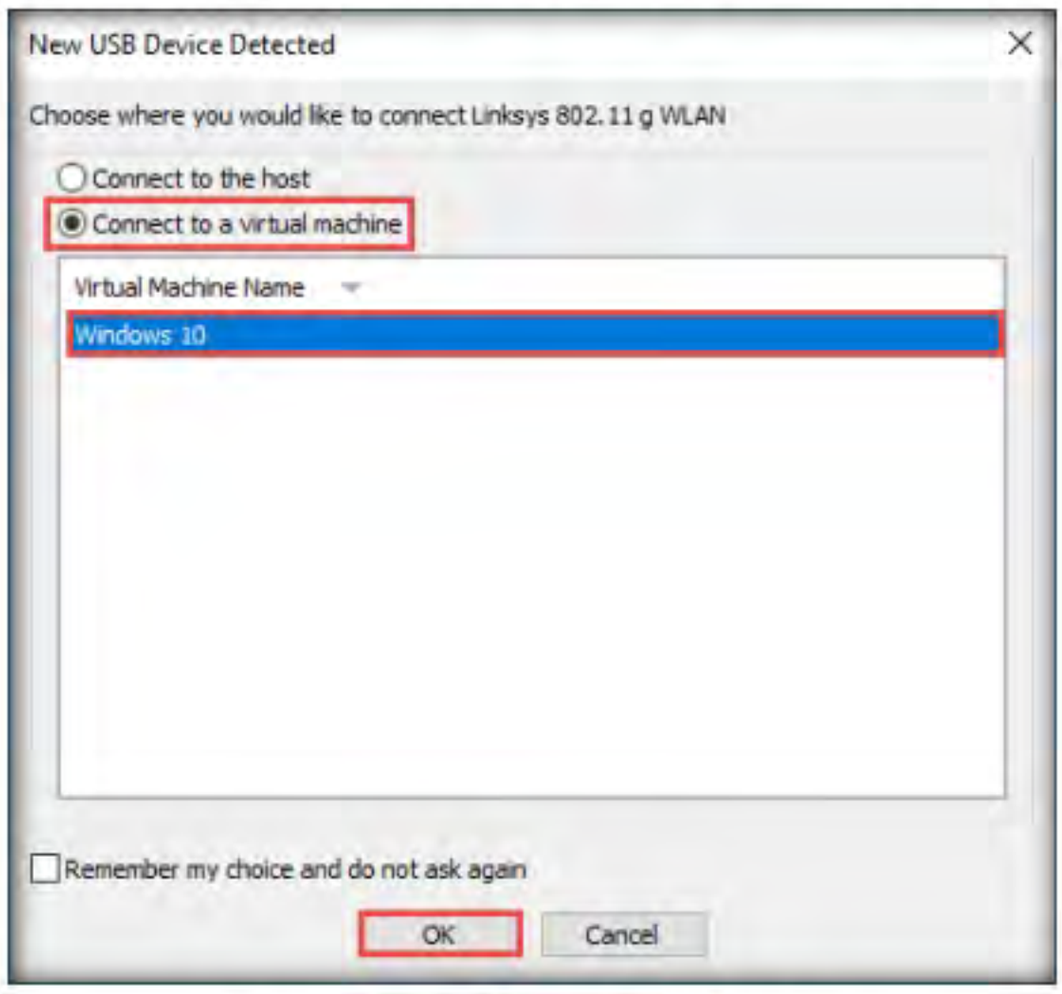

Figure 7: New USB Device Detected window

13. In the **Linksys Adapter Setup Wizard** window, observe that the adapter starts **Installing....**

14. After the installation completes, a **Congratulations! Your adapter has been installed correctly** notification appears; click **Next**.

Figure 8: Adapter Installed notification

15. An **Installing Linksys Wireless Manager** wizard appears and installs the Linksys software. On completion, the **Connect to a Wireless Network** wizard appears and the adapter starts searching for available wireless networks.
16. The list of the available wireless network in range appears, as shown in the screenshot.
17. Select **CEH-LABS** and click the **Connect** button.

Figure 9: Connect to a Wireless Network wizard

18. In the **Quickly Connect Using Push Button** wizard, click **Skip**.
19. In the **Connect to a Wireless Network** wizard, type the password of wireless network **CEH-LABS** (in this example, **password1**) in the **Your network requires a security key. Enter it here:** field, and click **Next**.

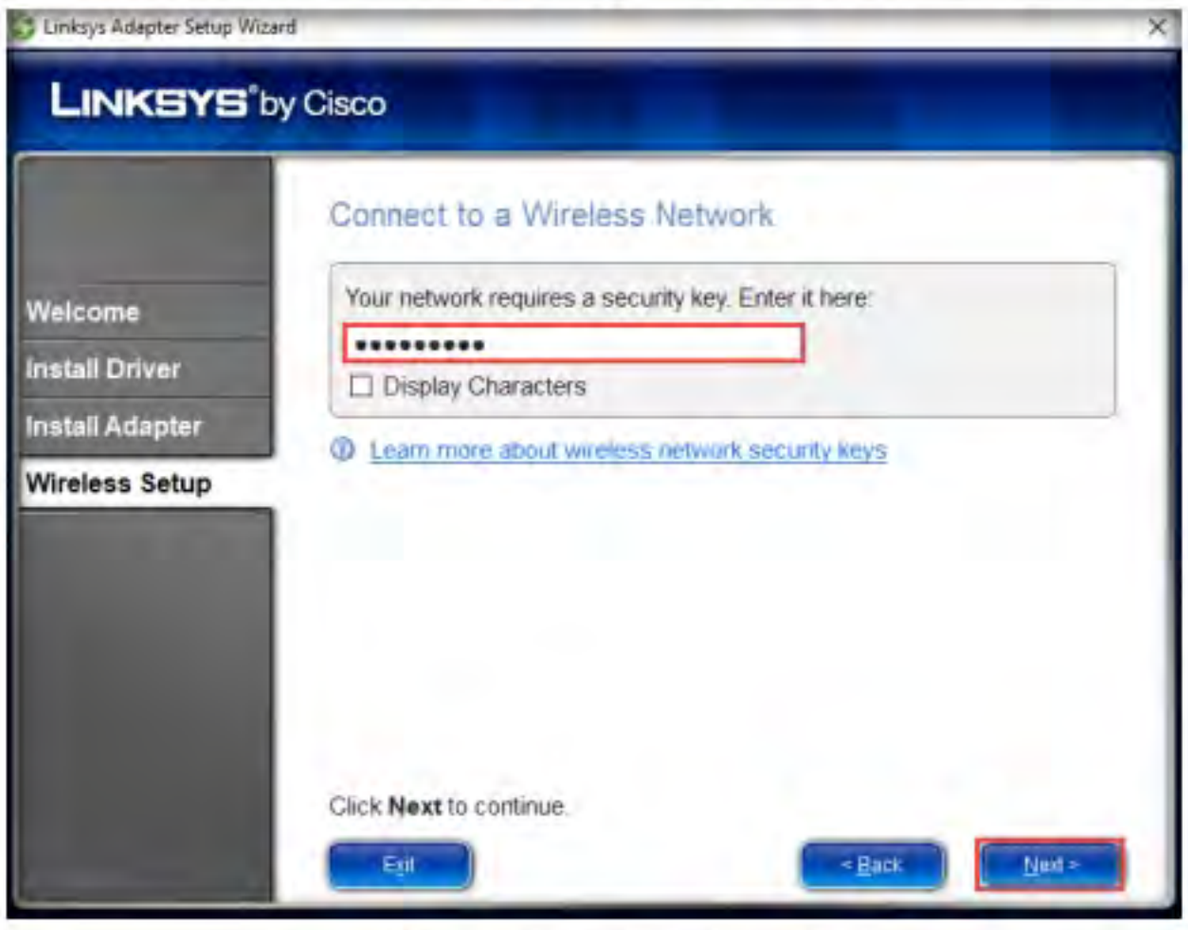

Figure 10: Connect to a Wireless Network wizard

20. The wizard shows the message **Checking Connection** as the adapter attempts to connect to the network.
21. The **Connected to Your Network** screen appears in the wizard once the connection has been established. Click **Finish** to exit the setup.

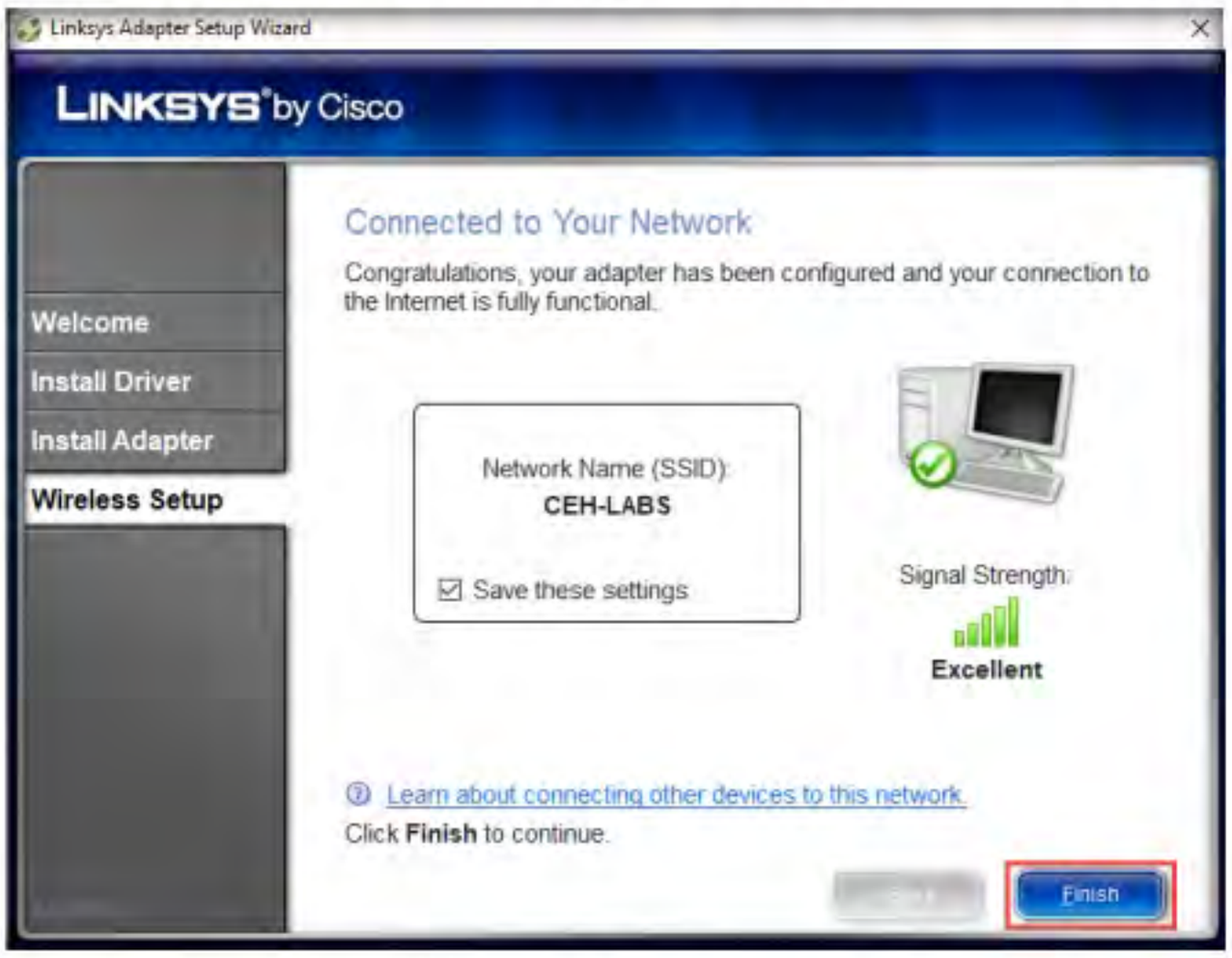

Figure 11: Connected to Your Network message

22. When the **Linksys Adapter Setup Wizard** notification appears, click **OK**.

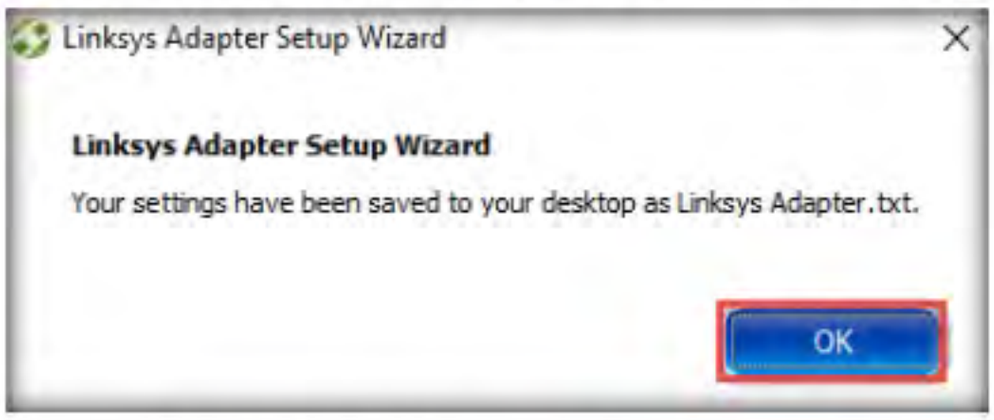

Figure 12: Linksys Adapter Setup Wizard notification

23. A **Manage your wireless networks** pop-up appears, click **OK**.

Figure 13: Manage your wireless networks pop-up

24. Close all windows and click **Show hidden icons** ( ) from the bottom-right corner of **Desktop**. You can observe the **Wireless Network Connection** icon ( ), as shown in the screenshot.

25. You can double-click the **Wireless Network Connection** icon ( ) to manage wireless network connections.

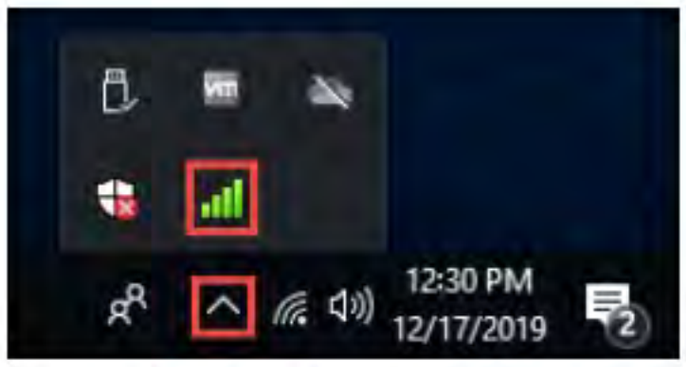

Figure 14: Wireless Network Connection icon

26. Your **Linksys 802.11 g WLAN** adapter has been configured successfully.

27. In this way, you can connect your virtual machines to a wireless network. Repeat these steps if you wish to connect to the wireless network with another virtual machine.

Note: You can use the adapter for only one virtual machine at a time.

Now that we have set up the wireless adapter, we shall disable the ethernet adapter. To do this, follow these steps:

28. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.

29. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.

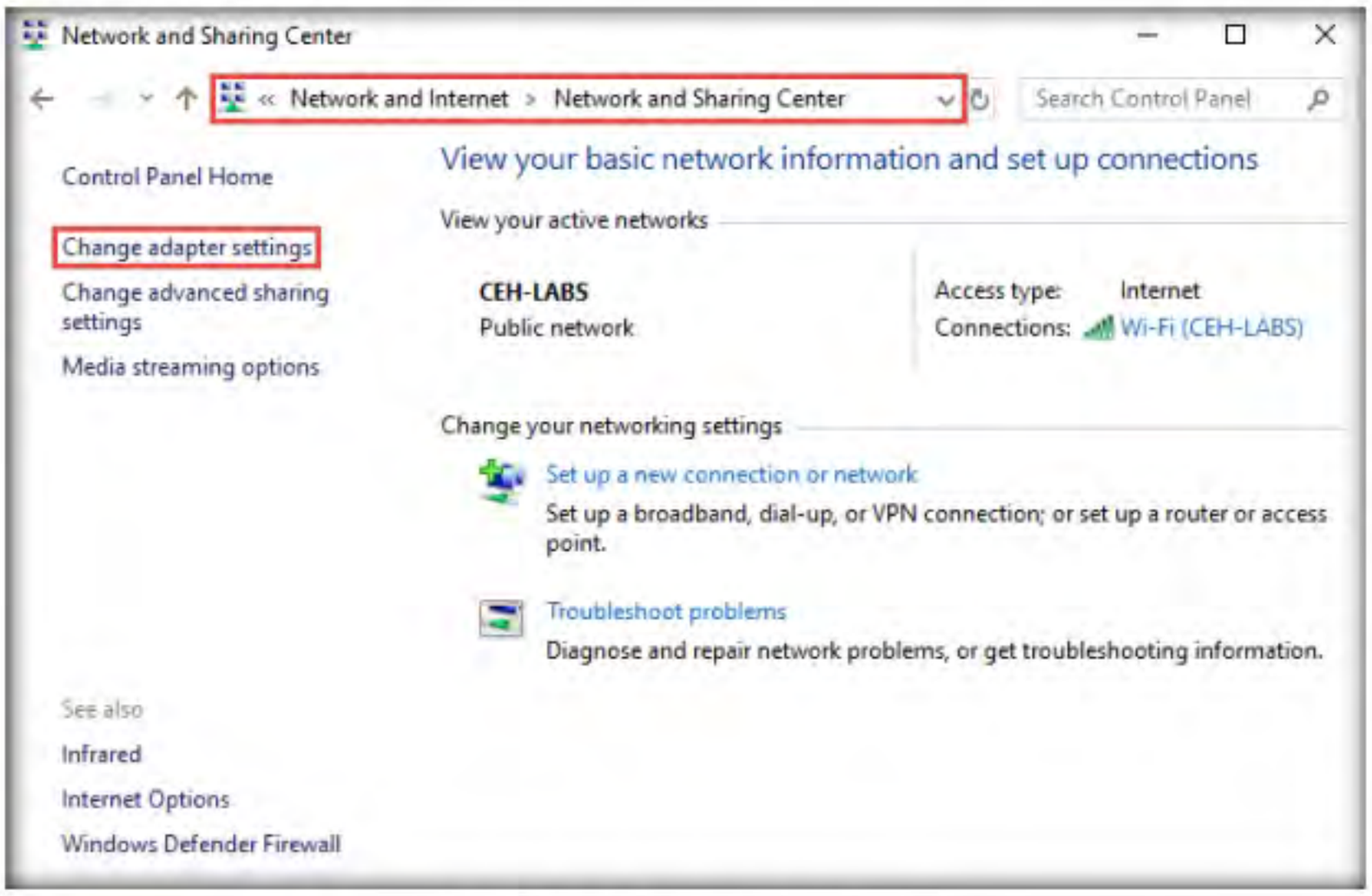

Figure 15: Network and Sharing Center window

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

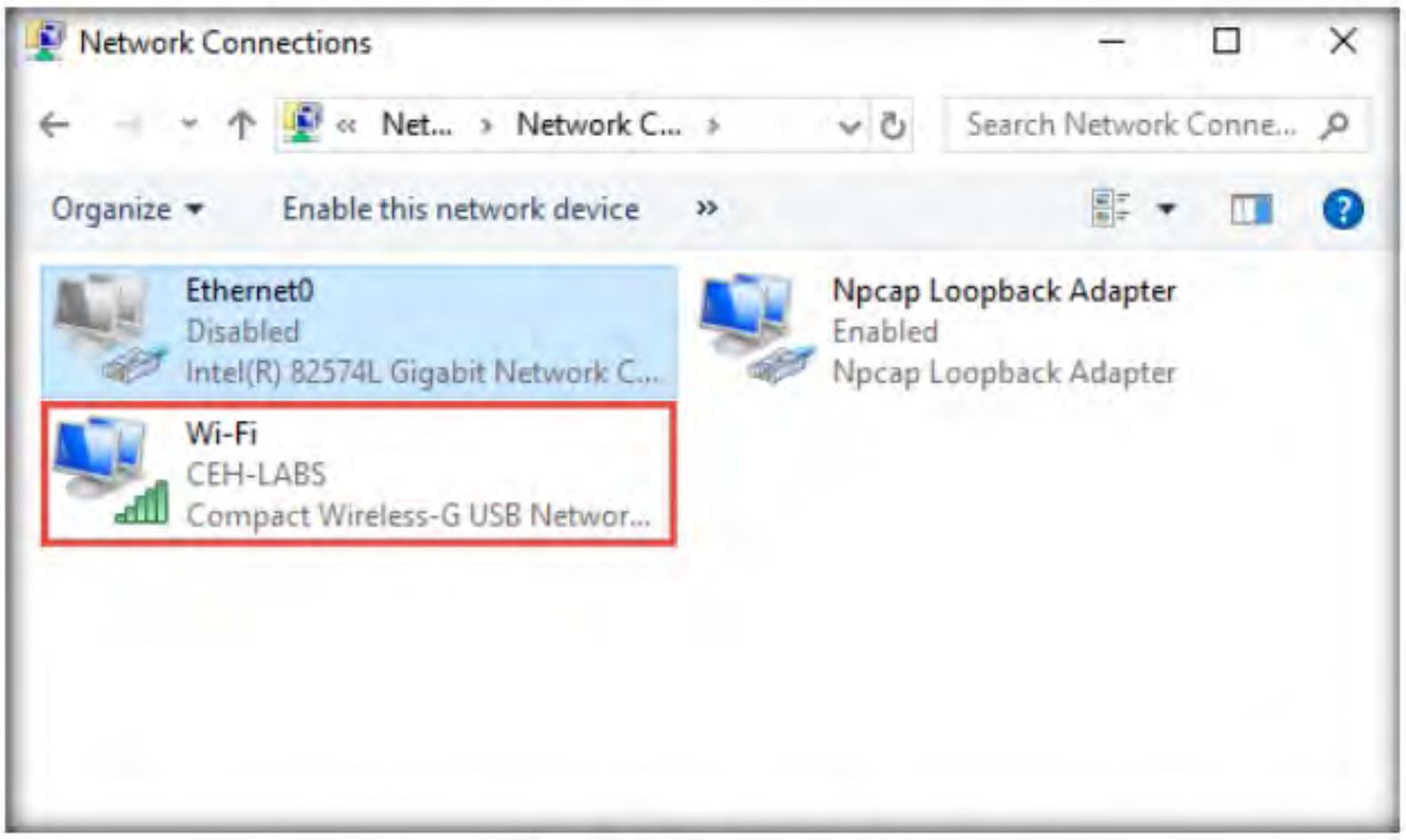

Figure 16: Wi-Fi adapter activated

32. Close all open windows and turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

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

Lab 1

Footprint a Wireless Network

Footprinting a wireless network involves discovering and footprinting the wireless network in an active or passive way.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step in hacking wireless networks is to find a Wi-Fi network or device. You can locate a target wireless network using various Wi-Fi discovery tools and procedures, including wireless footprinting and identifying an appropriate target that is in range.

Attackers scan for Wi-Fi networks with the help of wireless network scanning tools, which tune to the various radio channels of networking devices. The SSID (Service Set Identifier), which is the wireless network's name, is found in beacons, probe requests, and responses, as well as association and re-association requests. Attackers can obtain the SSID of a network by passive or active scanning. After doing so, they can connect to the wireless network and launch attacks.

As an ethical hacker and pen tester, you must perform footprinting to detect the SSID of a wireless network in the target organization. This will help to predict how effective additional security measures will be in strengthening and protecting your target organization's networks.

The labs in this exercise demonstrate how to footprint a wireless network using various tools and techniques.

Lab Objectives

- Find Wi-Fi networks in range using NetSurveyor

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

- NetSurveyor located at **E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor**
- You can also download the latest version of **NetSurveyor** from the official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of Footprinting a Wireless Network

To footprint a wireless network, you must identify the BSS (Basic Service Set) or Independent BSS (IBSS) provided by the access point. This is done with the help of the wireless network's SSID, which can be used to establish an association with the access point to compromise its security. Therefore, you need to find the SSID of the target wireless network.

Footprinting methods to detect the SSID of a wireless network include:

- **Passive Footprinting**, in which you detect the existence of an access point by sniffing packets from the airwaves
- **Active Footprinting**, in which a wireless device sends a probe request with the SSID to see if an access point responds

TASK 1 Find Wi-Fi Networks in Range using NetSurveyor

Here, we will use NetSurveyor to find the Wi-Fi networks in range.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

   Note: Ensure that the **Linksys 802.11 g WLAN** adapter is plugged in and connected to the **Windows 10** virtual machine.

   If the adapter is not connected to the virtual machine, unplug and plug it in again. A **New USB Device Detected** window appears: select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 10**; click **OK**.

TASK 1.1 Install and Launch NetSurveyor

2. Navigate to **E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor** and double-click **NetSurveyor-Setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

NetSurveyor is an 802.11 (Wi-Fi) network discovery tool that gathers information about nearby wireless access points in real-time and displays it in useful ways. It also reports the SSID for each wireless network it detects, along with the channel used by the access point servicing that network. Using NetSurveyor, reports can be generated in Adobe PDF format.

3. The **Setup - NetSurveyor** window appears; click **Next**.

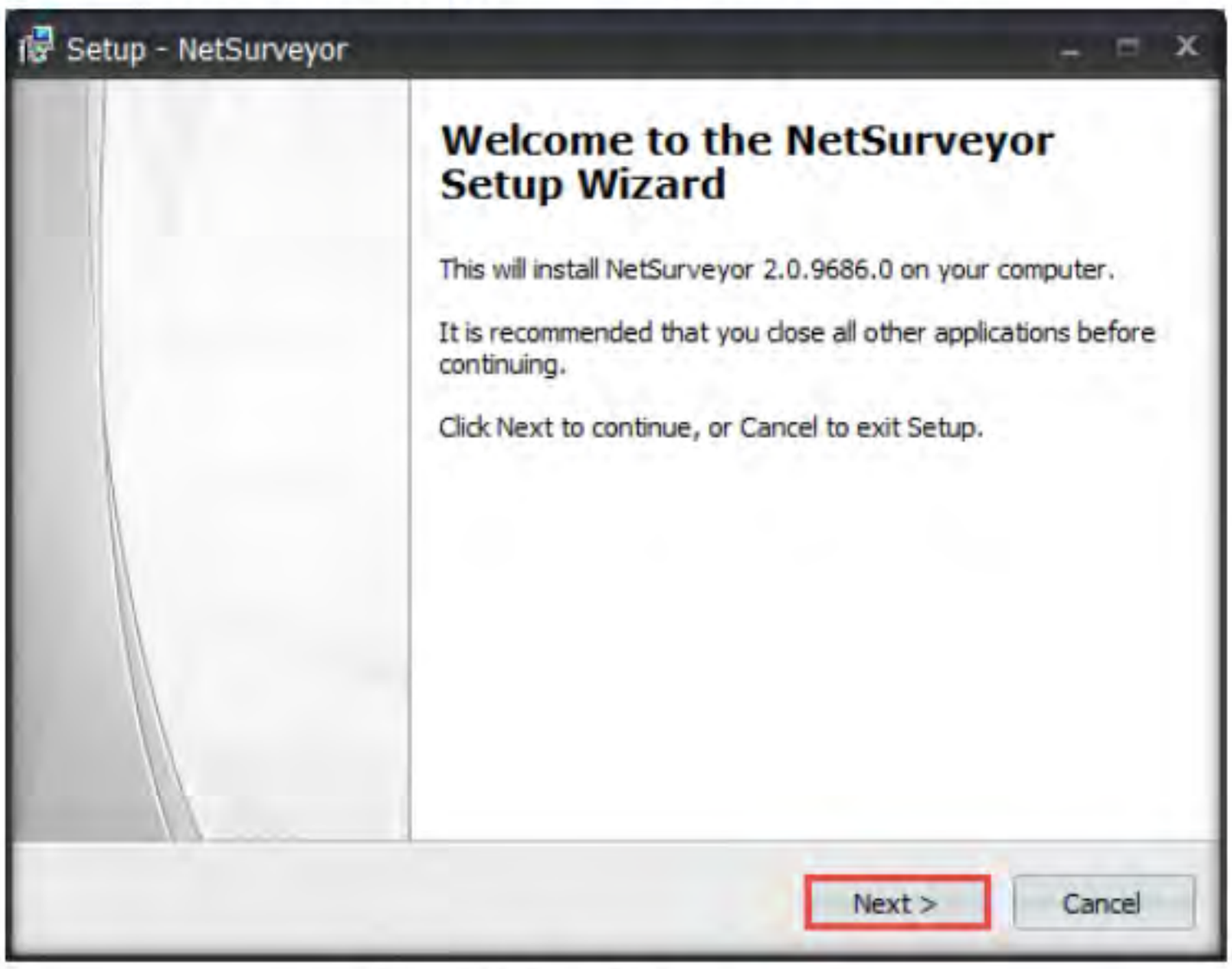

Figure 1.1.1: Setup - NetSurveyor window

4. Follow the steps to install the application using the default settings.
5. After the installation completes, the **Completing the NetSurveyor Setup Wizard** screen appears. Ensure that the **Yes, restart the computer now** radio button is selected and click **Finish**.

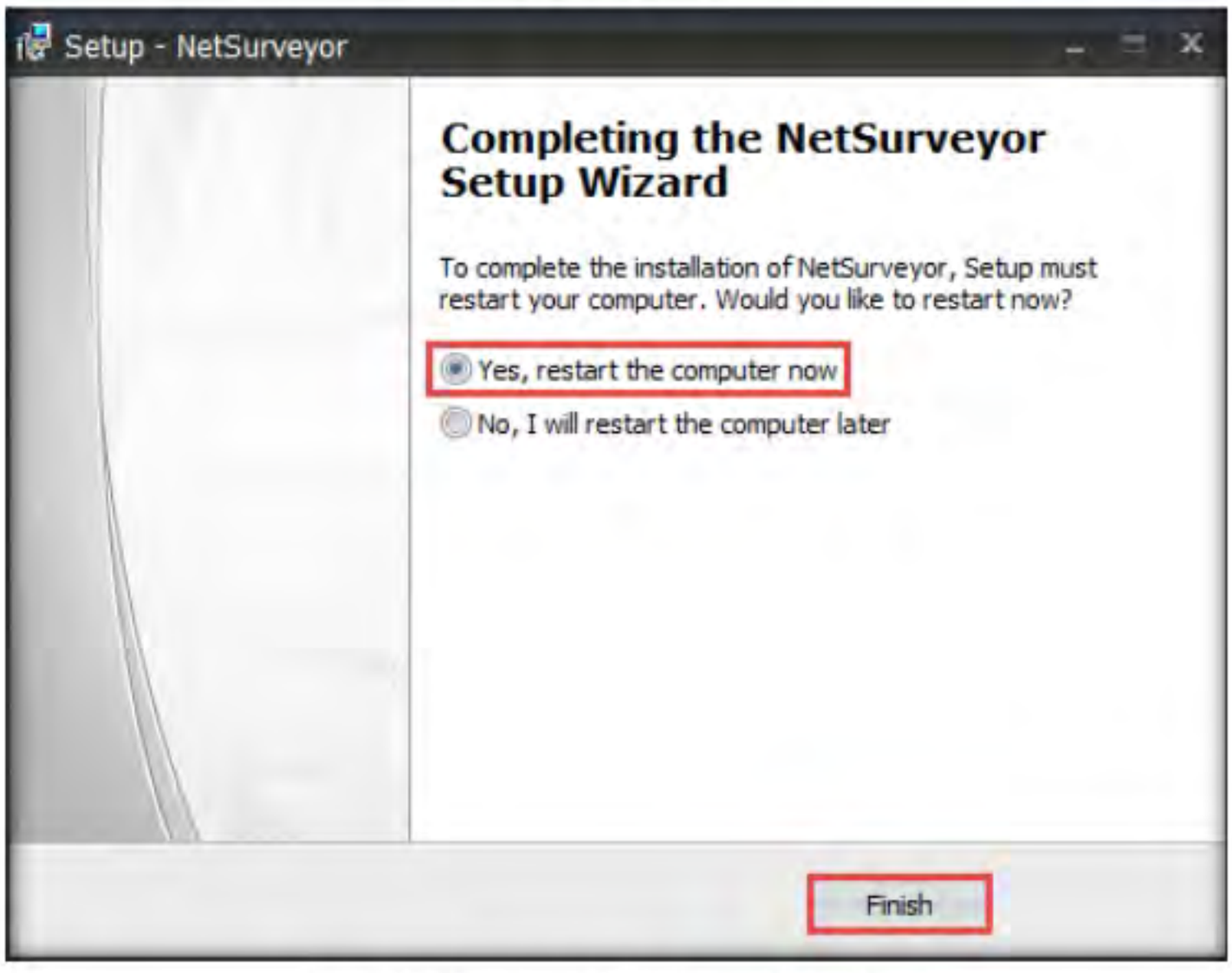

Figure 1.1.2: Completing the NetSurveyor Setup Wizard

6. After the system reboots, log in with the credentials **Admin/Pa$$w0rd**.

Note: Ensure that the **Linksys 802.11 g WLAN** adapter is connected to the **Windows 10** virtual machine.

As before, if the adapter is not connected, unplug and plug it in again. A **New USB Device Detected** window appears: select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 10**; click **OK**.

7. Launch **NetSurveyor** by double-clicking the **NetSurveyor** shortcut from **Desktop**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

TASK 1.2

Discover Access Points in the Network

8. **NetSurveyor** initializes, and a list of discovered access-points in the network appears under the **Network Discovery** tab, along with details such as SSID, BSSID, Channel, Beacon Strength, etc. as shown in the screenshot.

9. In the lower section of the window, the **Channel Usage** tab displays a graphical view of the usage of 802.11 channels by discovered access points.

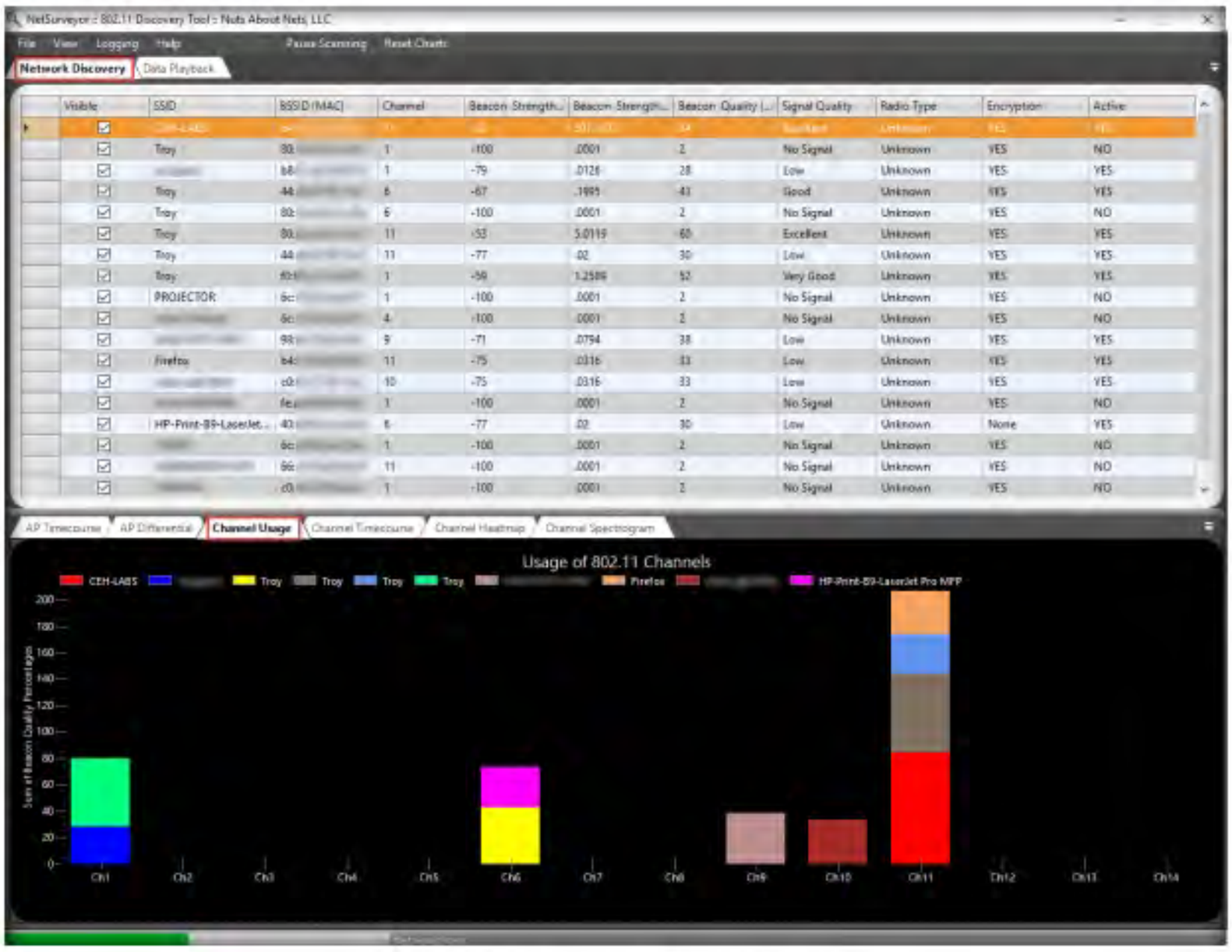

Figure 1.1.3: NetSurveyor: Channel Usage tab

10. In the lower section of the window, click the **AP Timecourse** tab to view the timecourse of Beacon qualities by SSID in a graphical format.

Figure 1.1.4: NetSurveyor: AP Timecourse tab

11. Click the **Channel Spectrogram** tab to view the spectrogram of the 802.11 channel usage. This information can be used to perform spectrum analysis, actively monitor spectrum usage in a particular area, and detect the spectrum signal of the target network.

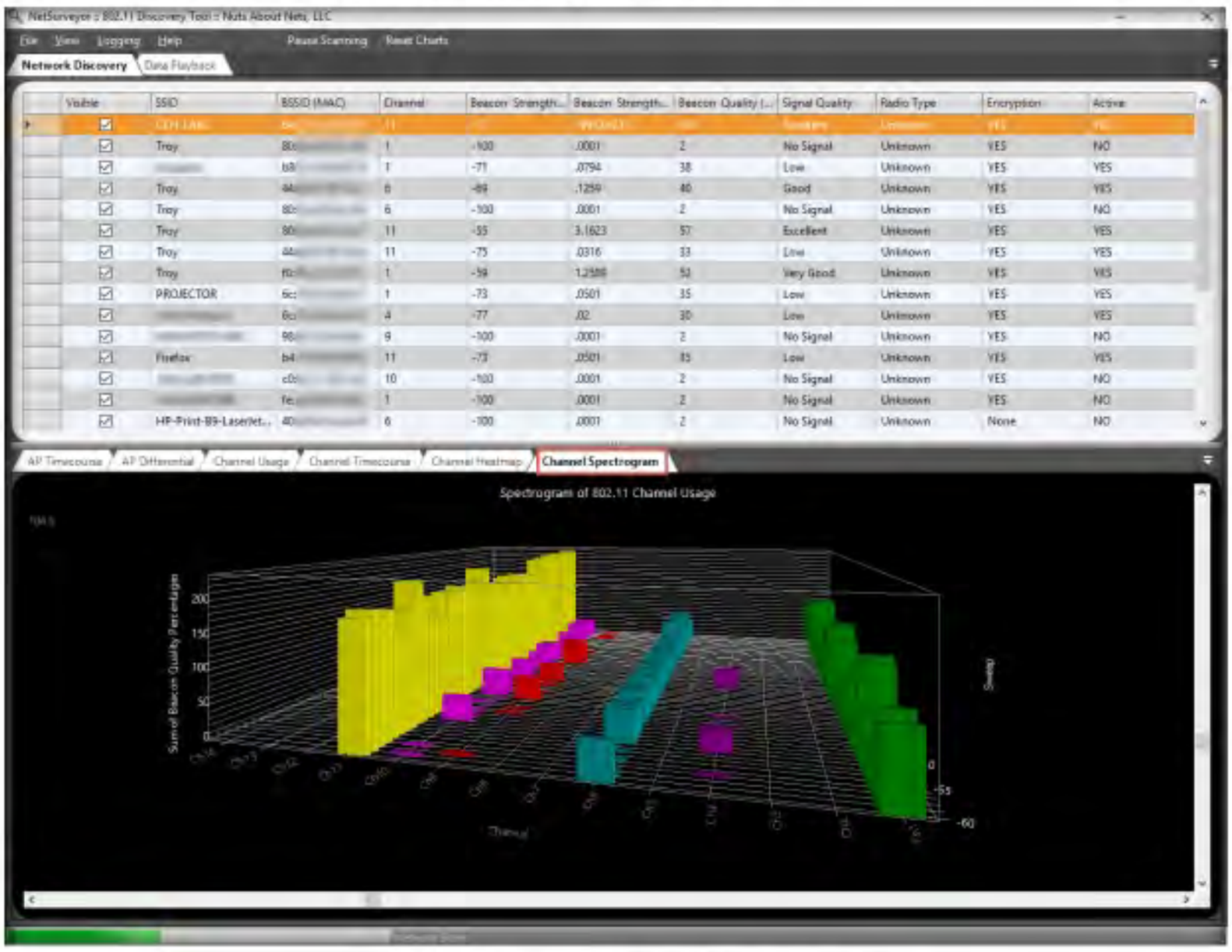

Figure 1.1.5: NetSurveyor: Channel Spectrogram tab

12. Similarly, you can gather detailed information about the discovered access points with other graphical diagnostic views by navigating to different tabs in the lower section. Information you can discover includes differential beacon qualities by SSID, the timecourse of 802.11 channel usage, and a heatmap of 802.11 channel usage.

TASK 1.3

Generate a Report

13. To save the gathered information in a report, click **File** from the menu bar and select **Create Report...** from the options.

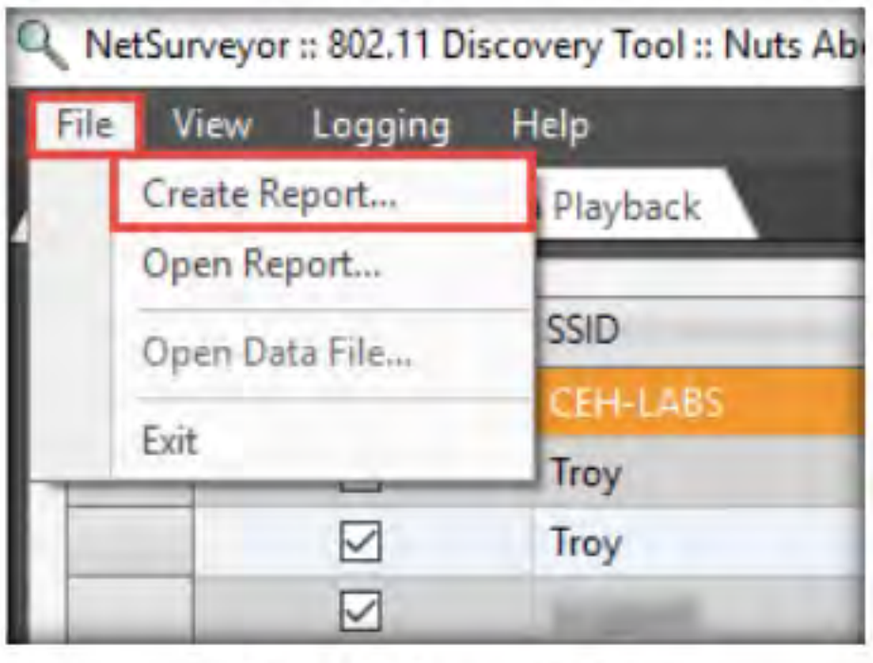

Figure 1.1.6: Generate a report

14. The **Report Charts As An Adobe PDF File (*.pdf)** window appears. Navigate to the location where you want to save the file (in this case, **Downloads**), ensure the **File name** is **NetSurveyor Report**, and click **Save**.

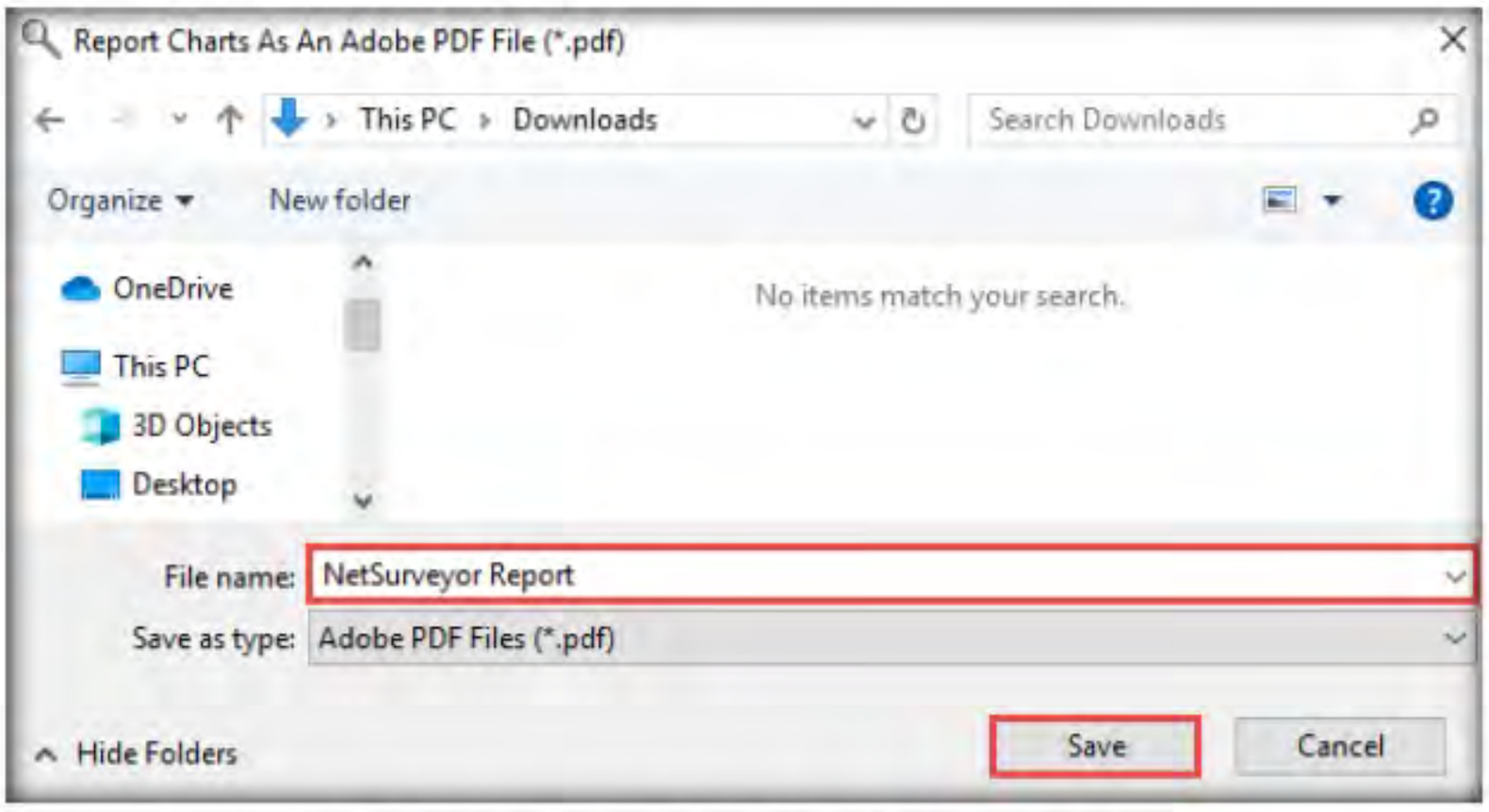

Figure 1.1.7: Report Charts As An Adobe PDF File (*.pdf) window

15. A **How do you want to open this file?** pop-up appears. Choose any option (in this example, we will use **Microsoft Edge**) and click **OK**.
16. The **NetSurveyor Report** opens in the default pdf viewing application (here, **Microsoft Edge**), displaying a list of discovered access points. Scroll down to view the detailed report about them.

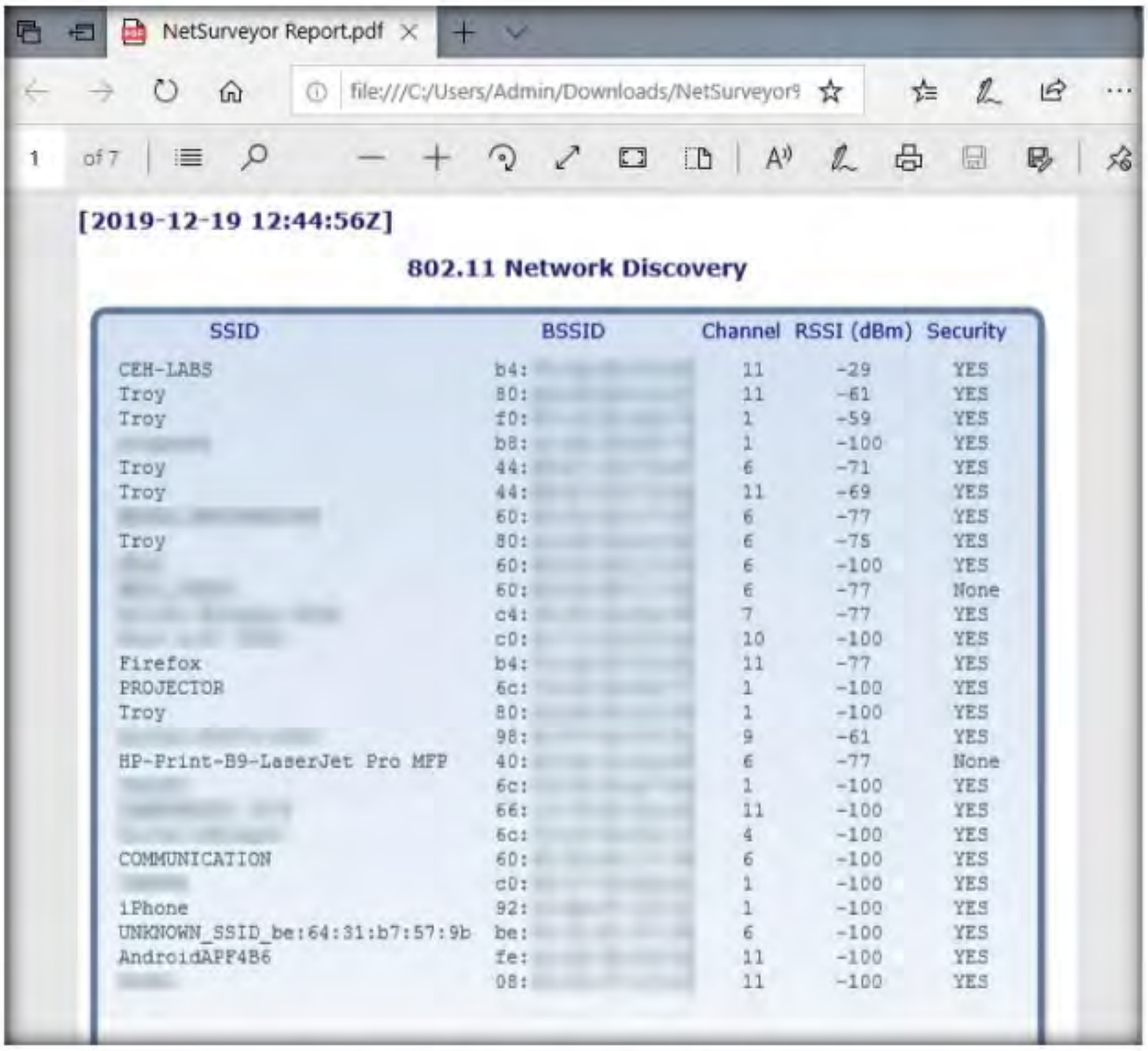

Figure 1.1.8: NetSurveyor Report: List of access points

You can also use other Wi-Fi discovery tools such as **inSSIDer Plus** (https://www.metageek.com), **Wi-Fi Scanner** (https://lizardsystems.com), **Acrylic Wi-Fi Home** (https://www.acrylicwifi.com), **WirelessMon** (https://www.passmark.com), and **Ekahau HeatMapper** (https://www.ekahau.com) to discover access points.

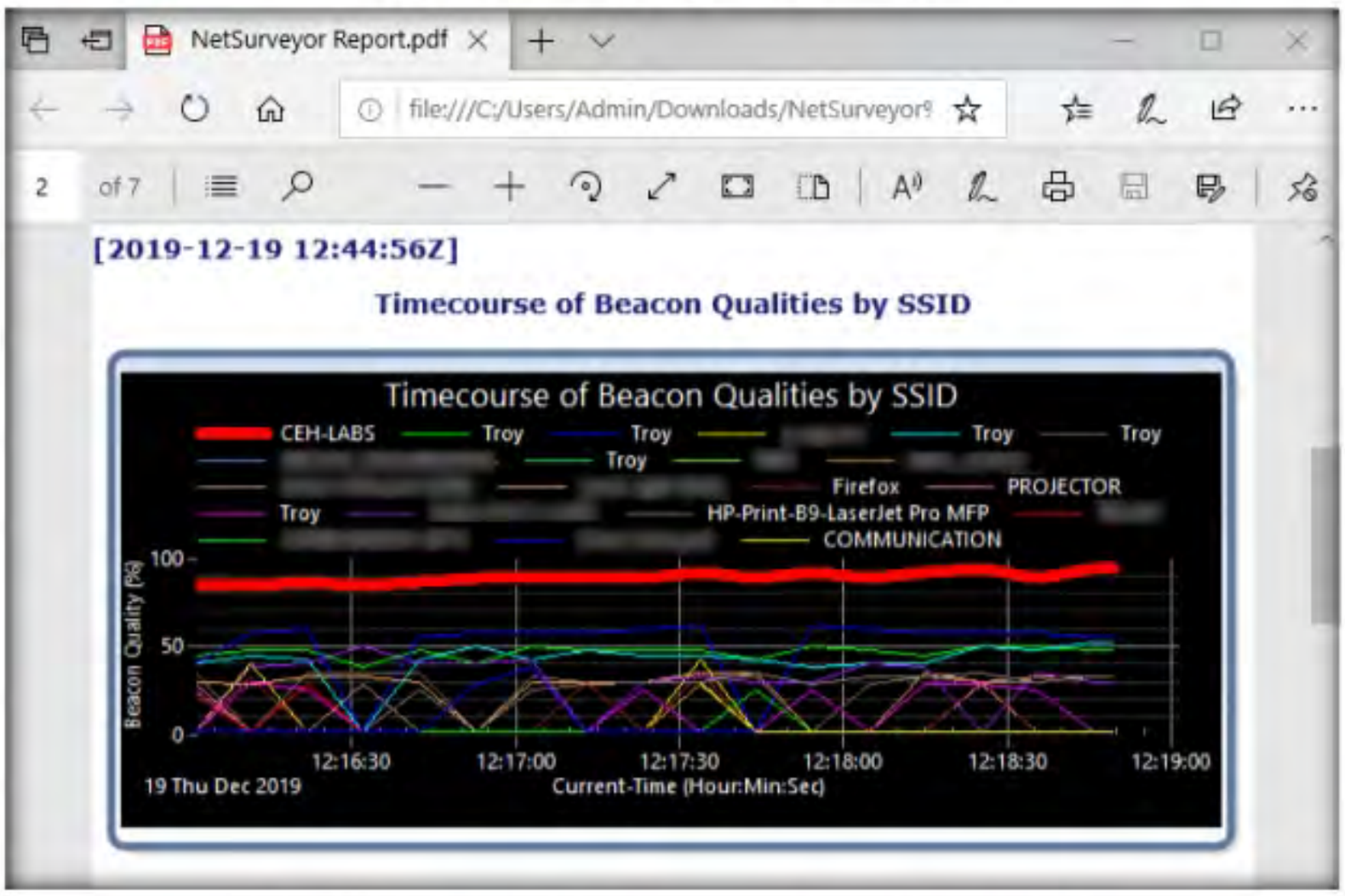

Figure 1.1.9: NetSurveyor Report: Timecourse of Beacon Qualities by SSID

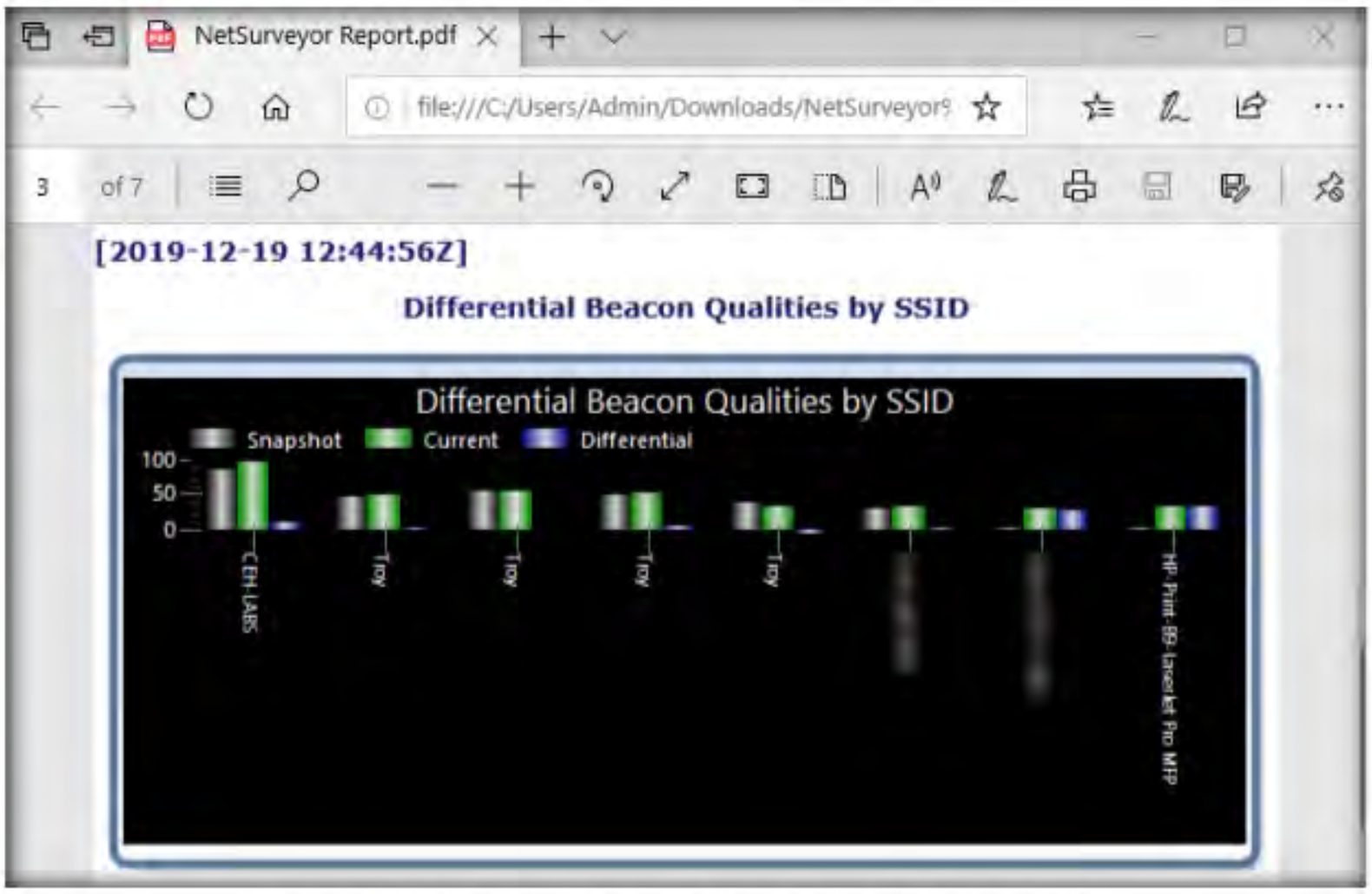

Figure 1.1.10: NetSurveyor Report: Different Beacon Qualities by SSID

17. This concludes the demonstration of how to find Wi-Fi networks in range using Wi-Fi discovery tools.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 10** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Lab 2

Perform Wireless Traffic Analysis

Wireless traffic analysis is the process of identifying vulnerabilities and susceptible victims in a target wireless network.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your next step in hacking wireless networks is to capture and analyze the traffic of the target wireless network.

This wireless traffic analysis will help you to determine the weaknesses and vulnerable devices in the target network. In the process, you will determine the network's broadcasted SSID, the presence of multiple access points, the possibility of recovering SSIDs, the authentication method used, WLAN encryption algorithms, etc.

The labs in this exercise demonstrate how to use various tools and techniques to capture and analyze the traffic of the target wireless network.

Lab Objectives

- Find Wi-Fi networks and sniff Wi-Fi packets using Wash and Wireshark

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Wireless Traffic Analysis

Wireless traffic analysis helps in determining the appropriate strategy for a successful attack. Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets. You can use various Wi-Fi packet-sniffing tools to capture and analyze the traffic of a target wireless network.

TASK 1

Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark

Here, we will use Wash to find Wi-Fi networks and Wireshark to sniff Wi-Fi packets.

Wash is a utility that can be used to identify WPS-enabled access points in the target wireless network. It also enables you to check if the access point is in a locked or unlocked state. This is important, because most WPS-enabled routers automatically lock after five or more unsuccessful login attempts (an attempted brute-force attack), and can be unlocked only manually in the administrator interface of the router.

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.

Figure 2.1.1: Parrot Security login

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.

TASK 1.1

Put the Wireless Interface in Monitor Mode

2. Plug in the **Linksys 802.11 g WLAN** adapter.
3. 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**.

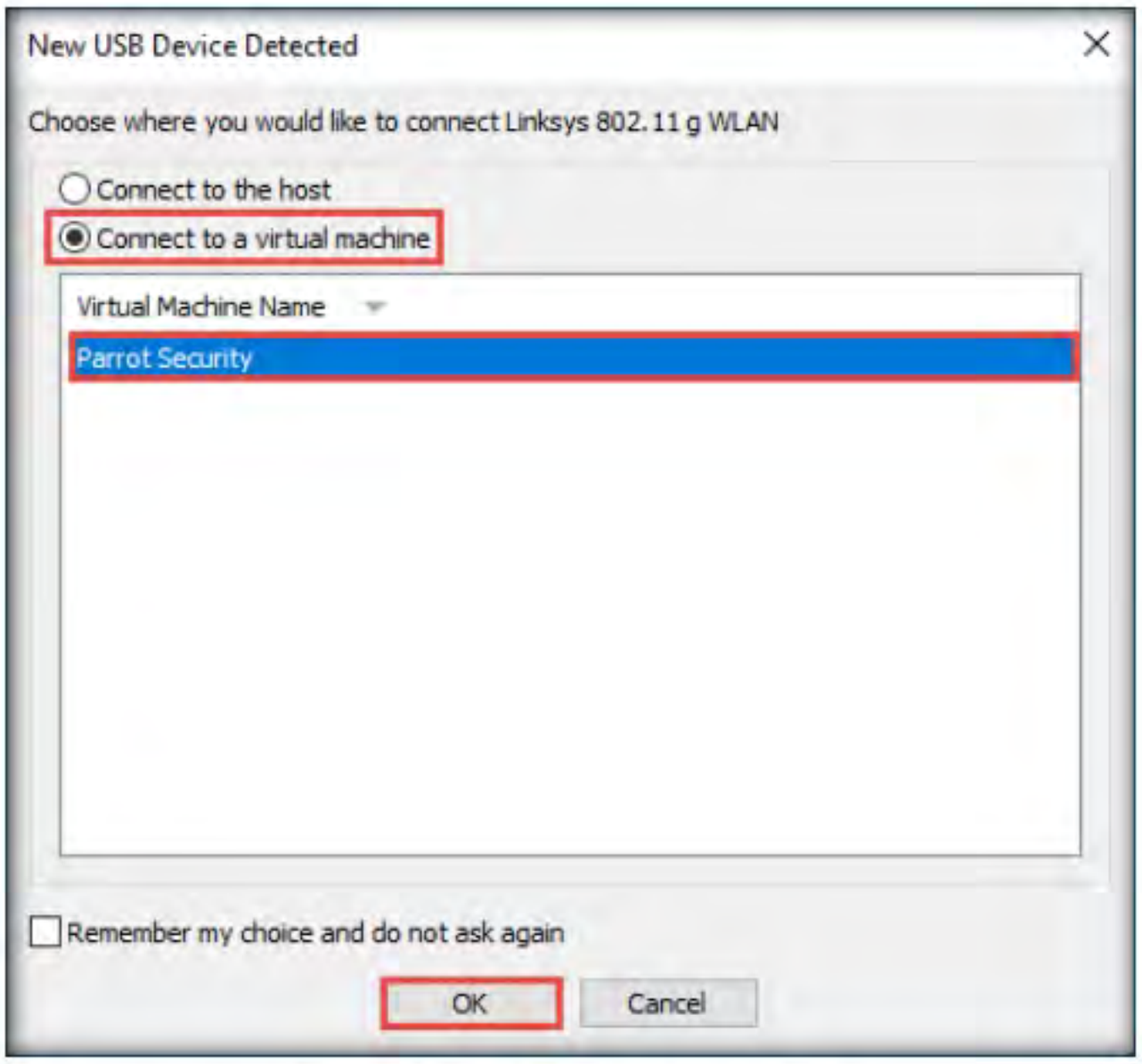

Figure 2.1.2: New USB Device Detected window

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

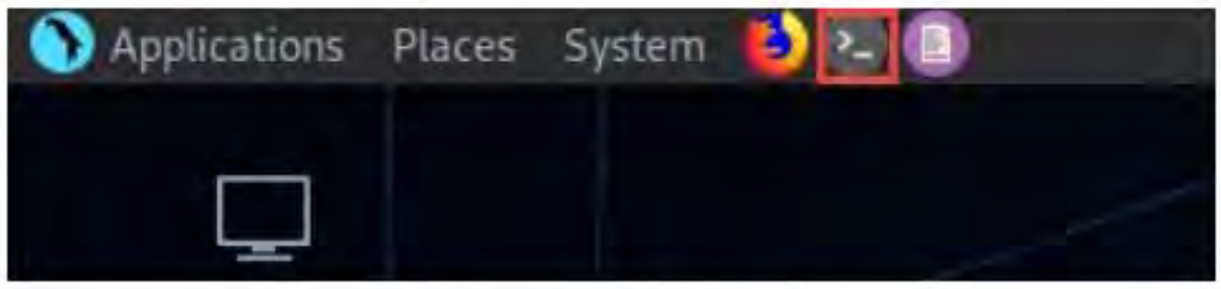

Figure 2.1.3: MATE Terminal icon

5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. 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

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

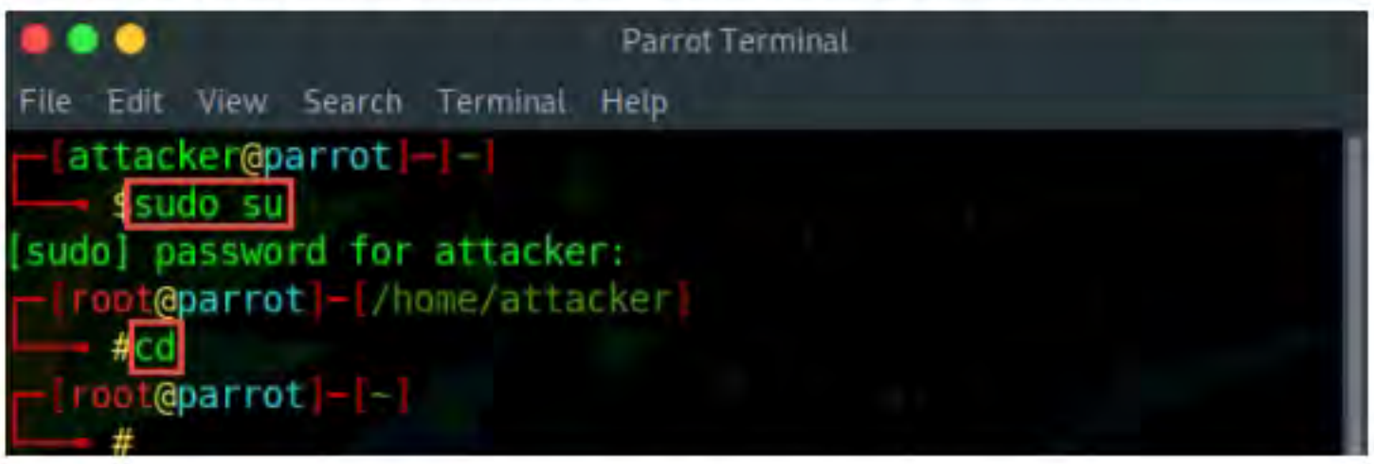

Figure 2.1.4: Running the programs as a root user

8. In the **Parrot Terminal** window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlan0**) gets connected to the machine, as shown in the screenshot.

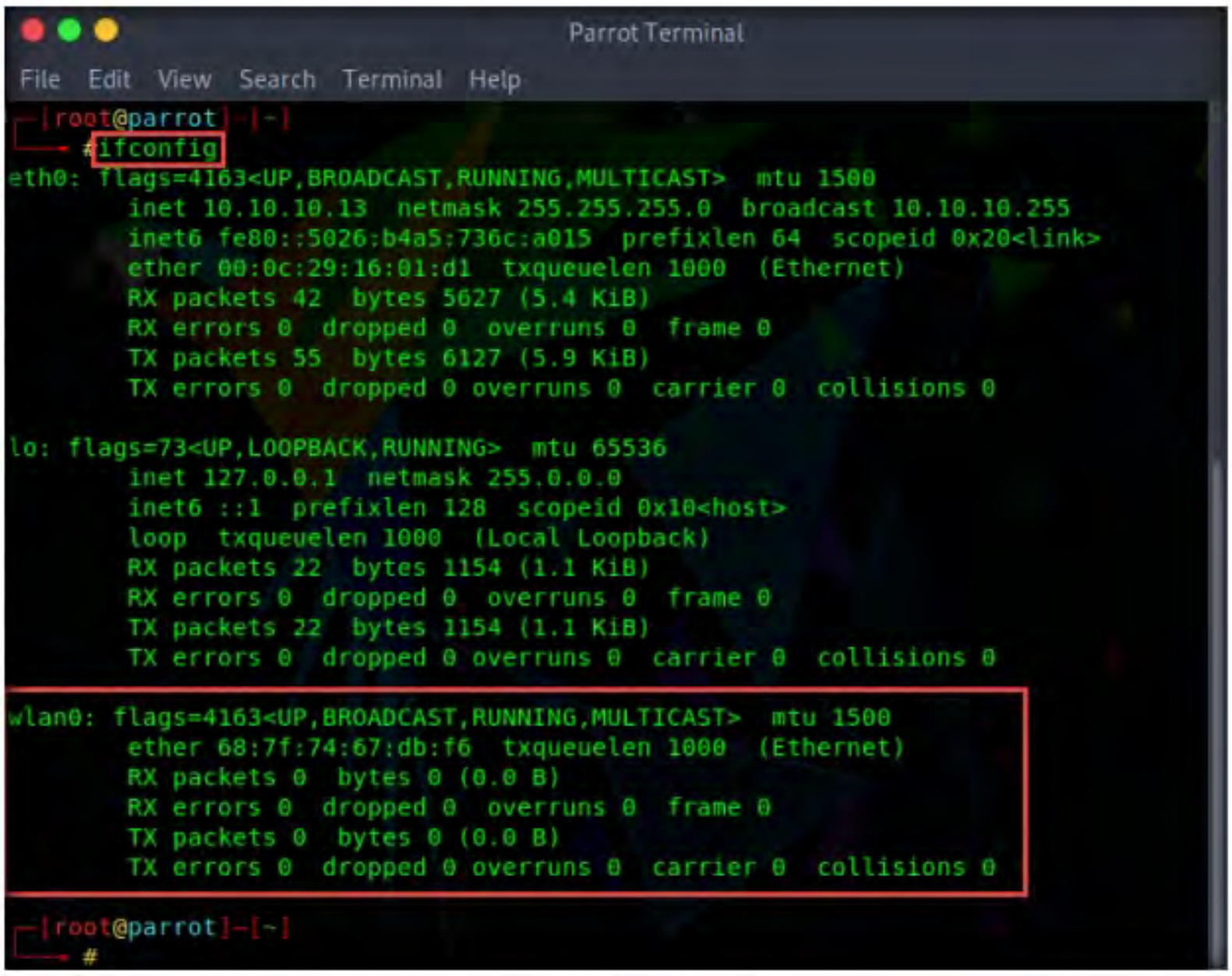

Figure 2.1.5: ifconfig: displaying wlan0

9. In the terminal window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. 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.
11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

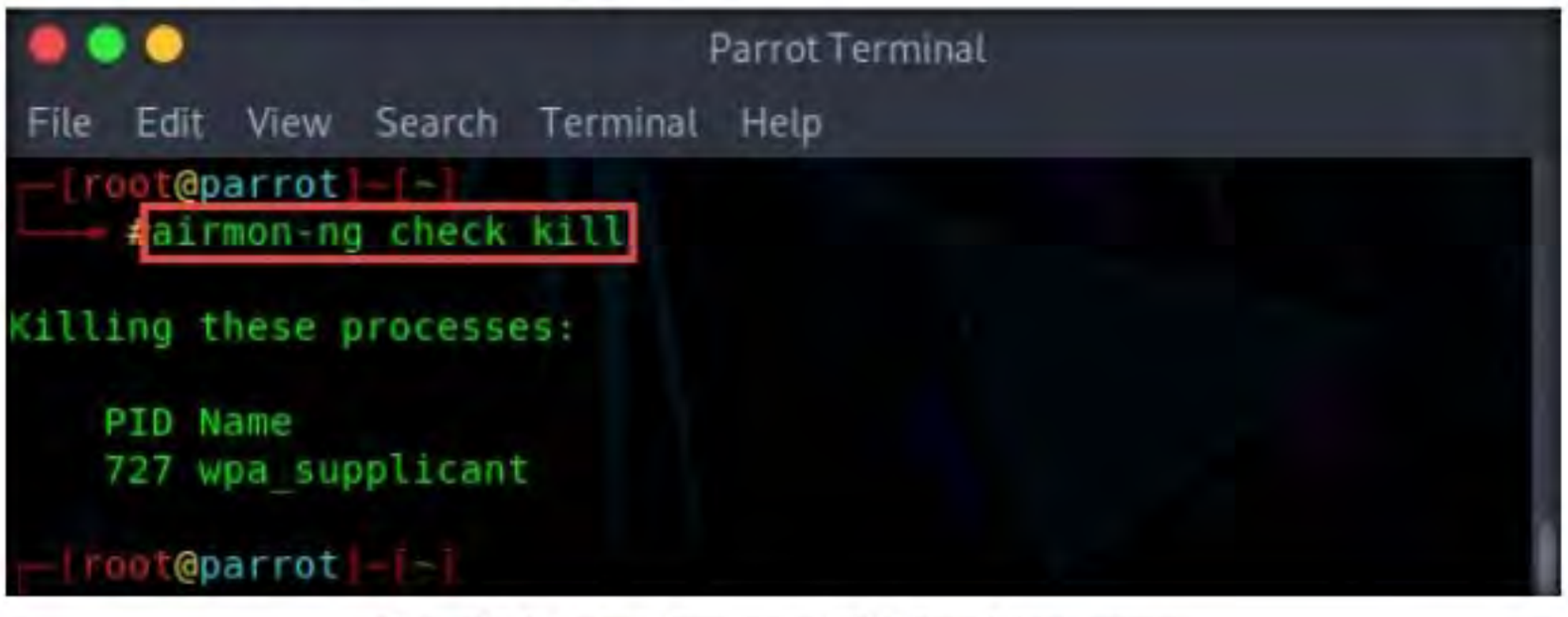

Figure 2.1.6: Issuing the command to kill interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless interface in monitor mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

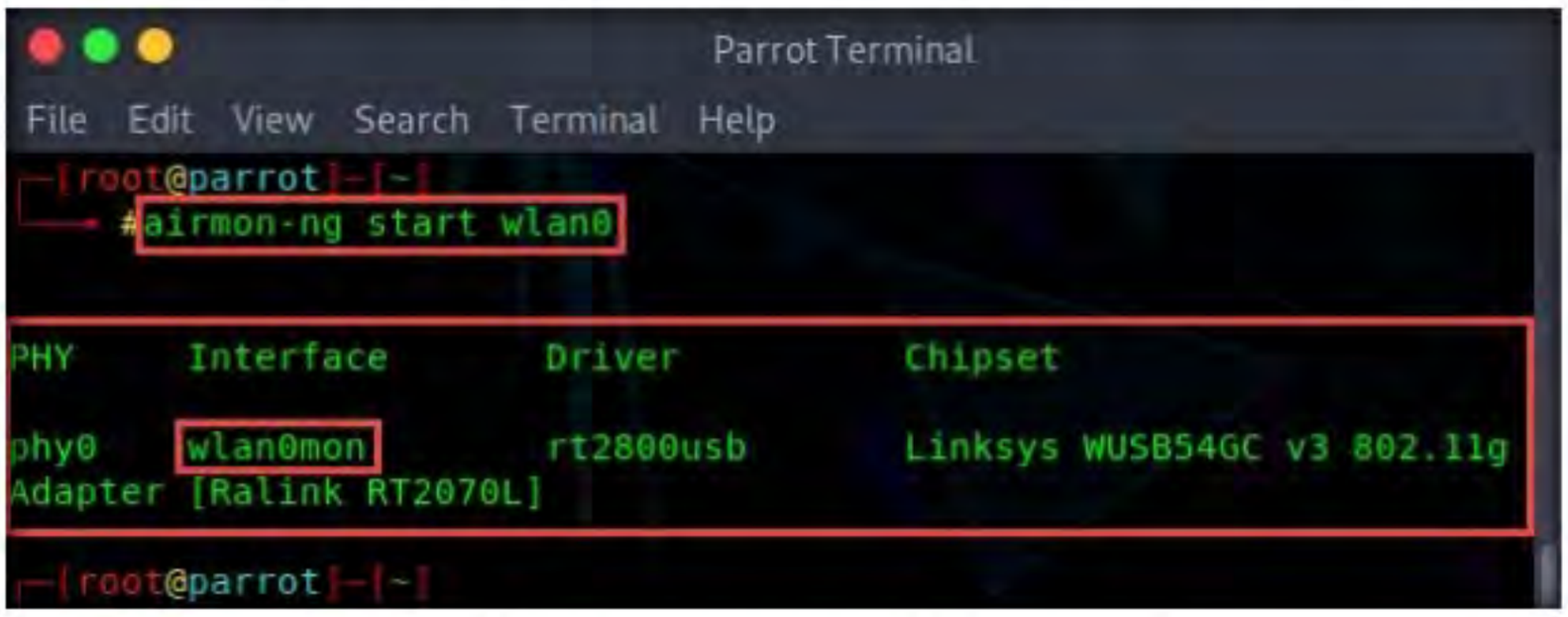

Figure 2.1.7: Setting up the wireless interface in monitor mode

TASK 1.2

Discover Access Points

14. Now, we shall find Wi-Fi networks (access points) by using the wireless interface **wlan0mon**.
15. Type **wash -i wlan0mon** and press **Enter** to detect WPS-enabled devices.

Note: The command **-i, --interface=<iface>** specifies the interface to capture the packets.

16. The results appear, displaying the discovered Wi-Fi access points, as shown in the screenshot.

Note: If no results appear, restart the **Parrot Security** virtual machine and perform **Steps 1 - 8**, type **wash -i wlan0mon** in the **Terminal** window, and press **Enter**.

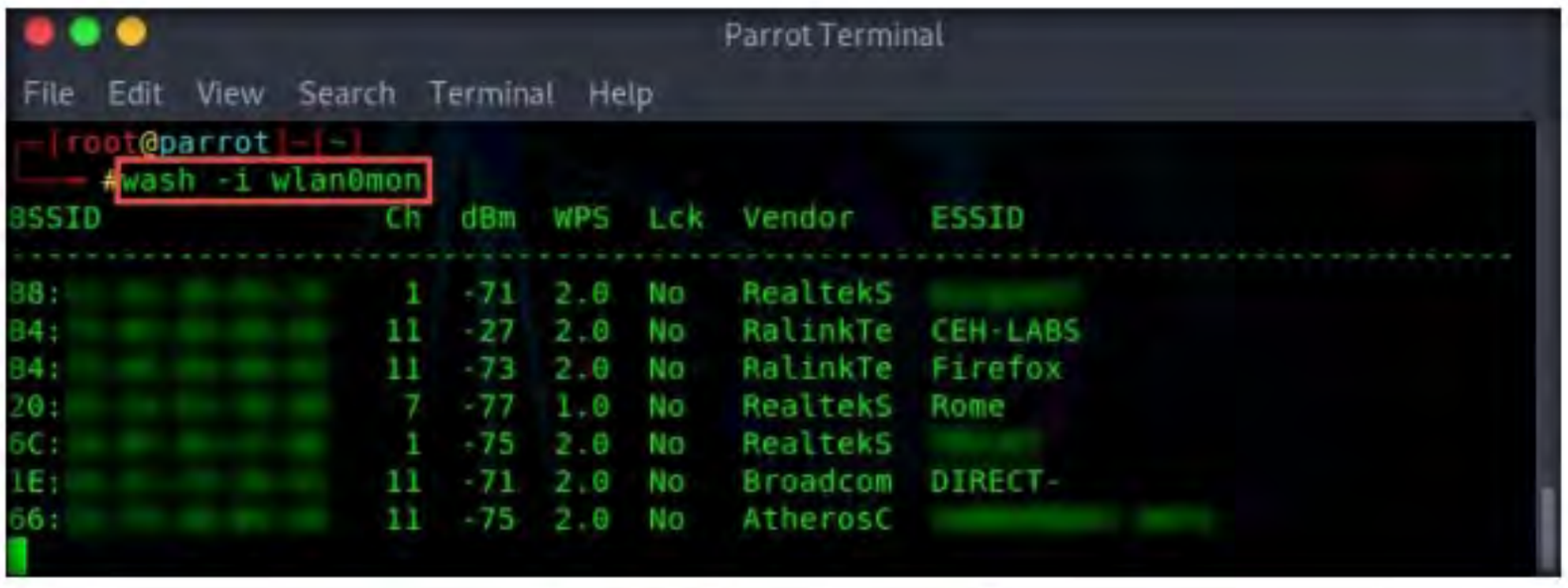

Figure 2.1.8: Discovering access points

TASK 1.3

Capture Wireless Traffic

17. Now, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
18. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

19. The **Wireshark Network Analyzer** window appears; double-click the wireless network interface (in this case, **wlan0mon**) to start capturing network traffic.

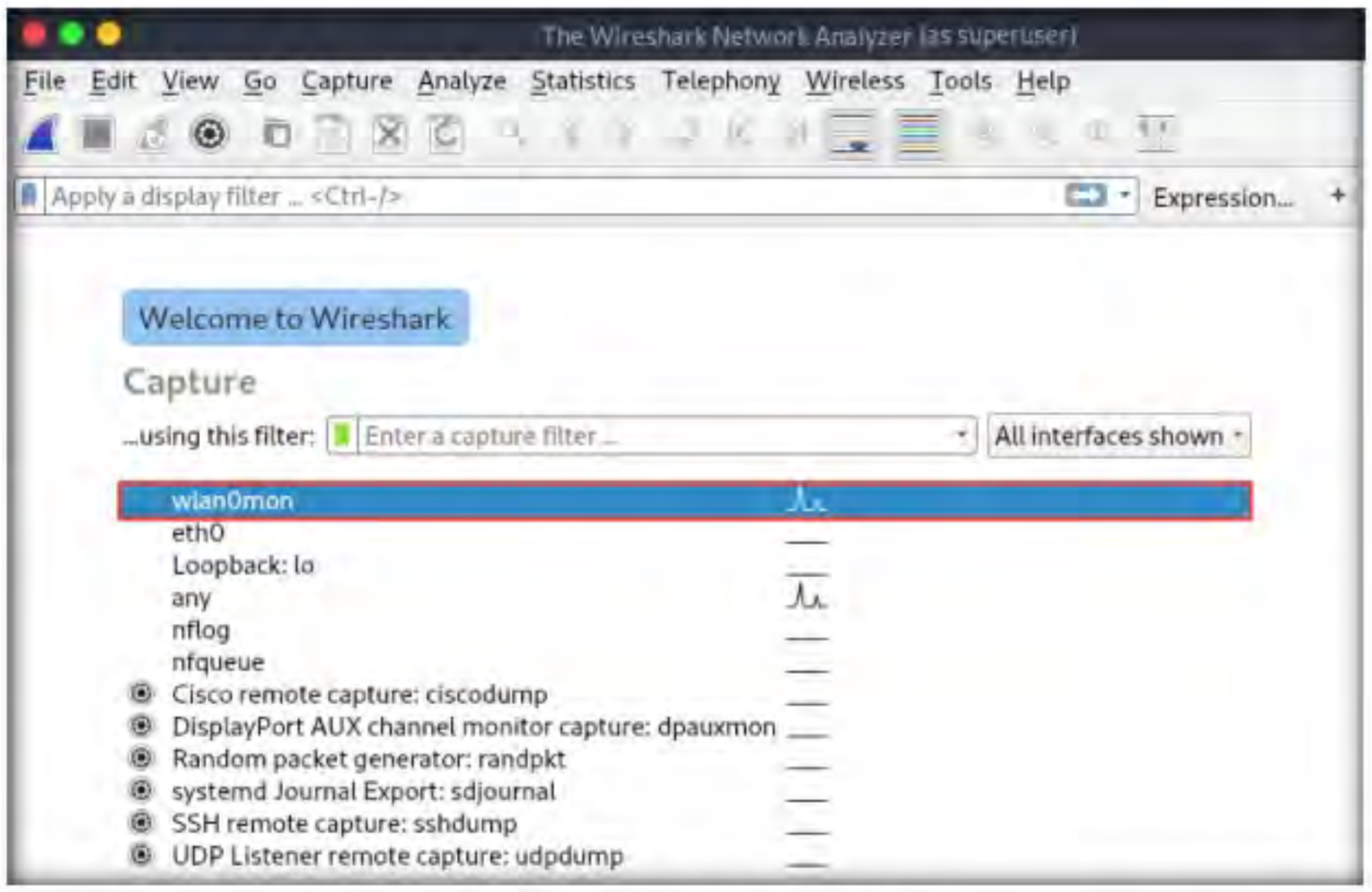

Figure 2.1.9: The Wireshark main window

20. **Wireshark** starts capturing network traffic. Note that the captured wireless packets are labeled **802.11** under the **Protocol** column, as shown in the screenshot.

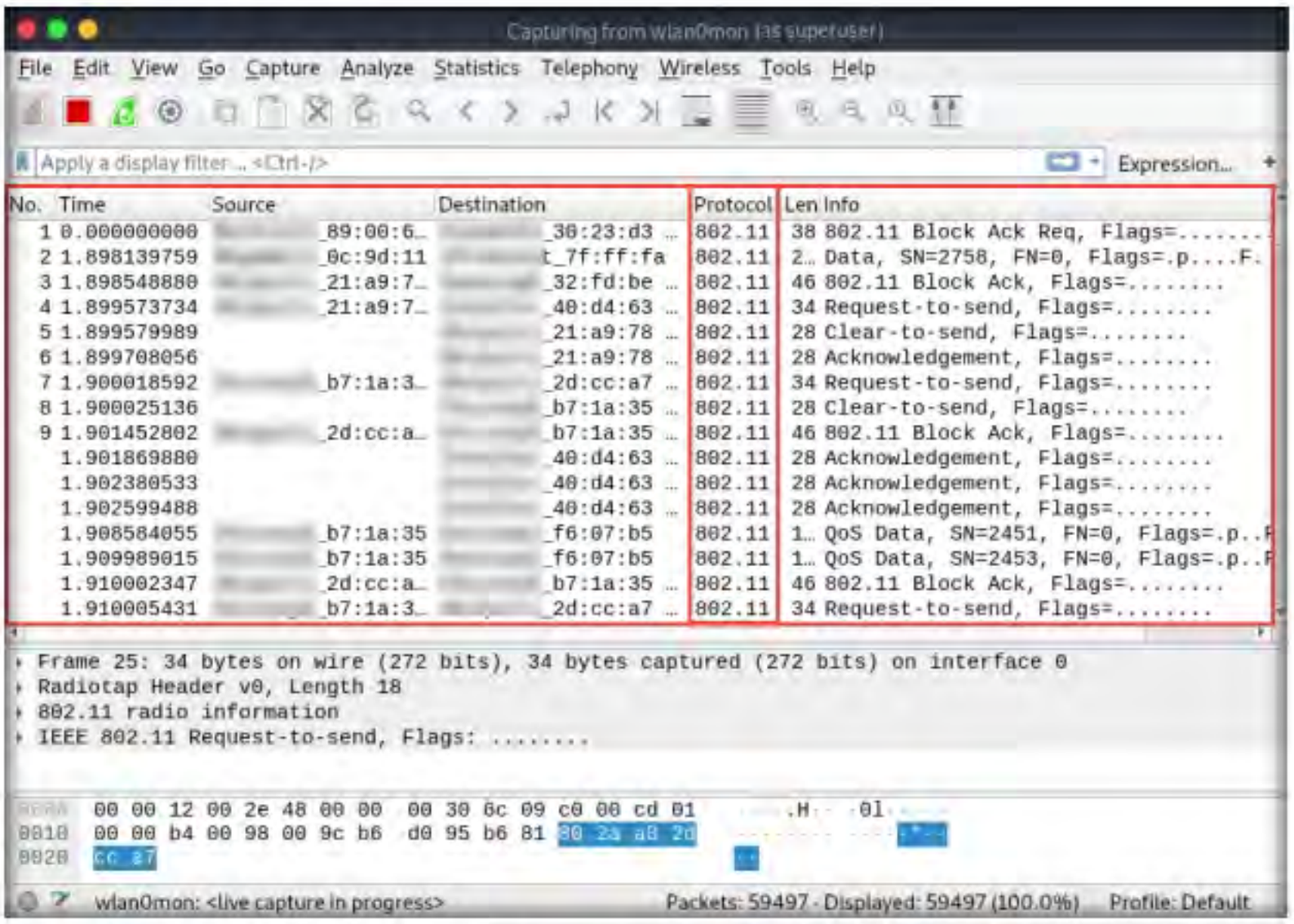

Figure 2.1.10: Wireshark window: captured packets

Wireshark is a network protocol sniffer and analyzer. It lets you capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

You can also use other wireless traffic analyzers such as **AirMagnet WiFi Analyzer PRO** (https://www.netally.com), **SteelCentral Packet Analyzer** (https://www.riverbed.com), **Omnipeek Network Protocol Analyzer** (https://www.liveaction.com), **CommView for Wi-Fi** (https://www.tamos.com), and **Capsa Portable Network Analyzer** (https://www.colasoft.com) to analyze Wi-Fi traffic.

Note: In a real-life attack, attackers use packet capture and filtering techniques to capture packets containing passwords (only for HTTP websites), perform attacks such as session hijacking, etc.

21. This concludes the demonstration of how to find Wi-Fi networks and sniff Wi-Fi packets using Wireshark.
22. Close all open windows and document all the acquired information.
23. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Lab 3

Perform Wireless Attacks

Various tools and techniques can be used to launch attacks on target wireless networks and so test their security status.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As an expert ethical hacker or pen tester, you must have the required knowledge to perform wireless attacks in order to test the target network's security infrastructure.

After performing the discovery, mapping, and analysis of the target wireless network, you have gathered enough information to launch an attack. You should now carry out various types of attacks on the target network, including Wi-Fi encryption cracking (WEP, WPA, and WPA2), fragmentation, MAC spoofing, DoS, and ARP poisoning attacks.

WEP encryption is used for wireless networks, but it has several exploitable vulnerabilities. When seeking to protect a wireless network, the first step is always to change your SSID from the default before you actually connect the wireless router to the access point. Moreover, if an SSID broadcast is not disabled on an access point, ensure that you do not use a DHCP server, which would automatically assign IP addresses to wireless clients. This is because war-driving tools can easily detect your internal IP address.

As an ethical hacker and pen tester of an organization, you must test its wireless security, exploit WEP flaws, and crack the network's access point keys.

The labs in this exercise demonstrate how to perform wireless attacks using various hacking tools and techniques.

Lab Objectives

- Find hidden SSIDs using Aircrack-ng
- Crack a WEP network using Wifiphisher
- Crack a WEP network using Aircrack-ng
- Crack a WPA network using Fern Wifi Cracker
- Crack a WPA2 network using Aircrack-ng
- Create a rogue access point to capture data packets using MANA-Toolkit

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Windows 10 virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 Minutes

Overview of Wireless Attacks

There are several different types of Wi-Fi attacks that attackers use to eavesdrop on wireless network connections in order to obtain sensitive information such as passwords, banking credentials, and medical records, as well as to spread malware.

These include:

- **Fragmentation attack**: When successful, such attacks can obtain 1,500 bytes of PRGA (pseudo random generation algorithm)
- **MAC spoofing attack**: The attacker changes their MAC address to that of an authenticated user in order to bypass the access point's MAC-filtering configuration
- **Disassociation attack**: The attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the access point and client
- **Deauthentication attack**: The attacker floods station(s) with forged deauthentication packets to disconnect users from an access point
- **Man-in-the-middle attack**: An active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers
- **Wireless ARP poisoning attack**: An attack technique that exploits the lack of a verification mechanism in the ARP protocol by corrupting the ARP cache maintained by the OS in order to associate the attacker's MAC address with the target host
- **Rogue access points**: Wireless access points that an attacker installs on a network without authorization and that are not under the management of the network administrator
- **Evil twin**: A fraudulent wireless access point that pretends to be a legitimate access point by imitating another network name
- **Wi-Jacking attack**: A method used by attackers to gain access to an enormous number of wireless networks

TASK 1

Find Hidden SSIDs using Aircrack-ng

Here, we will use Aircrack-ng to reveal a hidden SSID.

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.

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**.

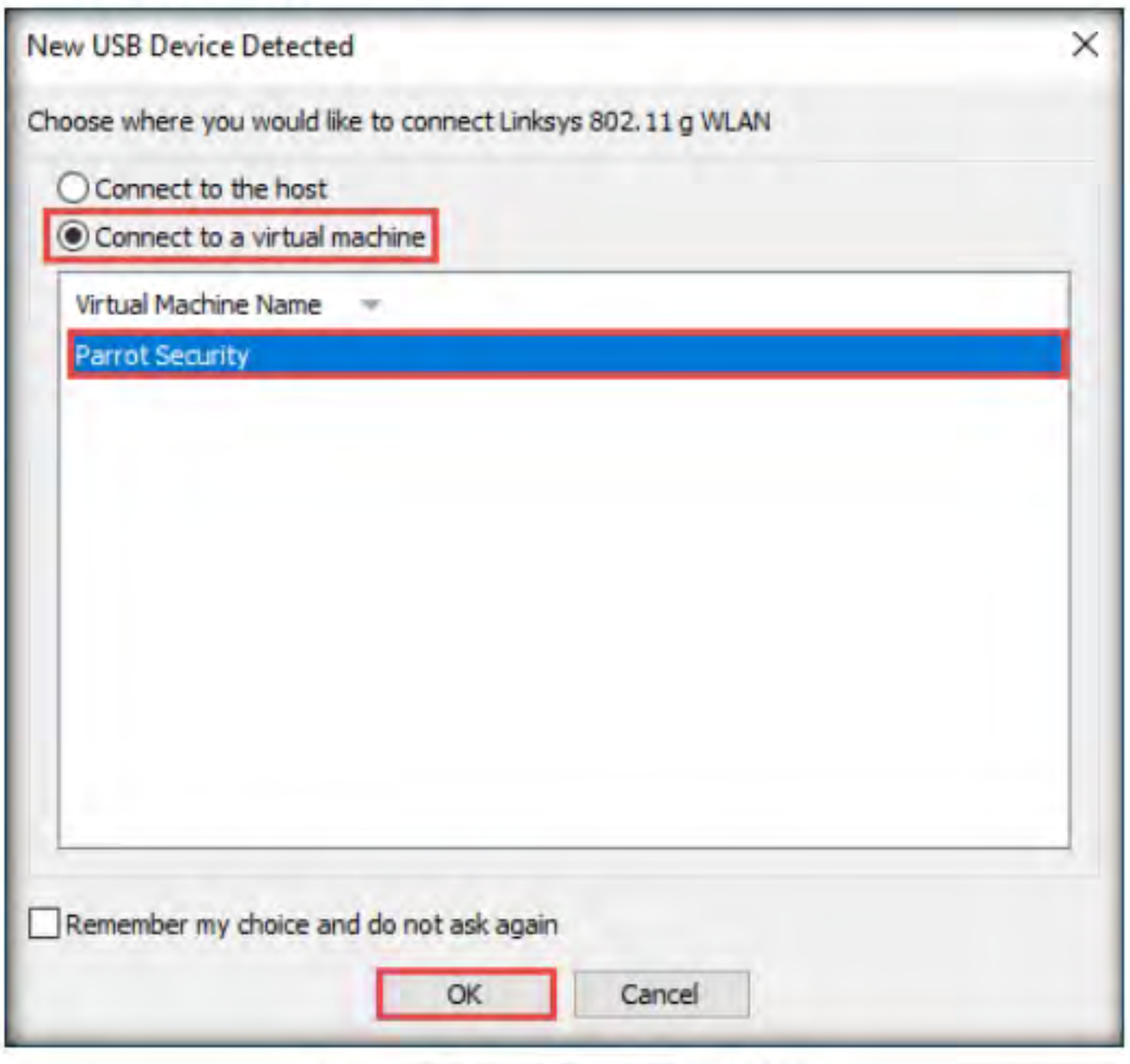

Figure 3.1.1: New USB Device Detected window

Based on the principle of "security through obscurity," many organizations hide the SSID of a wireless network by not broadcasting it. Because they are part of the security policy of an organization, SSIDs can be used by attackers to breach the security of the wireless networks. However, hiding an organization's SSID does not, in fact, add any level of security.

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows.

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

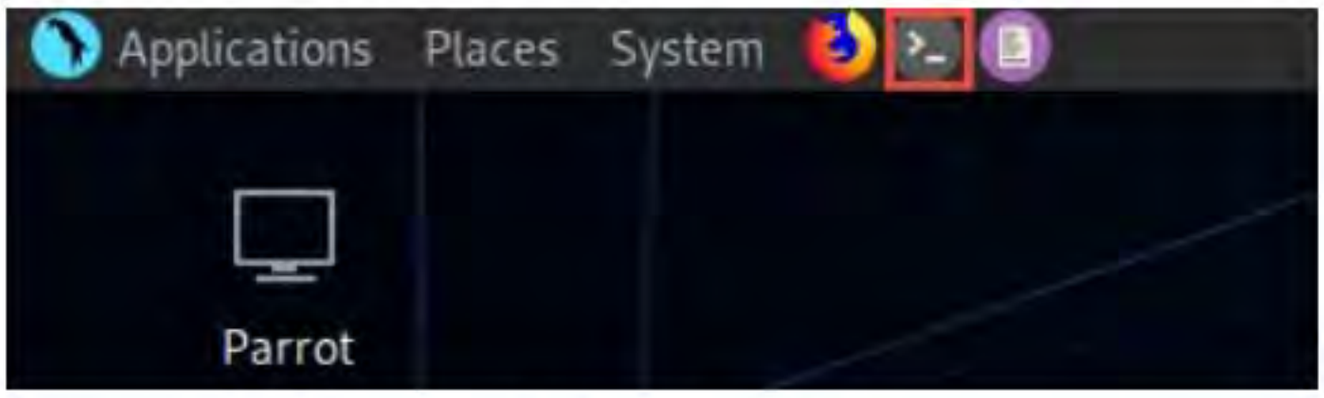

Figure 3.1.2: MATE Terminal icon

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.

TASK 1.1

Put the Wireless Interface into Monitor Mode

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. 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.

Note: This process might differ in your lab environment.

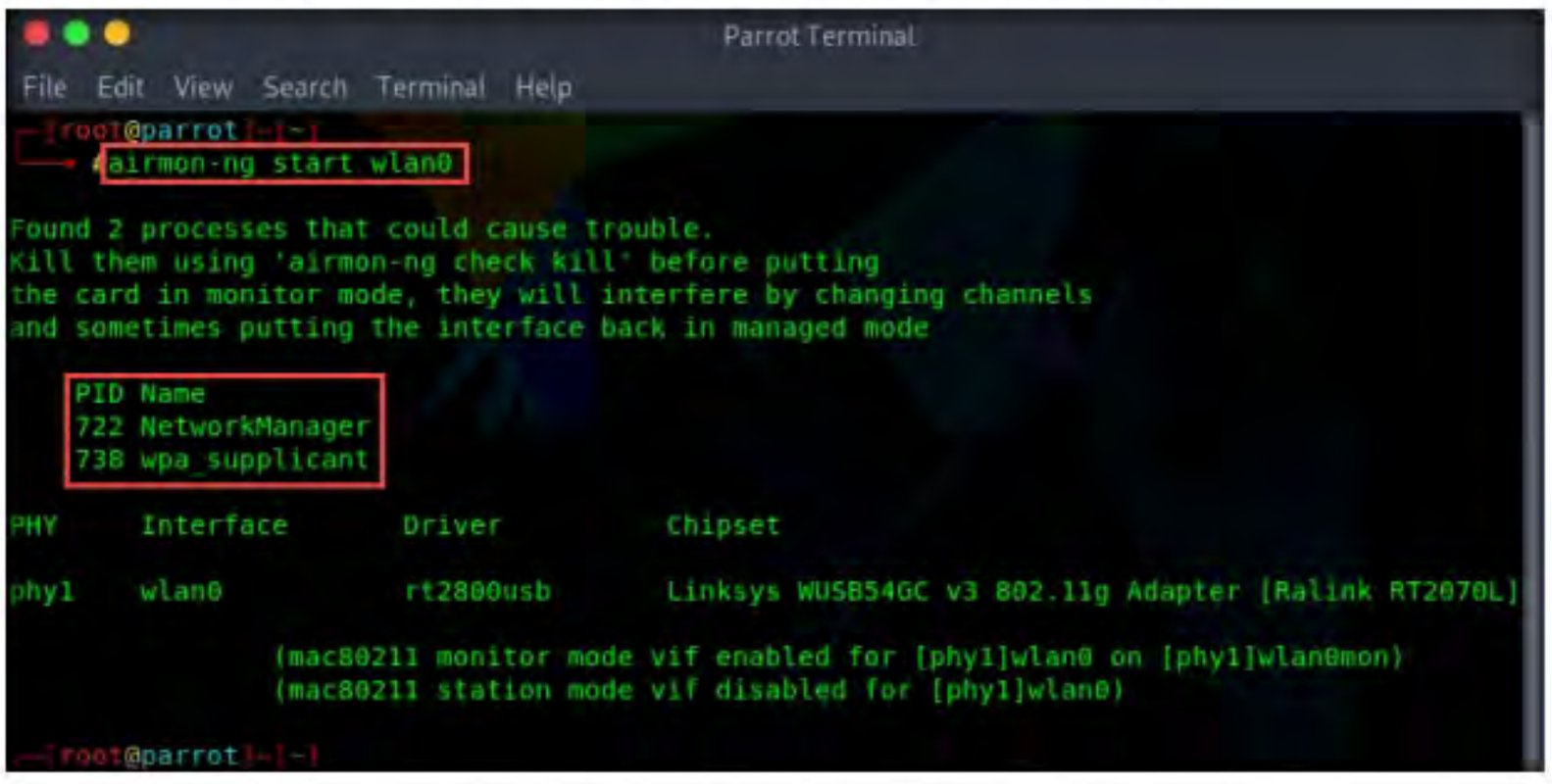

Figure 3.1.3: Found 2 processes that could cause trouble error

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

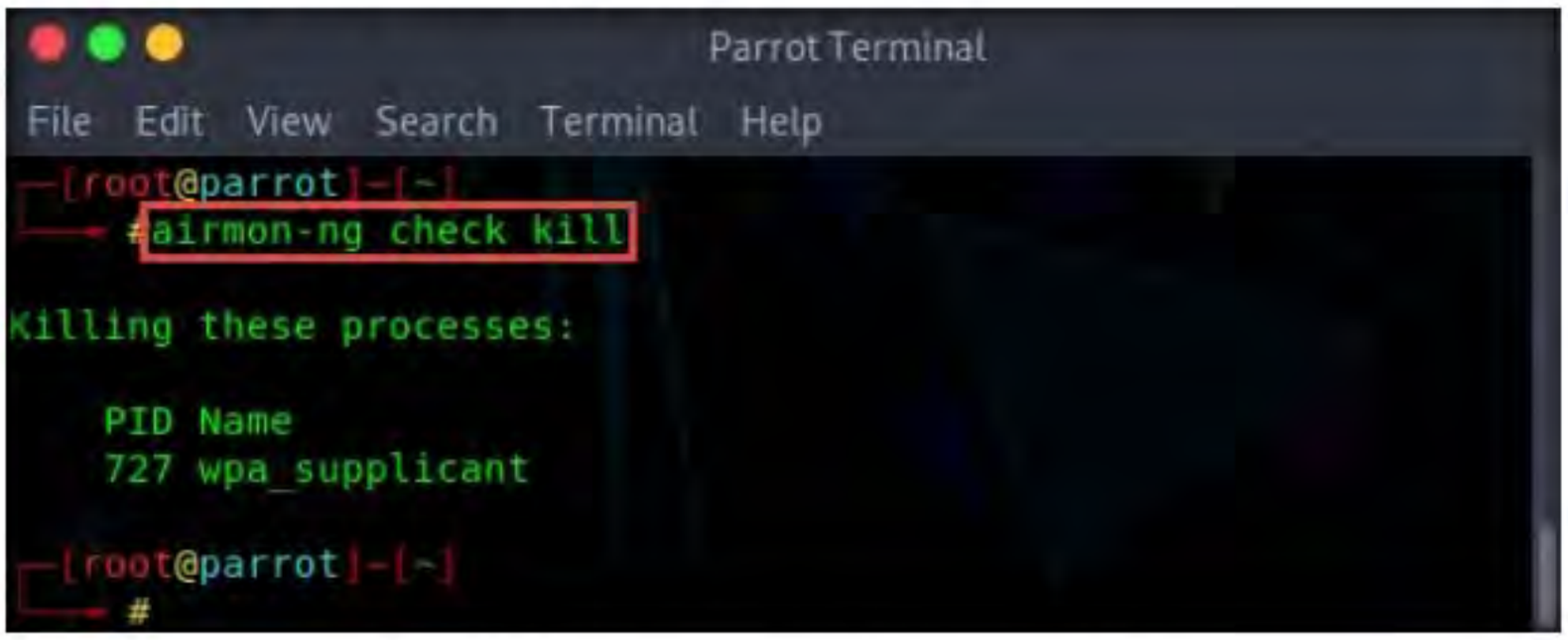

Figure 3.1.4: Issuing command to kill the interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

Note: The interface name might differ in your lab environment.

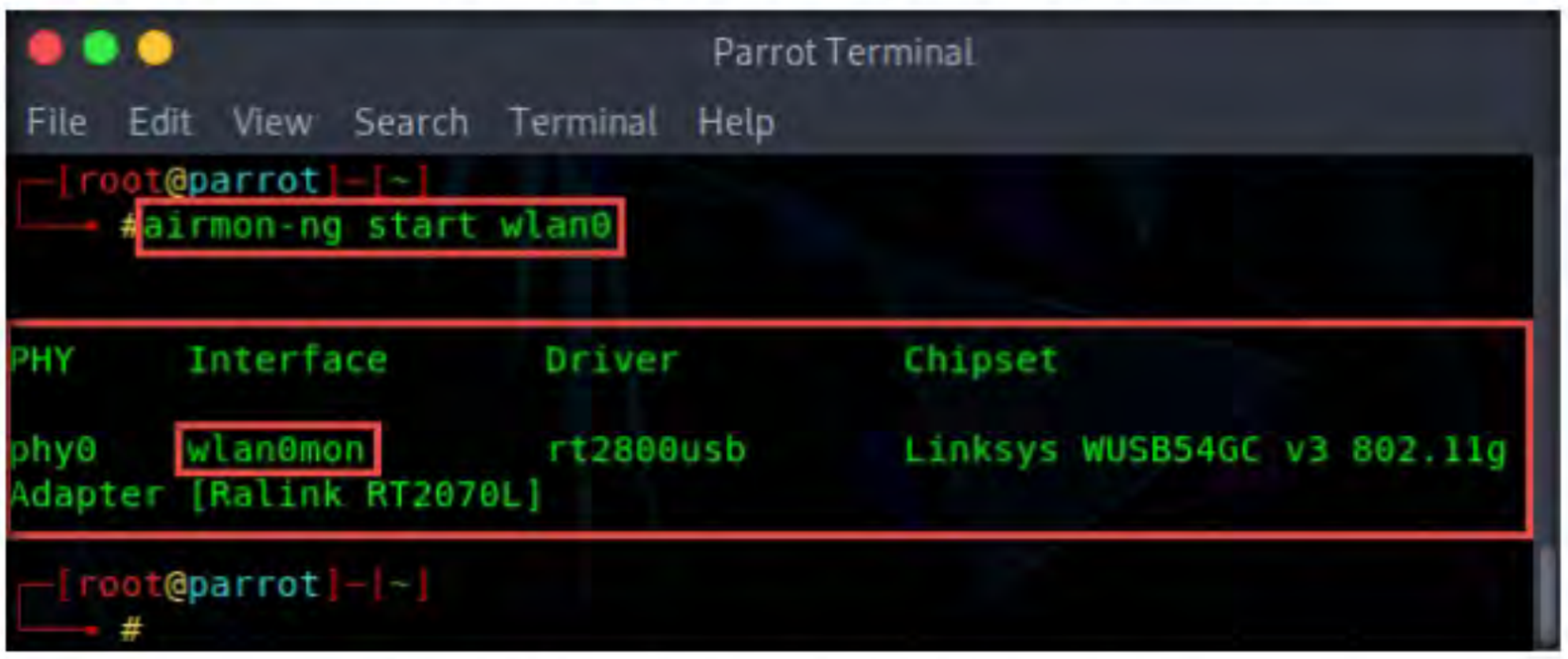

Figure 3.1.5: Putting the wireless interface in monitor mode

TASK 1.2

Discover the Available Access Points

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

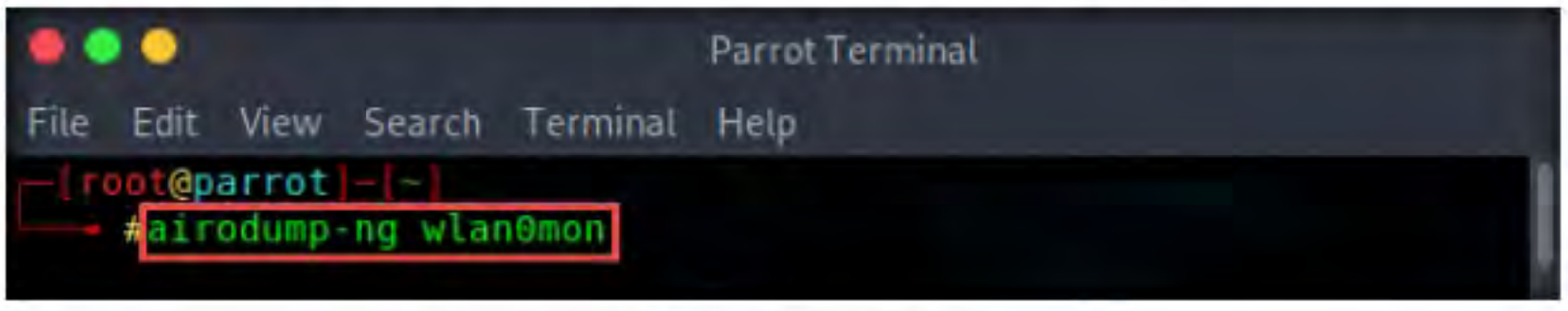

Figure 3.1.6: Launching airodump-ng

15. The result appears, displaying the available access points. Note the hidden **ESSID** associated with **BSSID**: **B4:75:0E:89:00:60**.

Note: The BSSID associated with the hidden ESSID will differ in your lab environment.

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.

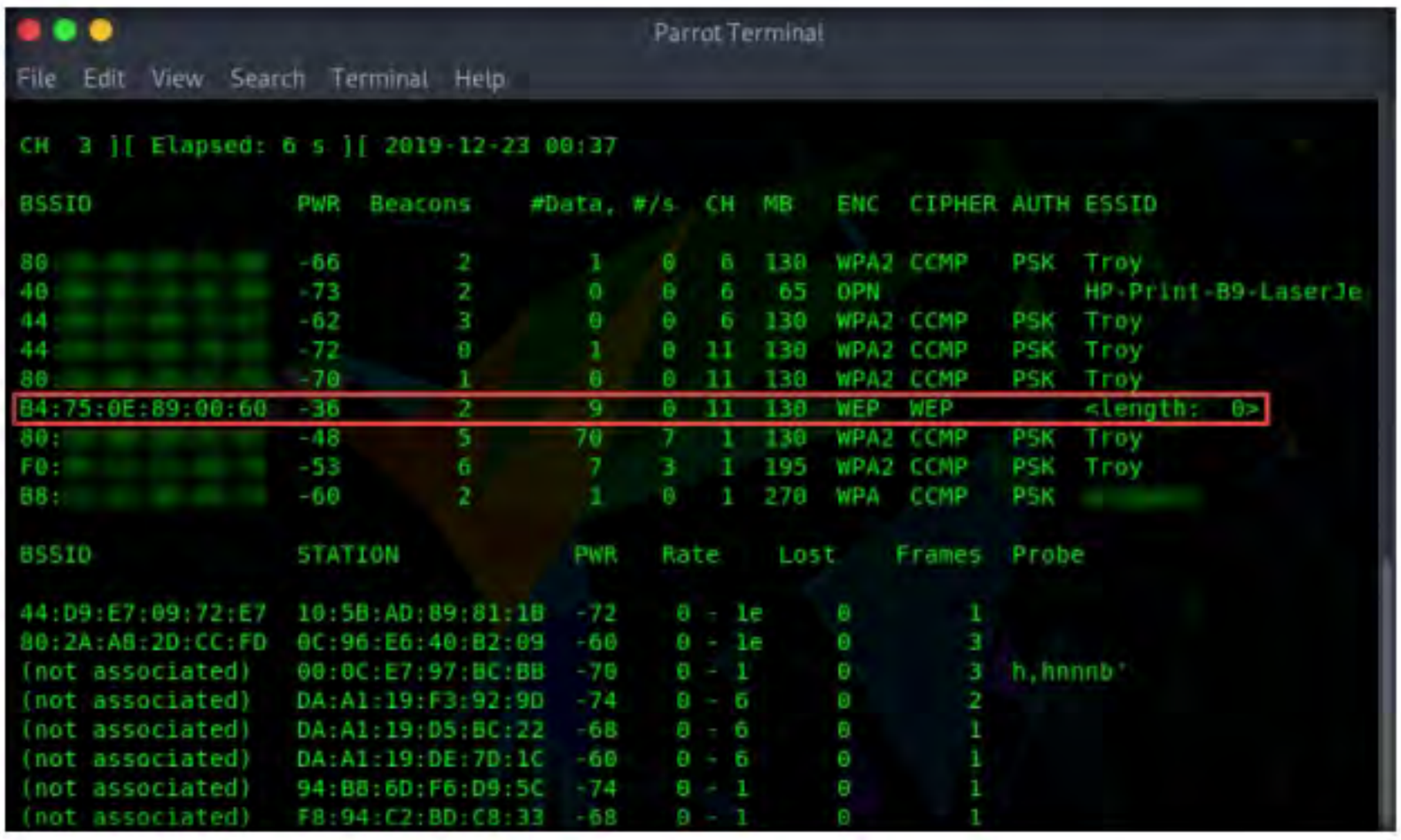

Figure 3.1.7: airodump-ng searching for available access points

TASK 1.3

Capture IV Packets from the Target Access Point

16. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
17. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. 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.

19. Now, type **cd** and press **Enter** to jump to the root directory.
20. In the terminal window, type **airodump-ng --bssid B4:75:0E:89:00:60 wlan0mon** and press **Enter**.

Note: In this command,

- **--bssid**: MAC address of the target access point (in this example, **B4:75:0E:89:00:60**).
- **wlan0mon**: Wireless interface

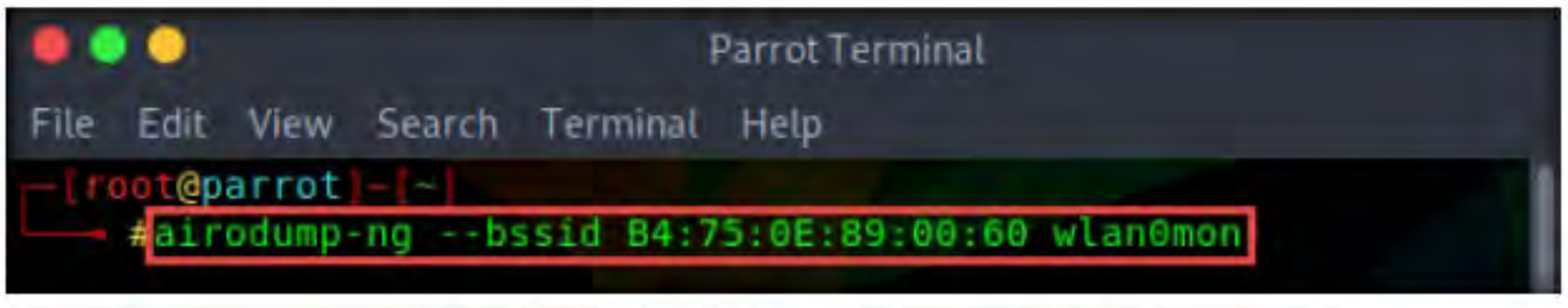

Figure 3.1.8: Starting airodump-ng to capture the packets

21. Airodump-ng starts capturing the Initialization Vector (IV) from the target AP, as shown in the screenshot.
22. The list of connected clients ("stations") appears. You can observe that there are two clients connected to the target access point (**B4:75:0E:89:00:60**). In this task, we will send deauthentication packets to the client **STATION**: **20:A6:0C:30:23:D3**. Leave airodump-ng running.

Note: The client station BSSID will differ in your lab environment.

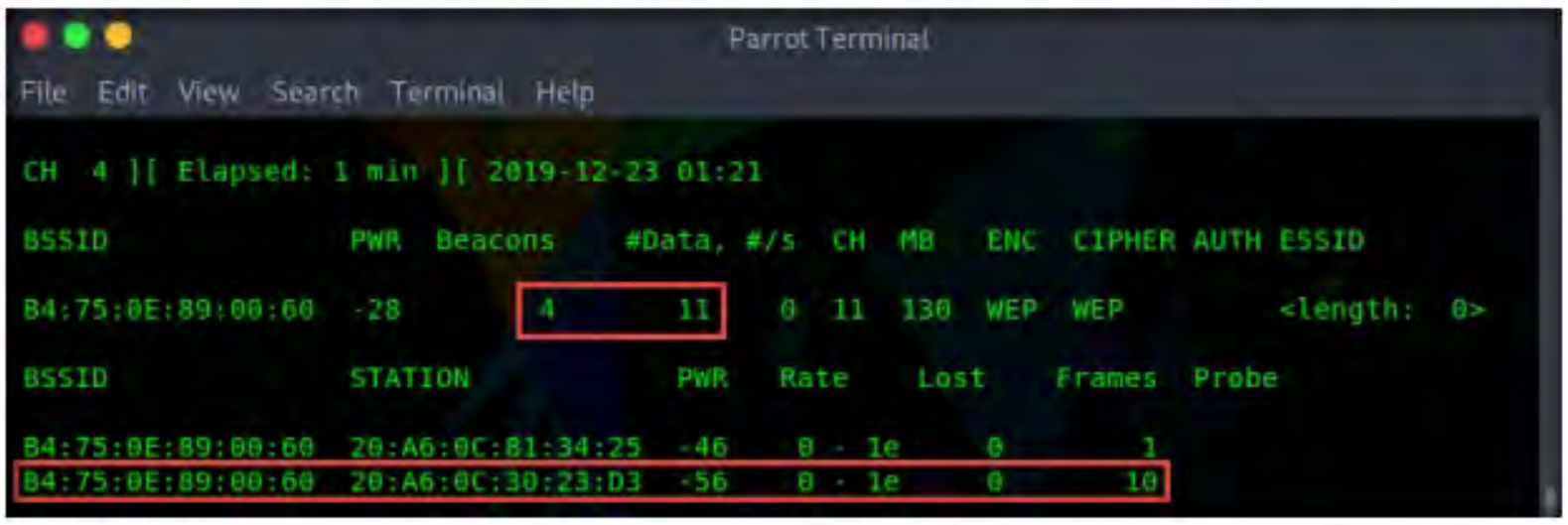

Figure 3.1.9: airodump-ng capturing the packets

TASK 1.4

Send De-Auth Packets to the Client

23. Open another terminal by clicking the **MATE Terminal** icon ( ) from the top of **Desktop**.
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.

26. Now, type **cd** and press **Enter** to jump to the root directory.
27. In the new terminal window, type **aireplay-ng --deauth 15 -a B4:75:0E:89:00:60 -c 20:A6:0C:30:23:D3 wlan0mon** and press **Enter** to generate de-authentication packets.

Note: In this command,

- **--deauth**: Activates deauthentication mode
- **15**: Number of deauthentication packets to be sent
- **-a**: Sets the access point MAC address
- **-c**: Sets the destination MAC address
- **wlan0mon**: Wireless interface

Note: If you get any errors while running the command, reissue the command multiple times until it executes successfully.

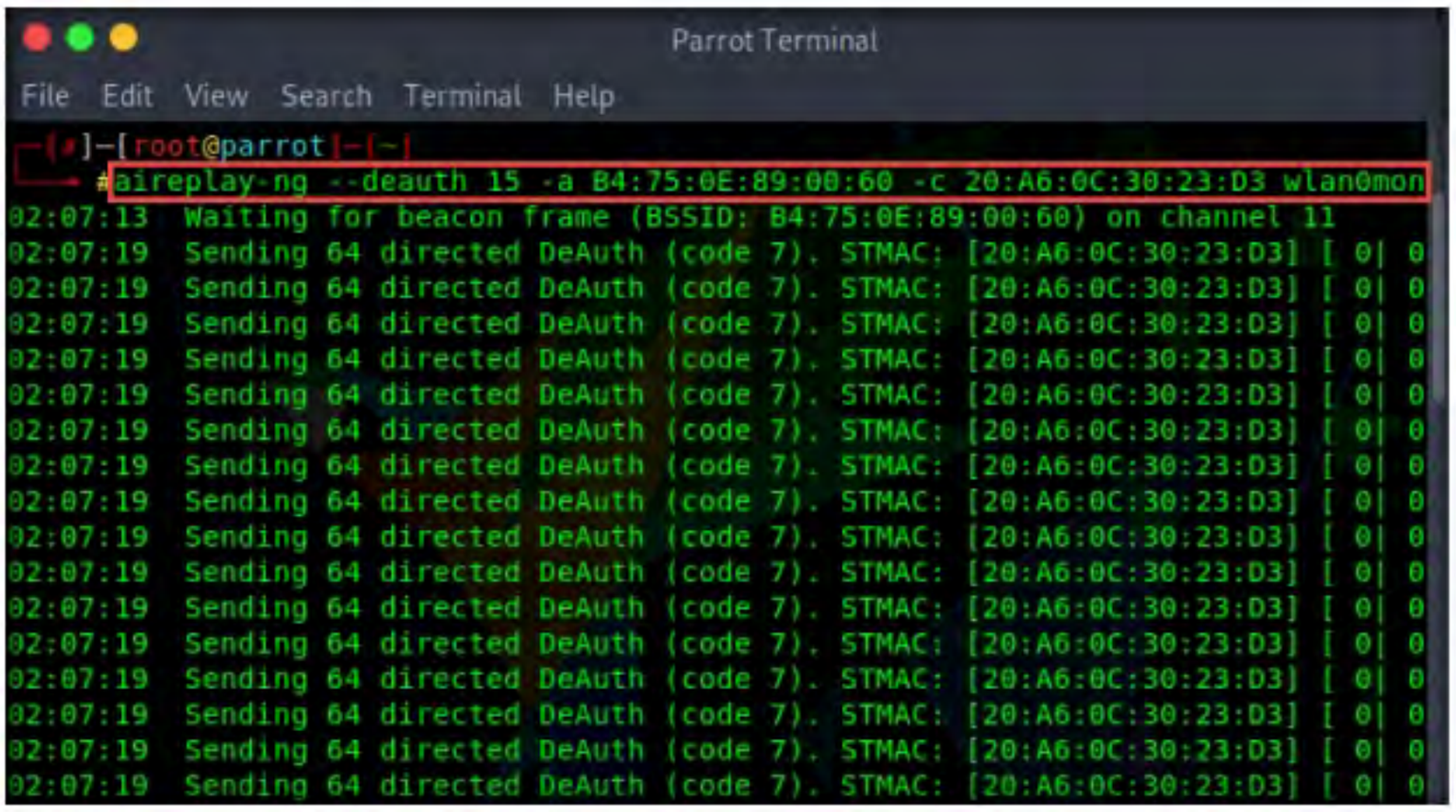

Figure 3.1.10: aireplay-ng generating traffic

28. The source MAC address should be associated with the access point in order to accept the packet. Because, in this case, the source MAC address used to inject the packets has no connection with the access point, the access point usually ignores the packets and sends out a deauthentication packet, which contains the access point's SSID, in plain text. In order to create a fake authentication, we need to associate it with the access point.
29. Switch back to the terminal window where airodump-ng is running. You will observe that the hidden SSID associated with **BSSID B4:75:0E:89:00:60** appears under ESSID as **CEH-LABS**, as shown in the screenshot.

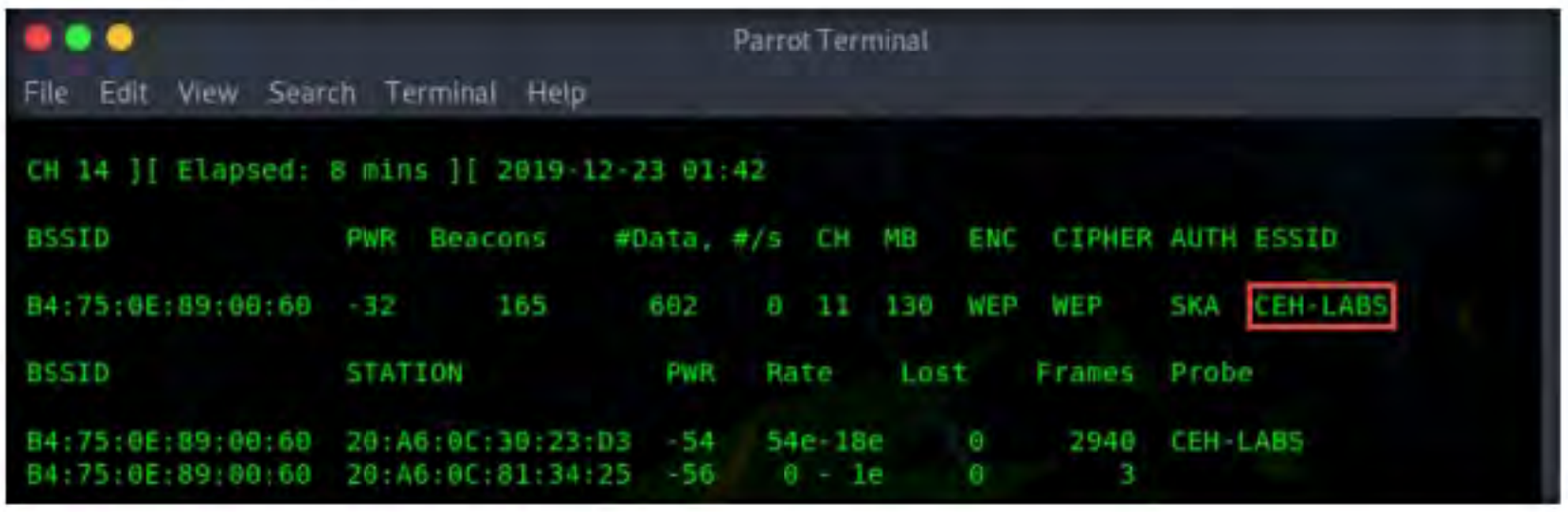

Figure 3.1.11: Stop capturing the packets in airodump-ng

Note: In real-life attacks, attackers will obtain the hidden SSID of the target access point and crack the encryption method (WEP, WPA2) associated with it to obtain the access key or password.

30. This concludes the demonstration of how to use Aircrack-ng to reveal a hidden SSID.
31. Unplug the **Linksys 802.11 g WLAN** adapter.
32. Close all open windows and document all the acquired information.
33. Turn off the **Parrot Security** virtual machine.

TASK 2

Crack a WEP Network using Wifiphisher

Here, we will use Wifiphisher to crack a WEP network. You can also crack a WPA/WPA2 network with the same tool, but, if you do so, the steps might change.

Wifiphisher is a rogue access point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, pen testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks.

Note: Before starting this lab, unhide the hidden SSID of the target access point (**CEH-LABS**).

Note: To perform this task, you must have a mobile device (in this example, we are using an Android phone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created by Wifiphisher, and once he/she enters the pre-shared WEP key, it will be captured by the application.

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.

Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients in order to capture credentials (such as from third party login pages or WPA/WPA2 Pre-Shared Keys) or infect the victim stations with malware.

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**.

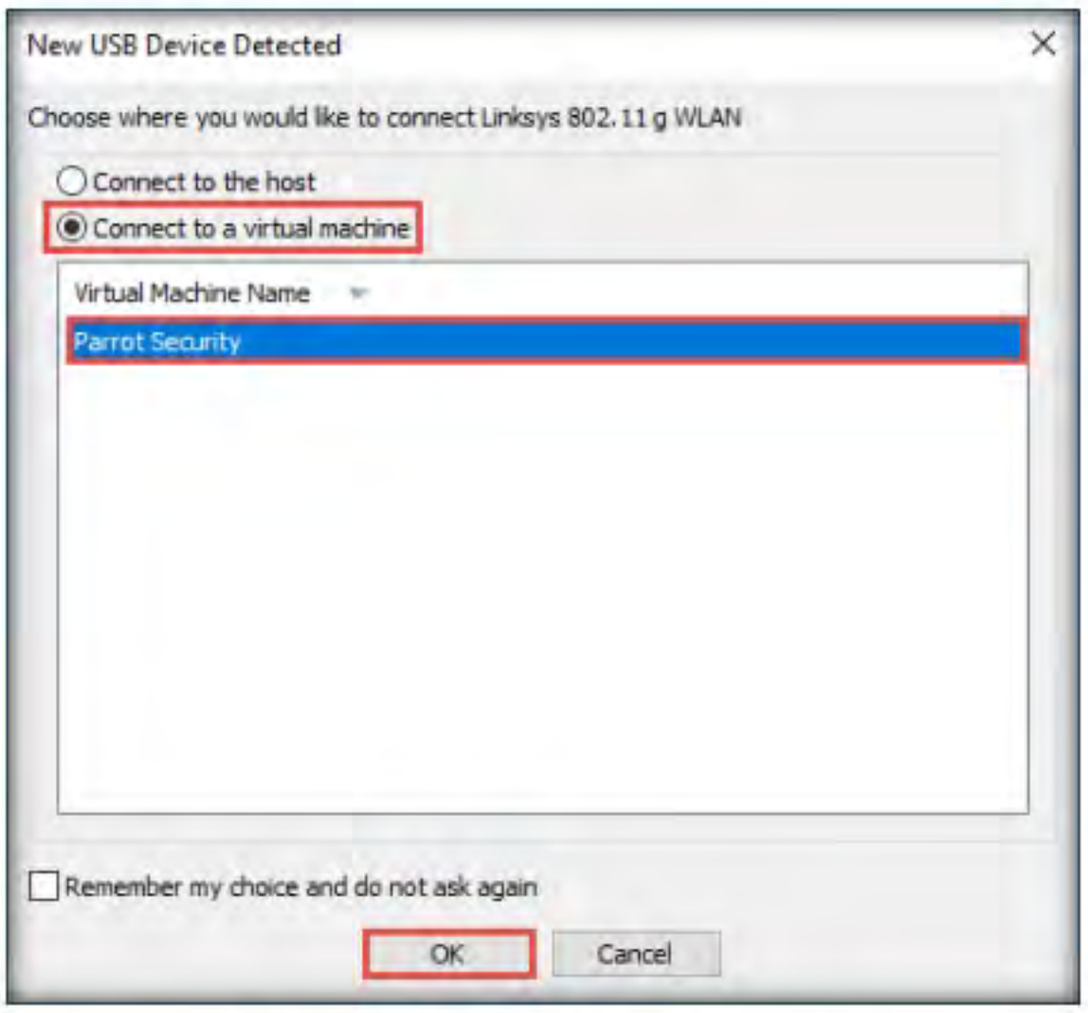

Figure 3.2.1: New USB Device Detected window

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.

TASK 2.1

Install Dependencies

9. In the **Parrot Terminal** window, type **apt-get install libnl-3-dev libnl-genl-3-dev** and press **Enter** to install the dependencies for Wifiphisher.

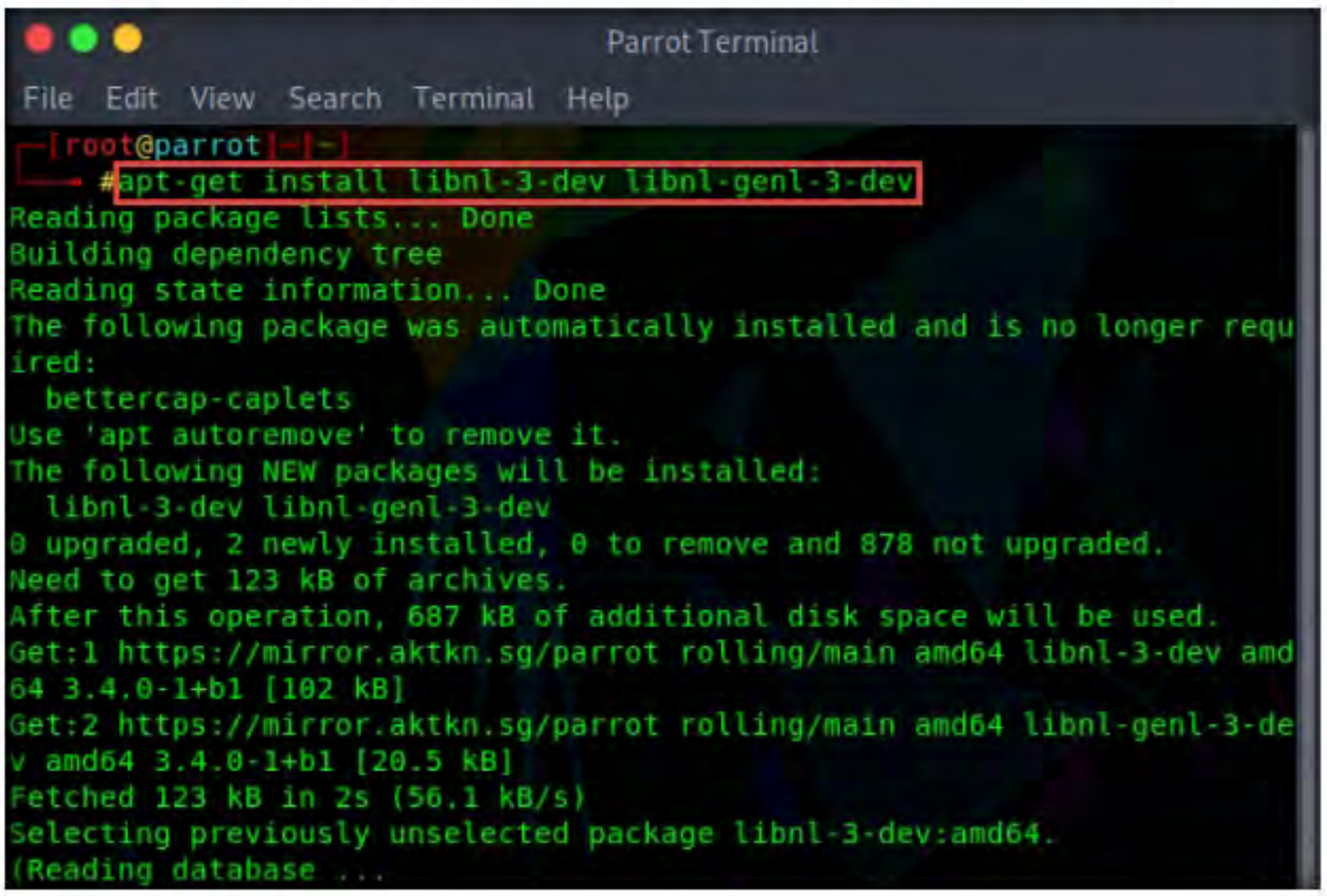

Figure 3.2.2: Installing the libnl-3-dev libnl-genl-3-dev dependency

10. Once the installation has finished, type **apt-get install libssl-dev** in the terminal window and press **Enter** to install the **libssl-dev** dependency.

Note: If the above command does not work, then run the **dpkg --configure -a** command before trying **apt-get install libssl-dev** again.

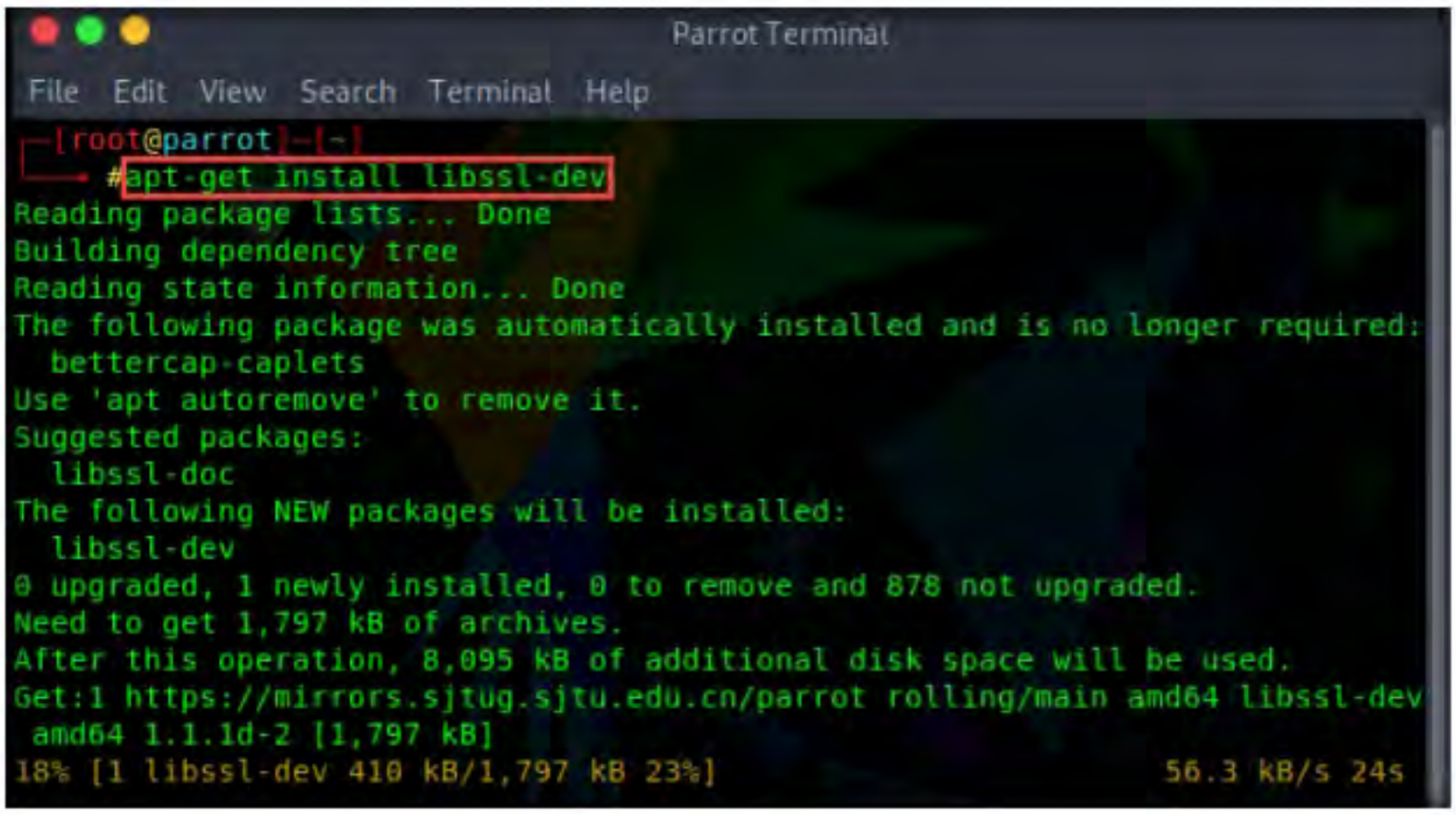

Figure 3.2.3: Installing the libssl-dev dependency

11. Once the installation has completed, type **git clone https://github.com/wifiphisher/roguehostapd** and press **Enter** to clone the **roguehostapd** repository.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks/GitHub Tools/** and copy the **roguehostapd** folder.
- Paste the copied **roguehostapd** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/roguehostapd /root/**.

12. After cloning roguehostapd, type **cd roguehostapd** and press **Enter** to navigate to the cloned repository.
13. Now, type **python setup.py install** and press **Enter** to install the roguehostapd application.

Note: Roguehostapd is a fork of hostapd, the famous user space software access point. It provides Python ctypes bindings and a number of additional attack features. It was primarily developed for use in the Wifiphisher project.

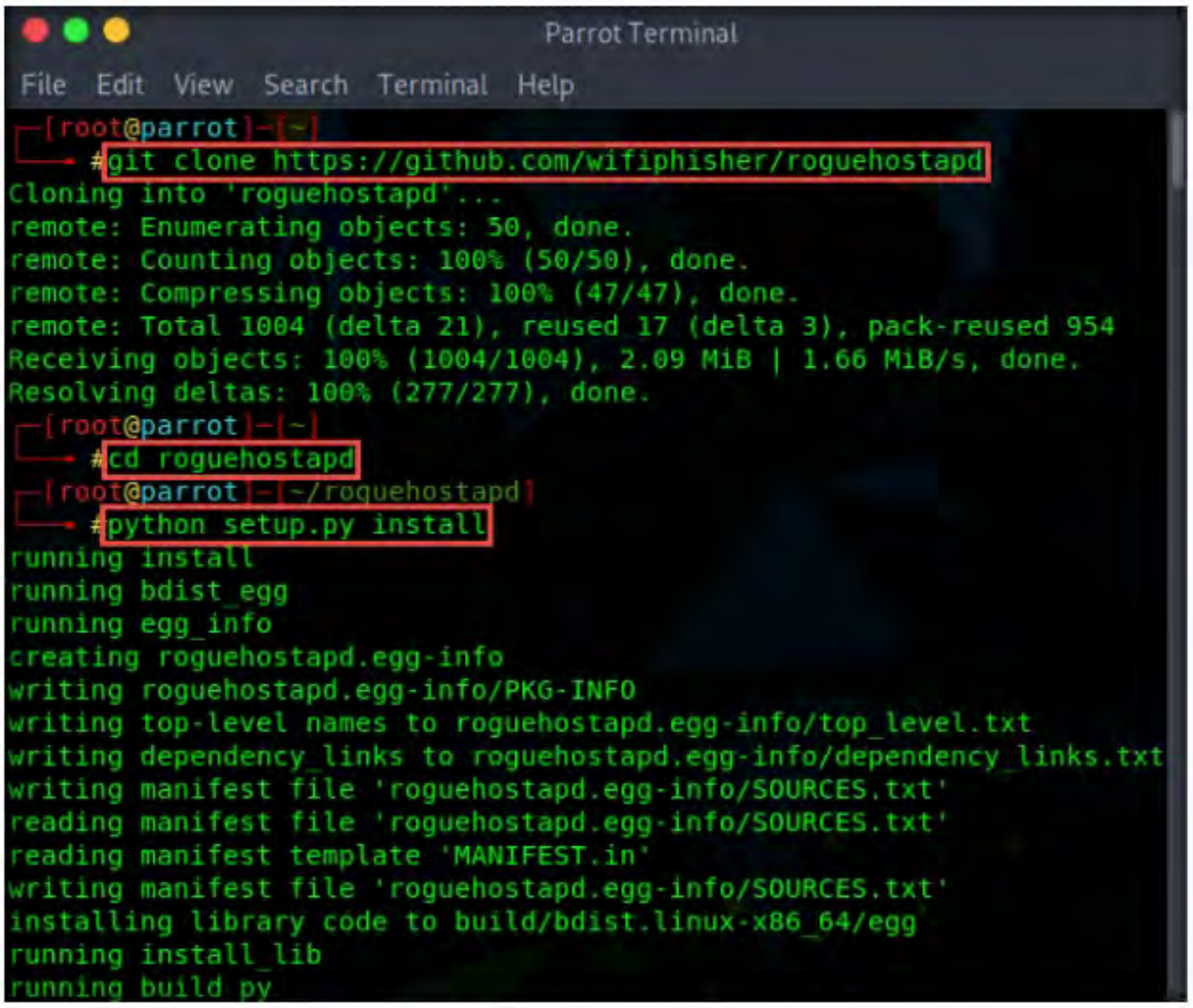

Figure 3.2.4: Cloning and installing roguehostapd

14. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the **root** directory.

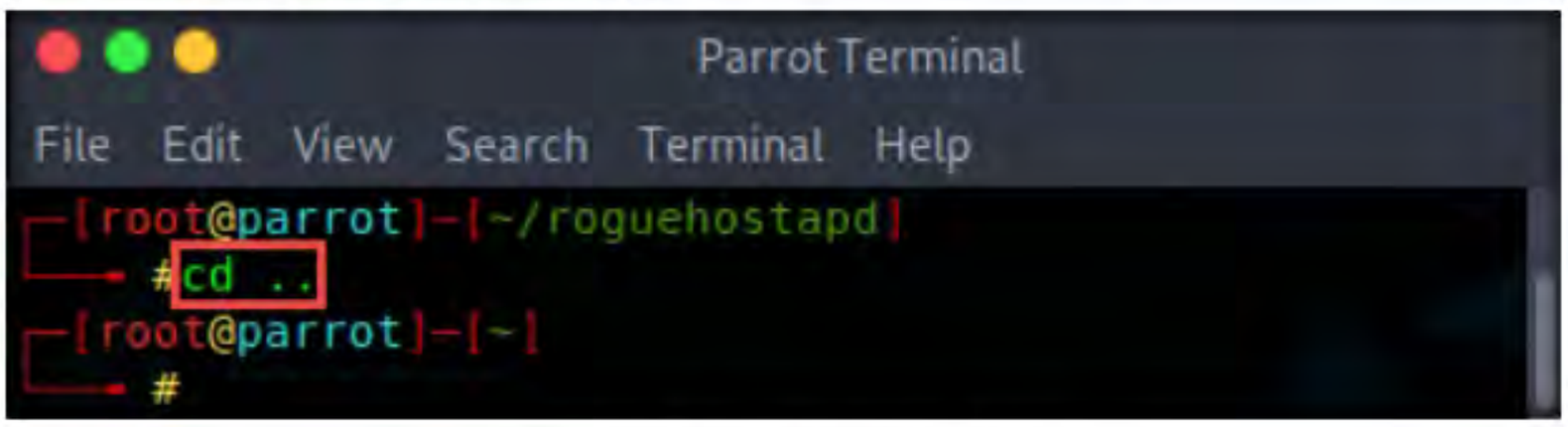

Figure 3.2.5: Navigating to the root directory

TASK 2.2

Clone Wifiphisher

15. Now that all the required dependencies have been installed, it is time to clone and install Wifiphisher. Type **git clone https://github.com/wifiphisher/wifiphisher** and press **Enter** to clone the Wifiphisher repository.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks/GitHub Tools/** and copy the **wifiphisher** folder.
- Paste the copied **wifiphisher** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/wifiphisher /root/**.

16. After cloning Wifiphisher, type **cd wifiphisher** and press **Enter** to navigate to the cloned repository.

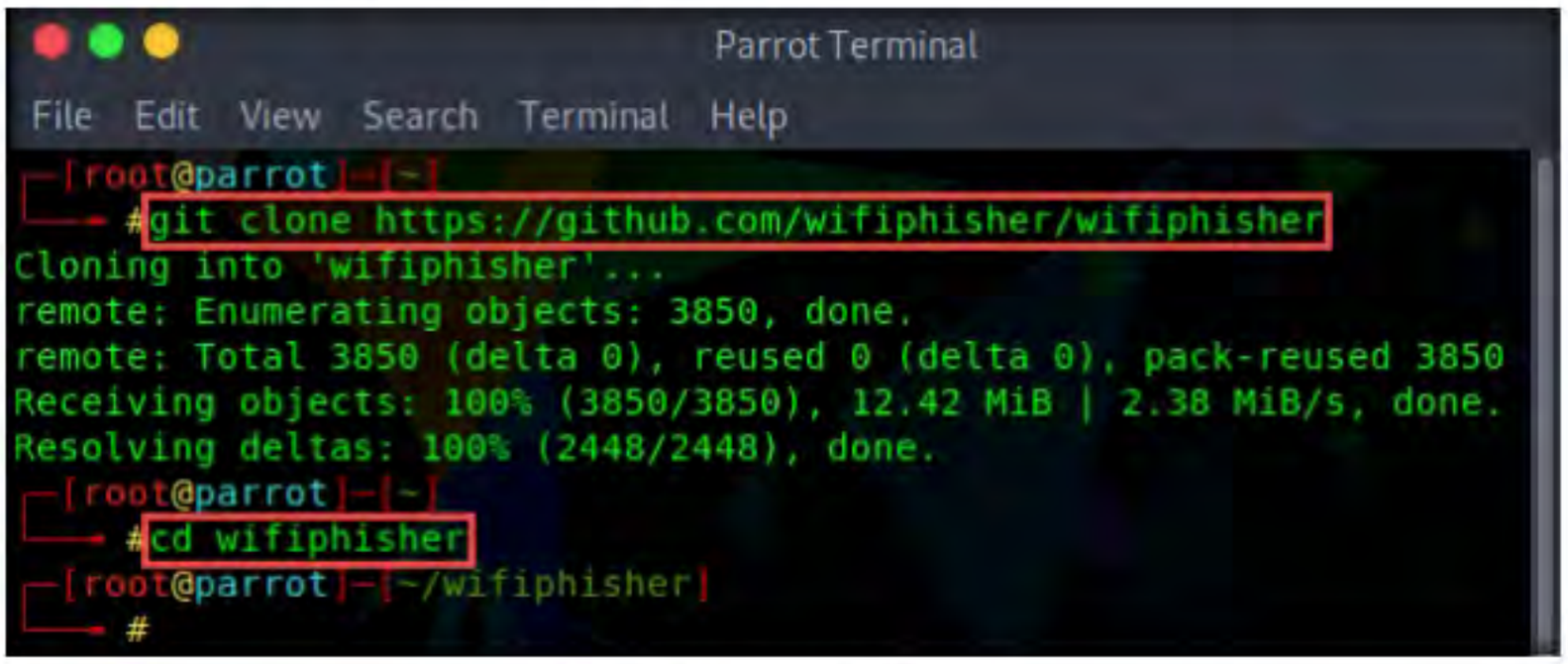

Figure 3.2.6: Cloning Wifiphisher

17. Now, type **python3 setup.py install** and press **Enter** to install Wifiphisher.

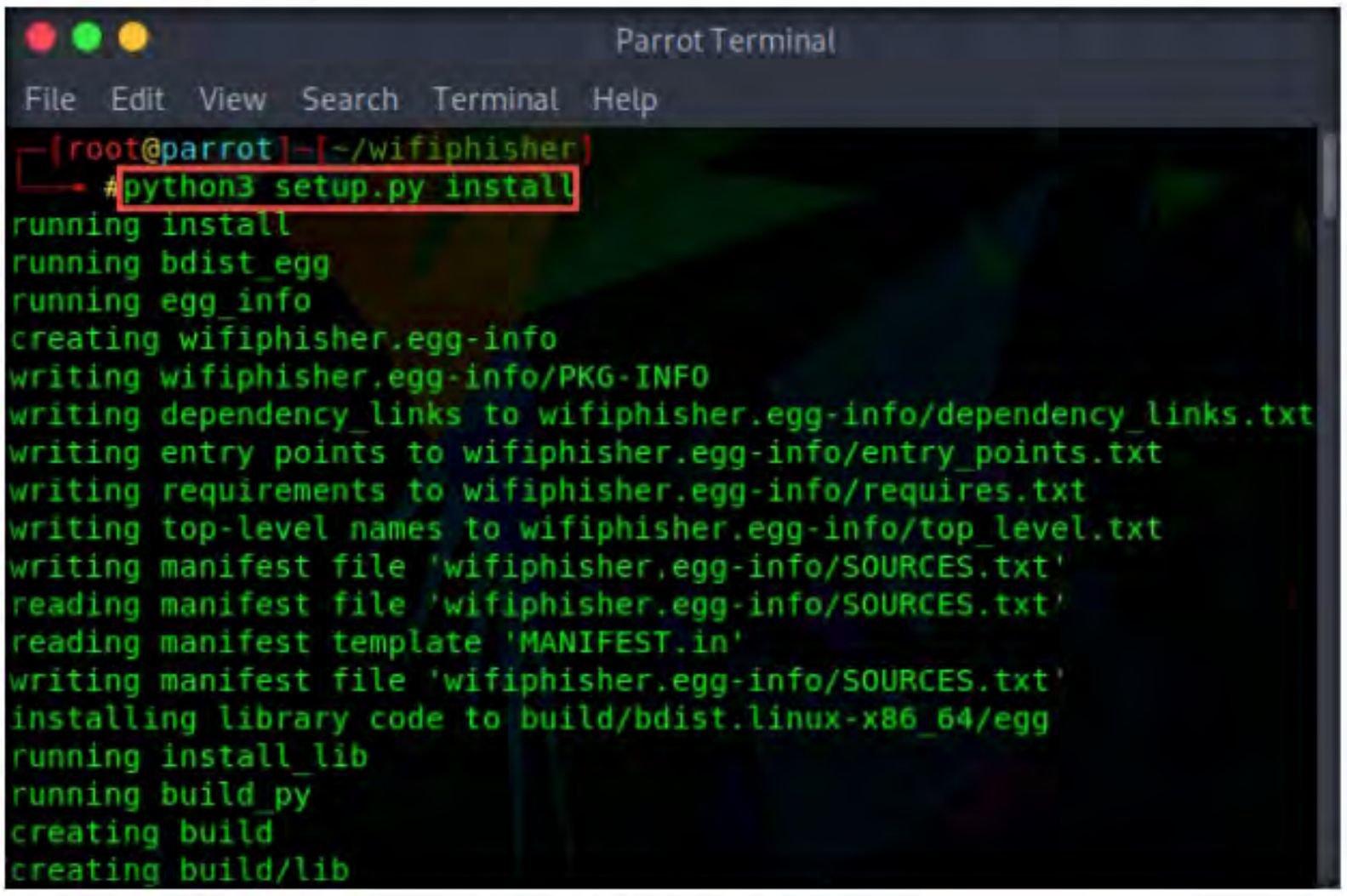

Figure 3.2.7: Installing Wifiphisher

18. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the **root** directory.

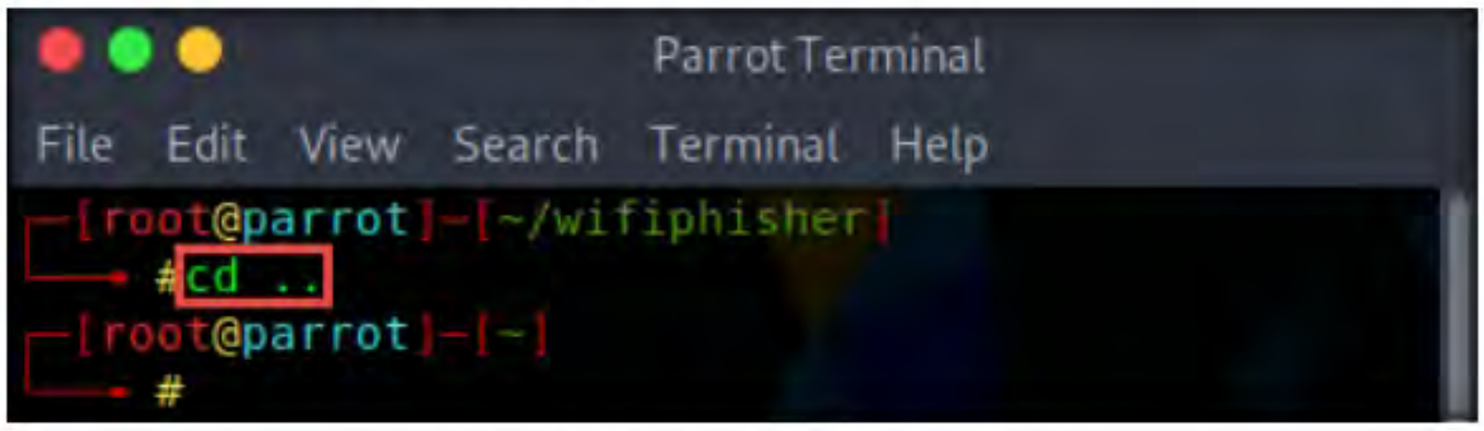

Figure 3.2.8: Navigating to the root directory

19. Type **wifiphisher --force-hostapd** and press **Enter** to launch the Wifiphisher application.

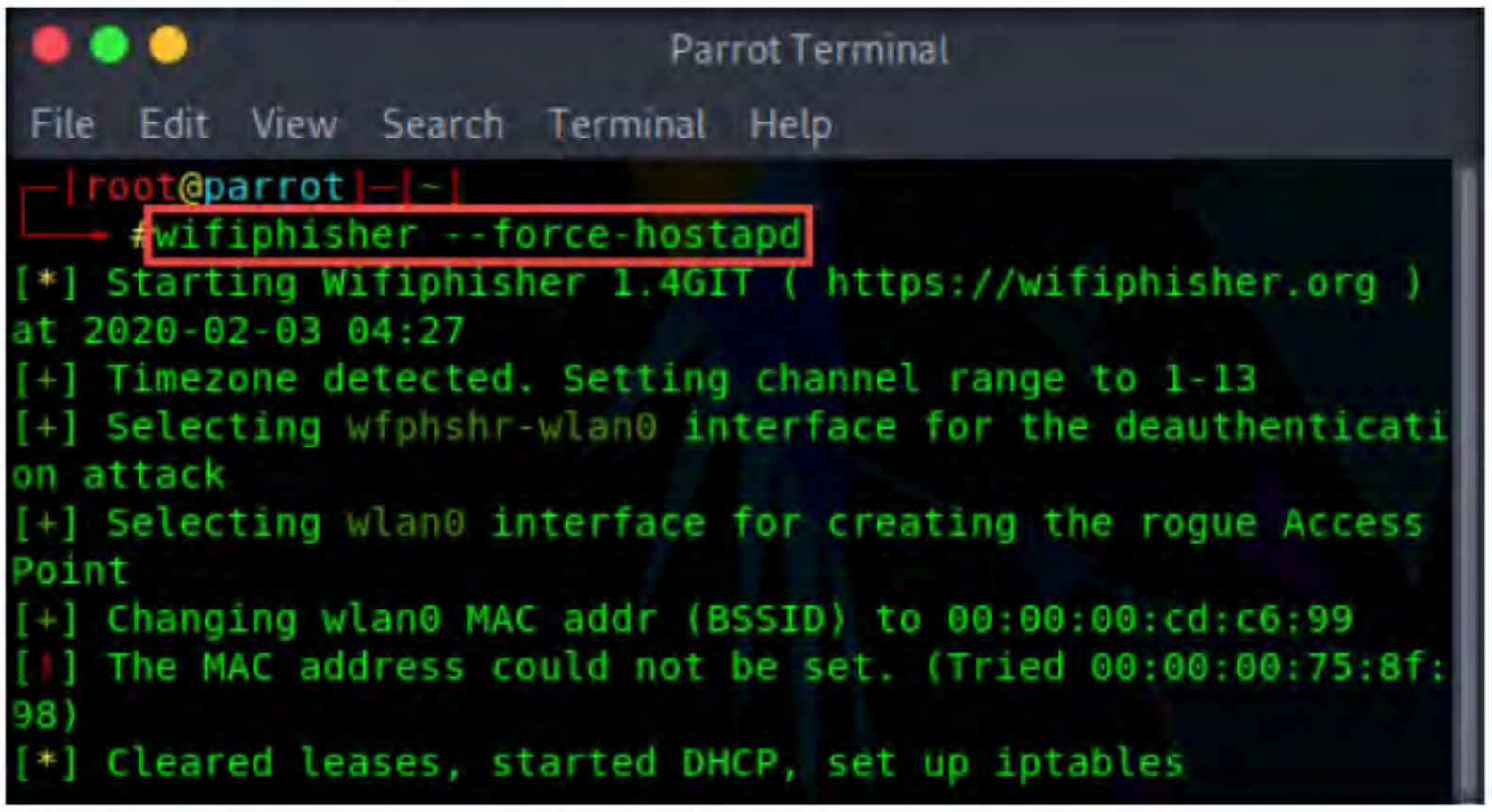

Figure 3.2.9: Launch Wifiphisher

20. **Wifiphisher** initializes and appears in the **Parrot Terminal** window.
21. It scans the network for available access points and displays them, as shown in the screenshot.
22. 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**.
23. Note the **YOU HAVE SELECTED CEH-LABS** notification in the lower section of the window.

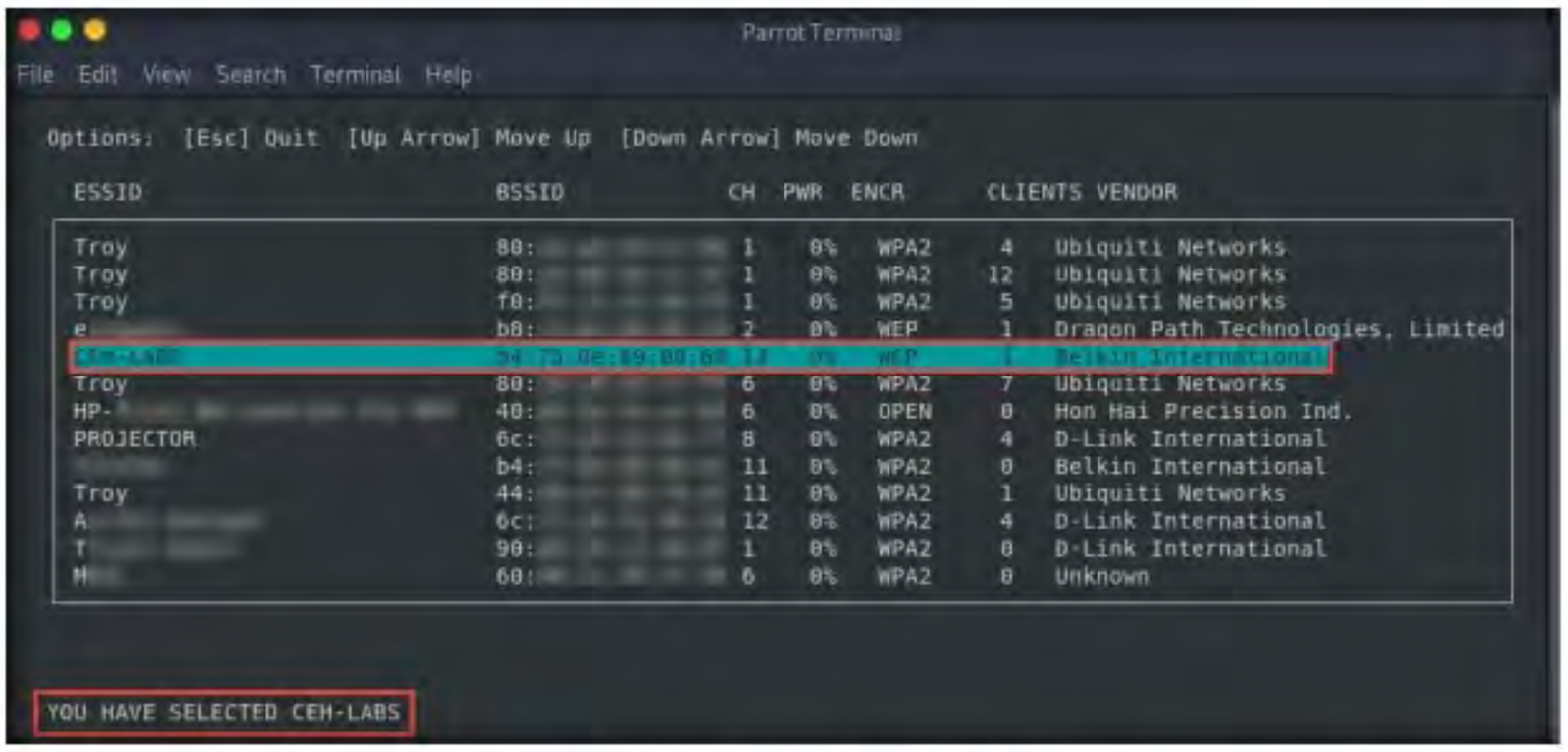

Figure 3.2.10: Discovered access points

24. 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.

25. 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.

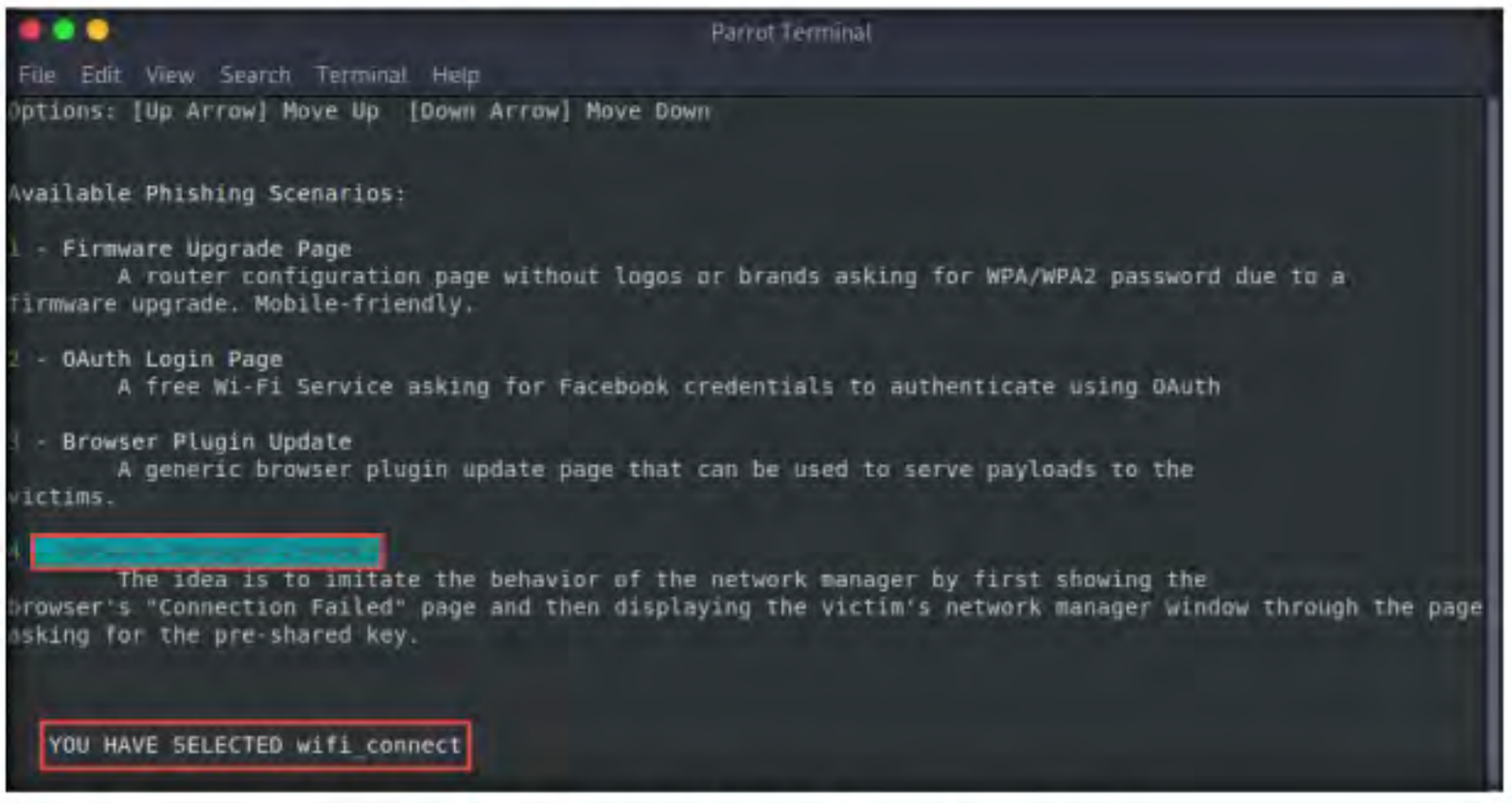

Figure 3.2.11: Selecting the Network Manager Connect option

26. 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.

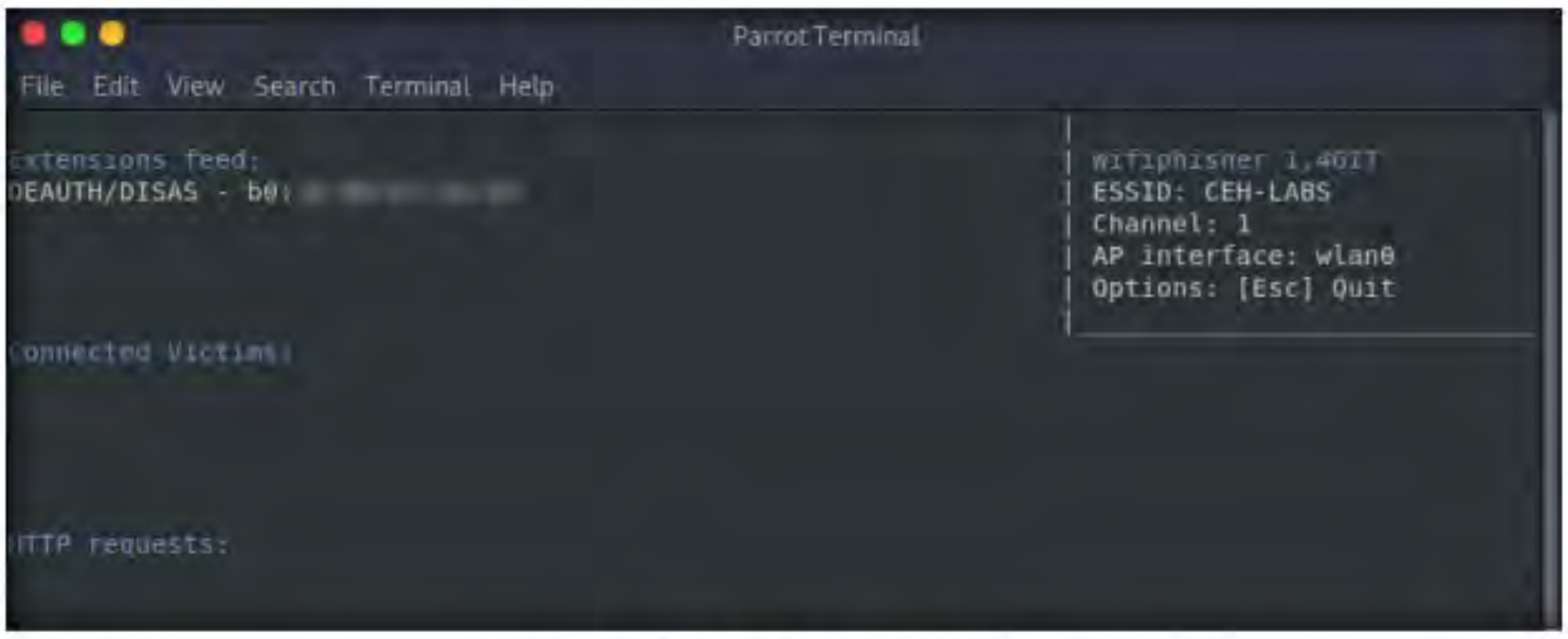

Figure 3.2.12: Sending deauth packets

27. 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.

TASK 2.3

Connect to Rogue Access Point Using Pre-shared Key

28. Observe that the rogue access point does not have any security enabled.

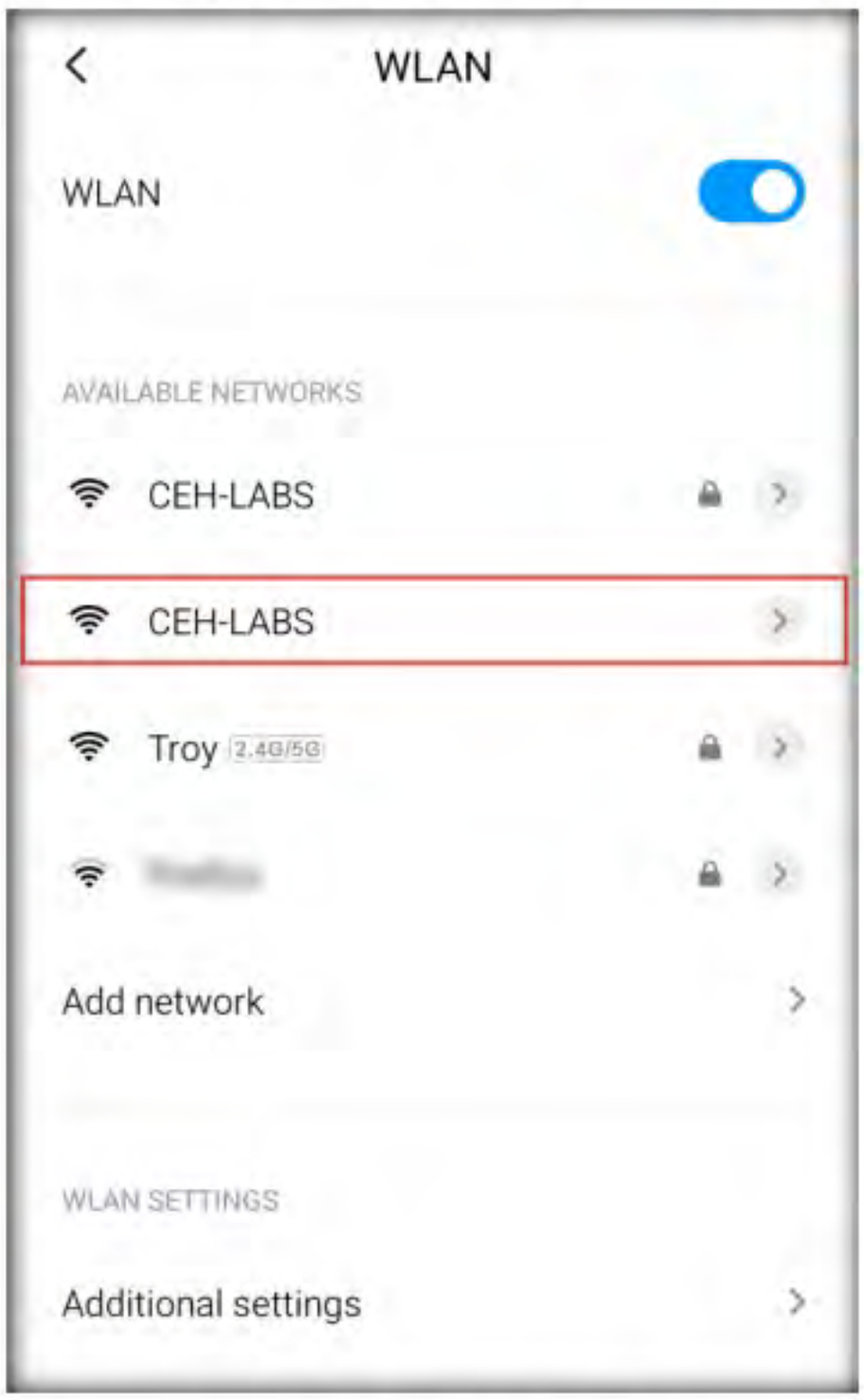

Figure 3.2.13: The new rogue access point

29. 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.

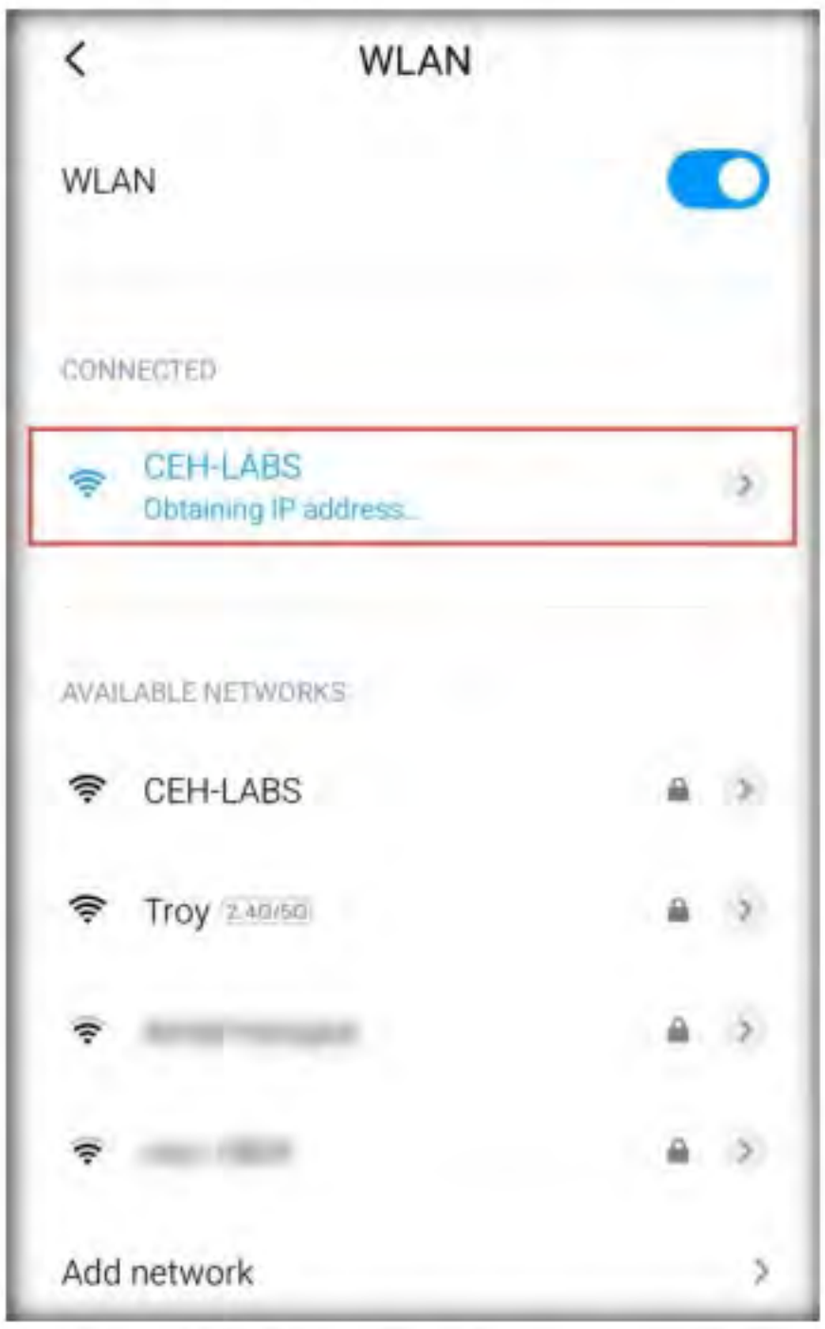

Figure 3.2.14: Connecting to the rogue access point

30. After your device has connected to the **CEH-LABS** access point, you will notice that there is no Internet.

Note: Connecting to the rogue access point may take some time.

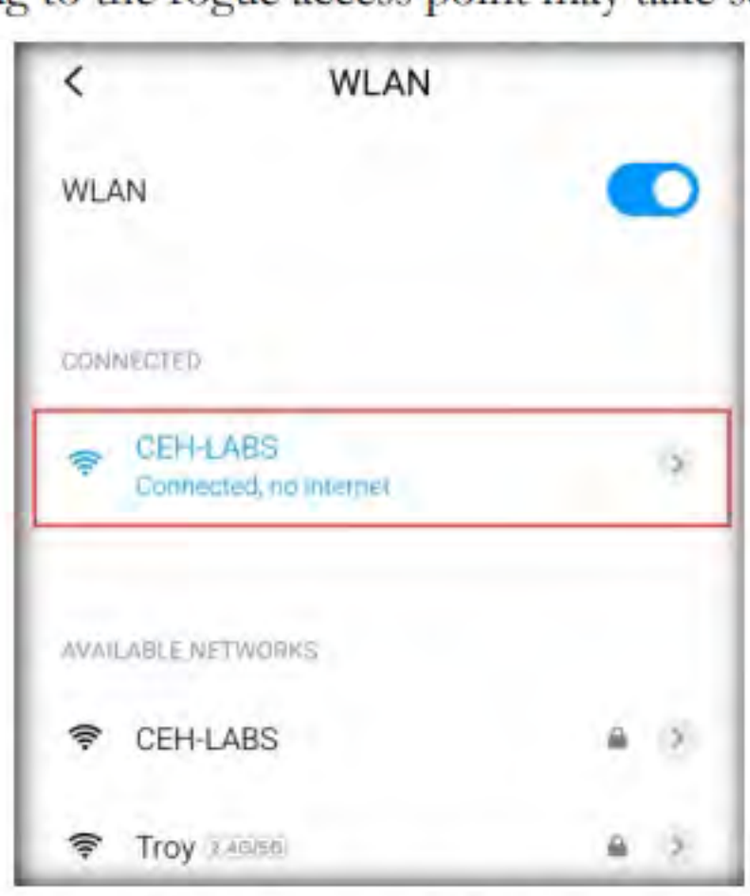

Figure 3.2.15: Connection established with no internet

31. 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.

Figure 3.2.16: The connected victim

32. Switch back to your connected **Android** device. Slide down from the top of the device and tap the **Connect to Wi-Fi** option, as shown in the screenshot.

Note: If you are immediately redirected to the **Enter the password for "CEH-LABS"** page, proceed directly to **Step 33**.

Figure 3.2.17: Connect to Wi-Fi

TASK 2.4

Crack WEP Pre-shared Key

33. 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**.

Figure 3.2.18: Enter the pre-shared WEP key

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

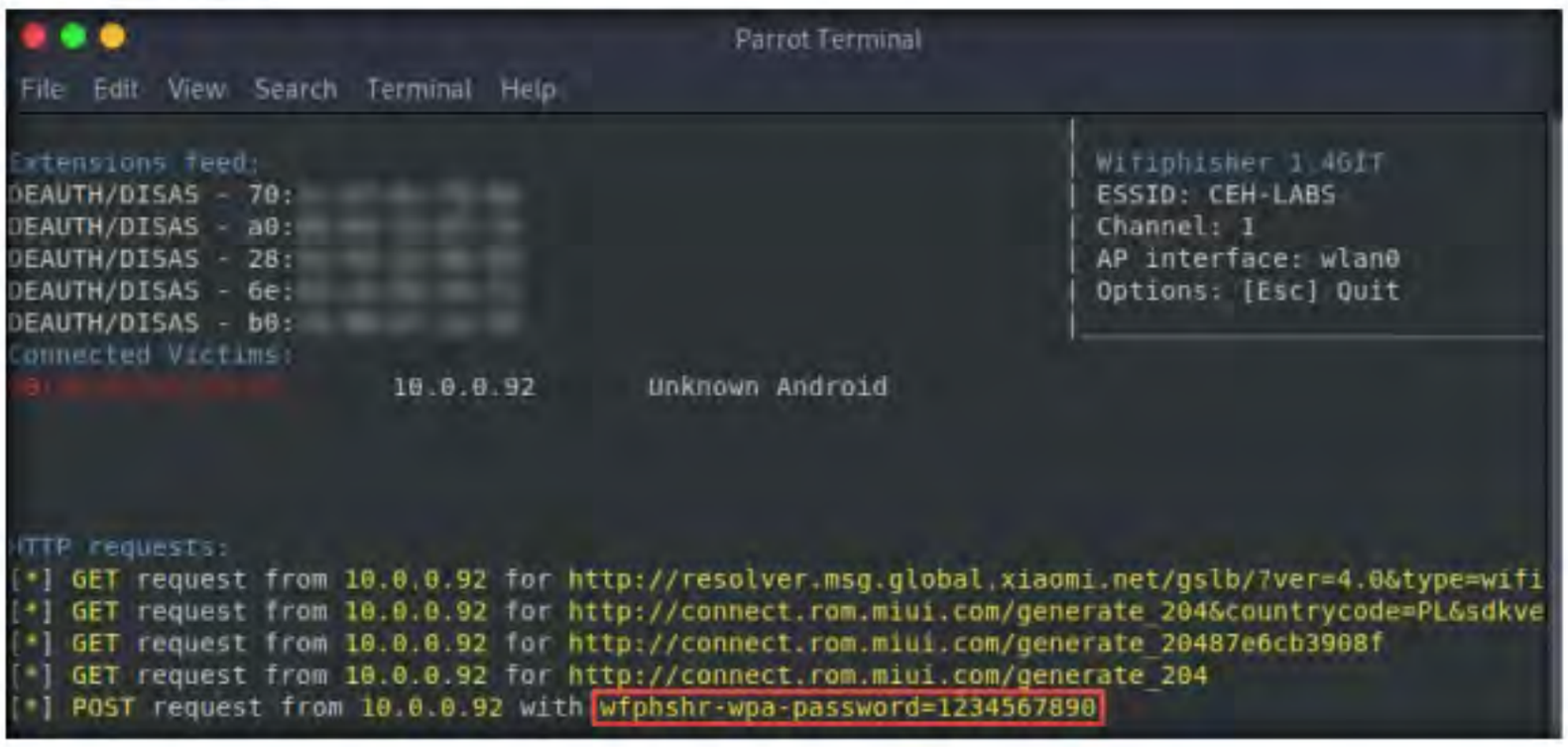

Figure 3.2.19: Captured WEP Key

35. After obtaining the key, press **Esc** in the **Wifiphisher** application window to quit.
36. This concludes the demonstration of how to crack a WEP network using Wifiphisher.
37. Close all open windows and document all the acquired information.

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: Before starting this lab, unhide the hidden SSID of the target 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**.

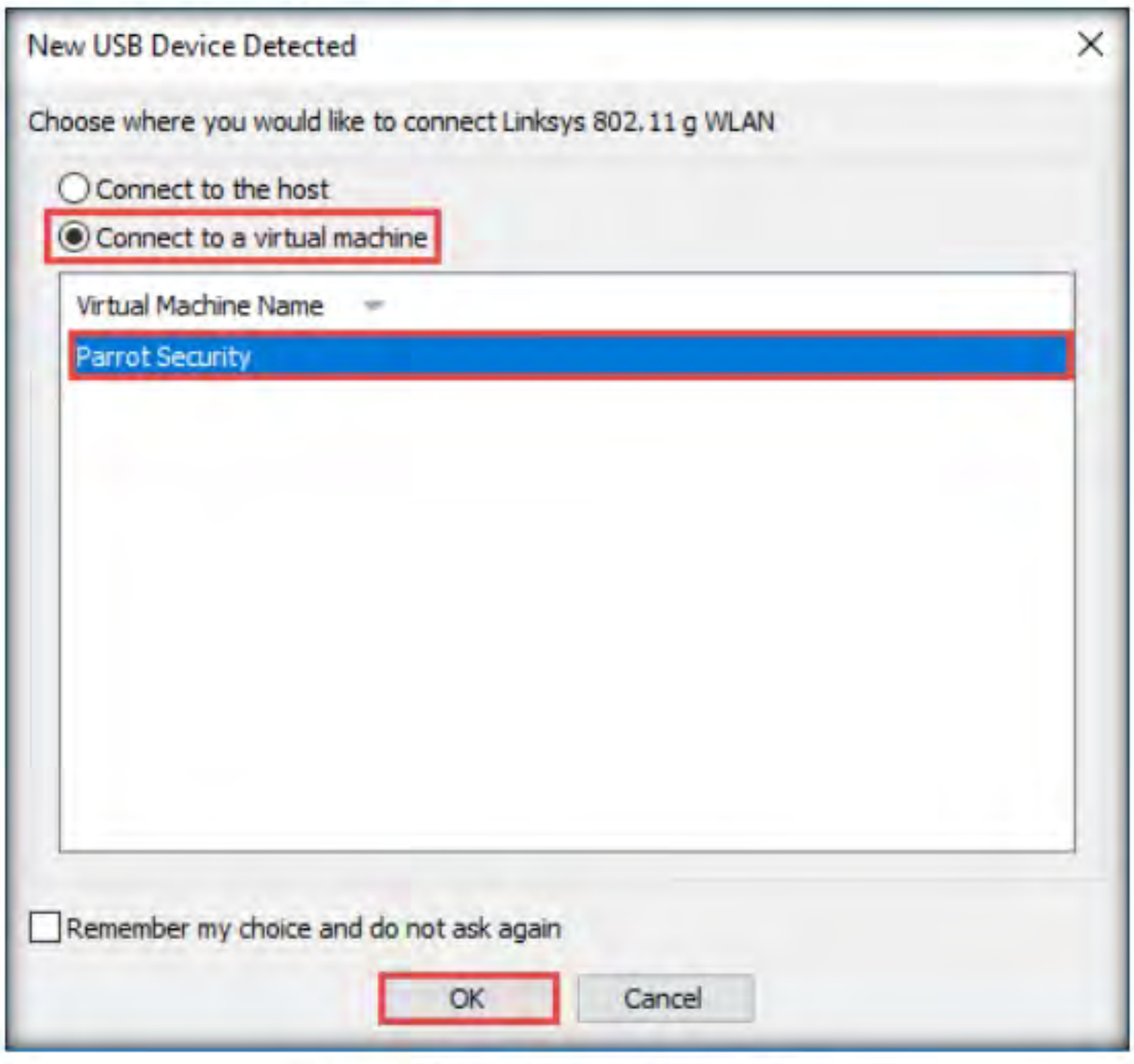

Figure 3.3.1: New USB Device Detected window

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

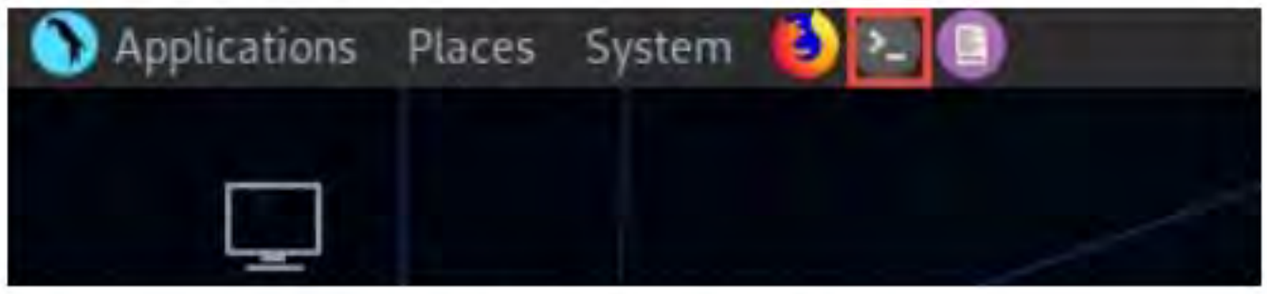

Figure 3.3.2: MATE Terminal icon

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.

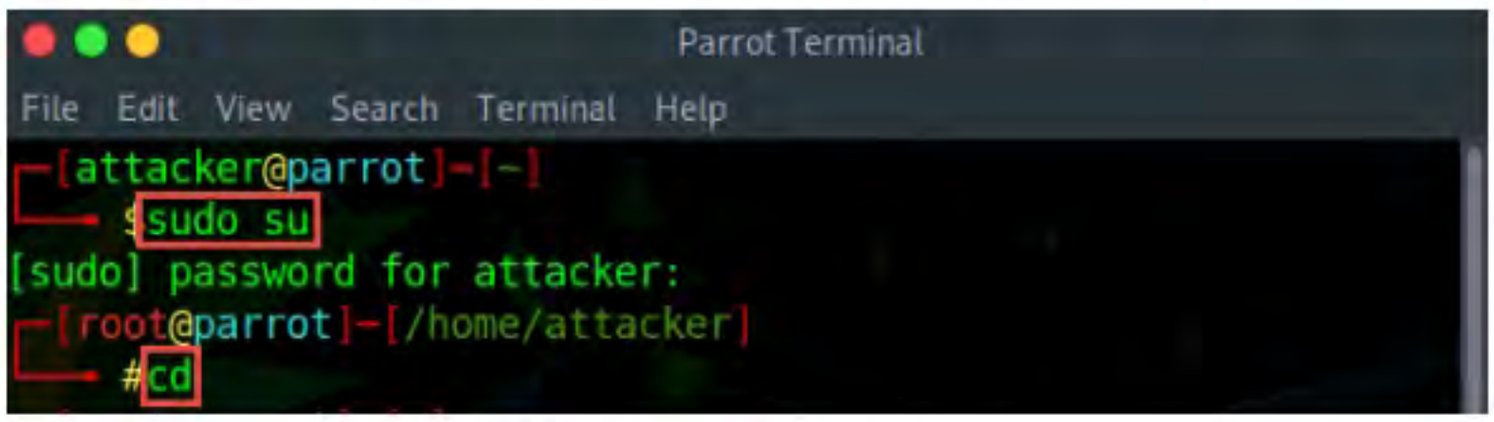

Figure 3.3.3: Running the programs as a root user

TASK 3.1

Put the Wireless Interface into Monitor Mode

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. 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.

Note: The processes might differ in your lab environment.

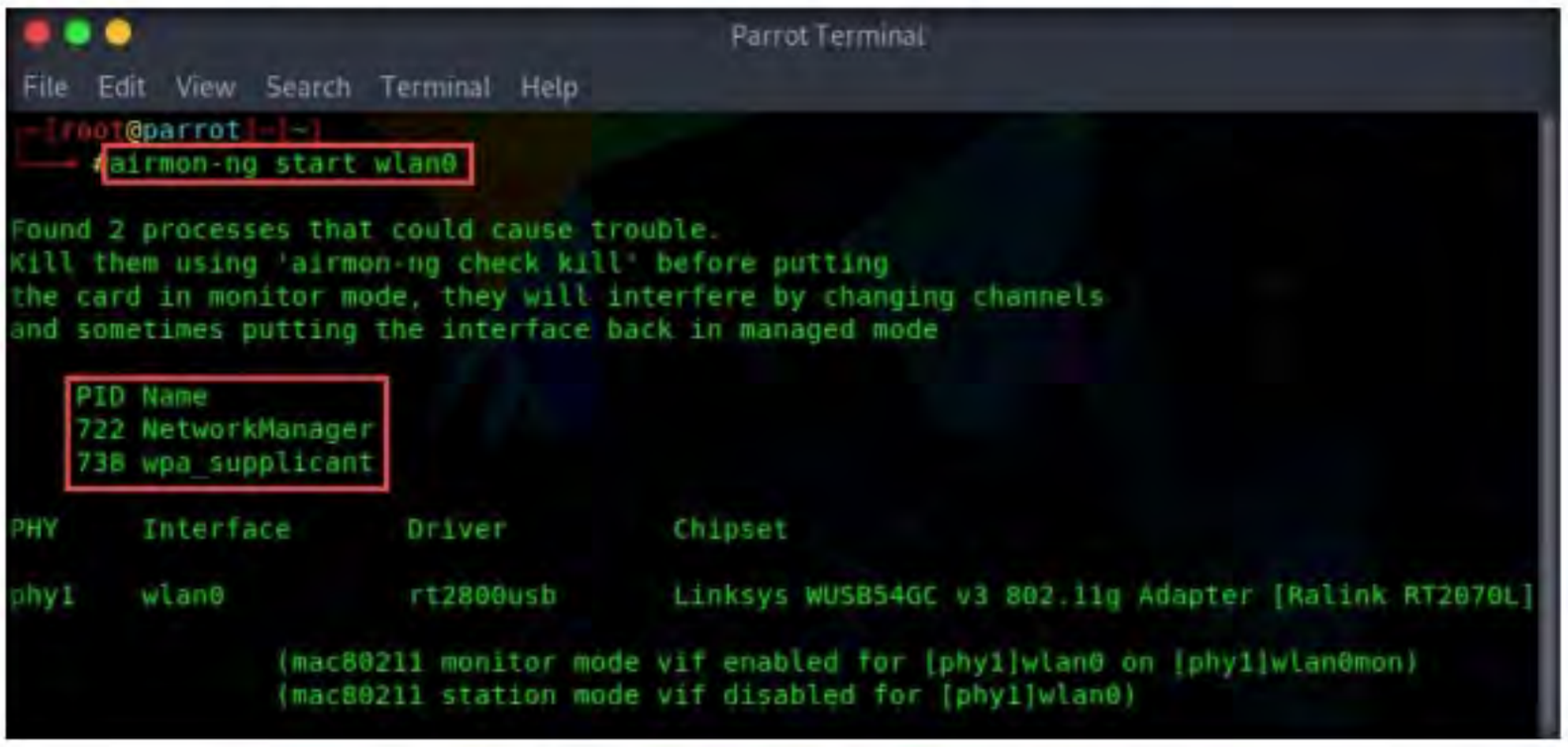

Figure 3.3.4: Found 2 processes that could cause trouble error

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

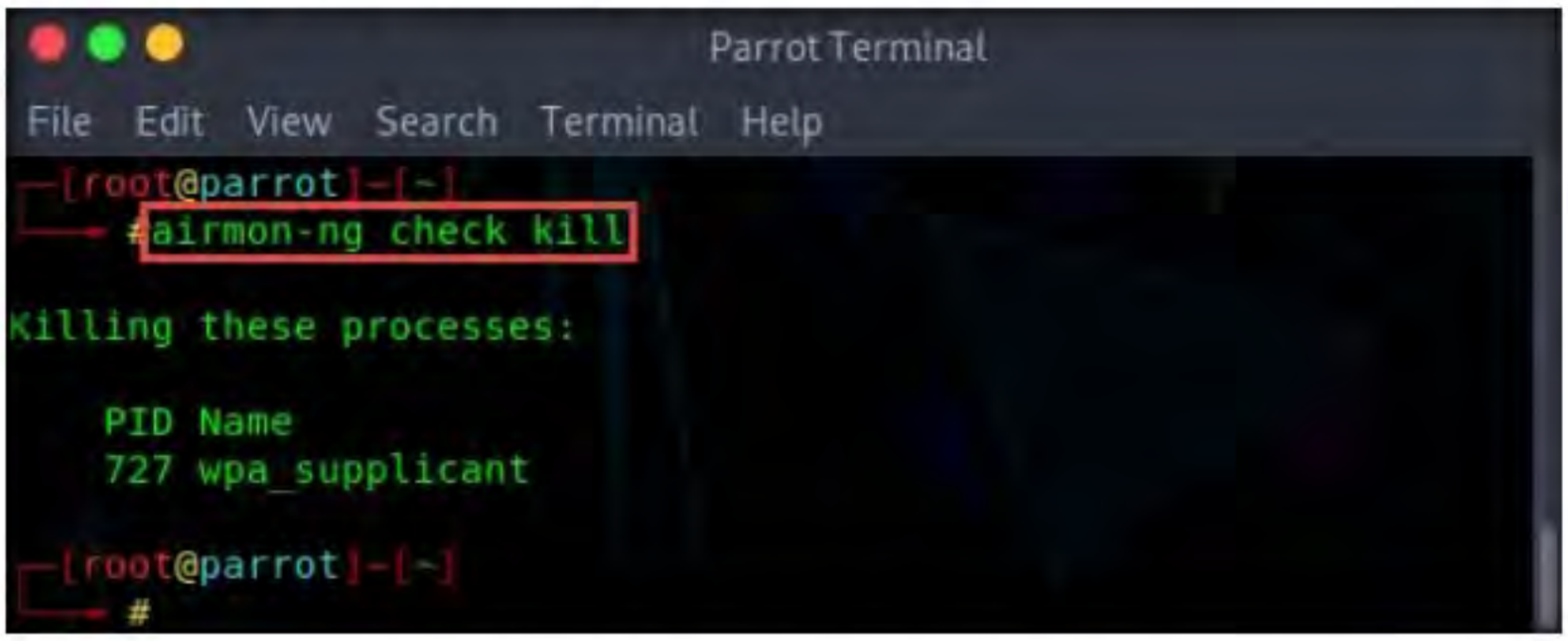

Figure 3.3.5: Issuing command to kill interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

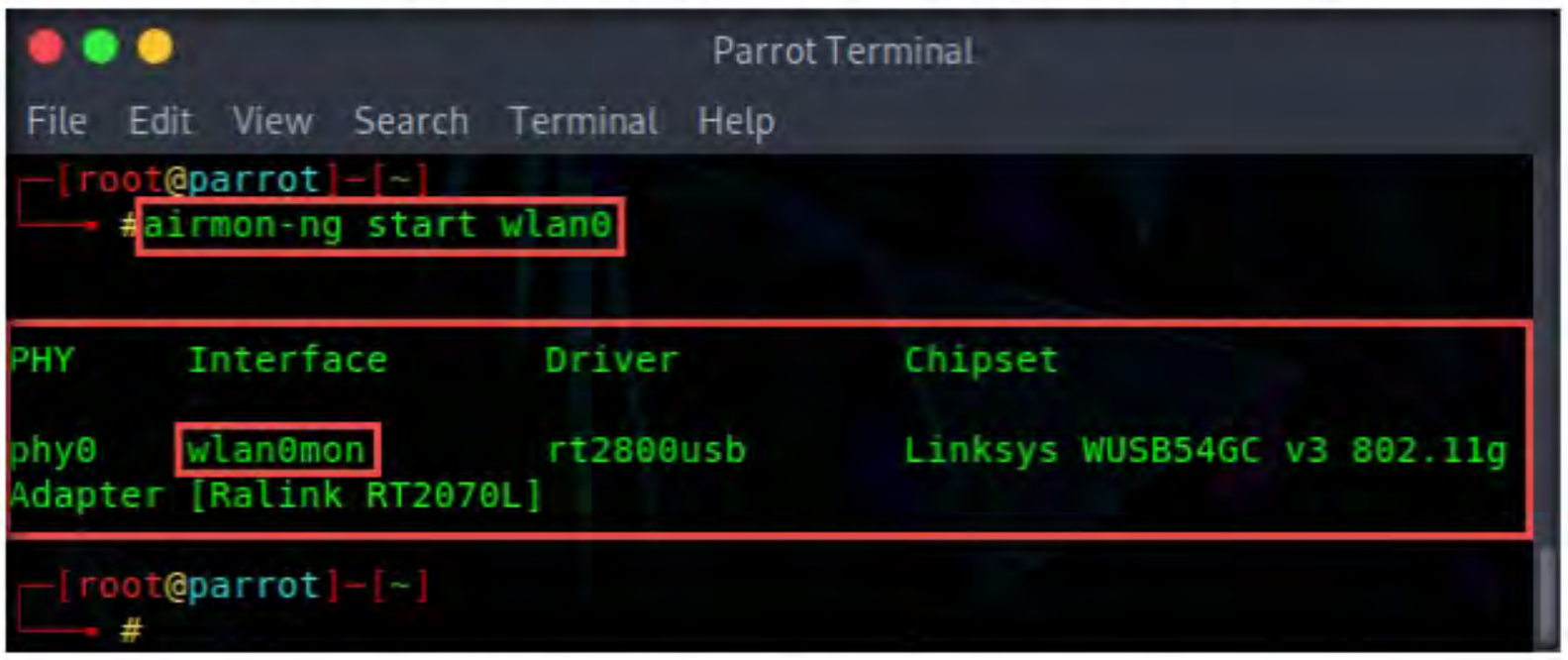

Figure 3.3.6: Setting up the wireless interface in monitor mode

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

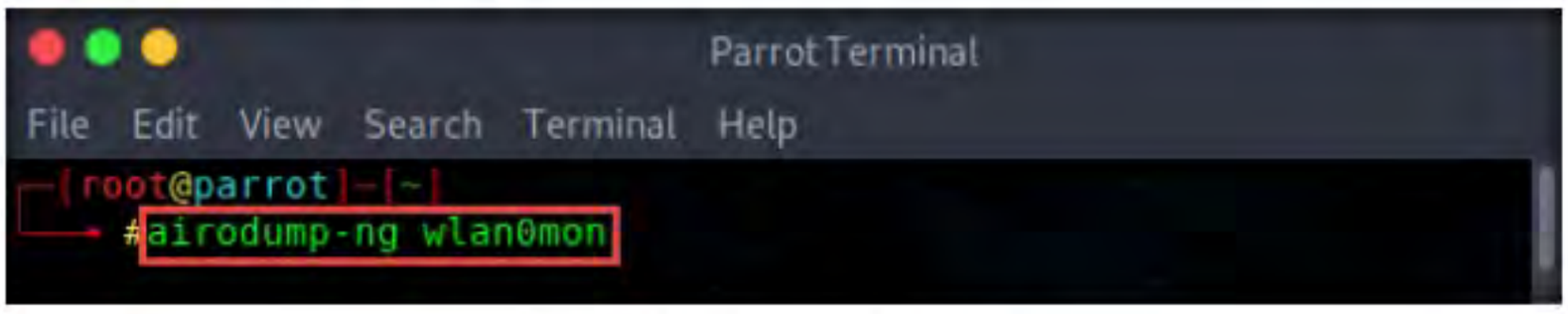

Figure 3.3.7: Launching airodump-ng

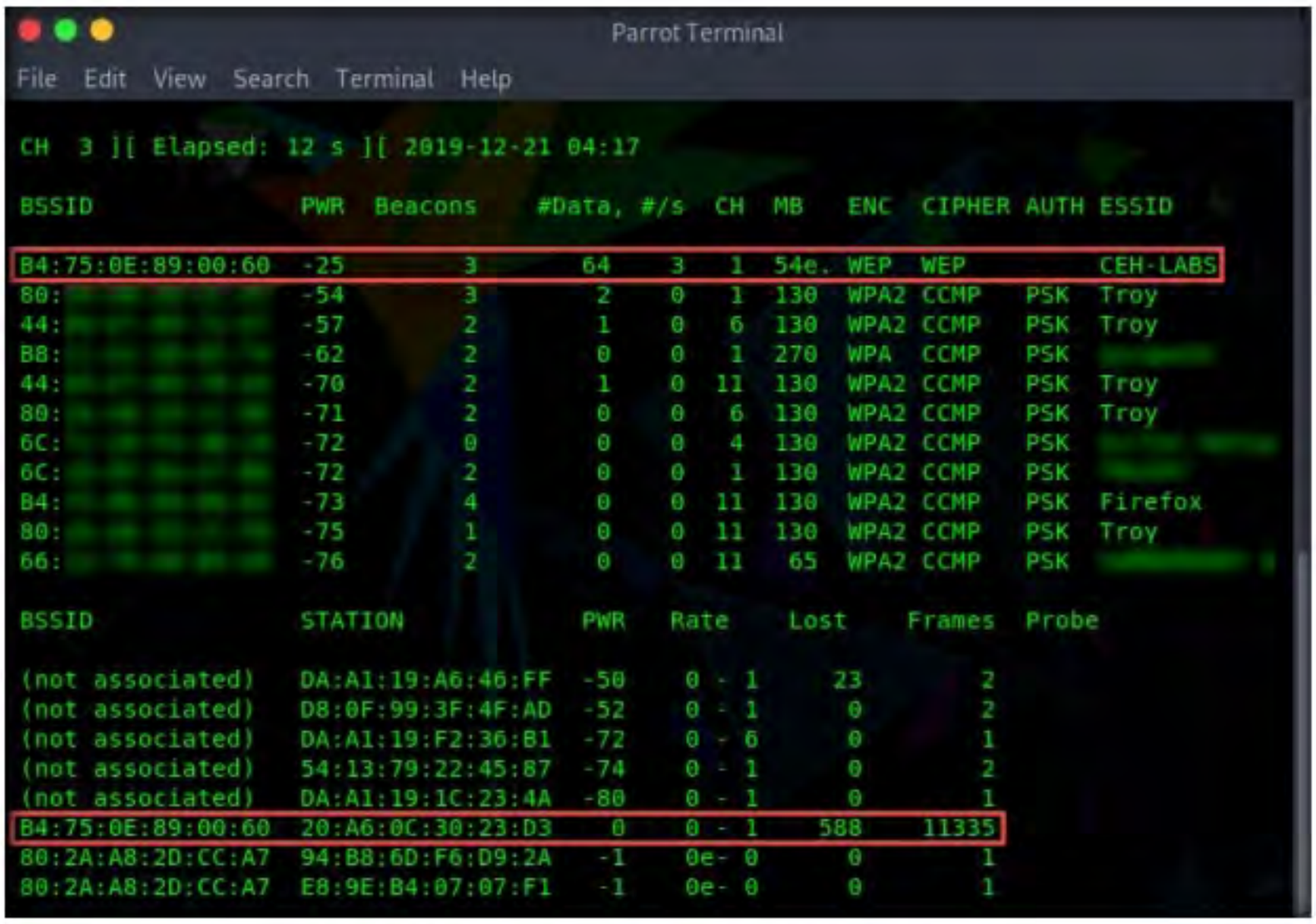

Figure 3.3.8: airodump-ng searching for available access points

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.

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.

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

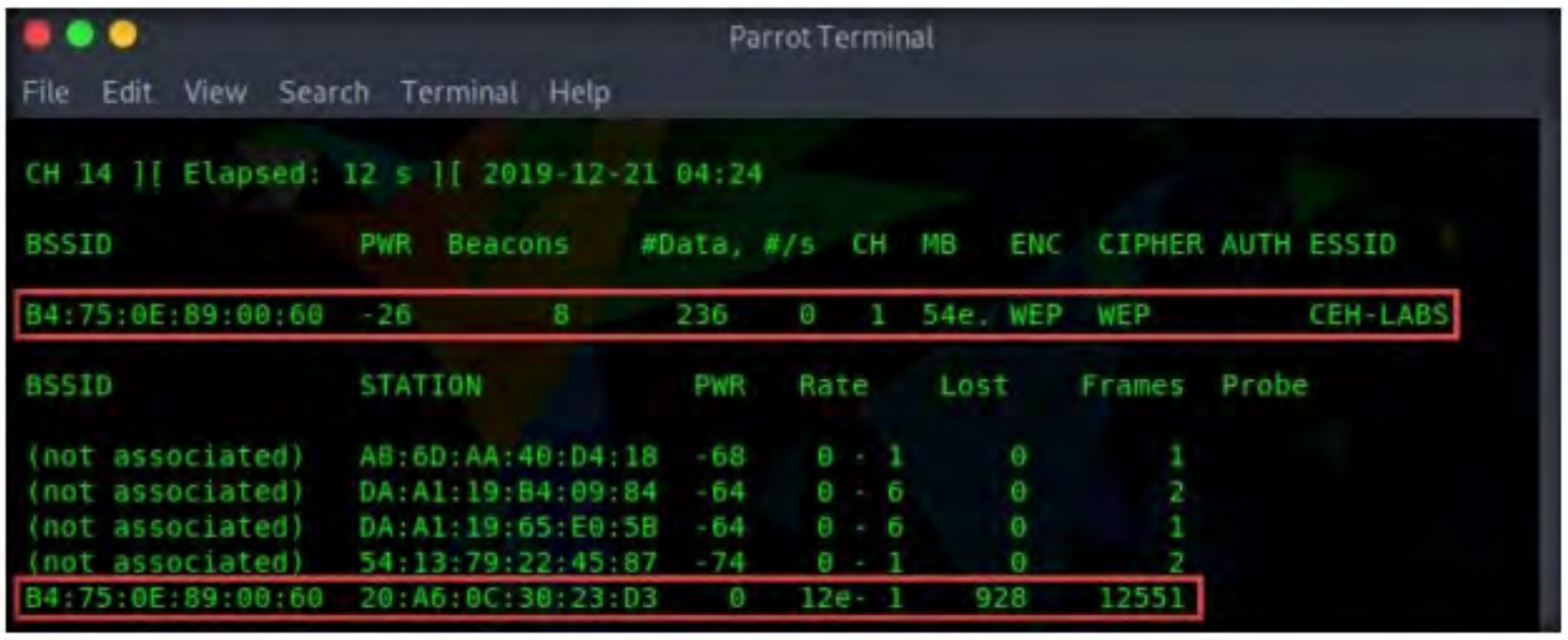

Figure 3.3.9: airodump-ng searching for WEP access points

17. Before proceeding, you must check if an injection attack can be performed on the target access point.

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 new 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.

TASK 3.2

Test for Wireless Device Packet Injection

22. In the terminal window, type **aireplay-ng -9 -e CEH-LABS -a B4:75:0E:89:00:60 wlan0mon** and press **Enter**.

Note: In this command, **-9**: tests injection and quality; **-e**: specifies the target IP access point SSID (in this case, **CEH-LABS**); **-a**: specifies the MAC address of the target access point (in this case, **B4:75:0E:89:00:60**); and **wlan0mon**: is the wireless interface.

23. The result appears, showing that **Injection is working!**, as shown in the screenshot.

Note: If you receive any errors, rerun the command multiple times until it executes successfully.

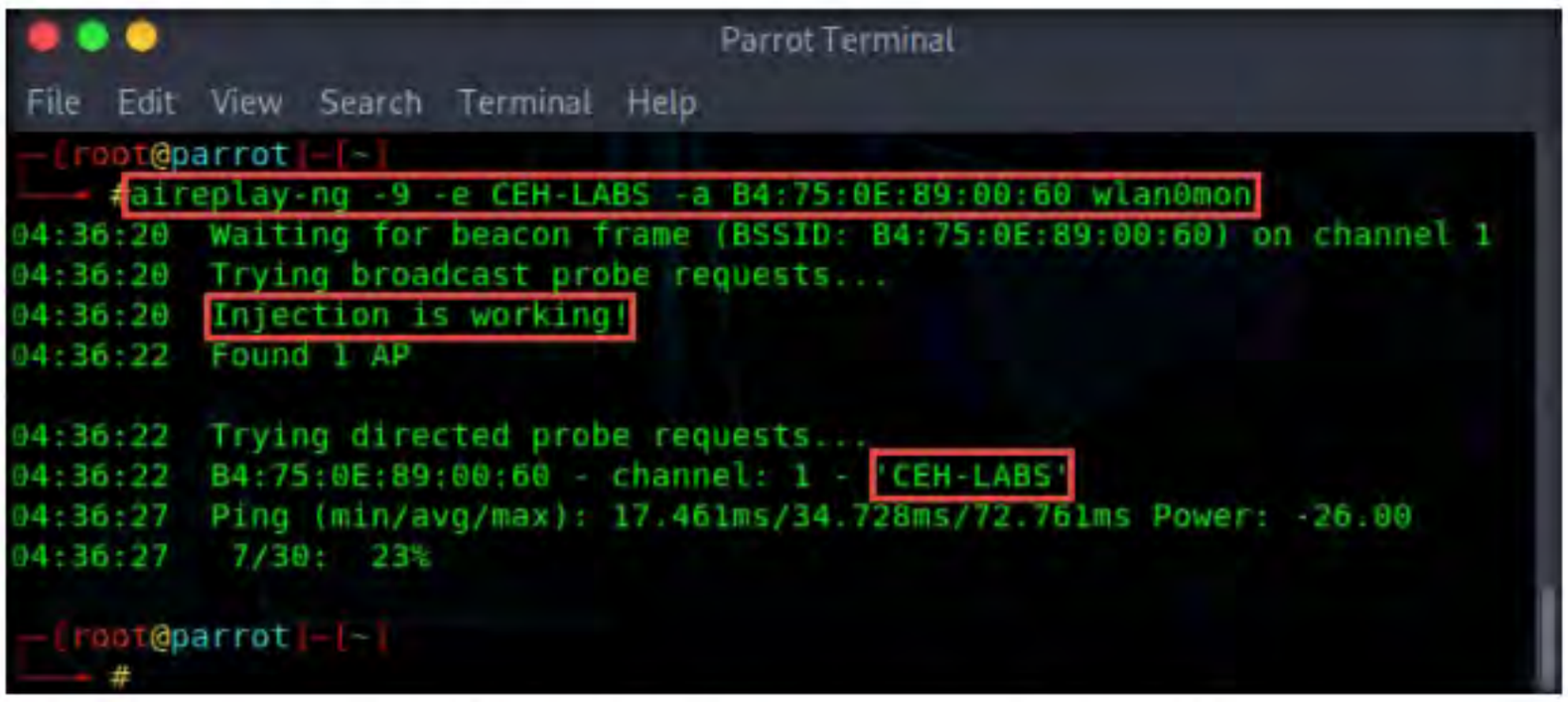

Figure 3.3.10: aireplay-ng checking if an injection attack is possible

TASK 3.3

Capture IV Packets from the Target Access Point

24. 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 B4:75:0E:89:00:60 -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, **B4:75:0E:89:00:60**); **-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

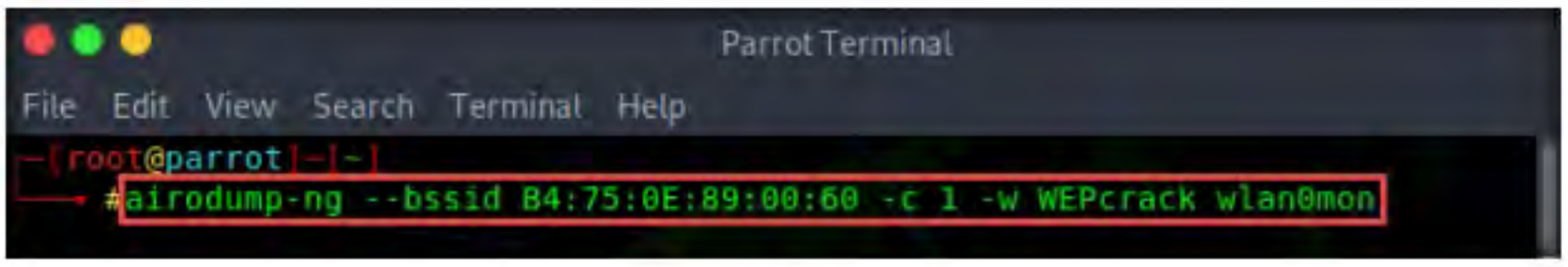

Figure 3.3.11: Instruct airodump-ng to capture packets

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

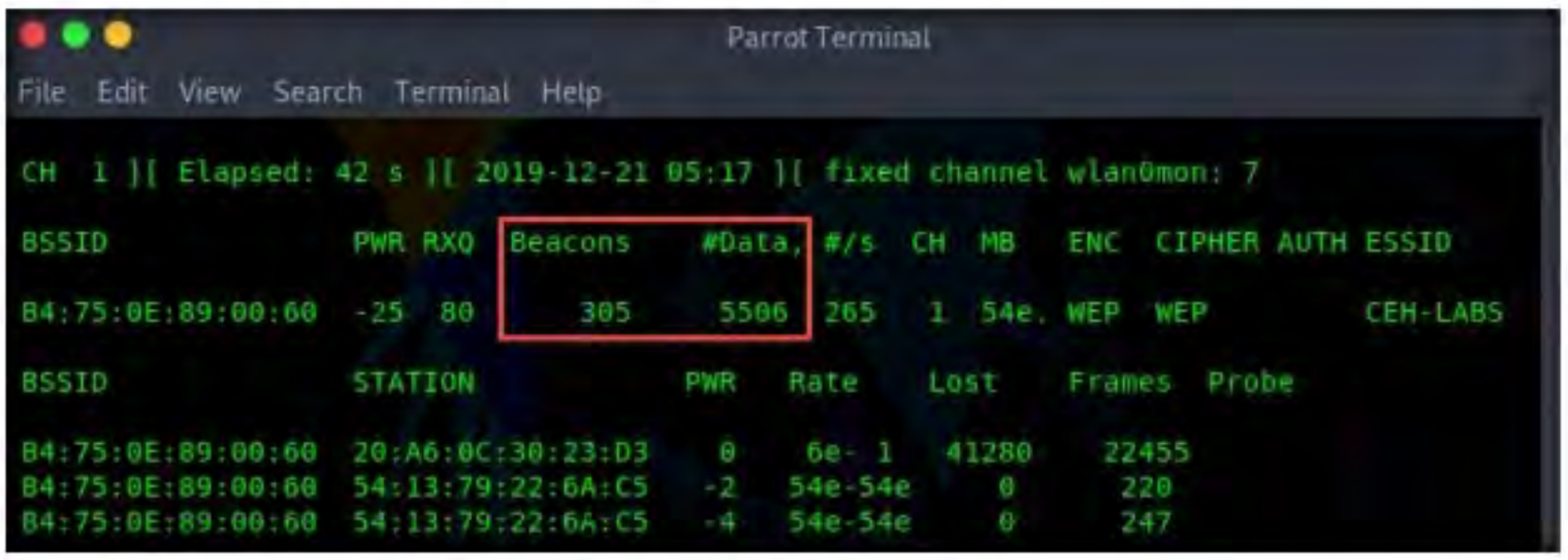

Figure 3.3.12: airodump-ng capturing packets

26. Open another terminal by clicking the **MATE Terminal** icon ( ) from the top of **Desktop**.
27. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
28. 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.

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

TASK 3.4

Generate ARP Traffic

30. In this new terminal window, type **aireplay-ng -3 -b B4:75:0E:89:00:60 -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.

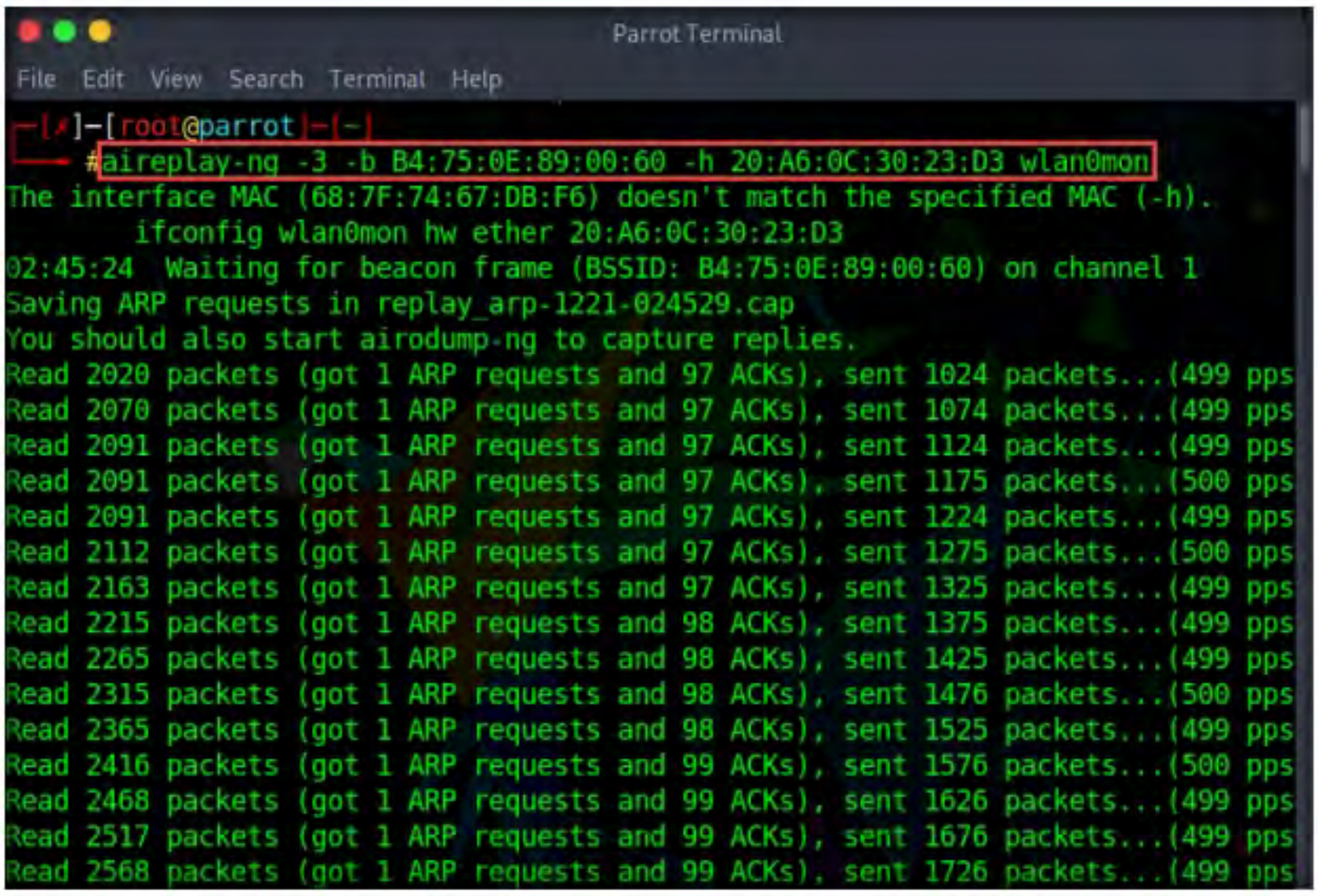

Figure 3.3.13: aireplay-ng generating traffic

31. Wait until the number of send ARP packets reaches the range of 15,000–20,000, and then press **Ctrl+C** to stop generating ARP traffic in the network.

32. Switch back to the terminal window where airodump-ng is running. Wait until the number of captured packets reaches the range of 15,000–20,000. Press **Ctrl+C** to stop the capture.

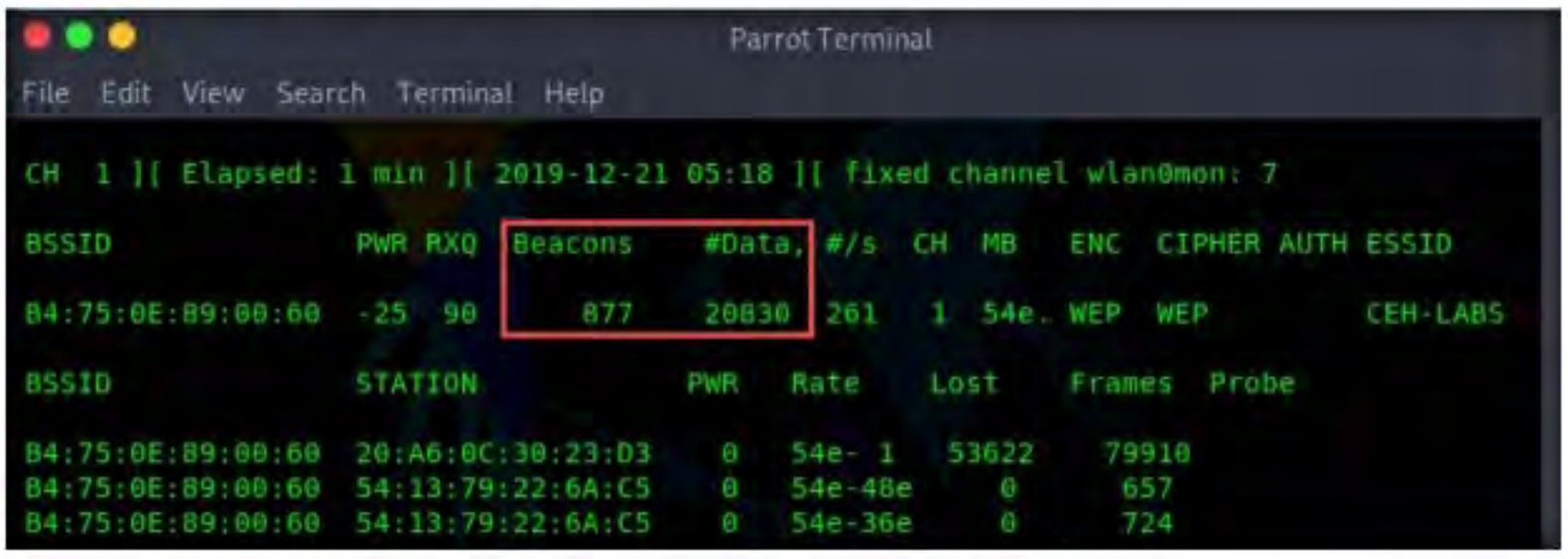

Figure 3.3.14: Stop capturing packets in airodump-ng

TASK 3.5

Obtain WEP Key

33. Now, launch aircrack-ng to recover the WEP key from the capture file. Type **aircrack-ng WEPcrack-01.cap** and press **Enter**.
34. Aircrack-ng will crack the WEP key of the **CEH-LABS**, as shown in the screenshot.

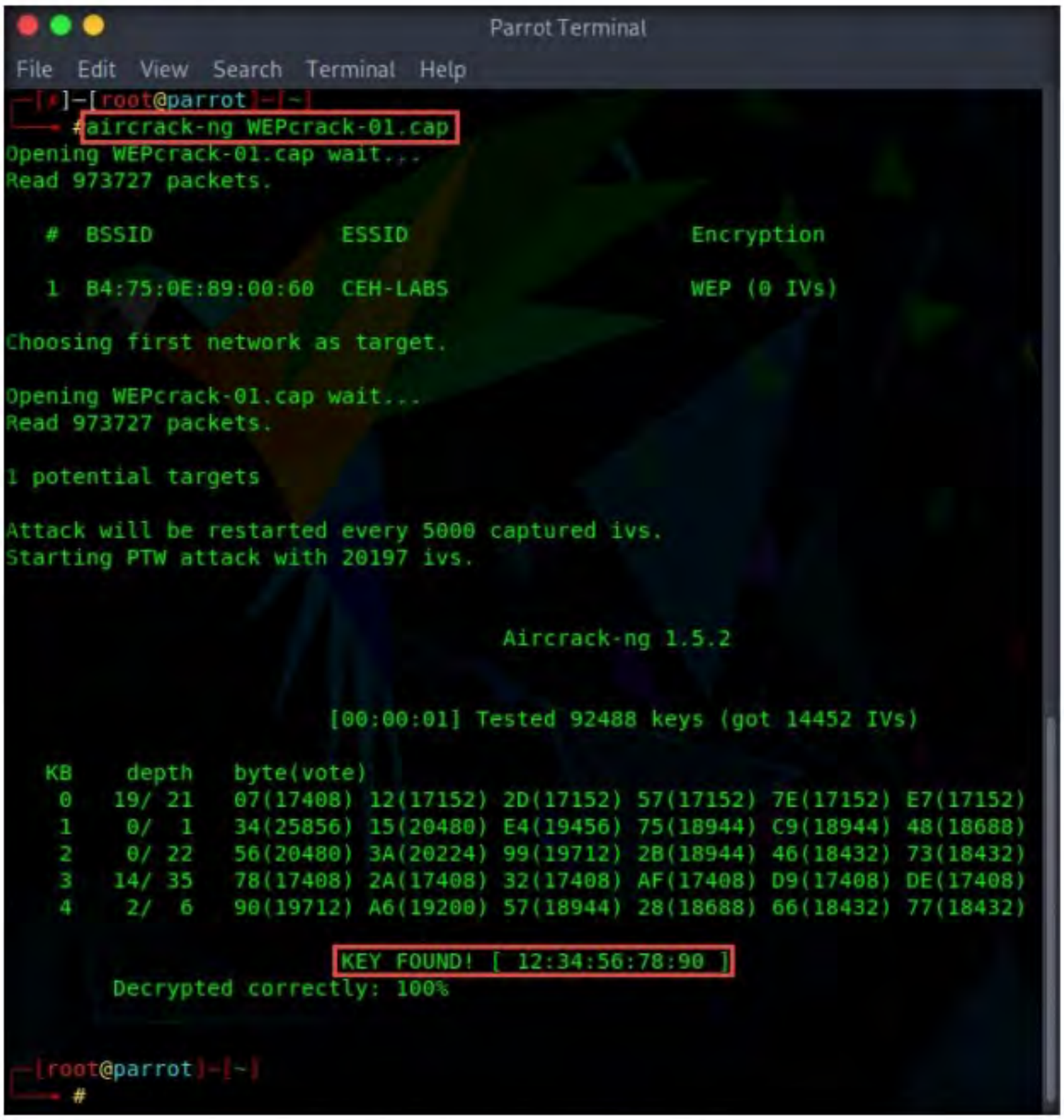

Figure 3.3.15: aircrack-ng recovering the WEP key

TASK 3.6

Connect to the Target Wi-Fi Network

35. 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**.
36. From the drop-down options under the **Wi-Fi Networks** section, click **CEH-LABS** from the available access points.

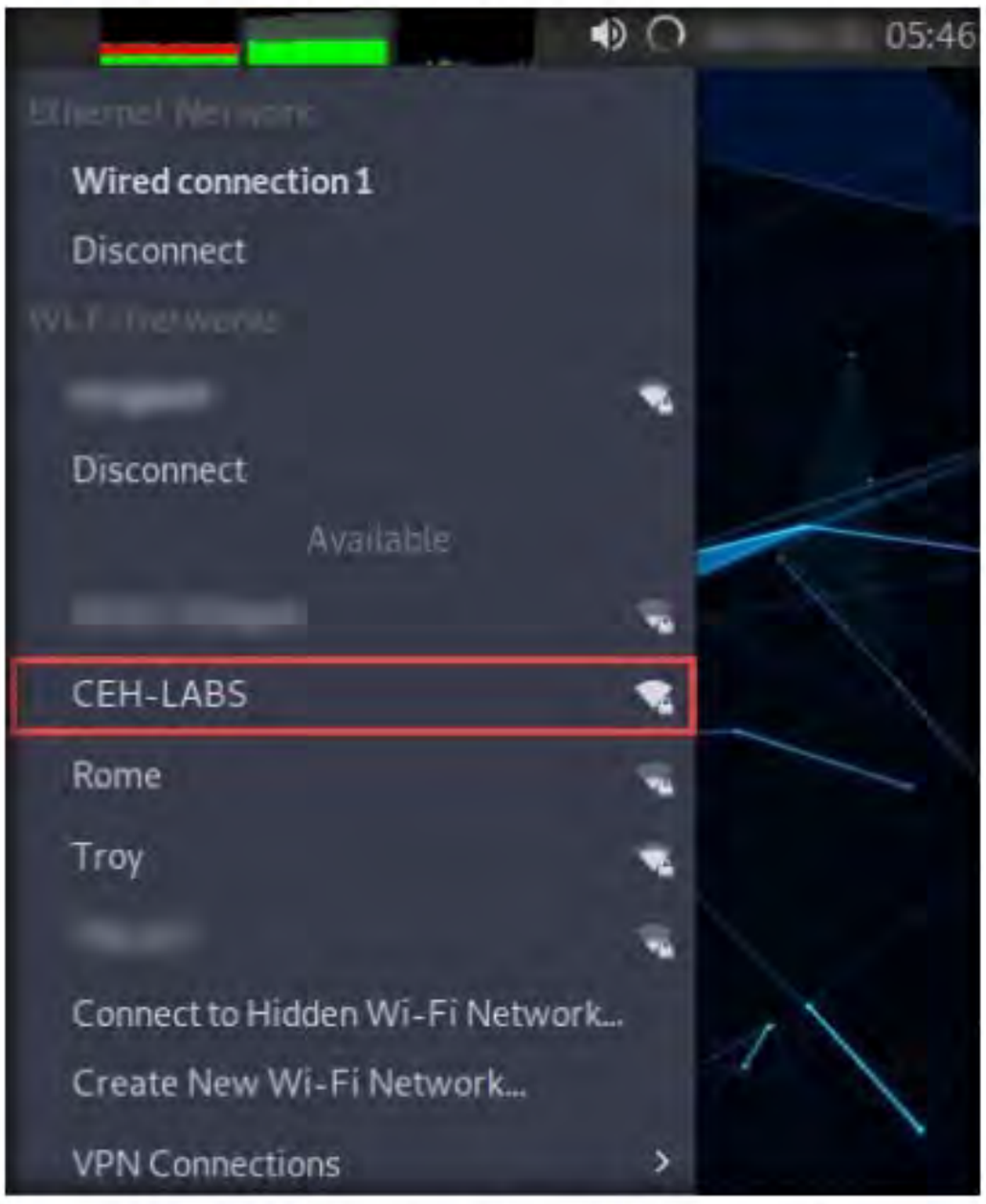

Figure 3.3.16: Connecting to the CEH-LABS access point

37. 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**.

Figure 3.3.17: Authentication required for wireless network

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

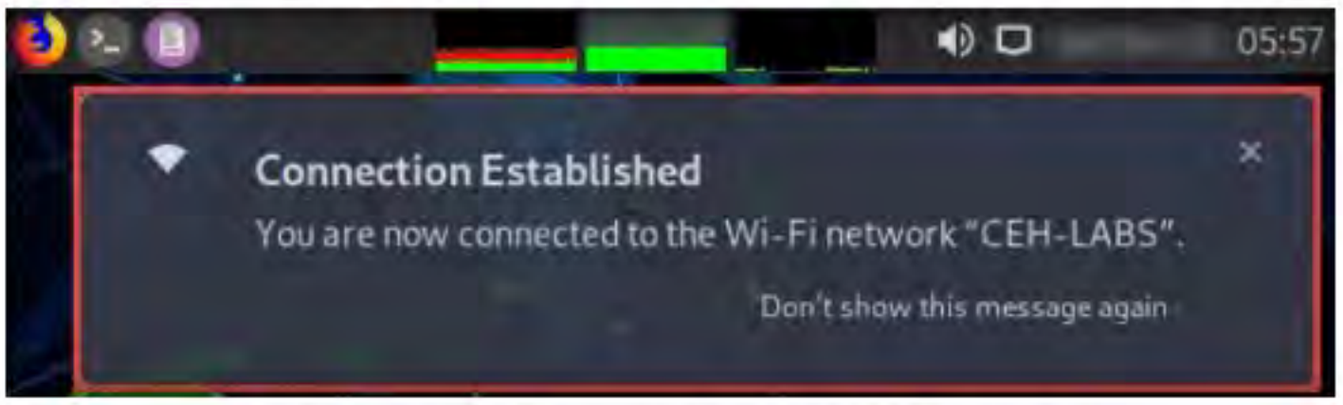

Figure 3.3.18: Successfully connected to the CEH-LABS access point

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.

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

TASK 4 Crack a WPA Network using Fern Wifi Cracker

Here, we will use Fern Wifi Cracker to crack a WPA network.

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.

Note: Before starting this task, you need to configure your access point router (**CEH-LABS**) to use WPA encryption. To do so, navigate to the router's default IP address and change the authentication settings from WEP to WPA. Set the password as **password1**.

Note: Before starting this task, you will also need to enable the ethernet adapter in the **Windows 10** virtual machine.

1. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
2. In the **Network and Sharing Center** window, click **Change adapter settings** from the left pane.
3. In the **Network Connections** window, right-click the **Ethernet0** adapter and click Enable from the options.
4. **Ethernet0** will now be enabled. Close all open windows.
5. Turn on the **Parrot Security** virtual machine.
6. 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.

The TKIP encryption protocol enables WPA to eliminate the weaknesses of WEP by including per-packet mixing functions, message integrity checks, extended initialization vectors, and rekeying mechanisms. Nonetheless, the WPA encryption method has its own vulnerabilities and can be cracked using various techniques and tools.

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.

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.

7. Plug in the **Linksys 802.11 g WLAN** adapter.
8. 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**.

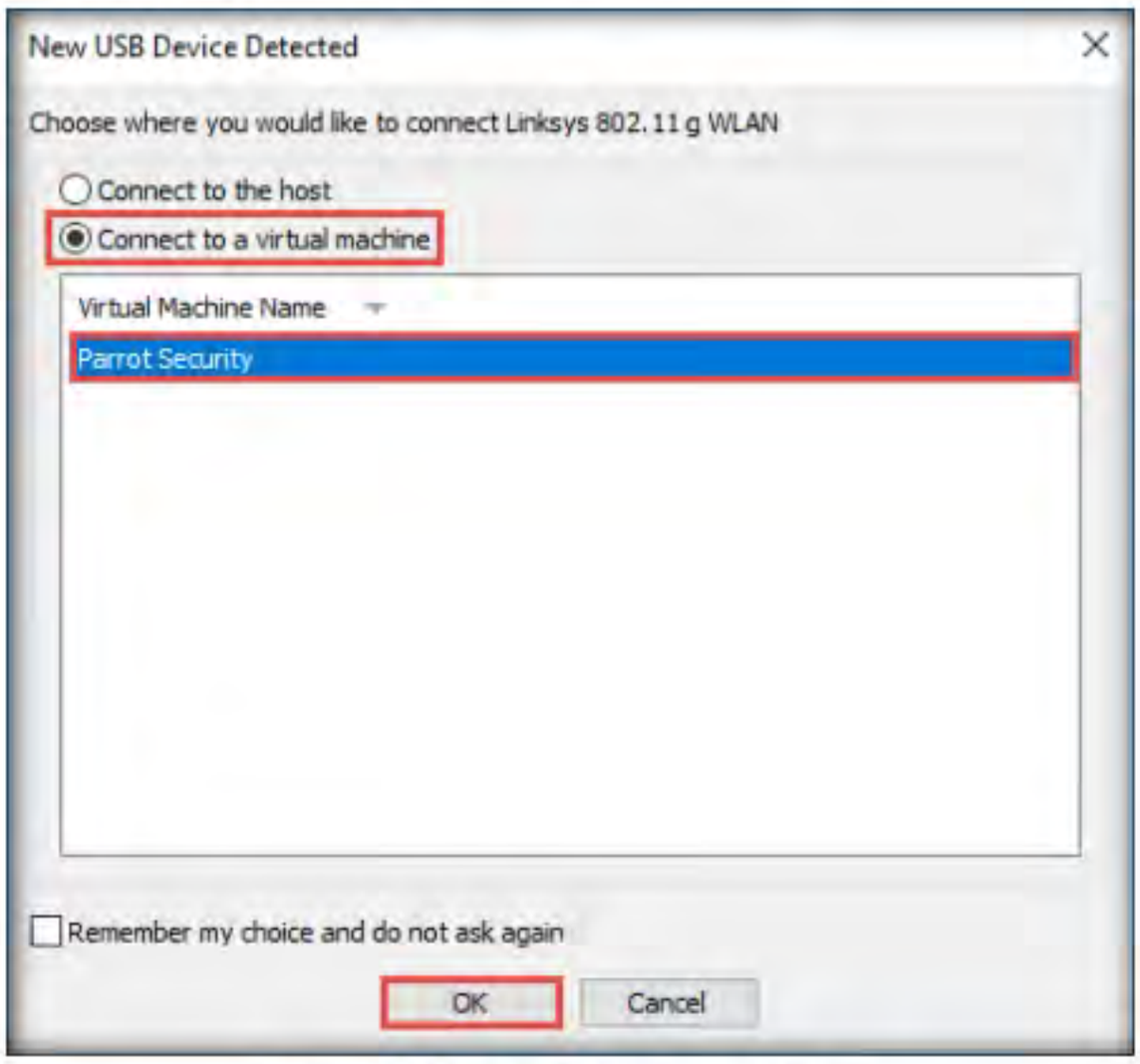

Figure 3.4.1: New USB Device Detected window

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

9. First, we will copy the **password.txt** file from the shared network drive to the **Desktop** of the **Parrot Security** virtual machine.
10. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
11. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
12. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

13. Navigate to **CEHv11 Module 16 Hacking Wireless Networks\Wordlist** and copy the file **password.txt**. Close the window.

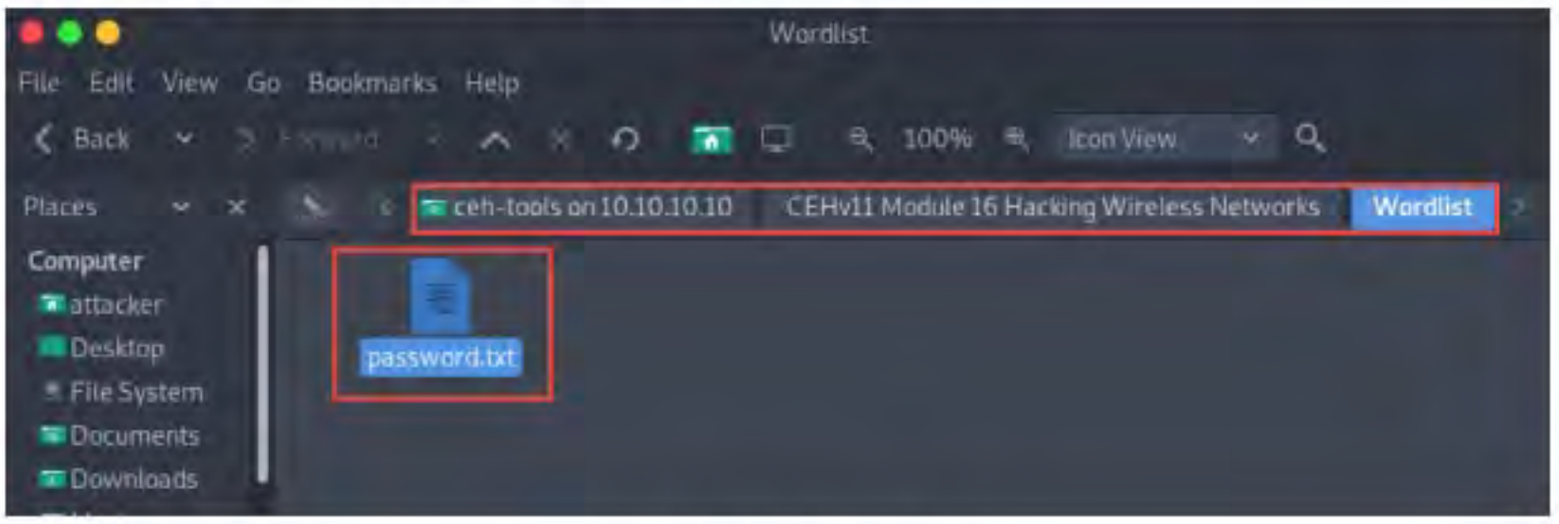

Figure 3.4.2: Copy password.txt

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

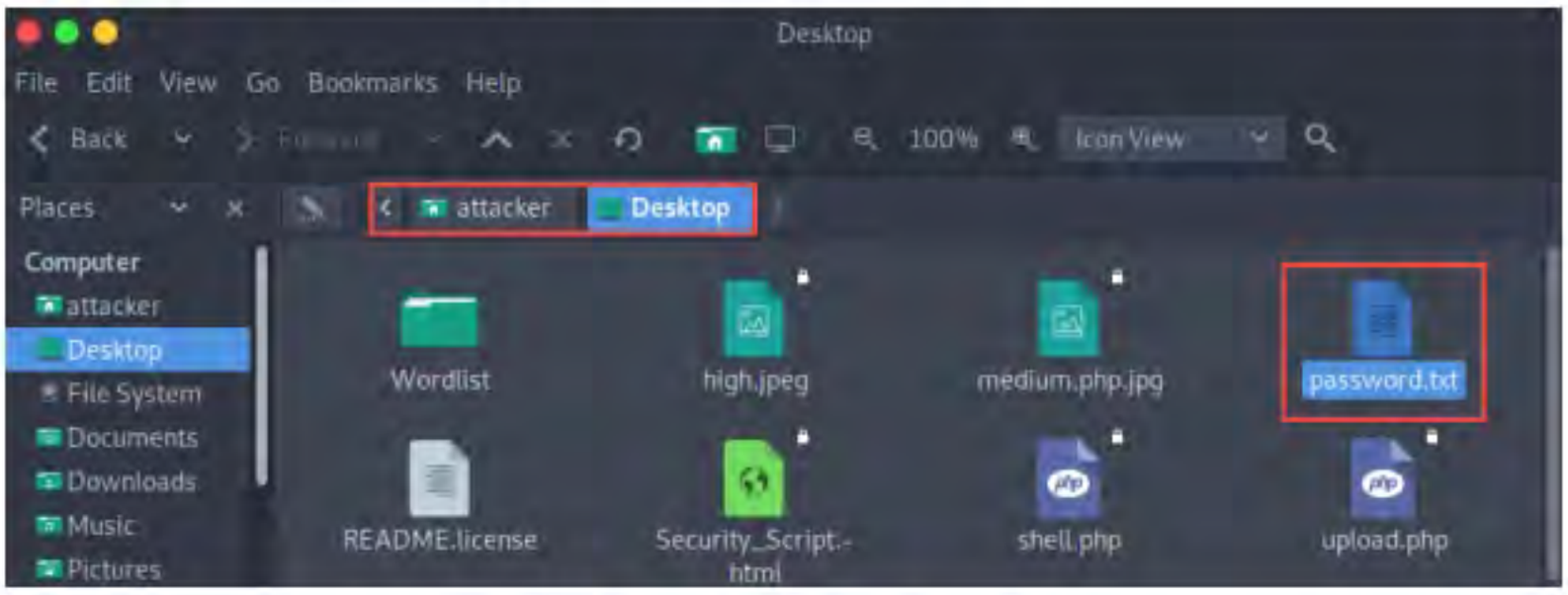

Figure 3.4.3: Paste password.txt file in the root directory

15. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
16. 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.

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

TASK 4.1

Launch Fern Wifi Cracker Application

18. In the **Parrot Terminal** window, type **fern-wifi-cracker**, and press **Enter** to launch the Fern Wifi Cracker application.

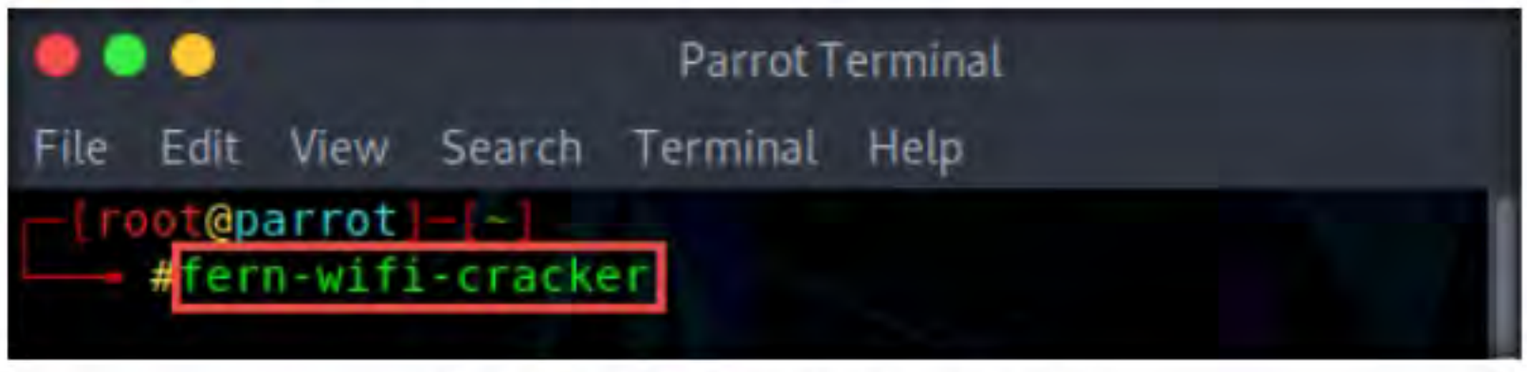

Figure 3.4.4: Launch Fern Wifi Cracker Application

19. **Fern WIFI Cracker** opens. If a **Fern Professional** pop-up appears, click **No**.
20. Click **Select Interface** and from the drop-down list, select the **wlan0** interface.
21. A **Tips - Scan settings** pop-up appears, click **Ok**.
22. The selected adapter (**wlan0**) loads, and the notification **Monitor Mode Enabled on wlan0mon** appears in the selected network adapter field.

TASK 4.2

Discover WPA Enabled Access Points

23. Click the **Scan for Access points** button to initialize the scan for the access points.

Figure 3.4.5: Scan for access points

24. 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.

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

Figure 3.4.6: Click Wi Fi WPA button

TASK 4.3

Select the Target Access Point

26. 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.
27. Select **CEH-LABS** from the list and click the **Browse** button present at the bottom-right corner of the window.

Figure 3.4.7: Select the target access point

28. The **Select Wordlist** window appears. Navigate to the location **/attacker/Desktop**, and select **password.txt**. Click **Open**.
29. See that the selected **password.txt** file appears. Now, click the **Wi Fi Attack** button in the right pane to launch the attack.

TASK 4.4

Launch WPA Attack

Figure 3.4.8: Launch a Wi-Fi attack

30. 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.

Figure 3.4.9: Attacking the target access point

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

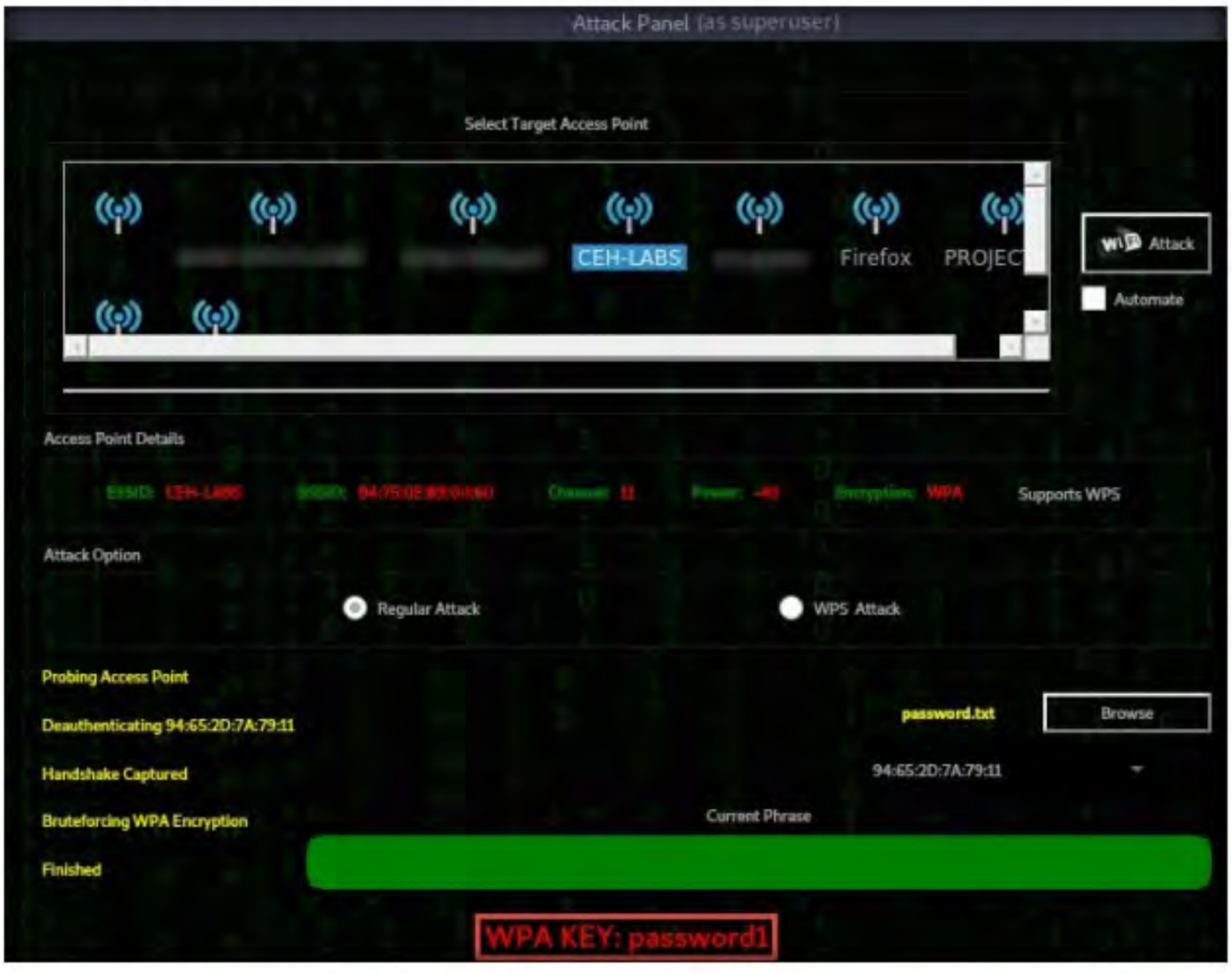

Figure 3.4.10: Cracked WPA KEY

32. If the **Attack Panel** window automatically closes, relaunch **Fern Wifi Cracker** from the terminal window and click the **Key Database** button.
33. The **Fern - Key Database** pop-up appears, displaying the acquired key for **CEH-LABS**, as shown in the screenshot.

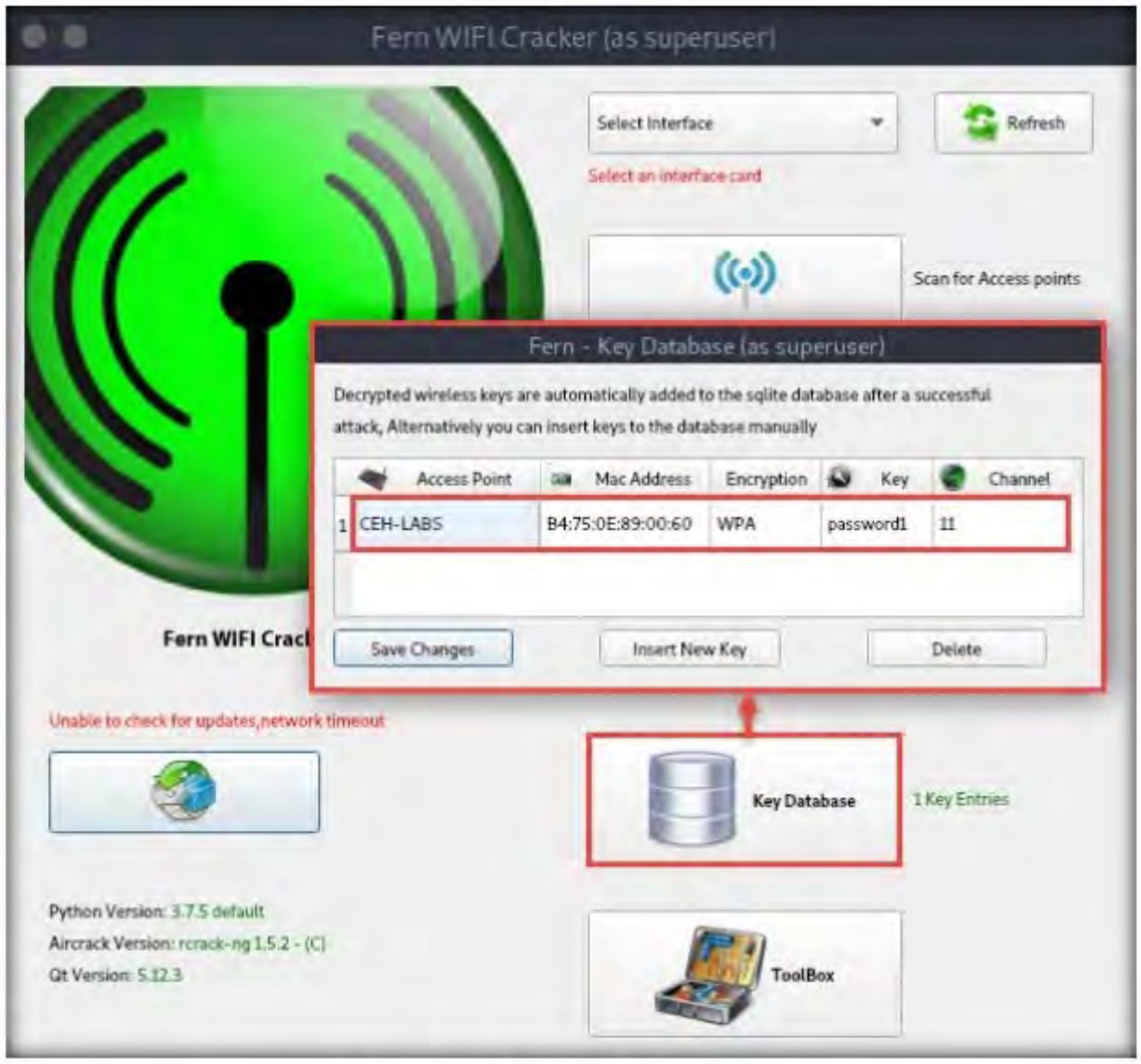

Figure 3.4.11: Fern - Key Database pop-up

34. This cracked key can be used to connect to the target access point **CEH-LABS**.
35. This concludes the demonstration of how to crack a WPA network using Fern Wifi Cracker.
36. Unplug the **Linksys 802.11 g WLAN** adapter.
37. Close all open windows and document all the acquired information.
38. Turn off the **Parrot Security** virtual machine.

After performing the task, disable the ethernet adapter in the **Windows 10** virtual machine:

39. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
40. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.
41. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
42. **Ethernet0** will be disabled. Close all open windows and turn off the **Windows 10** virtual machine.

TASK 5 Crack a WPA2 Network using Aircrack-ng

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

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.

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.

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.

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**.

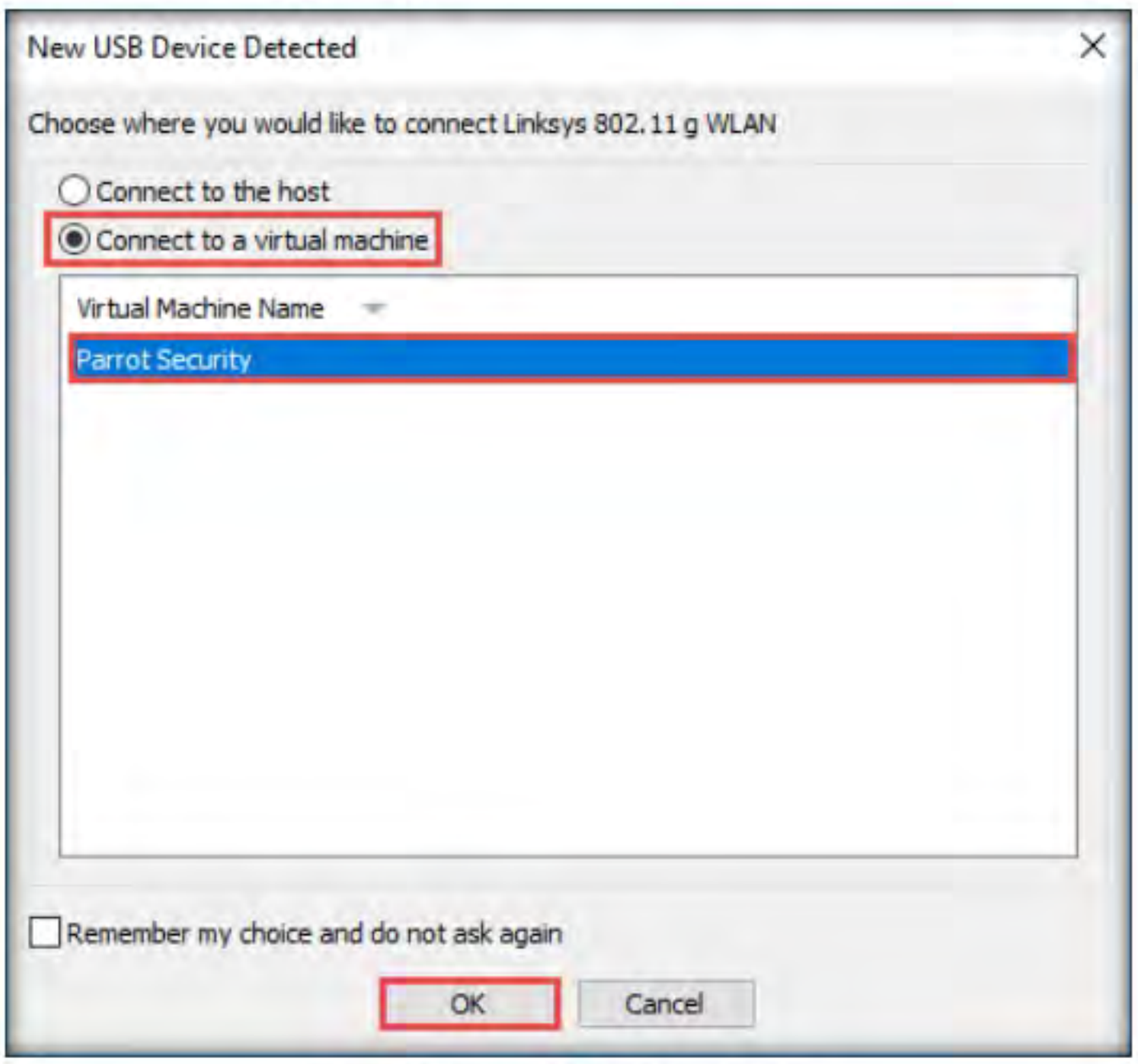

Figure 3.5.1 New USB Device Detected window

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

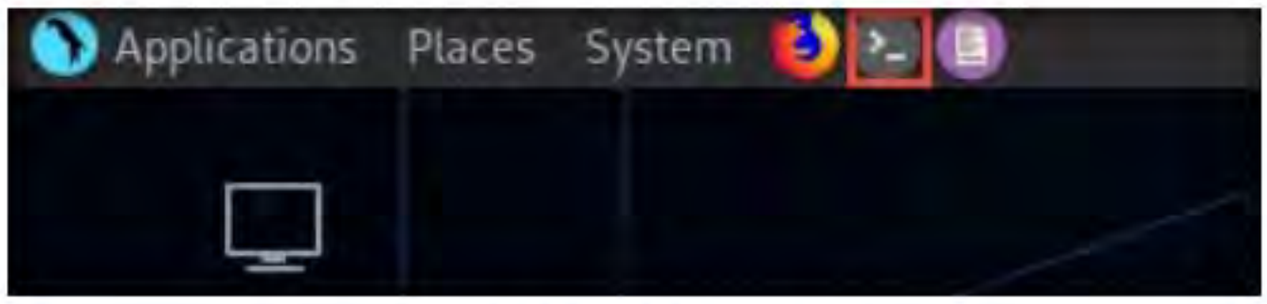

Figure 3.5.2: MATE Terminal icon

TASK 5.1

Put Wireless Adapter into Monitor Mode

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.

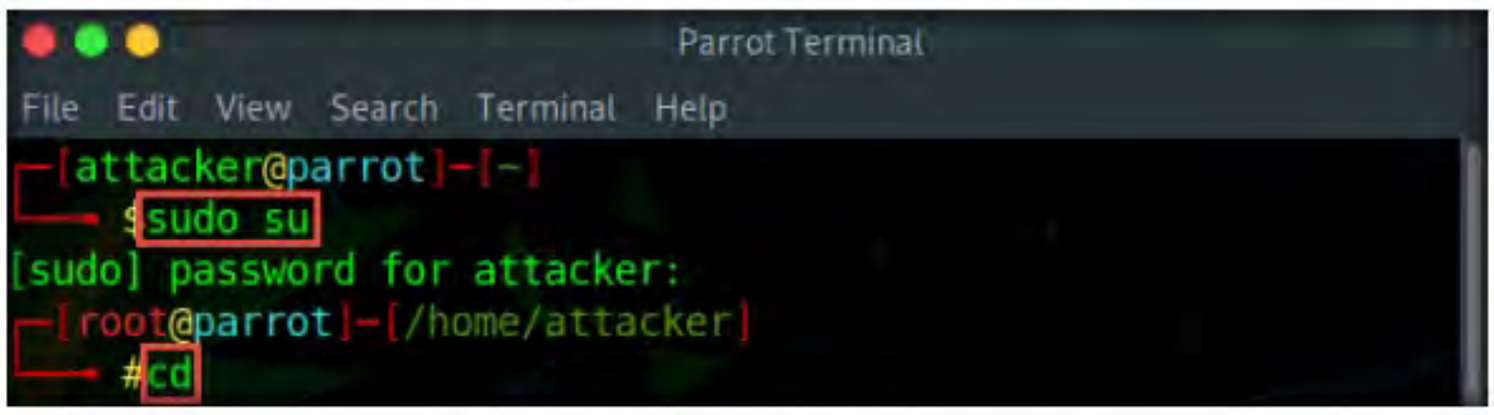

Figure 3.5.3: Running the programs as a root user

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. 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.
11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

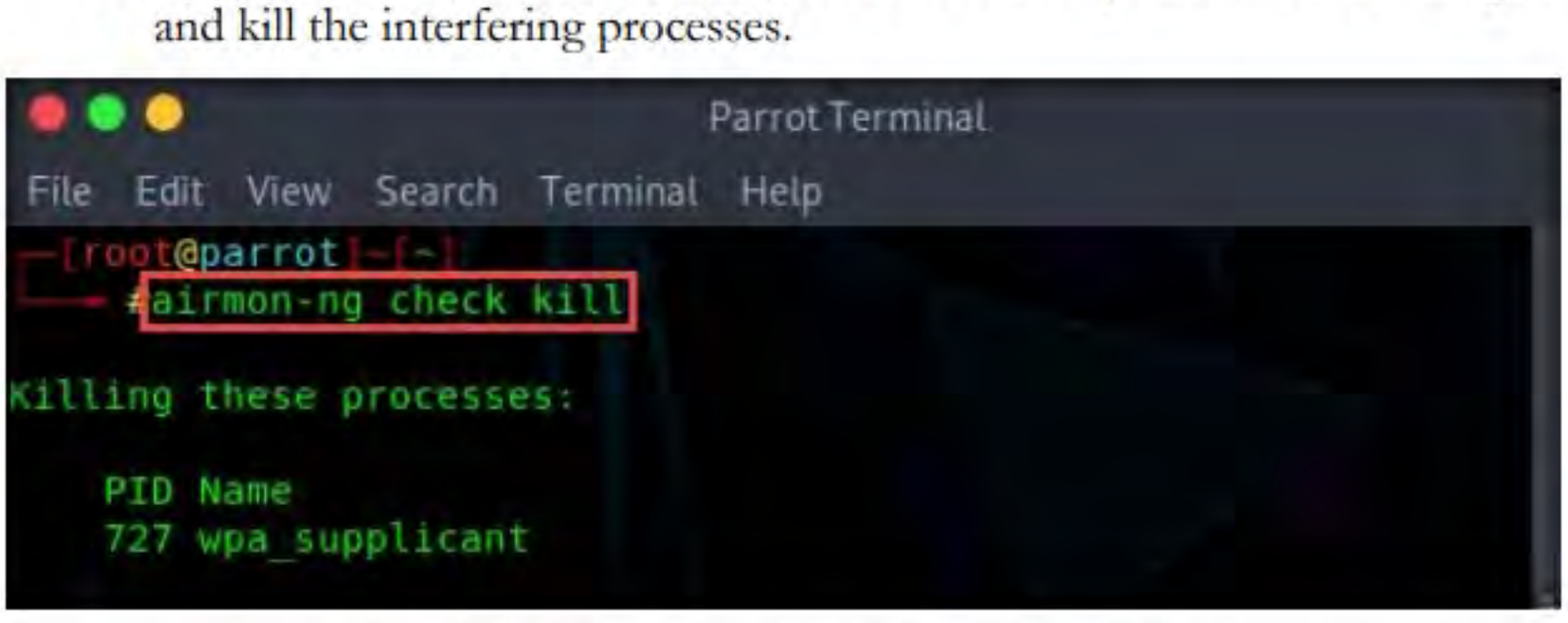

Figure 3.5.4: Issuing the command to kill the interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.

13. Observe that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

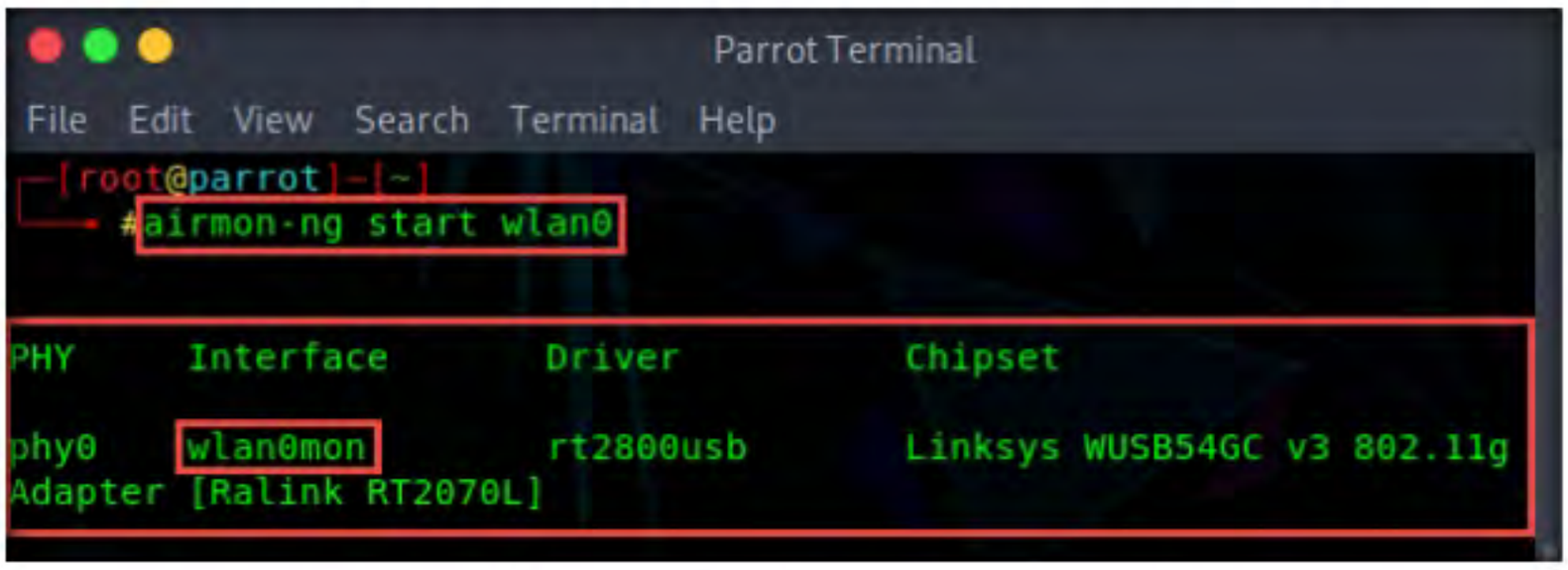

Figure 3.5.5: Setting up the wireless interface in monitor mode

14. 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.

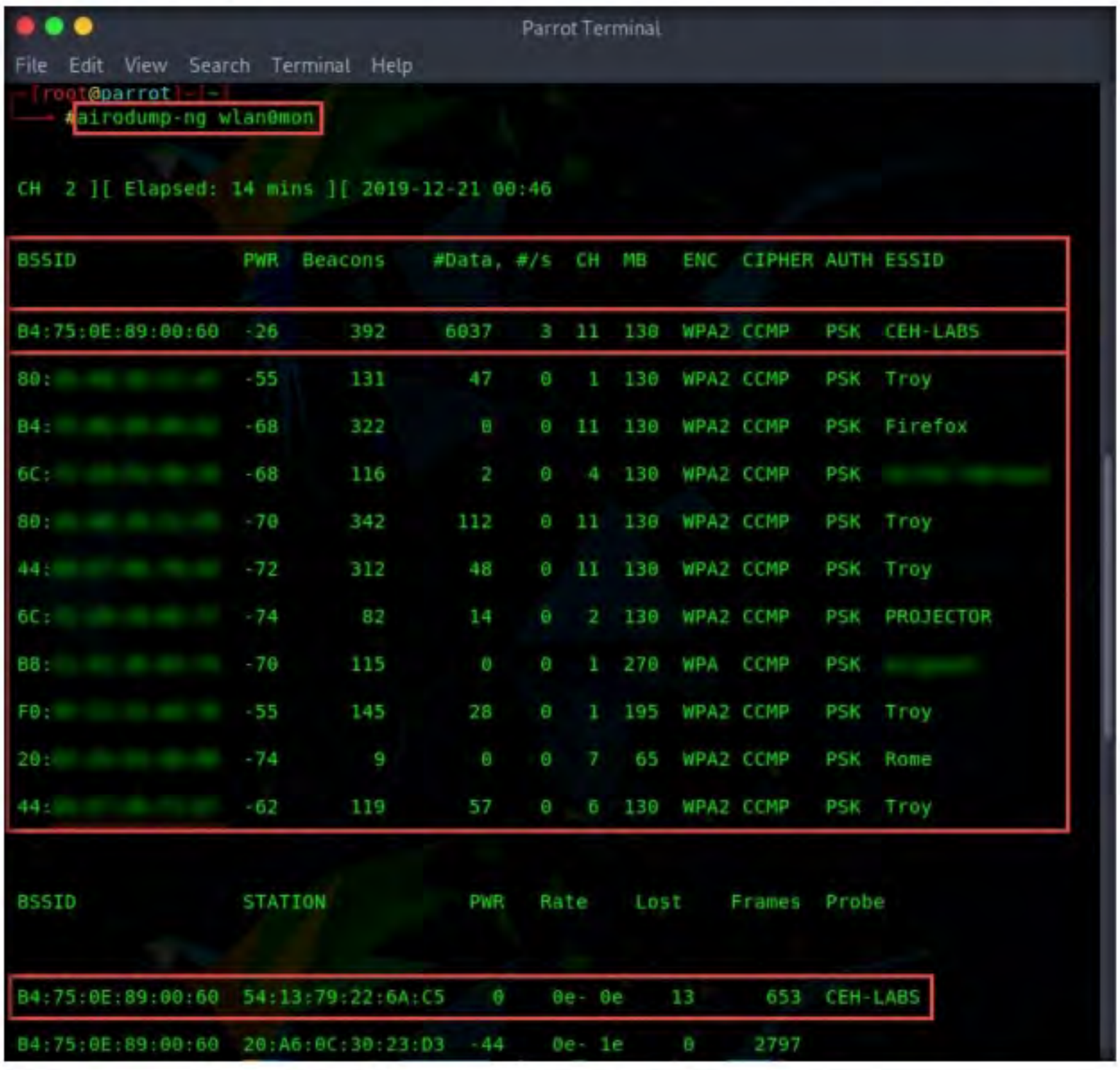

Figure 3.5.6: airodump-ng searching for available access points

Note: In this example, the connected client ("STATION") is **54:13:79:22:6A:C5**. It might differ in your lab environment.

15. In this lab, we will target the access point **CEH-LABS** to perform WPA2 cracking.

Note: If you are unable to obtain the station BSSID using this command, you can do so with the command in **Step 17**.

16. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. 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.

19. Now, type **cd** and press **Enter** to jump to the root directory.
20. 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 B4:75:0E:89:00:60 -c 11 -w CEH-LABS-01 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, **B4:75:0E:89:00:60**); **-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-01**); and **wlan0mon**: is the wireless interface

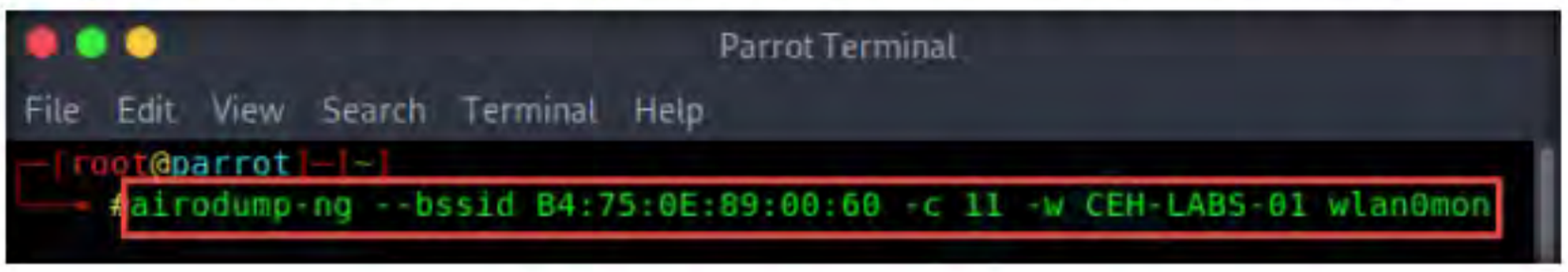

Figure 3.5.7: Run airodump-ng to capture the packets

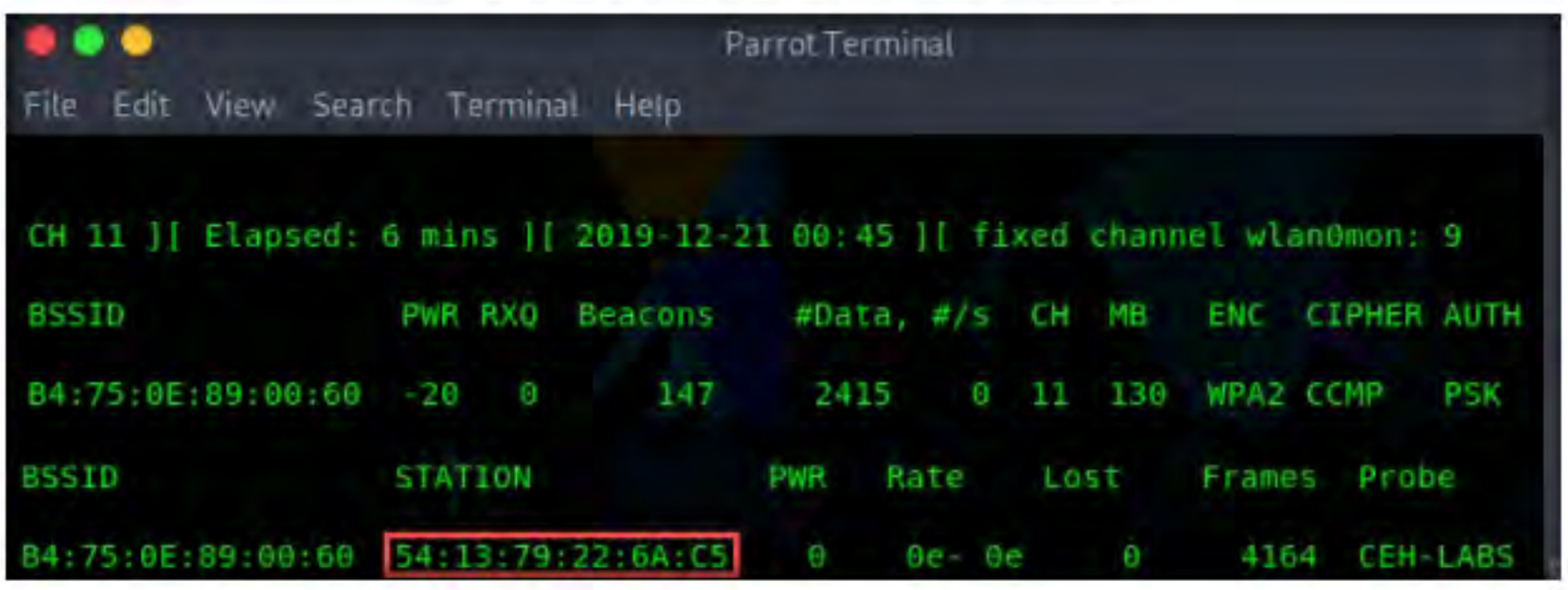

Figure 3.5.8: airodump-ng capturing the packets

21. Now, open another terminal by clicking the **MATE Terminal** icon ( ) at the top of the **Desktop** window.
22. A **Parrot Terminal** window appears. In the 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.

TASK 5.2

Send Deauth Packets

25. In this new terminal window, type **aireplay-ng -0 11 -a B4:75:0E:89:00:60 -c 54:13:79:22:6A:C5 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.

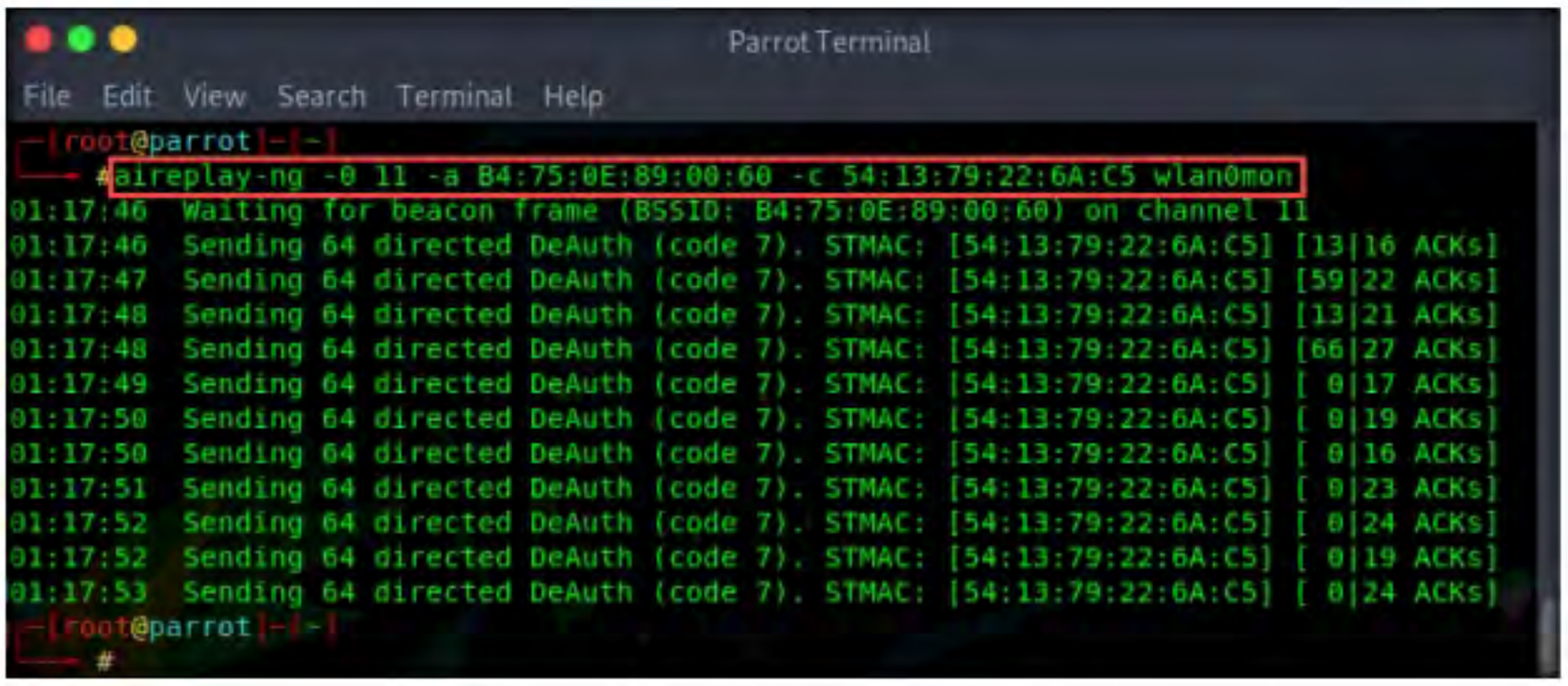

Figure 3.5.9: aireplay-ng generating traffic

26. Rerun the above command multiple times to send a large number of deauthentication packets.

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

TASK 5.3

Capture WPA Handshake Packet

27. Switch back to the terminal, where **airodump-ng** is running and keep capturing packets until you see the **WPA handshake: B4:75:0E:89:00:60** notification, which indicates that a WPA/WPA2 handshake was successfully captured for the target BSSID.
28. Press **Ctrl+C** to stop the capture.

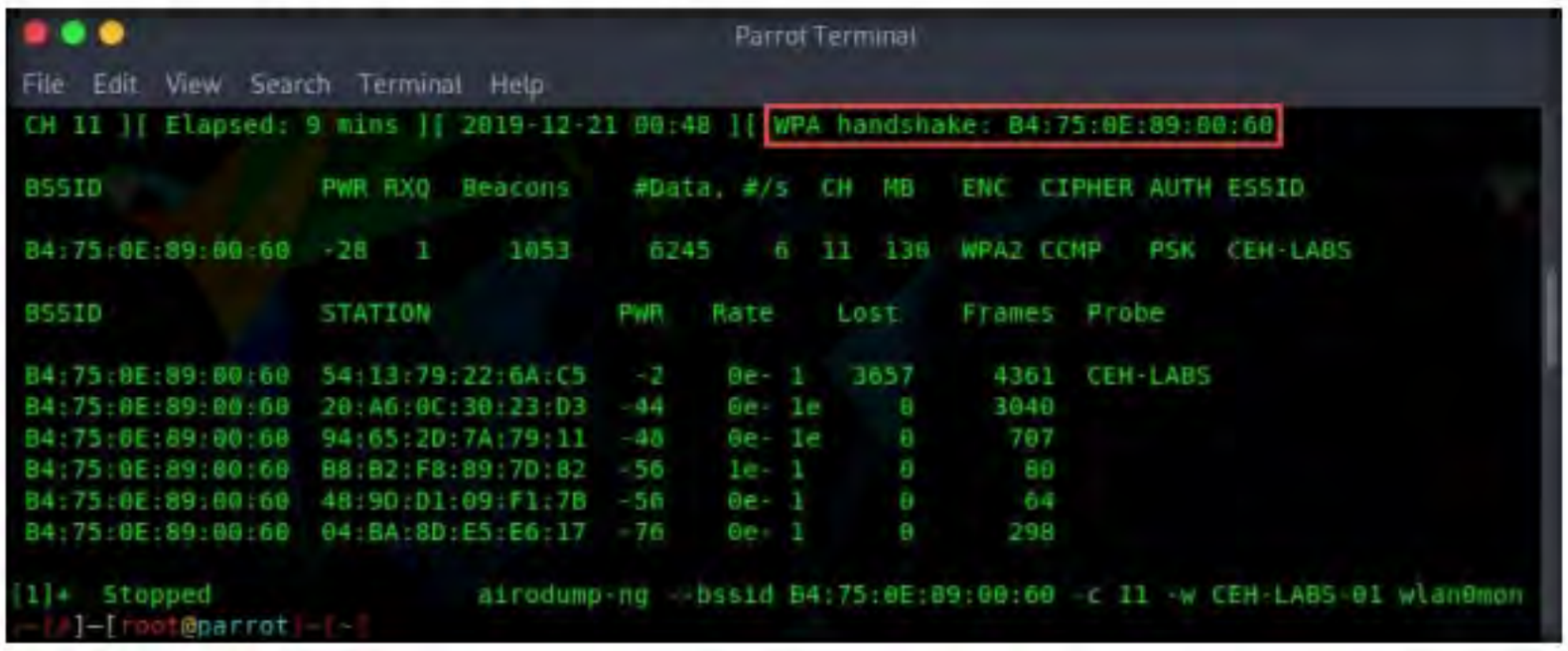

Figure 3.5.10: Stop airodump-ng traffic capture

TASK 5.4

Obtain WPA2 Key

29. Now, open a new terminal window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
30. 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.

31. Now, type **cd** and press **Enter** to jump to the root directory.
32. Type **cp /home/attacker/Desktop/password.txt /root/Desktop/** and press **Enter** to copy the **password.txt** file to the root directory.
33. In the terminal window, type **aircrack-ng -a2 B4:75:0E:89:00:60 -w /root/Desktop/password.txt /root/CEH-LABS-01-01.cap** and press **Enter**. The file **CEH-LABS-01-01.cap** contains captured packets located at **/root/Desktop**.

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.

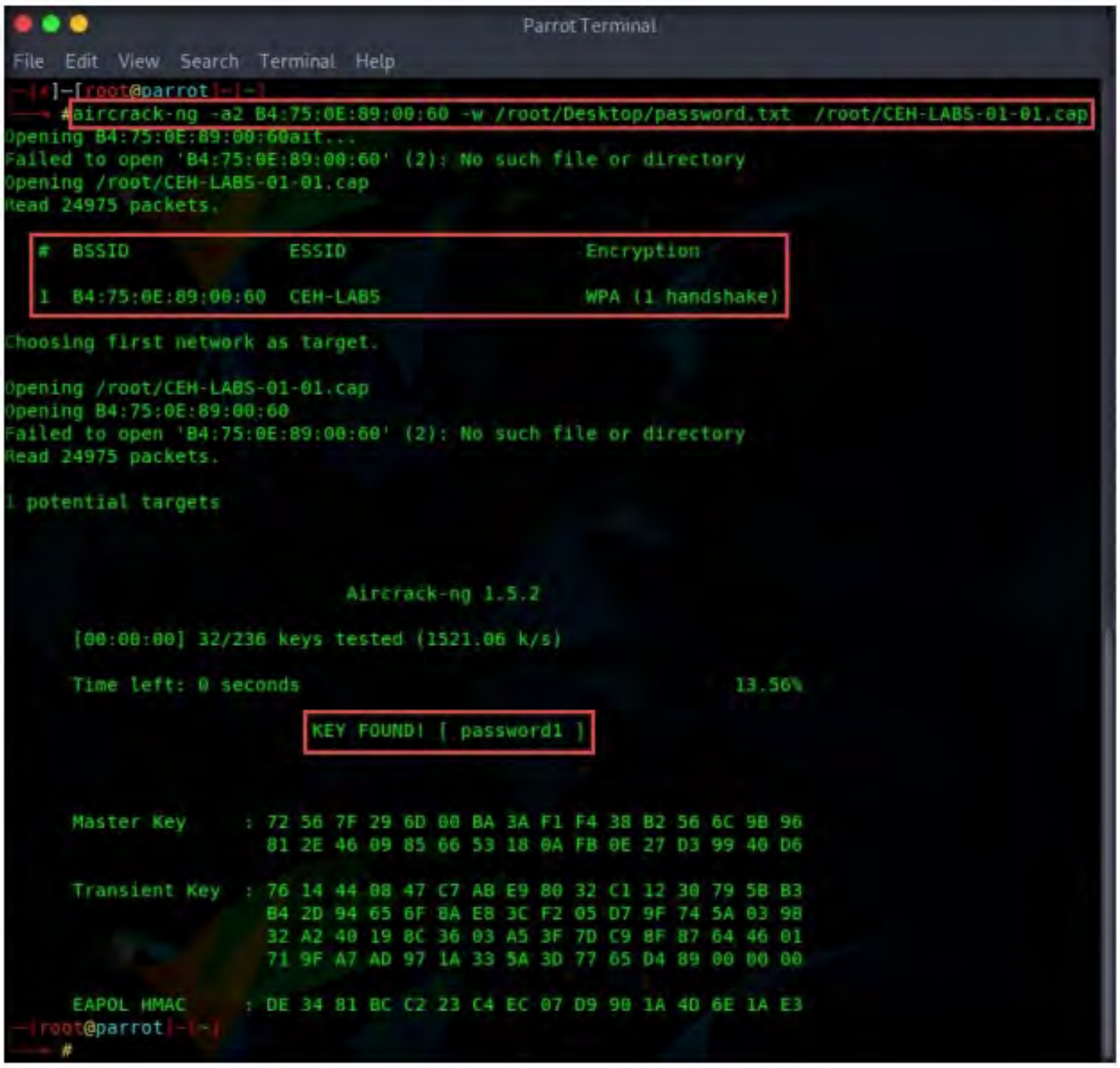

Figure 3.5.11: aircrack-ng has successfully cracked the WPA key

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.

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.
37. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

TASK 6 Create a Rogue Access Point to Capture Data Packets using MANA-Toolkit

Here, we will use MANA-Toolkit to create a rogue access point and capture data packets.

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

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.

MANA-Toolkit is a set of tools that are used by attackers to create rogue access points, carry out sniffing and MITM attacks, and bypass HTTPS and HSTS.

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**.

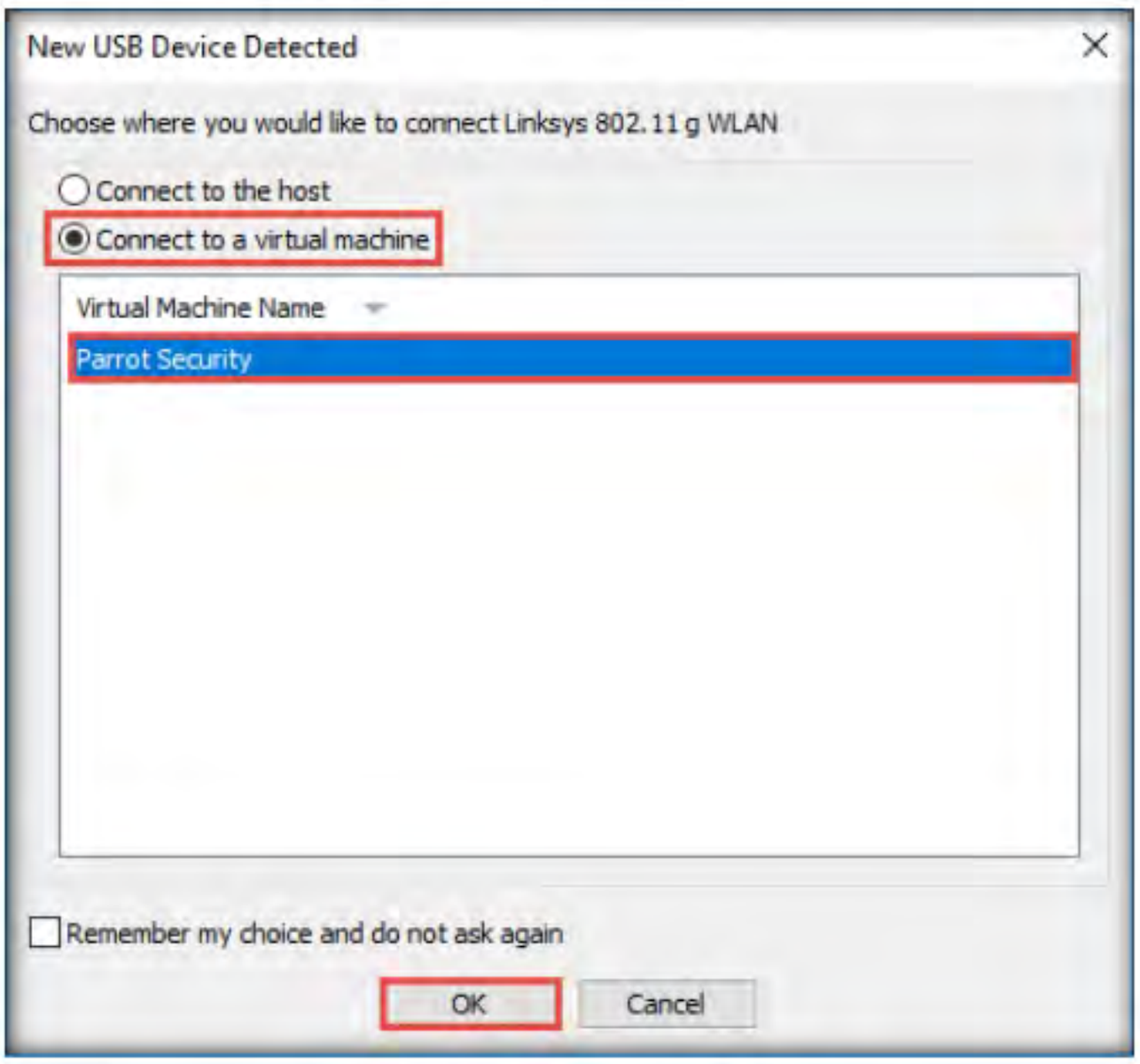

Figure 3.6.1: New USB Device Detected window

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

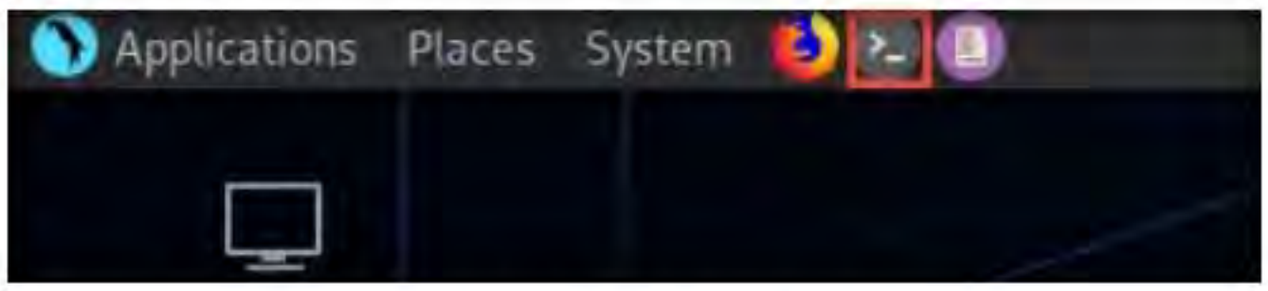

Figure 3.6.2: MATE Terminal icon

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.

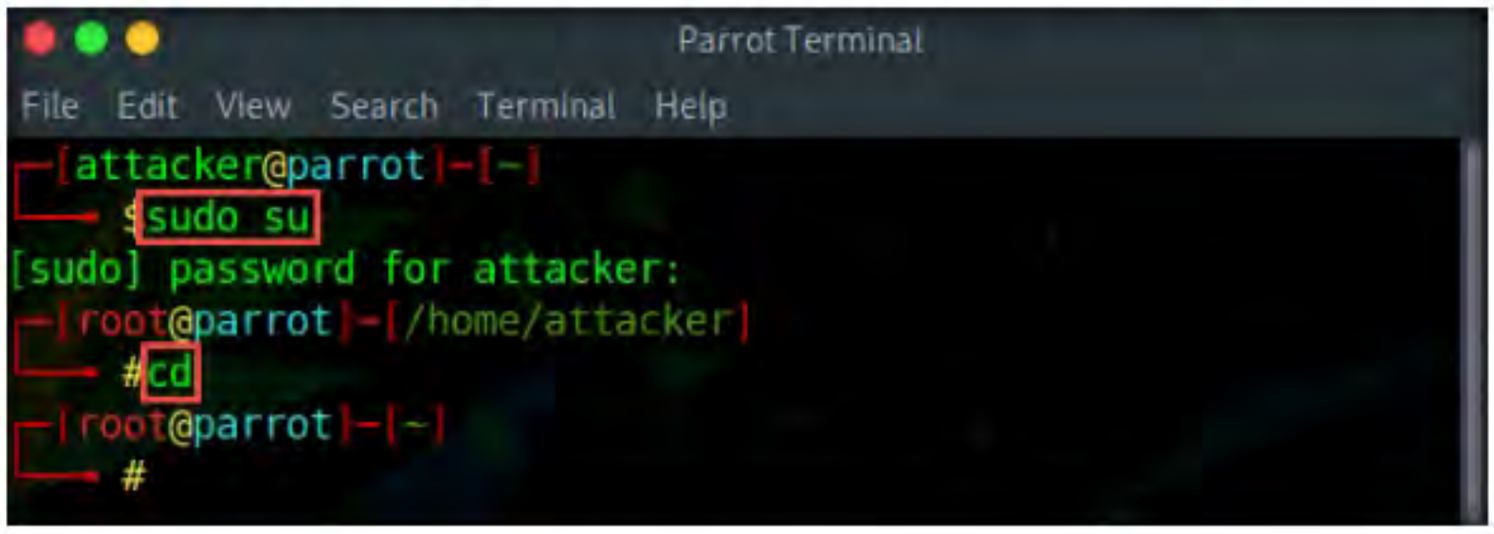

Figure 3.6.3: Running the programs as a root user

TASK 6.1

Clone MANA-Toolkit

9. In the **Parrot Terminal** window, type **git clone --depth 1 https://github.com/sensepost/mana** and press **Enter** to clone the MANA-Toolkit repository.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **mana** folder.
- Paste the copied **mana** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/mana /root/**.

10. Type **cd mana** and press **Enter** to navigate to the cloned repository of MANA-Toolkit.

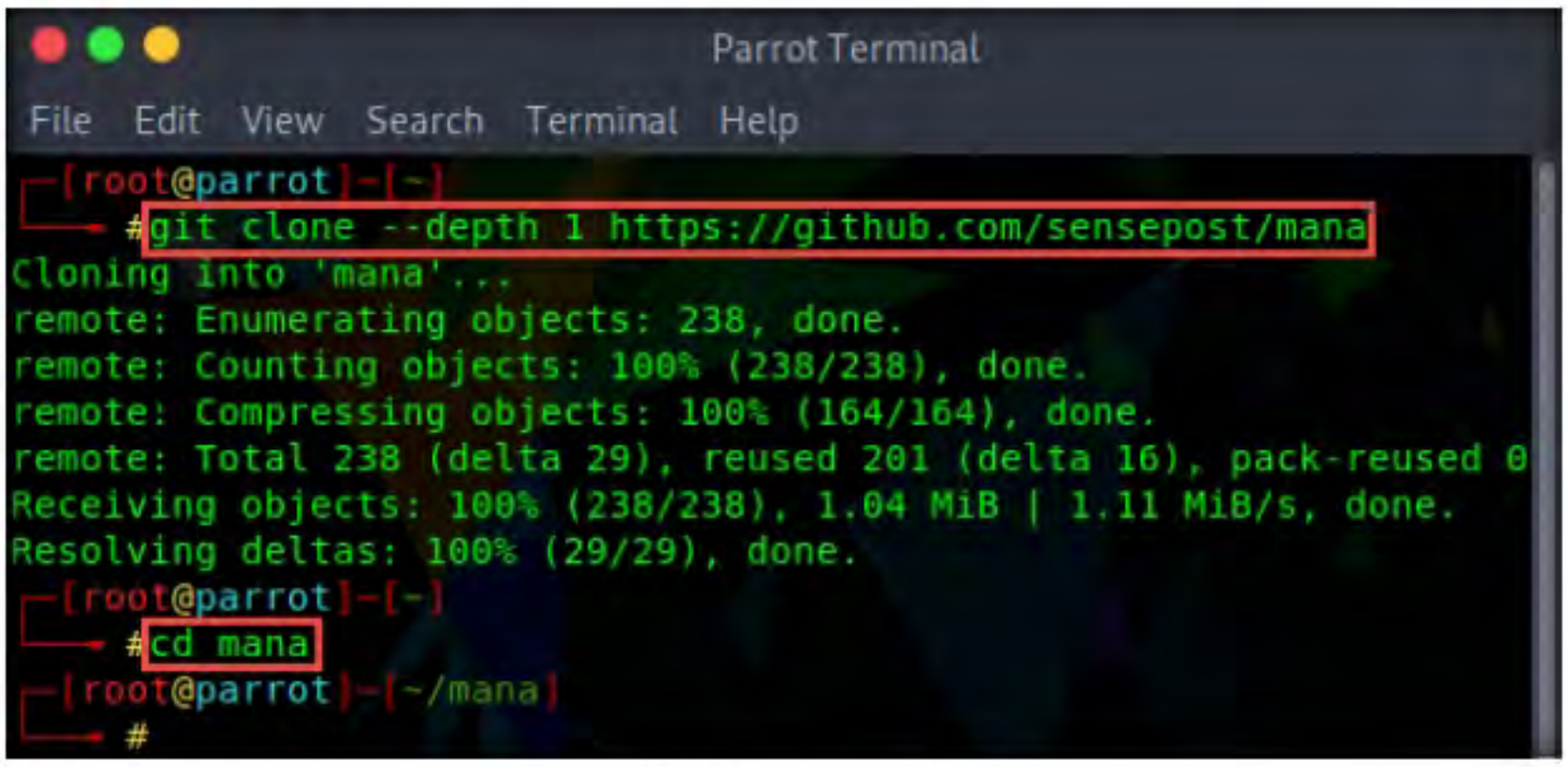

Figure 3.6.4: Clone MANA-Toolkit

11. Type **git submodule init** and press **Enter** to fetch the submodules of MANA-Toolkit.
12. The result appears, displaying the submodules that are required to launch MANA-Toolkit. These submodules must be cloned and placed in the respective specified paths. Minimize the **Terminal** window.

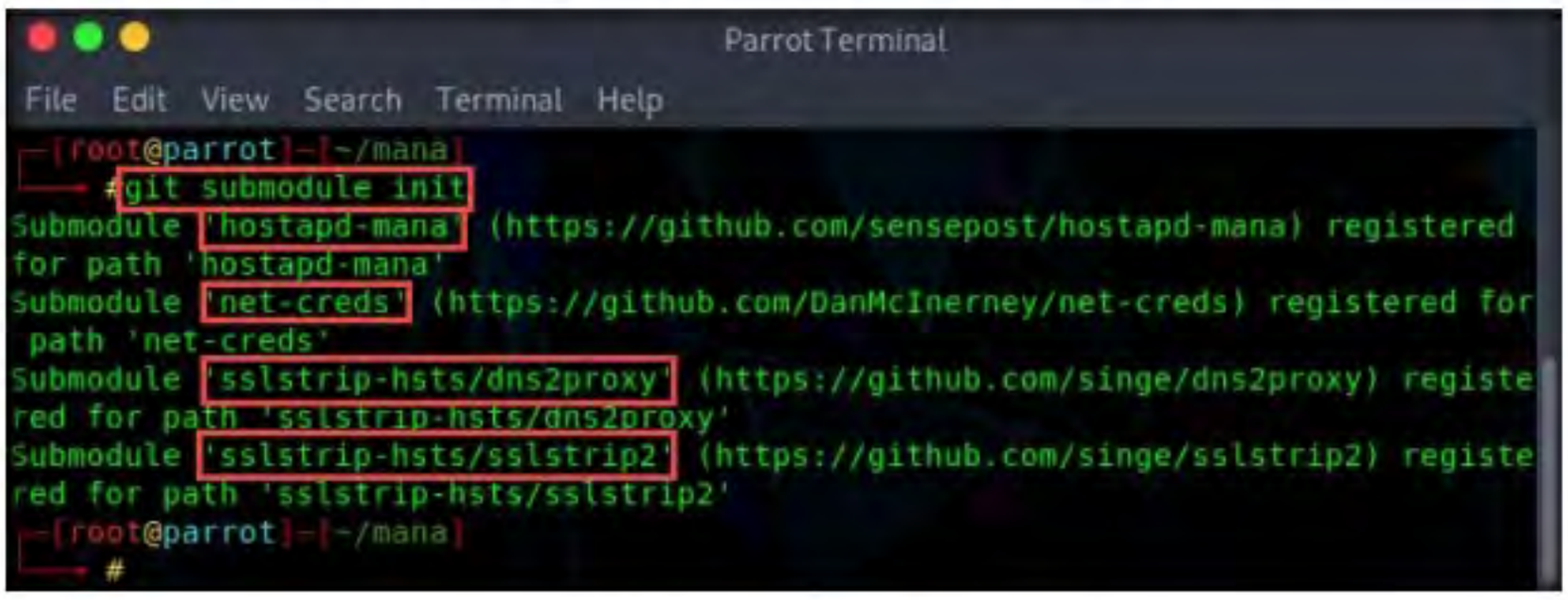

Figure 3.6.5: Fetching the required submodules

13. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open another **Terminal** window.
14. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
15. 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.

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

TASK 6.2

Install Submodules

17. In the new **Terminal** window, type **git clone https://github.com/sensepost/hostapd-mana** and press **Enter** to clone the hostapd-mana submodule.

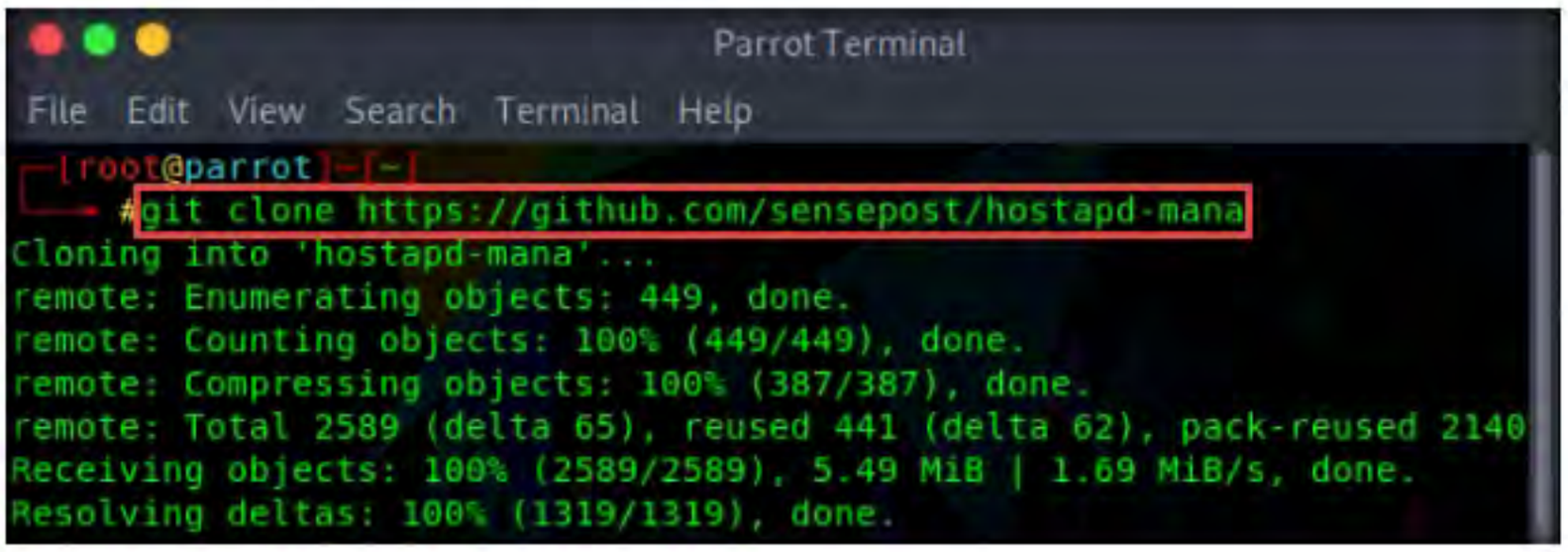

Figure 3.6.6: Cloning hostapd-mana

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **hostapd-mana** folder.
- Paste the copied **hostapd-mana** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/hostapd-mana /root/**.

18. By default, the application will be cloned in the **root** directory. We will need to copy the content of **hostapd-mana** repository and paste at the location **/root/mana/hostapd-mana/**, so that it is in the location required by MANA-Toolkit (see **Step 12**).
19. In the terminal window, type **cp -r /root/hostapd-mana /root/mana/** and press **Enter**.

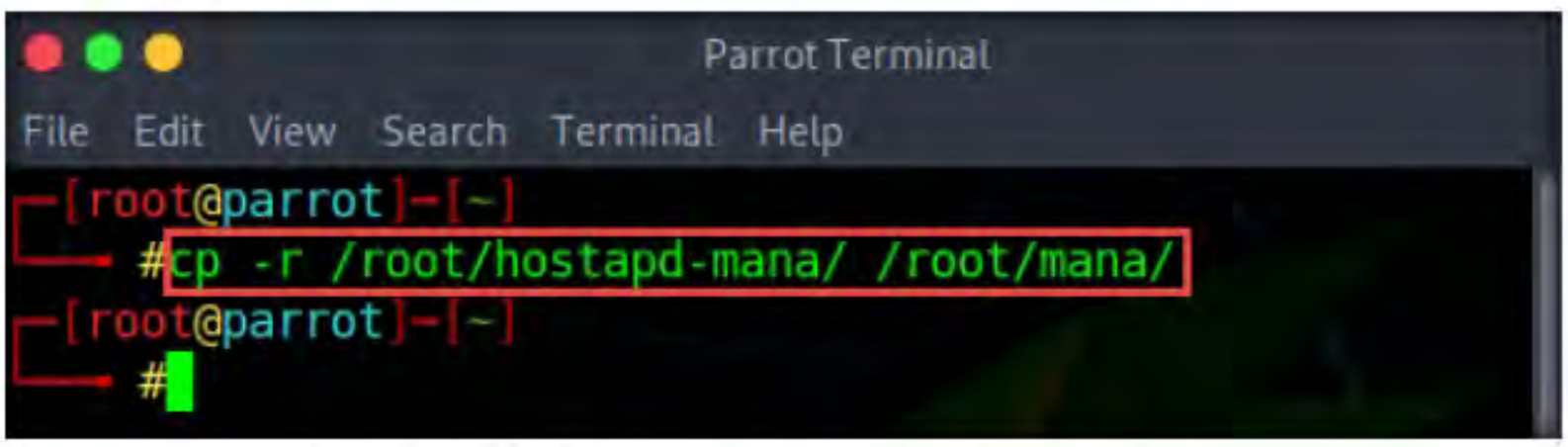

Figure 3.6.7: Copy hostapd-mana content to the mana folder

20. In the **Terminal** window, type **git clone https://github.com/DanMcInerney/net-creds** and press **Enter** to clone net-creds.

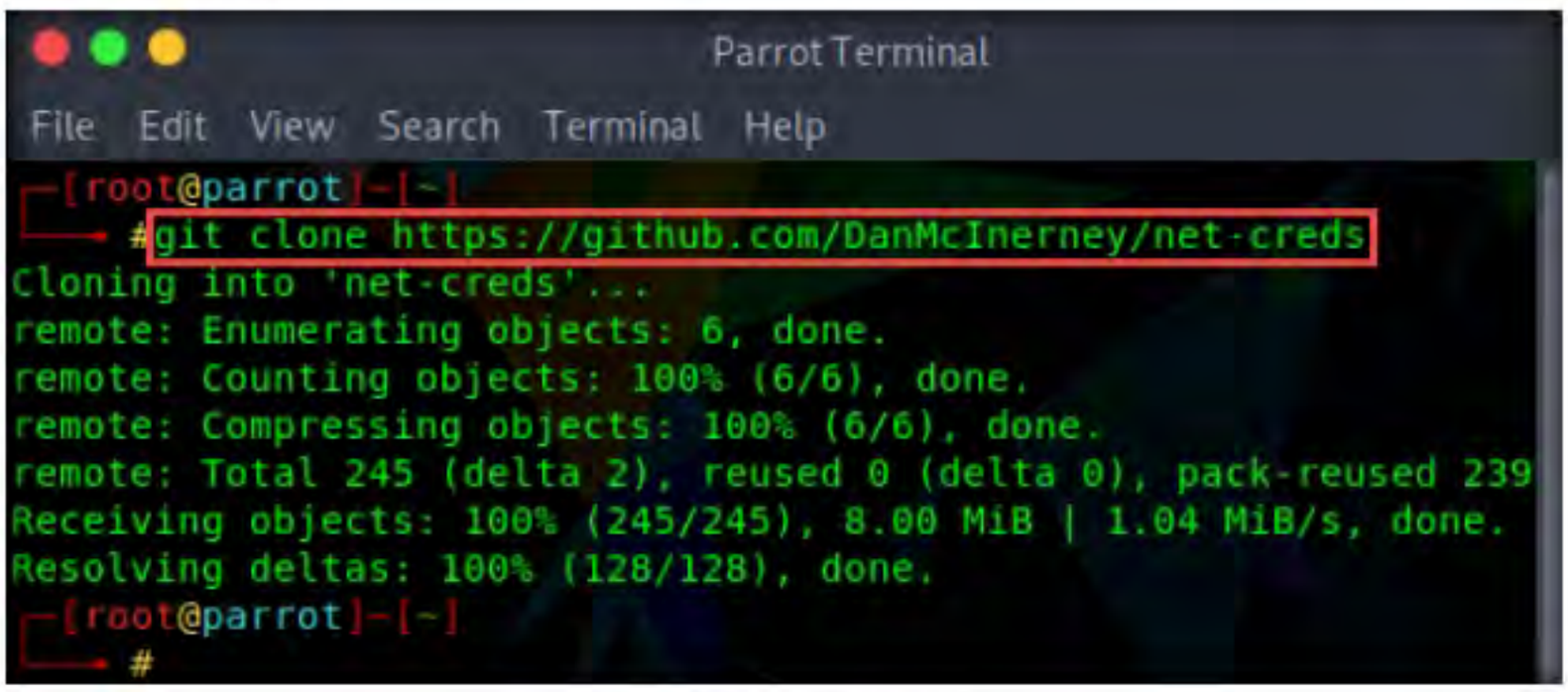

Figure 3.6.8: Cloning net-creds

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **net-creds** folder.
- Paste the copied **net-creds** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/net-creds /root/**.

21. In the terminal window, type **cp -r /root/net-creds /root/mana/** and press **Enter**.

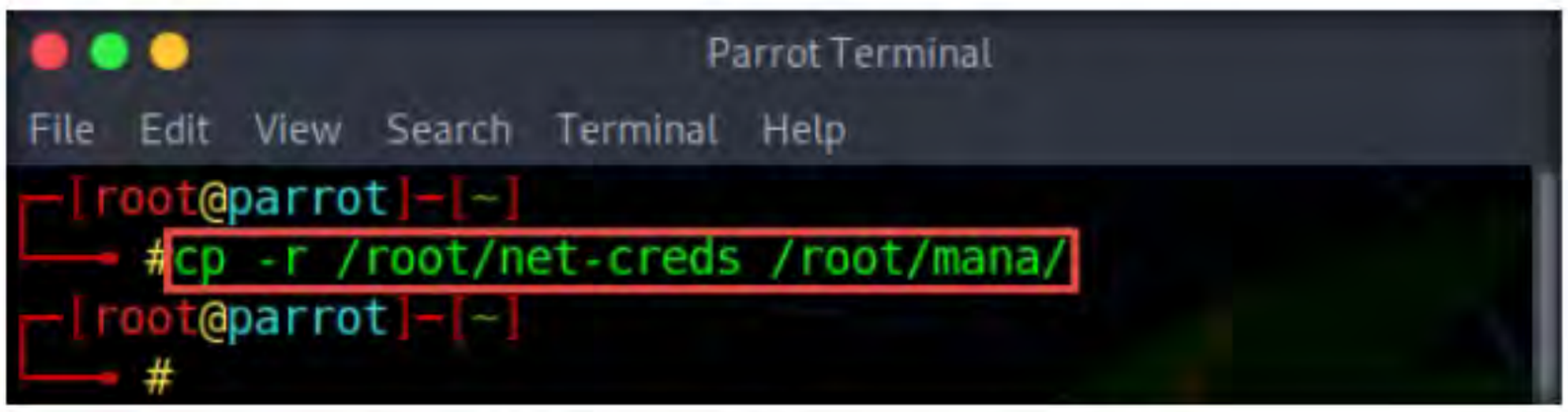

Figure 3.6.9: Copy net-creds folder content to the mana folder

22. In the **Terminal** window, type **git clone https://github.com/LeonardoNve/dns2proxy**, and press **Enter** to clone dns2proxy.

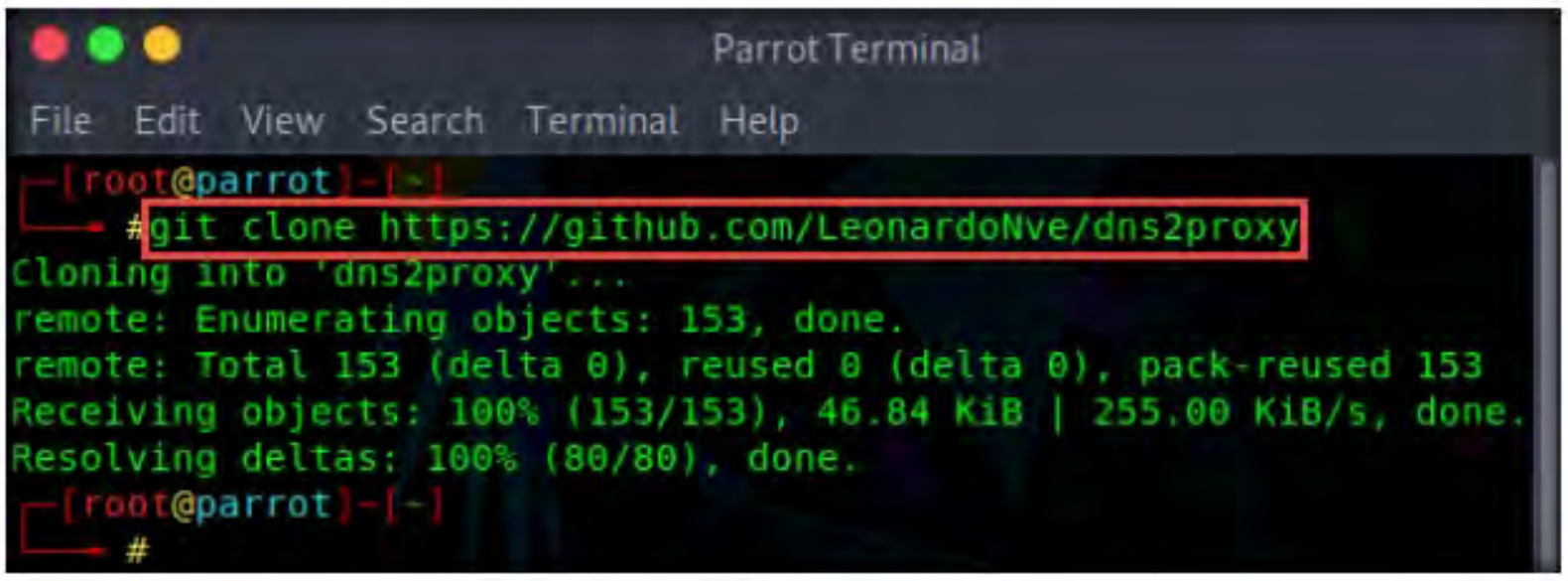

Figure 3.6.10: Cloning dns2proxy

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **dns2proxy** folder.
- Paste the copied **dns2proxy** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/dns2proxy /root/**.

23. In the terminal window, type **cp -r /root/dns2proxy /root/mana/sslstrip-hsts/** and press **Enter**.

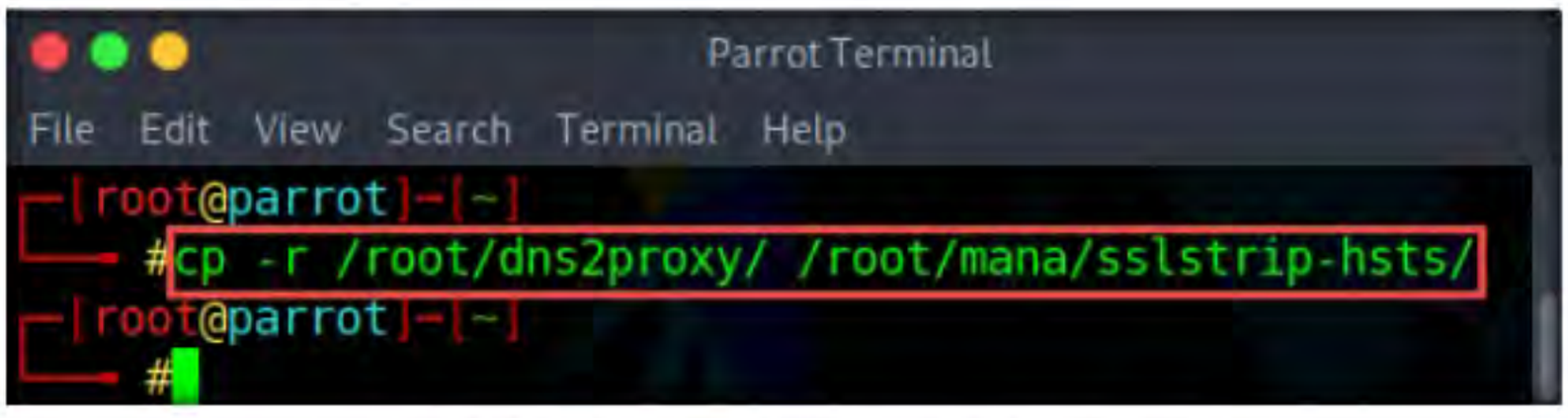

Figure 3.6.11: Copy dns2proxy folder content to the mana folder

24. In the **Terminal** window, type **git clone https://github.com/byt3bl33d3r/sslstrip2**, and press **Enter** to clone sslstrip2.

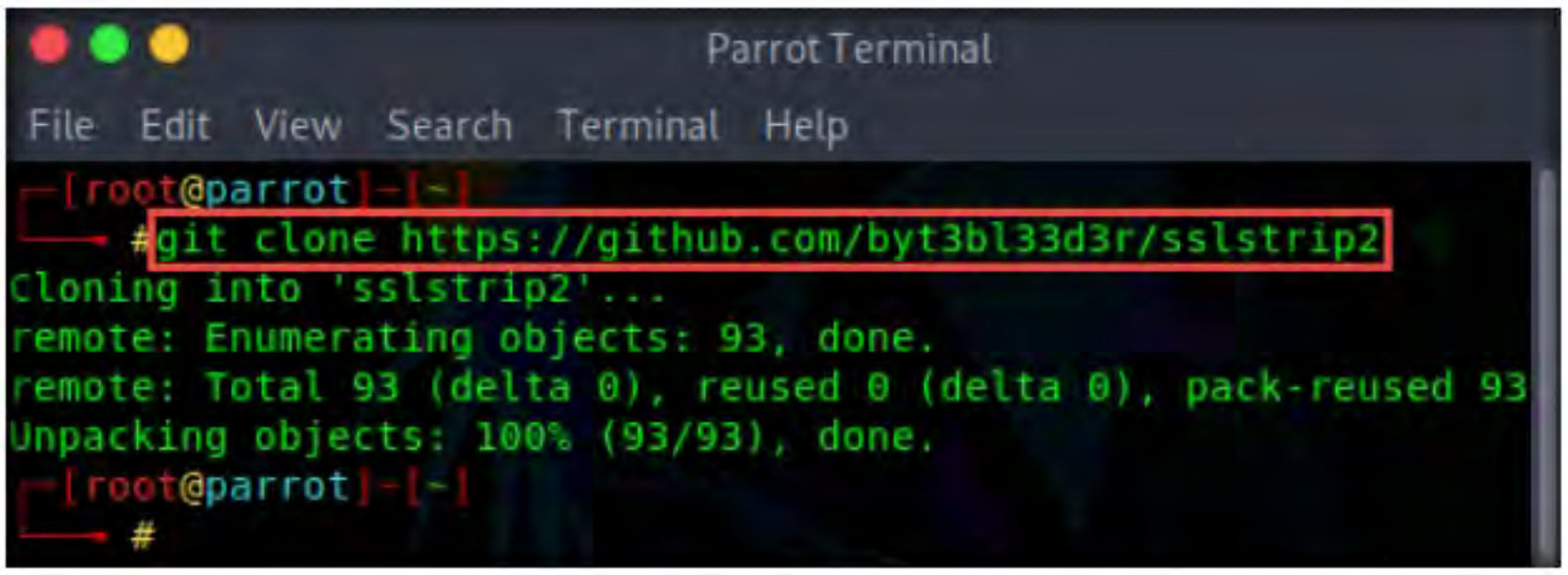

Figure 3.6.12: Cloning sslstrip2

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 16 Hacking Wireless Networks /GitHub Tools/** and copy the **sslstrip2** folder.
- Paste the copied **sslstrip2** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/sslstrip2 /root/**.

25. In the terminal window, type **cp -r /root/sslstrip2 /root/mana/sslstrip-hsts/** and press **Enter**.

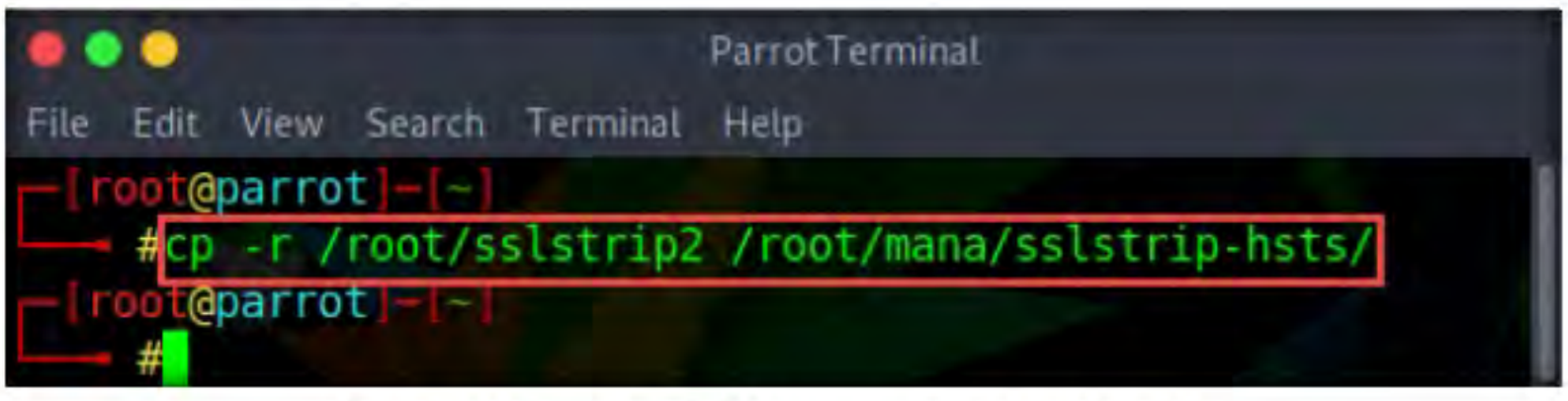

Figure 3.6.13: Copy sslstrip2 folder content to the sslstrip-hsts folder

TASK 6.3

Install and Configure MANA-Toolkit

26. Now, switch back to the **Terminal** window where we issued the **git submodule init** command.
27. Type **make** and press **Enter** to compile the MANA-Toolkit application.

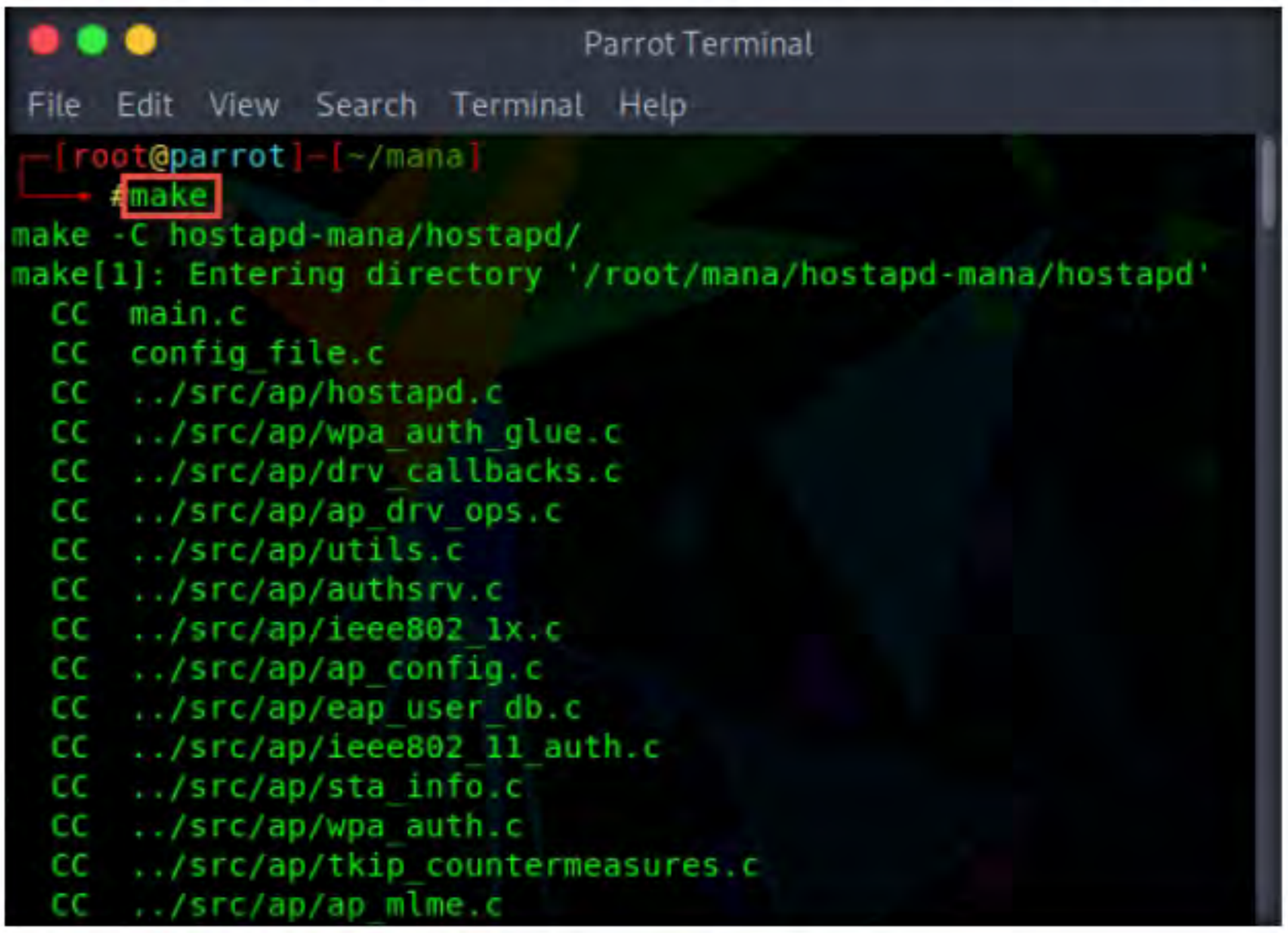

Figure 3.6.14: Compile MANA-Toolkit

28. Now, type **make install** and press **Enter** to install the application.

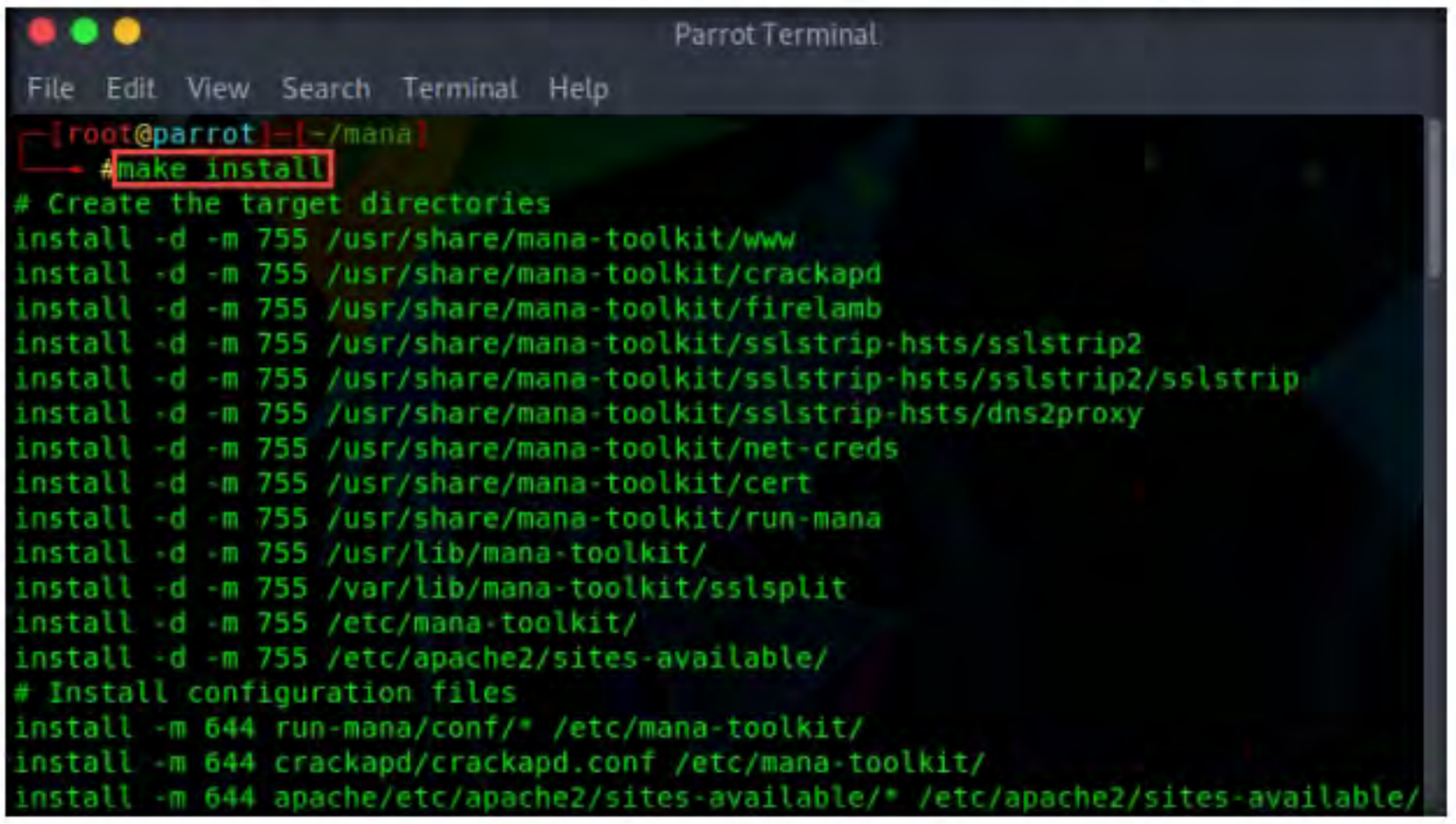

Figure 3.6.15: Install MANA-Toolkit

29. In the **Terminal** window, type **pluma /etc/mana-toolkit/hostapd-mana.conf** and press **Enter** to open the **hostapd-mana.conf** file in the **Pluma** text editor.

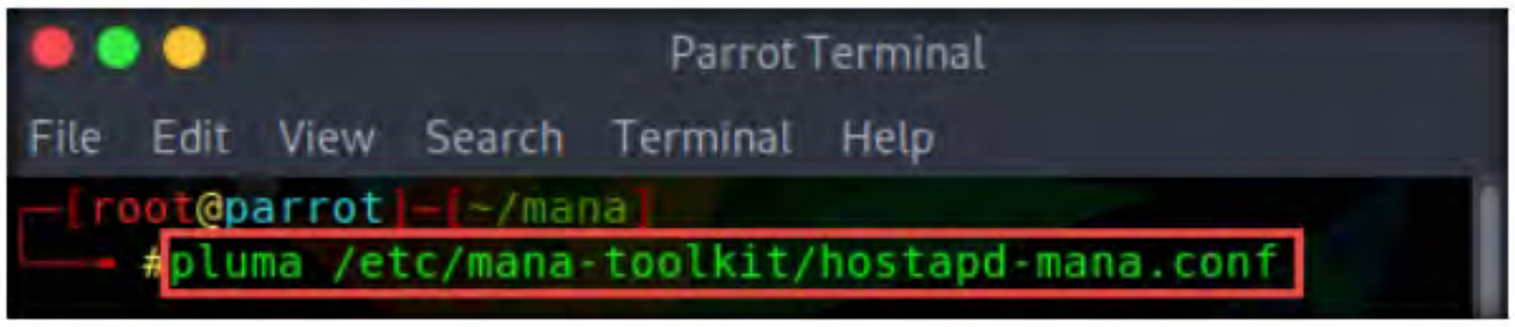

Figure 3.6.16: Open hostapd-mana.conf

30. On **Line 3**, change the **interface** name to **wlan0**, and on **Line 6**, change the **ssid** name to **Free Internet**, as shown in the screenshot.

Note: The name of the **interface** might differ in your lab environment.

Note: You can set an **ssid** name of your choice.

31. Press **Ctrl+S** to save the changes and close the **Pluma** text editor window.

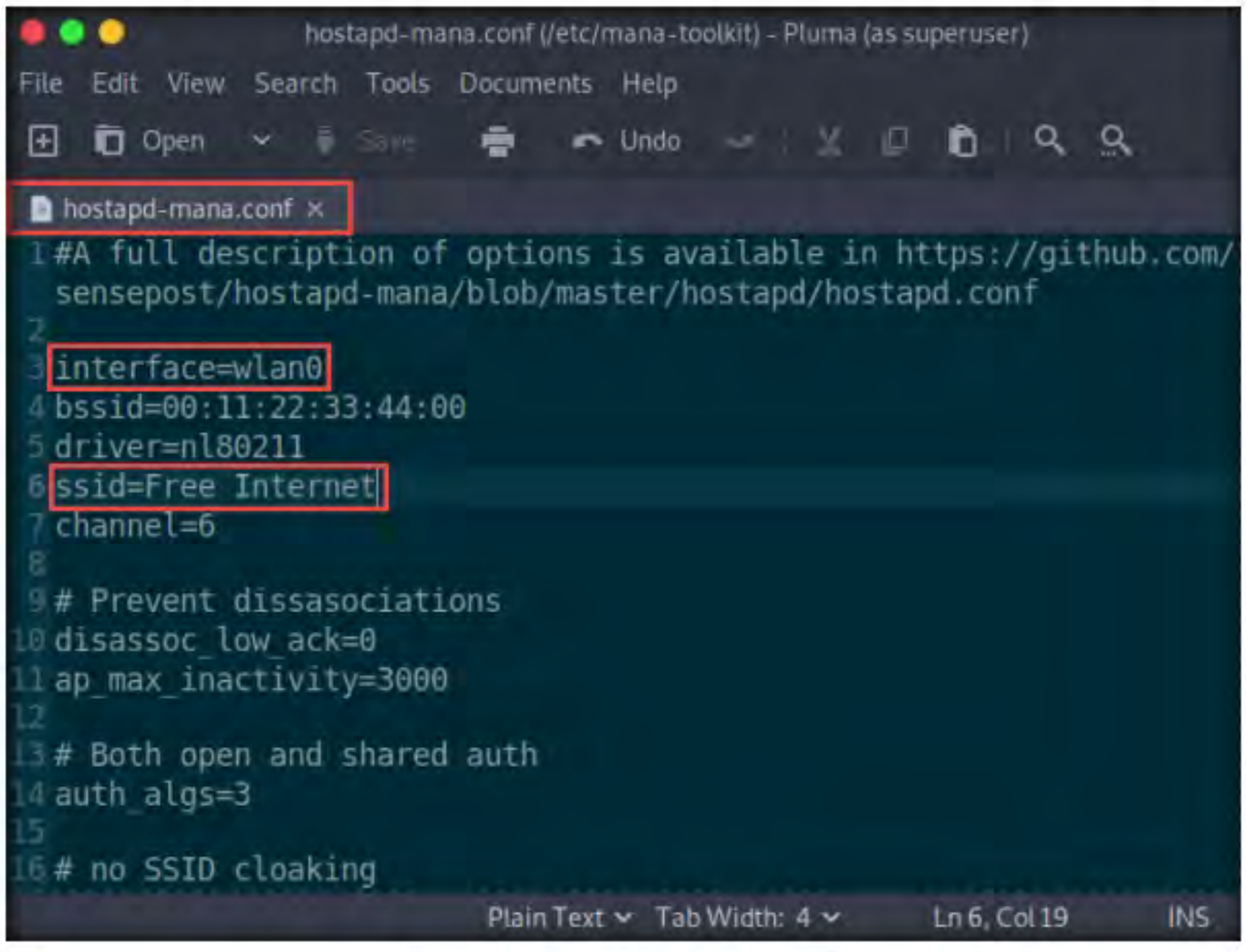

Figure 3.6.17: Edit hostapd-mana.conf

32. Switch back to the **Terminal** window, type **pluma /usr/share/mana-toolkit/run-mana/start-nat-simple.sh**, and press **Enter** to open the **start-nat-simple.sh** file in the **Pluma** text editor.

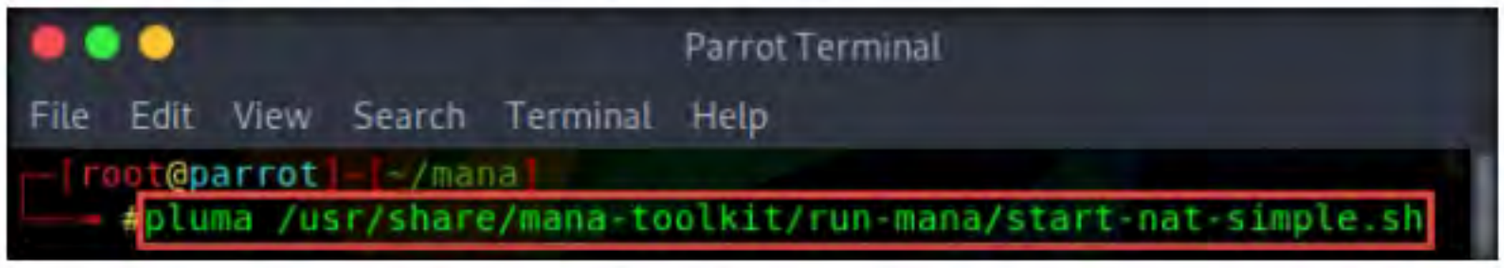

Figure 3.6.18: Open start-nat-simple.sh

33. On **Line 4**, change the **phy** name to **wlan0**, as shown in the screenshot.
34. Press **Ctrl+S** to save the changes and close the **Pluma** text editor window.

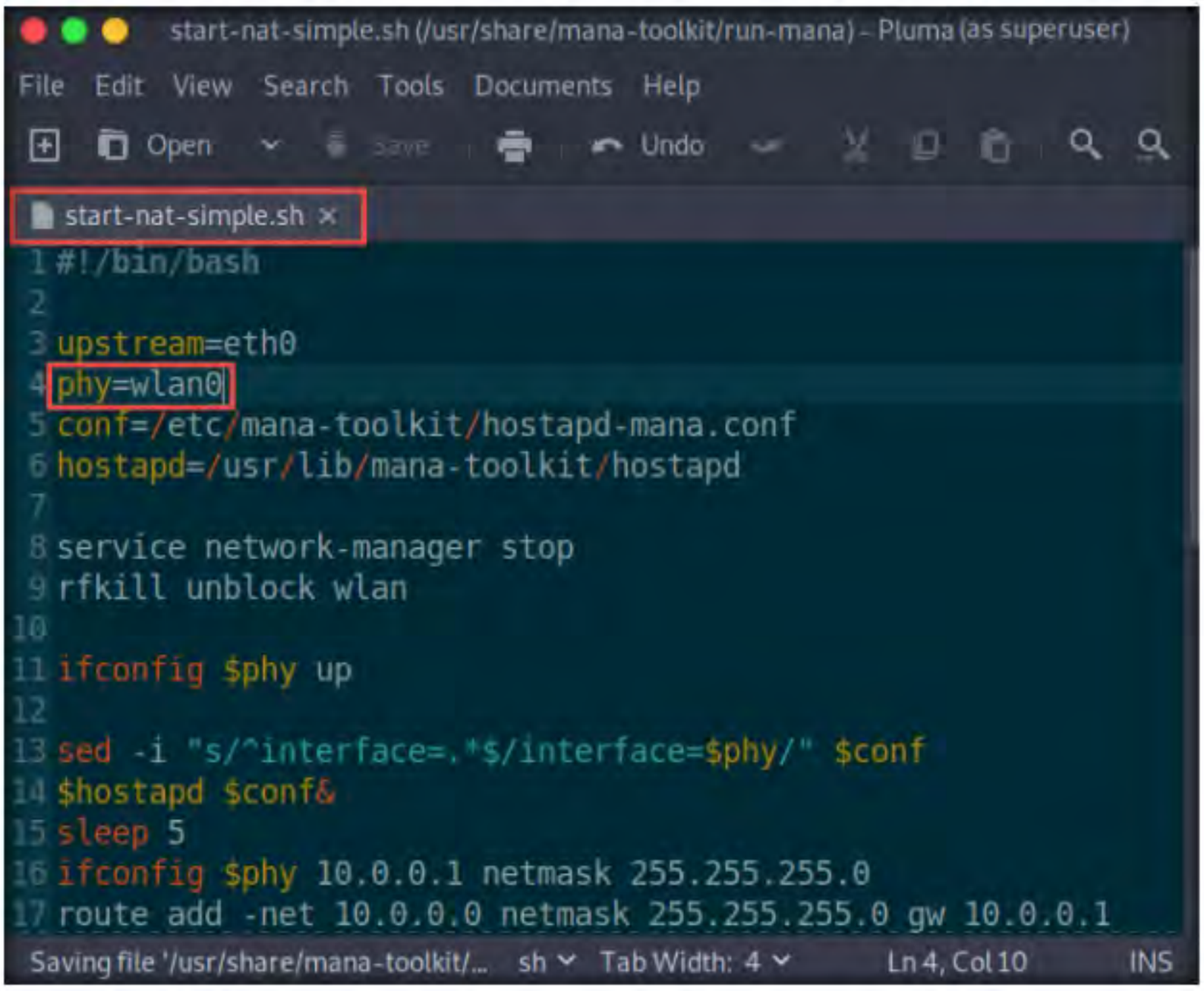

Figure 3.6.19: Edit start-nat-simple.sh

TASK 6.4

Create a Rogue Access Point

35. Now, in the terminal window, type **bash /usr/share/mana-toolkit/run-mana/start-nat-simple.sh** and press **Enter** to create a rogue access point.
36. Observe that a rogue access point has been created with the MAC address as **00:11:22:33:44:00** and the SSID as **Free Internet**.
37. This rogue access point (**Free Internet**) starts sending probe requests to all the available access points and Wi-Fi-enabled devices in the network, as shown in the screenshot.

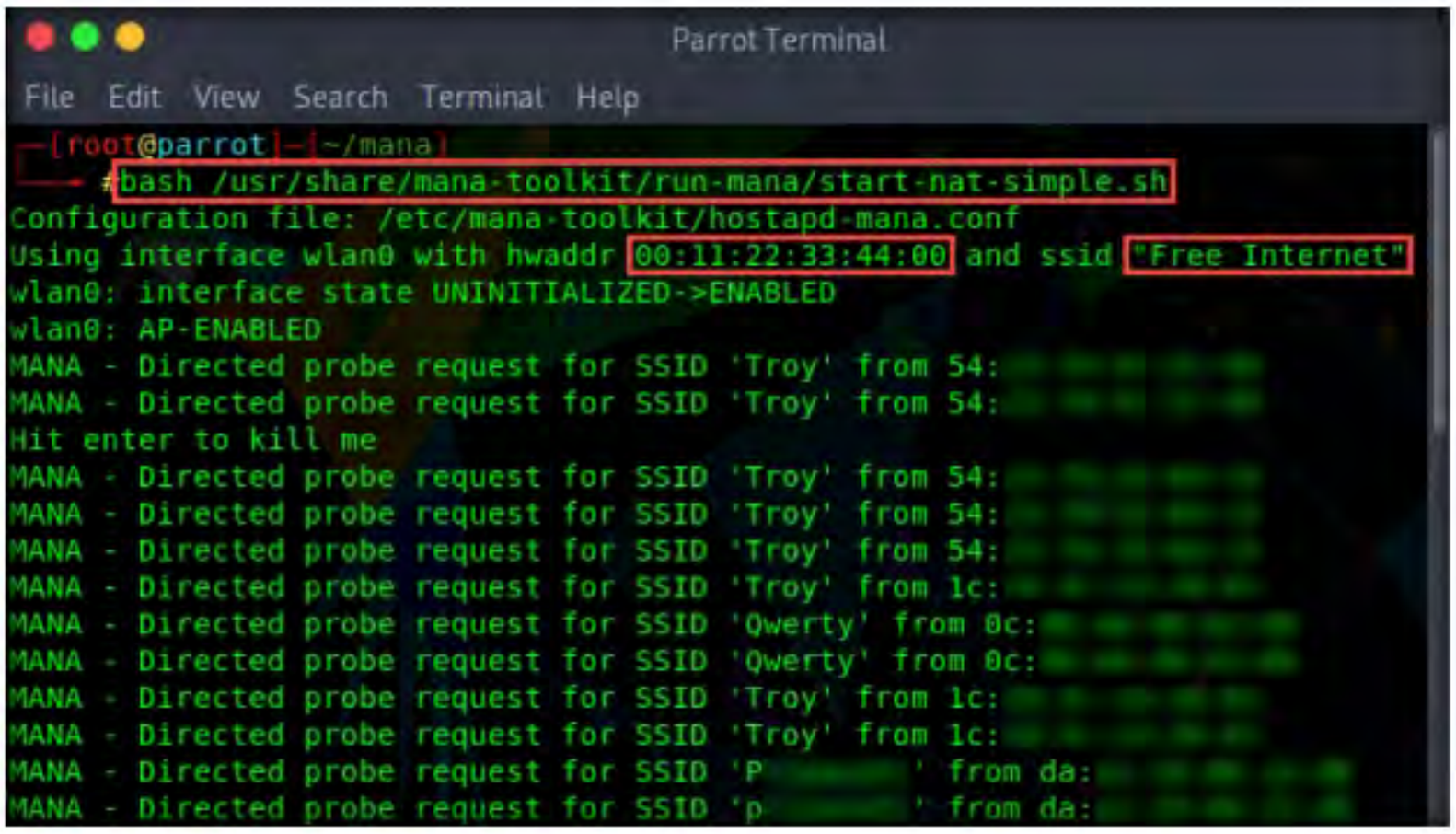

Figure 3.6.20: Rogue access point sending probe packets

TASK 6.5

Connect to the Rogue Access Point as a Victim

38. Now, switch to your **Android** mobile device; turn it on.
39. Turn on **Wi-Fi** and navigate to **WLAN** settings.
40. On the **WLAN** screen, you should see an access point with the SSID **Free Internet** under **AVAILABLE NETWORKS**.

Note: Ensure that your mobile device's Wi-Fi is turned on.

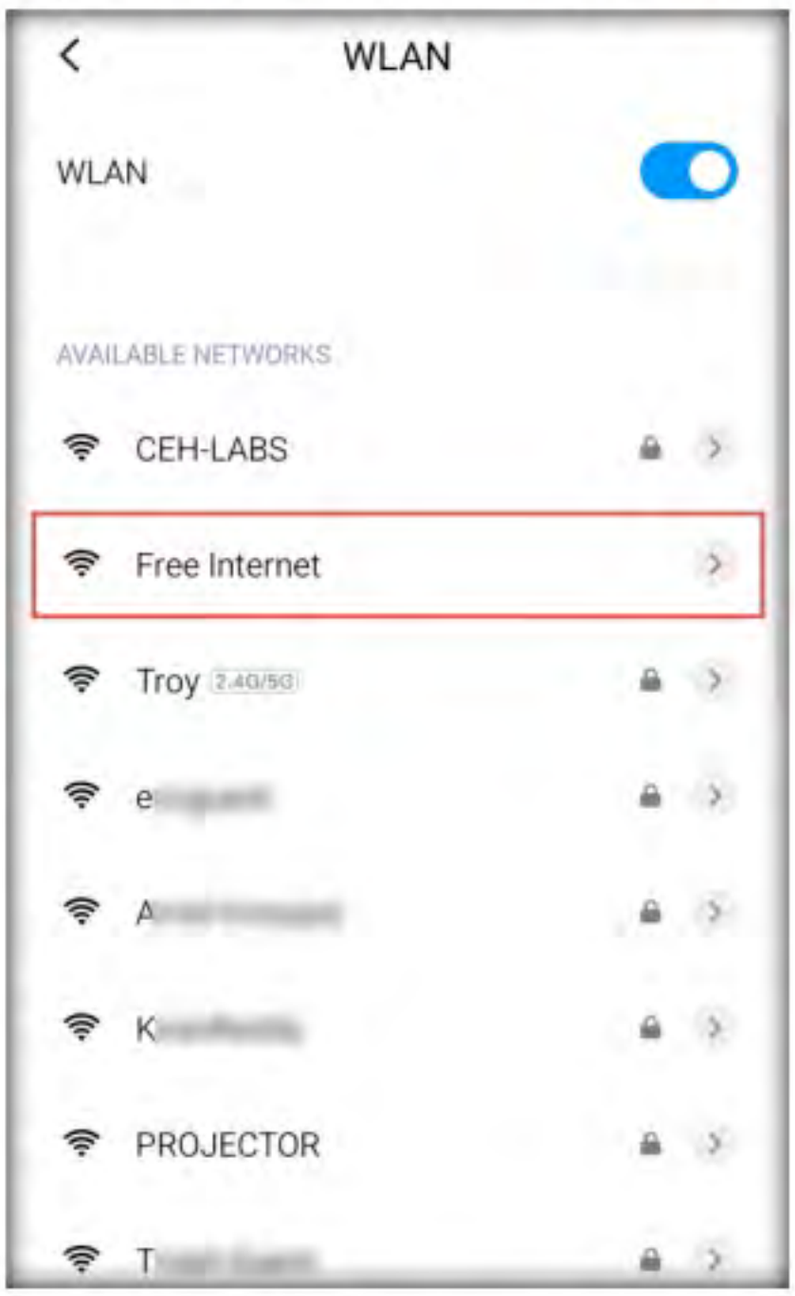

Figure 3.6.21: Rogue access point

41. Click the **Free Internet** access point. Your device obtains an IP address and establishes a connection with the access point, as shown in the screenshot.
42. Note the **Connected** status under **Free Internet**.

Figure 3.6.22: Connected to rogue access point

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

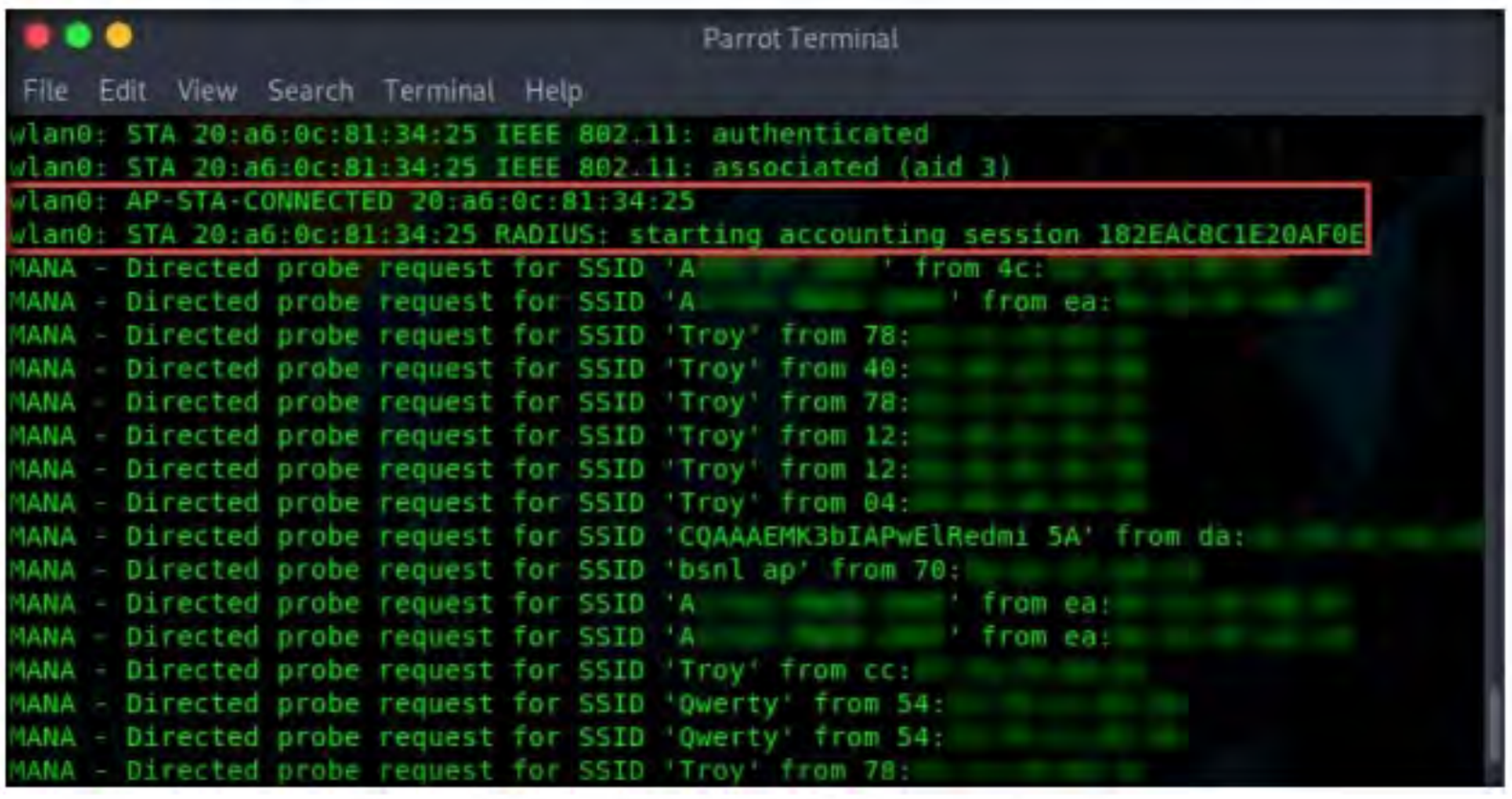

Figure 3.6.23: Connection established with the rogue access point

44. Minimize the **Terminal** window.
45. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
46. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

TASK 6.6

Launch and Analyze Wireless Traffic

Note: As in Lab 2, Task 1, we will use Wireshark to view the incoming and outgoing wireless network traffic.

47. In **The Wireshark Network Analyzer** window, double-click the wireless network interface (in this case, **wlan0**) to start capturing network traffic.

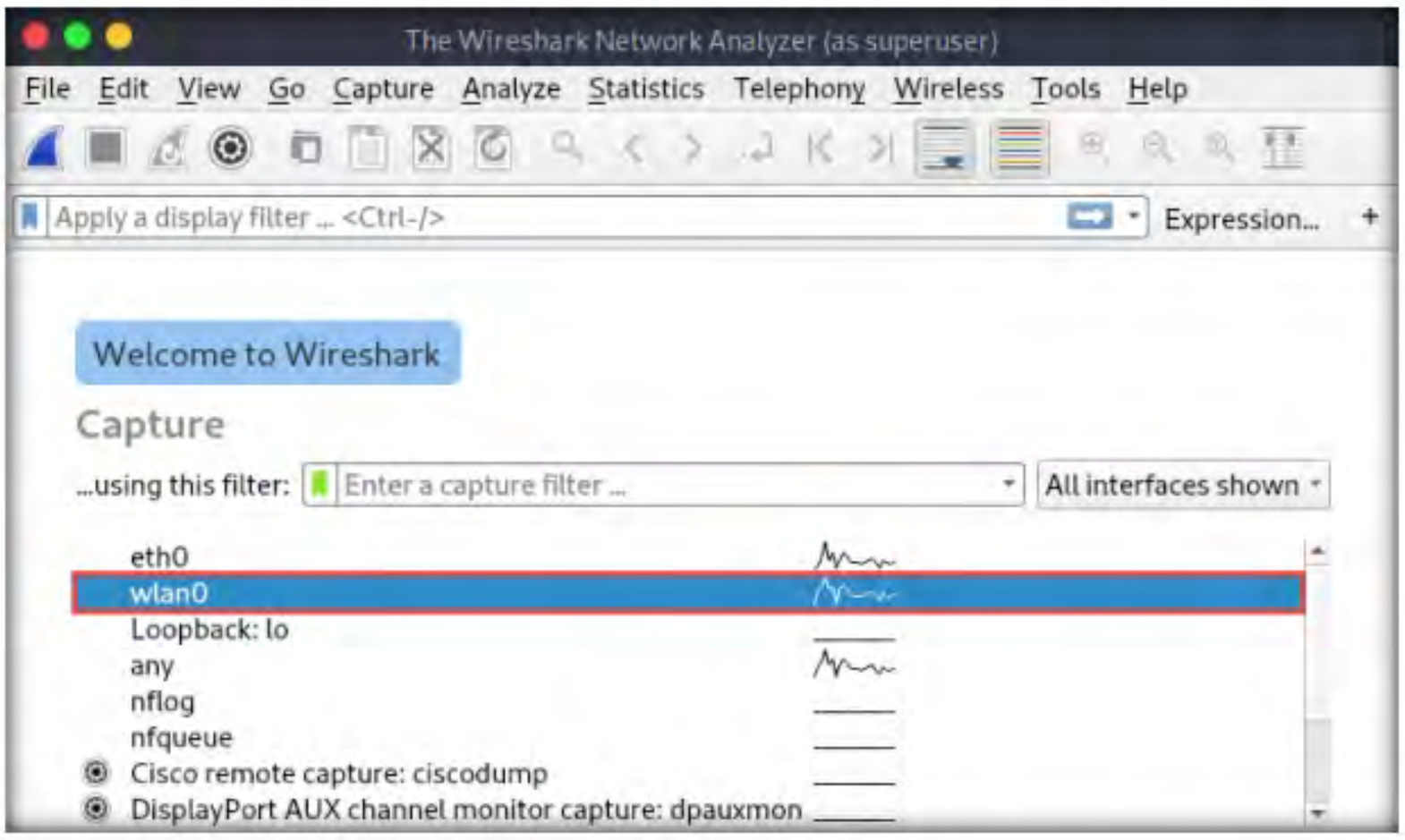

Figure 3.6.24: Wireshark window

48. **Wireshark** will begin capturing network traffic on the specified wireless interface, as shown in the screenshot.

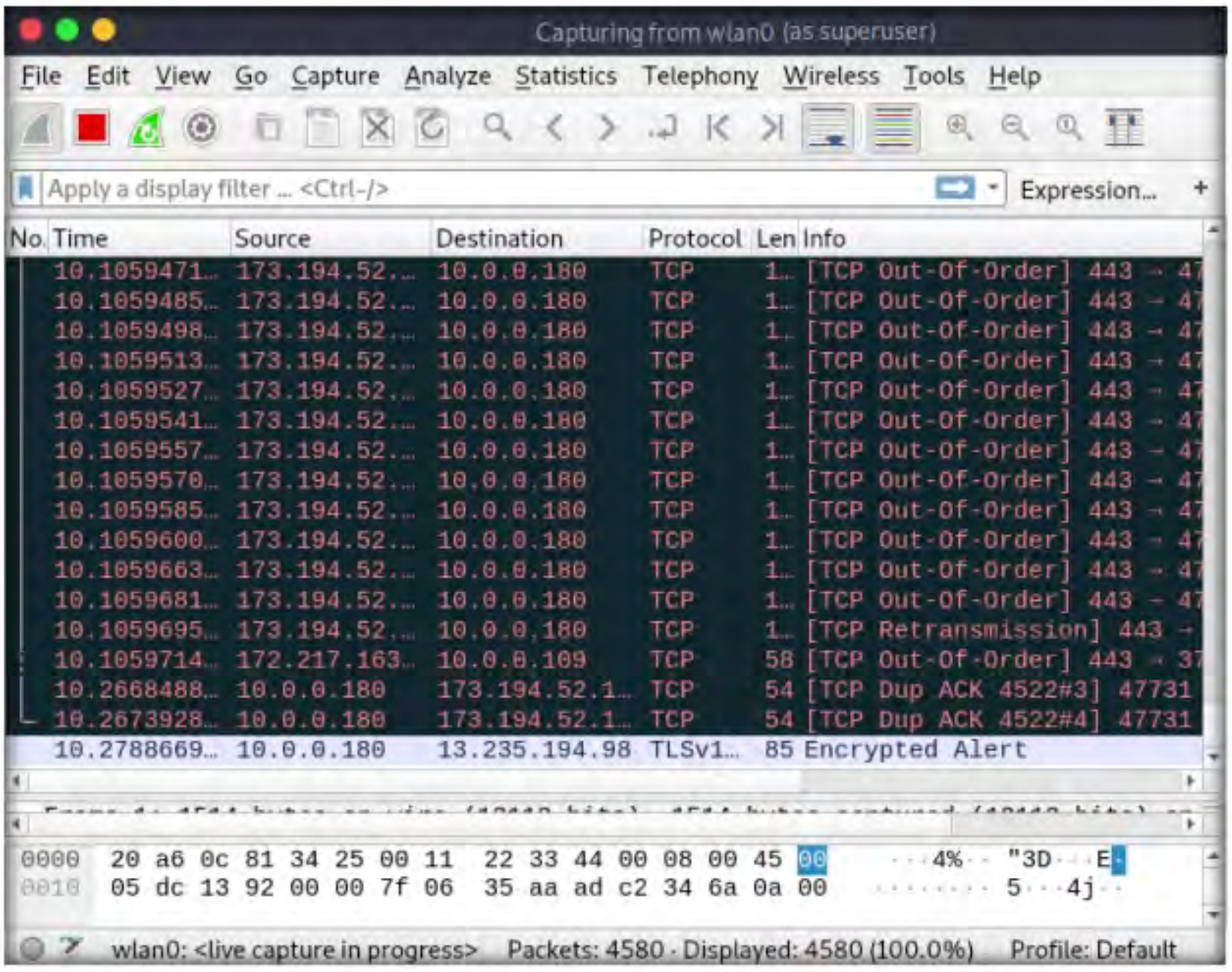

Figure 3.6.25: Wireshark window showing captured packets

49. Now, switch to the **Android** mobile device and open any web browser app.
50. In the browser, type **http://testphp.vulnweb.com/login.php** in the address bar and press **Enter**.
51. The **Acunetix Web Vulnerability Scanner** webpage will open. Enter random **Username** and **Password** values (in this case, 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 that 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 will need to launch MANA-Toolkit using **start-nat-full.sh**, after which you can attempt to capture user credentials on HTTPS websites.

Figure 3.6.26: Open an HTTP website

52. Switch back to the **Parrot Security** virtual machine.
53. In the **Wireshark** window, click the **Stop capturing packet** icon ( ) from the toolbar to stop capturing network packets.

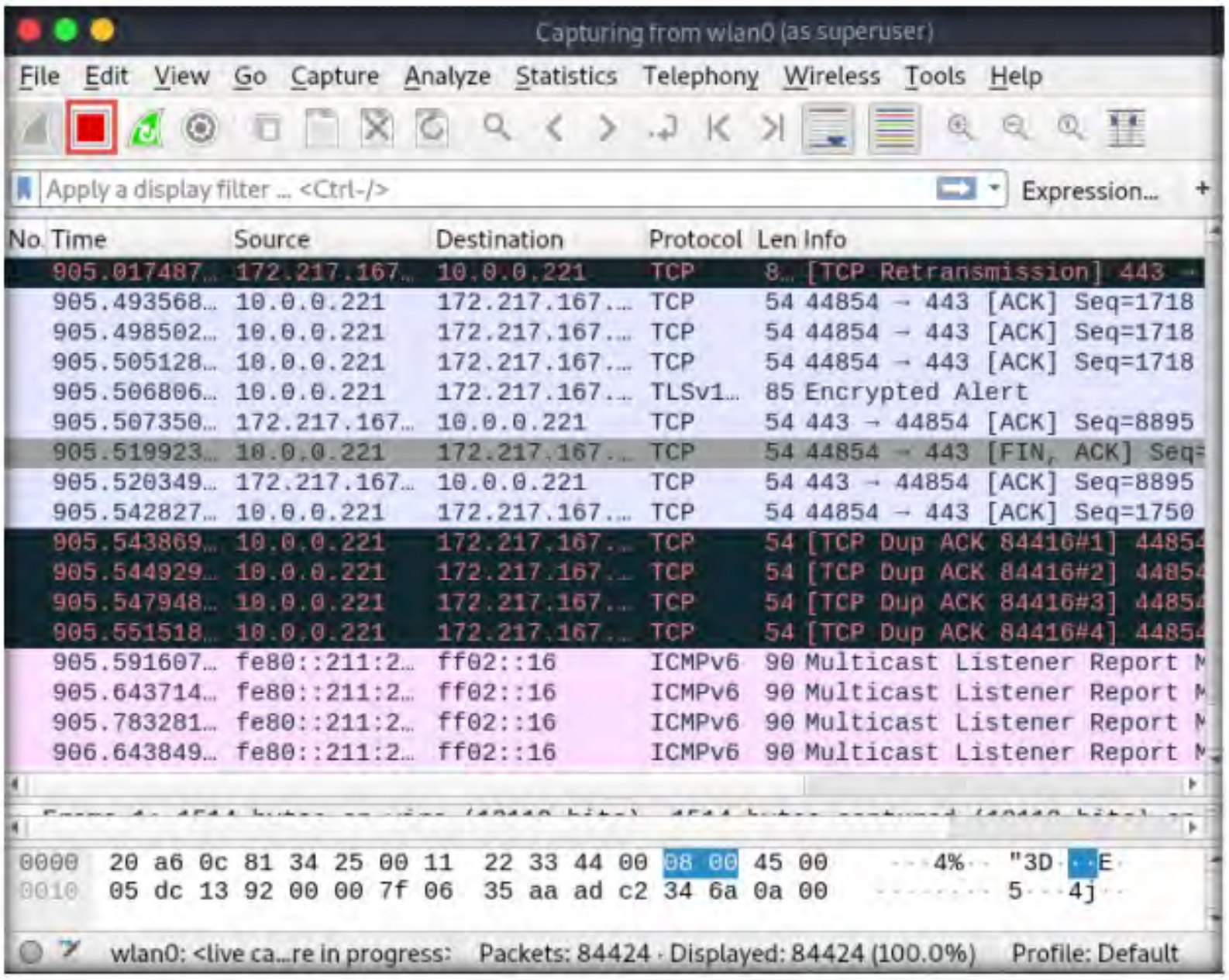

Figure 3.6.27: Wireshark: Stop capturing packets

54. Click **Edit** from the menu bar and click the **Find Packet...** option from the context menu.

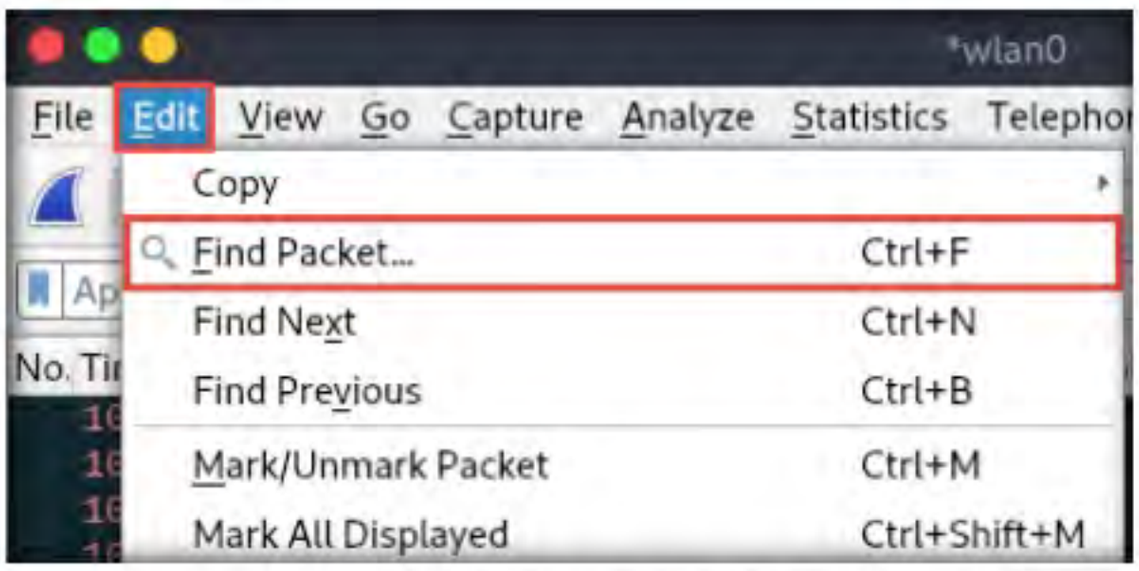

Figure 3.6.28: Wireshark: Click Find Packet...

55. A row of packet filter fields appear. In the **Case sensitive** field, click **String** from the drop-down options. Click **Packet list** and select **Packet bytes** from the drop-down options. Finally, in the **String** text field, type **pass**, and then click the **Find** button.

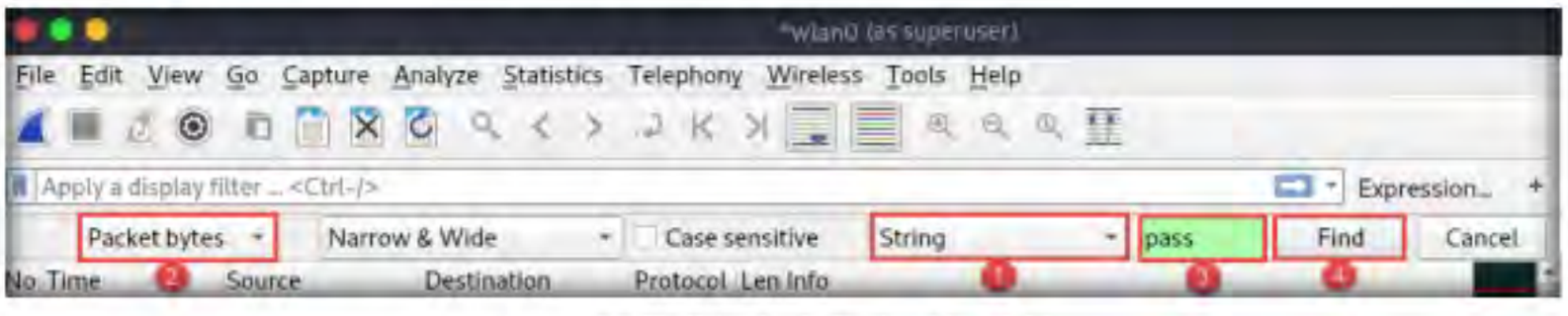

Figure 3.6.29: Wireshark: Packet filter fields

TASK 6.7

Obtain the User Credentials

56. **Wireshark** will now display the sniffed password packet from the captured packets.
57. Look in the **HTML Form URL Encoded: application/x-www-form-urlencoded** node in the packet details section to view the captured username and password, as shown in the screenshot.

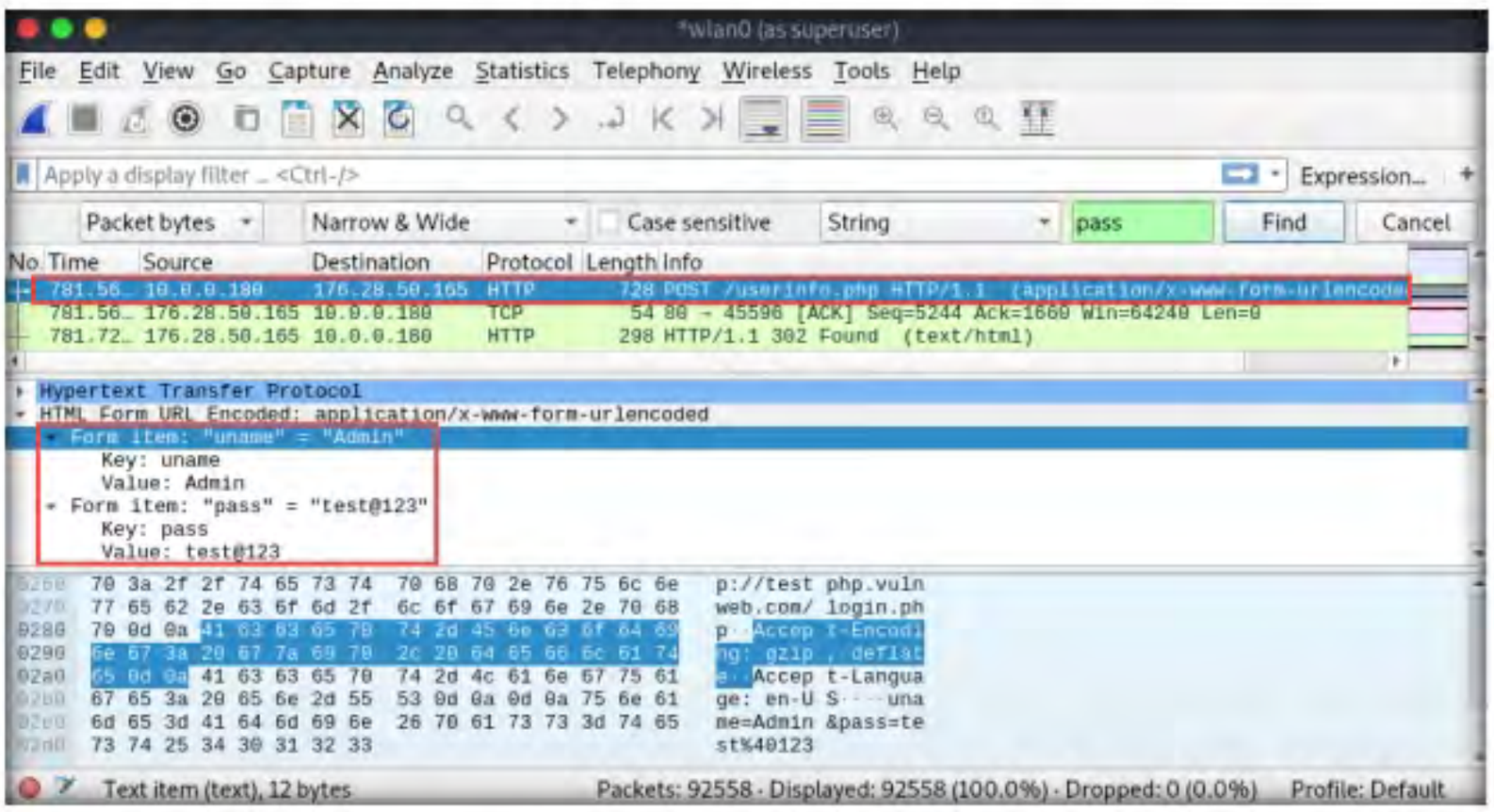

Figure 3.6.30: Wireshark: Captured user credentials

58. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Quit without Saving**.
59. In the **Terminal** window, press **Ctrl+C**, and then **Enter** to stop MANA-Toolkit and terminate the rogue access point **Free Internet**.
60. The state of **wlan0** changes from **ENABLED** to **DISABLED**, as shown in the screenshot.

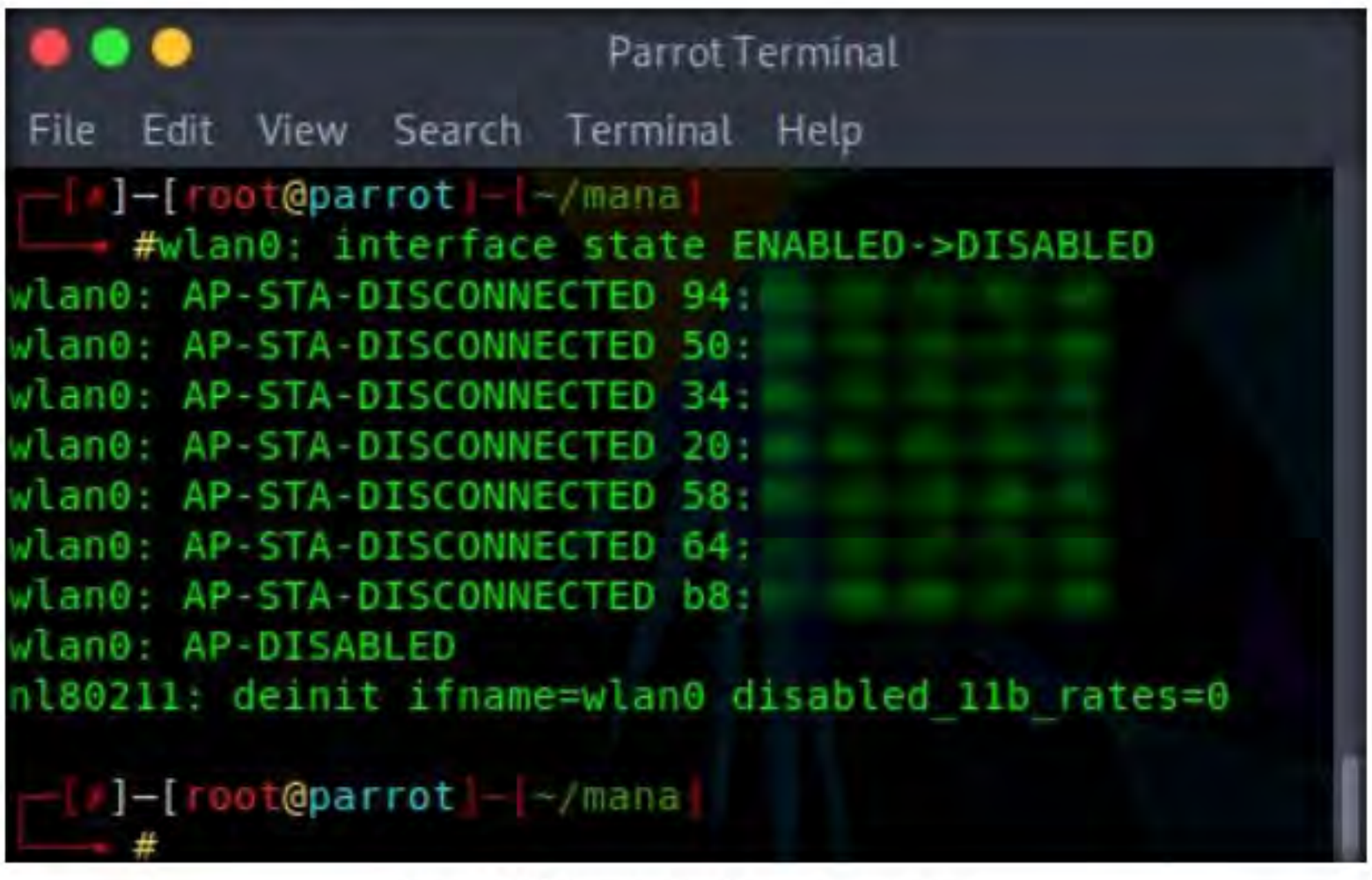

Figure 3.6.31: Terminating the rogue access point

61. This concludes the demonstration of how to create a rogue access point to capture data packets using MANA-Toolkit.
62. Close all open windows and document all the acquired information.
63. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Now that the lab exercises have been completed, it is necessary to re-enable the ethernet adapter on the **Windows 10** virtual machine.

64. Turn on the **Windows 10** virtual machine and login with the credentials **Admin/Pas$$w0rd**.
65. Open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
66. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.

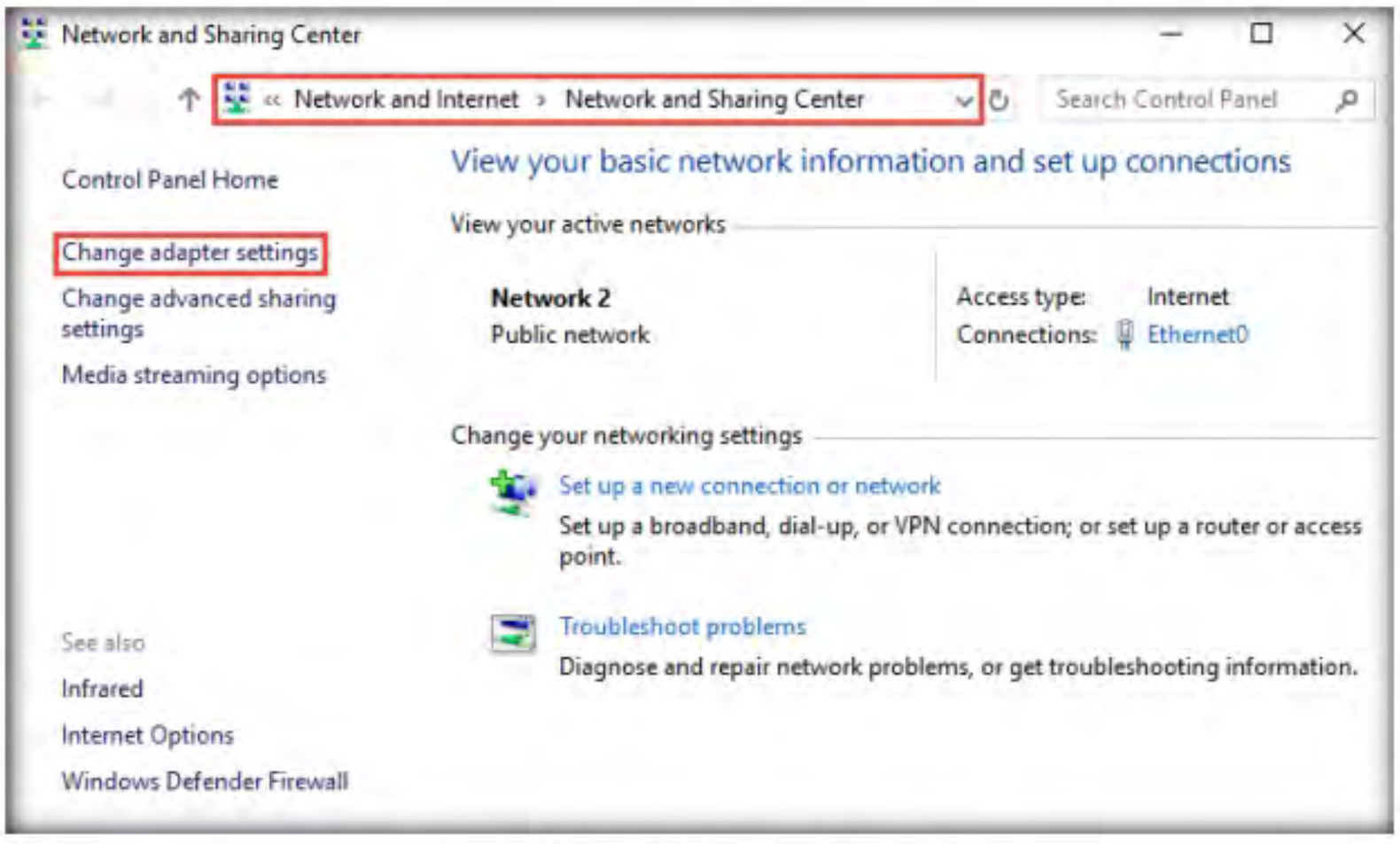

Figure 3.6.32: Network and Sharing Center window

67. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Enable** from the options.

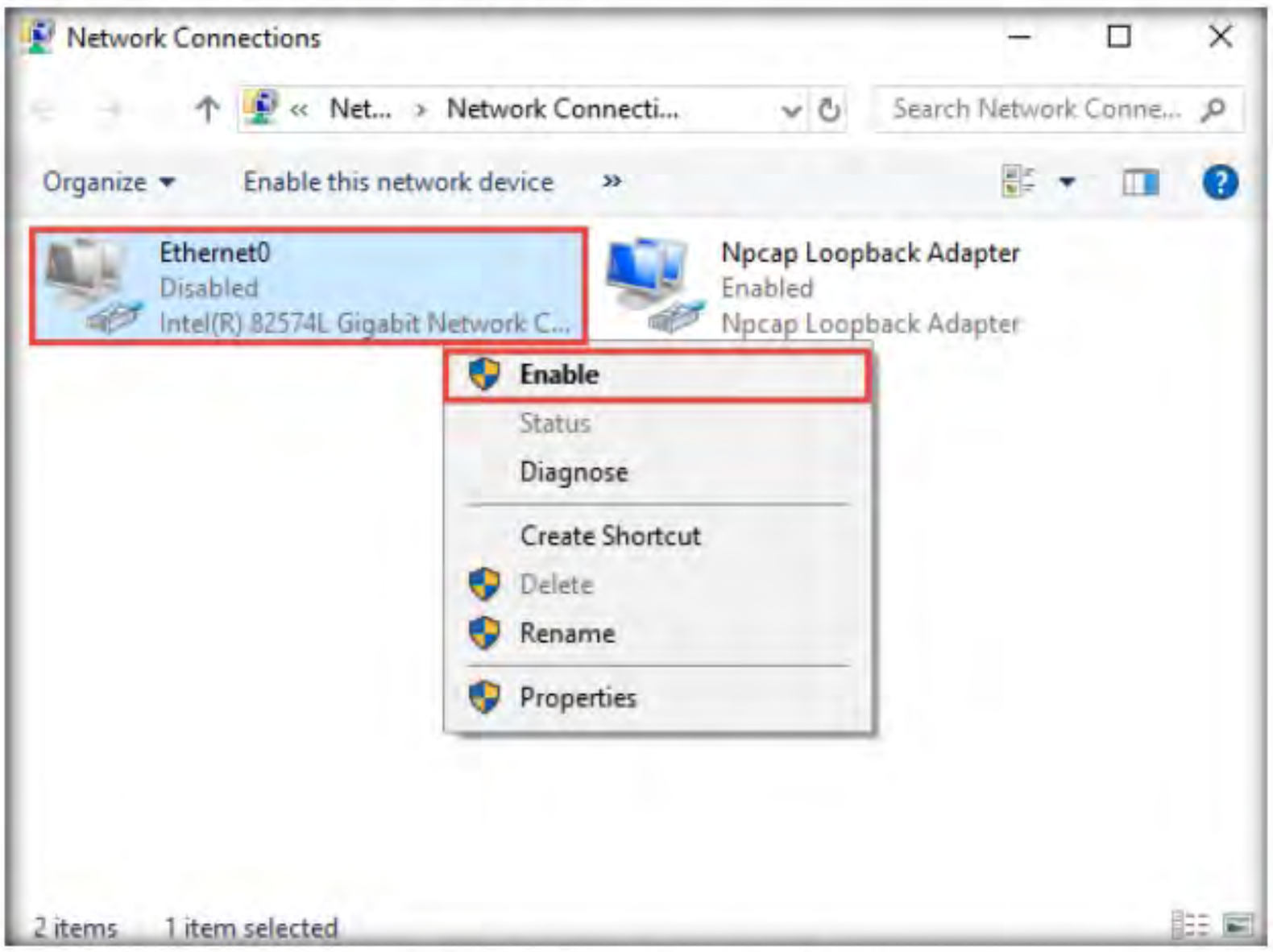

Figure 3.6.33: Network Connections window

68. **Ethernet0** is enabled, and you will observe that the system is now connected to the internet.
69. Close all open windows and turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Hacking Mobile Platforms

Module 17