Hacking Wireless Networks

Module 16

Hacking Wireless Networks

A wireless network is an unbounded data communication system that uses radio-frequency technology to communicate with devices and obtain data. Through radio frequency technology, Wi-Fi allows devices to access wireless networks without cables from anywhere within range of an access point. The wireless network can be at risk to various types of attacks, including access-control attacks, integrity attacks, confidentiality attacks, availability attacks, and authentication attacks.

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 Objective

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

To carry out this lab, you need:

- Windows 11 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**	CyberQ ***
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		√	

Remark

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

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

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

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

Lab 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.

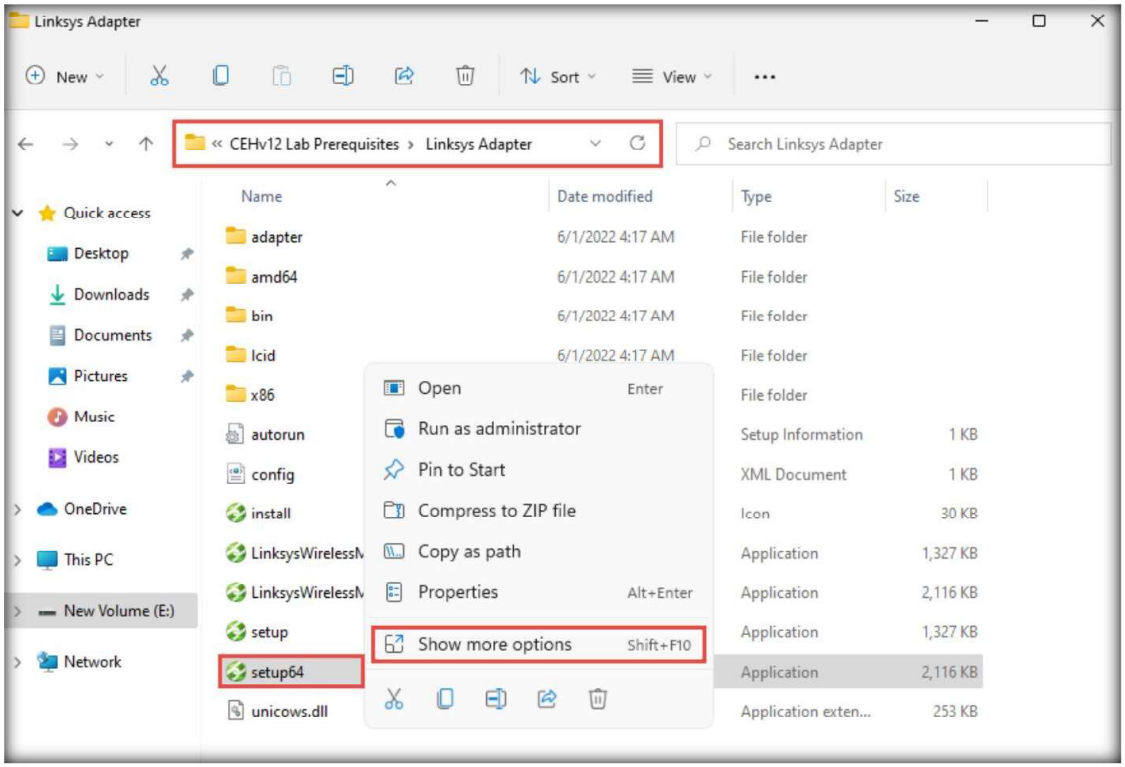
Note: If you decide to use a different wireless adapter, the steps to set up the adapter might differ.

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

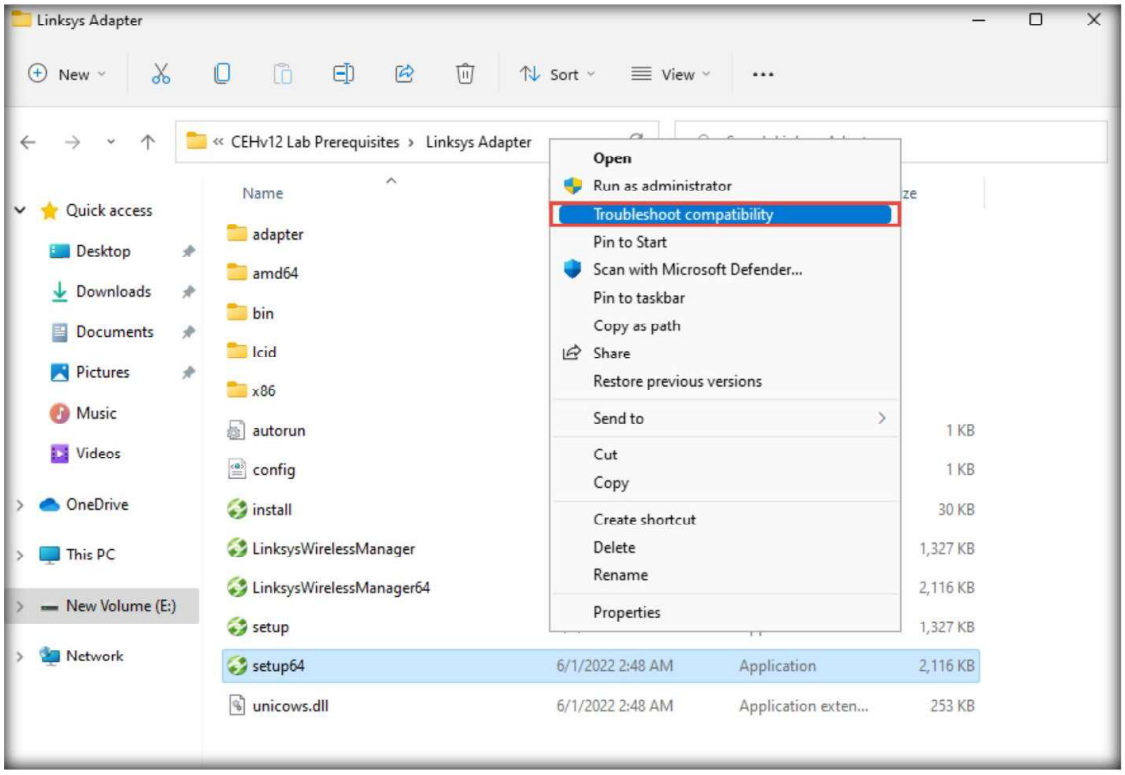
   Note: Ensure that wireless router is plugged in to the network/Internet.

2. Turn on the **Windows 11** virtual machine, and log in with the credentials **Admin** and **Pa$$w0rd**.

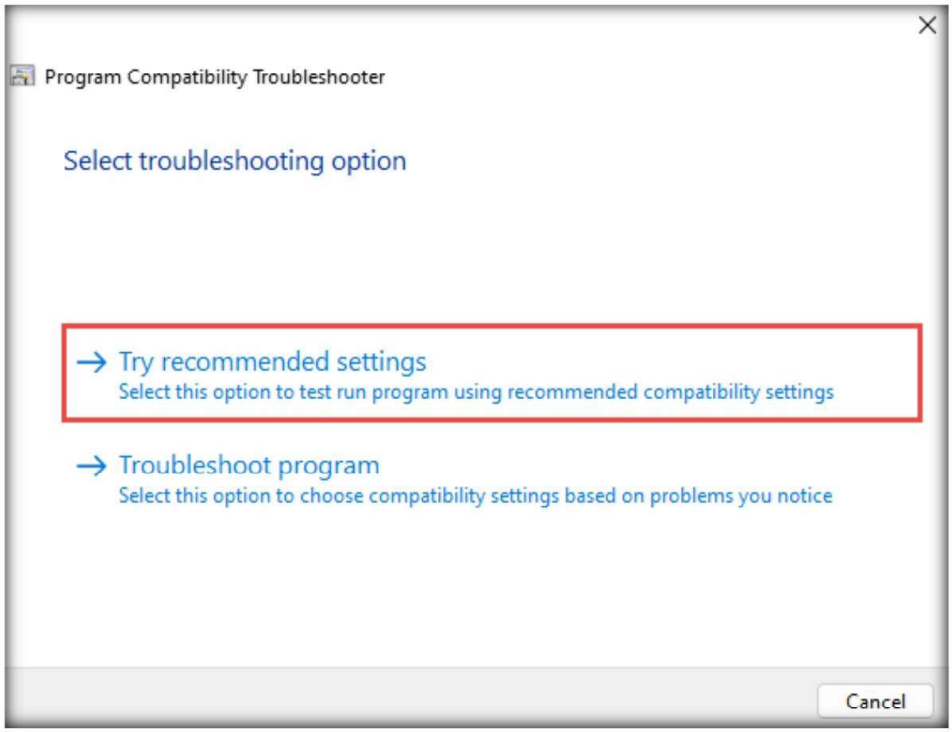
3. Navigate to **E:\CEH-Tools\CEHv12 Lab Prerequisites\Linksys Adapter**, right-click **setup64.exe**, and click the **Show more options** option.



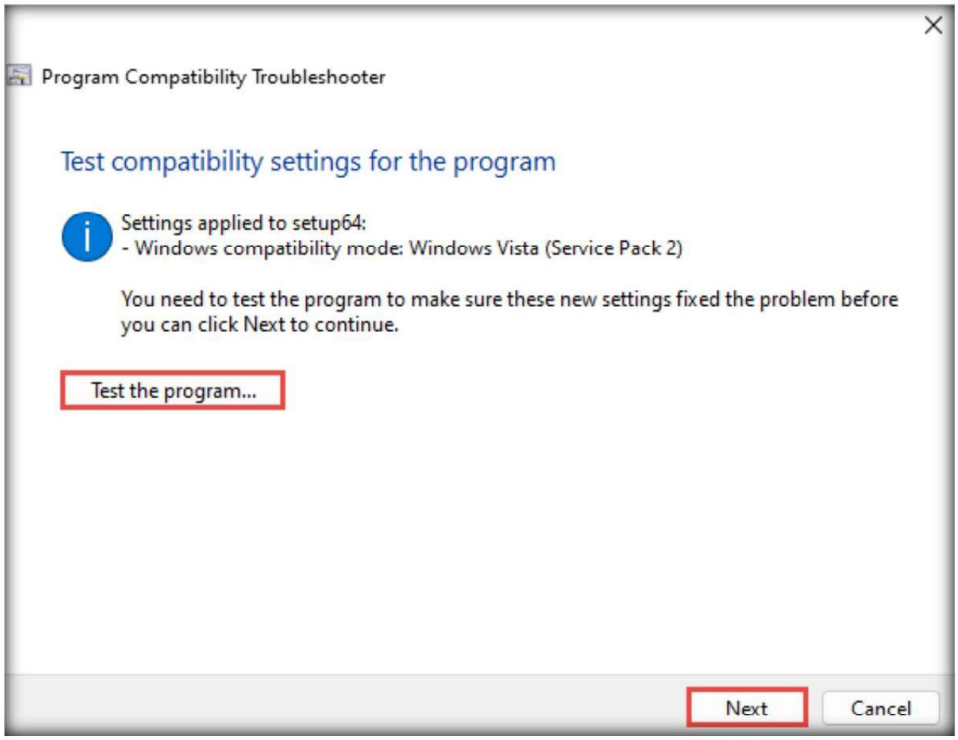
4. From the available options, select **Trouble compatibility** option.



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

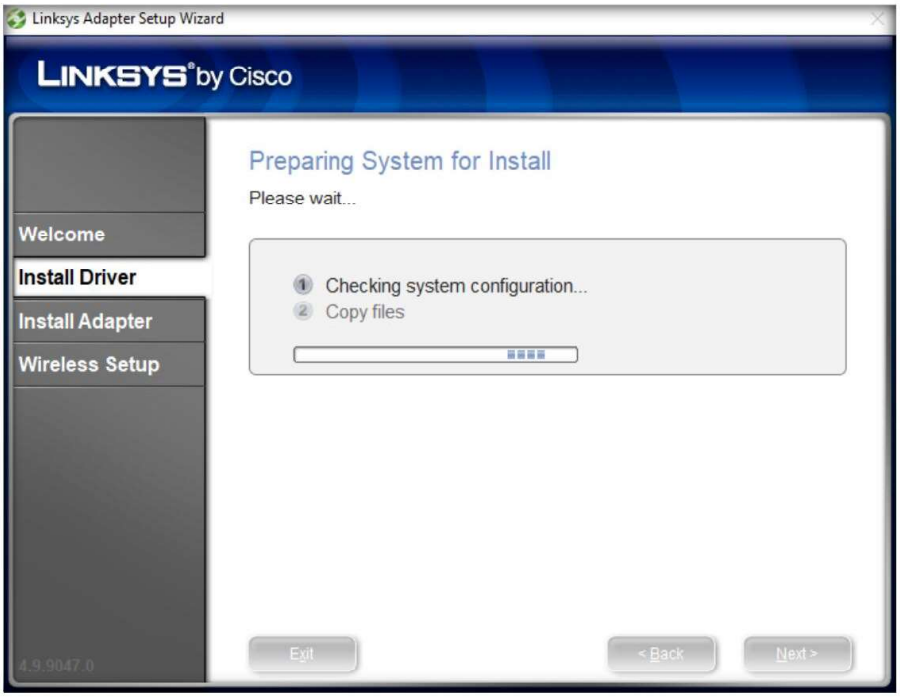


7. In the **Test compatibility settings for the program** wizard, click **Test the program…**



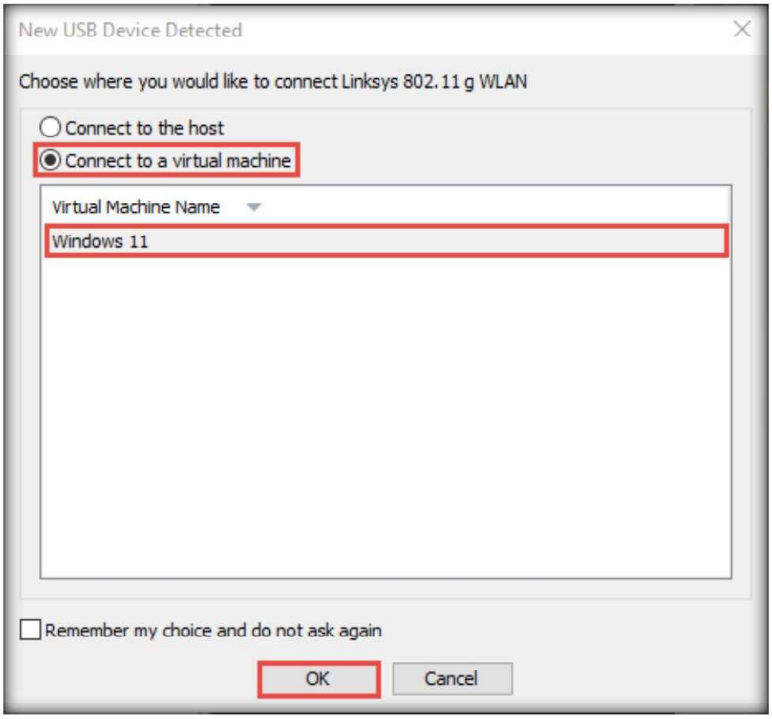
8. A **User Account Control** pop-up appears; click **Yes**.
9. The **Linksys Adapter Setup Wizard** appears; click **Next**.

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

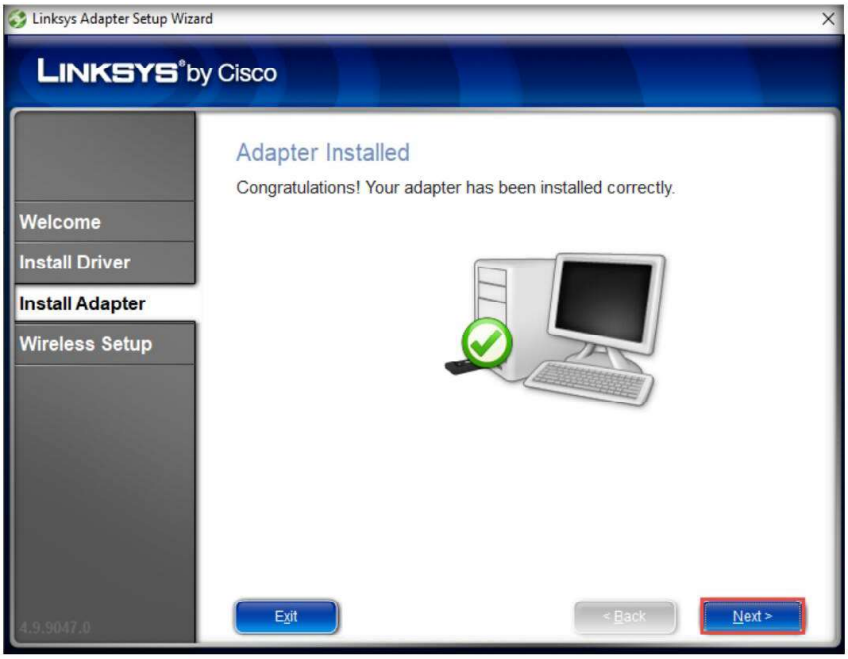


12. The **Insert Adapter** wizard appears. Plug your **Linksys 802.11 g WLAN** adapter into an available USB port.

13. 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 11**; click **OK**.



14. In the **Linksys Adapter Setup Wizard** window, observe that the adapter starts **Installing….**
15. After the installation completes, a **Congratulations! Your adapter has been installed correctly** notification appears; click **Next**.

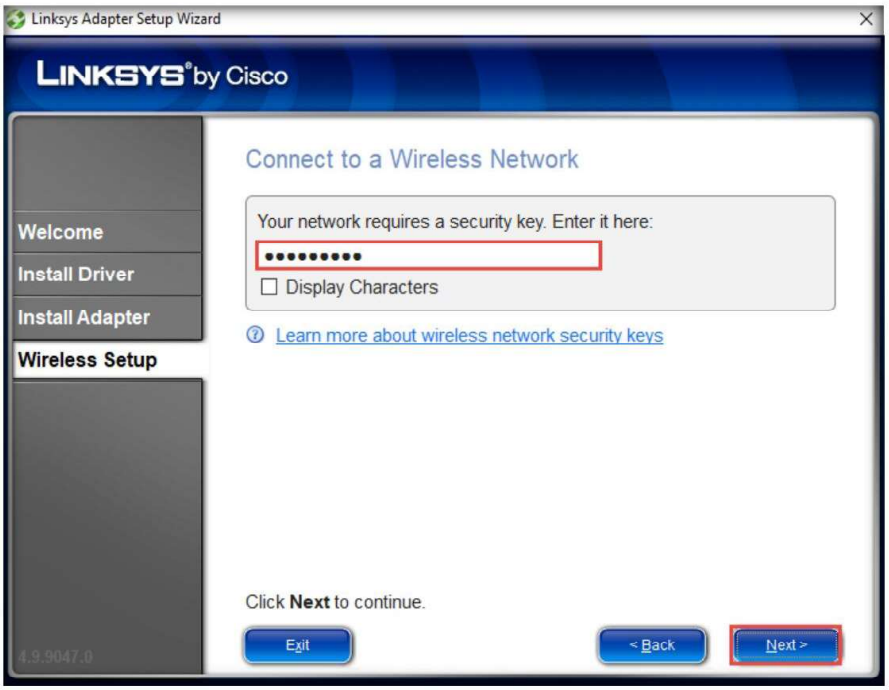


16. An **Installing Linksys Wireless Manager** wizard appears and installs the Linksys software. On completion, the **Connect to a Wireless Network** wizard appears and the adapter starts searching for available wireless networks.
17. The list of the available wireless network in range appears, as shown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

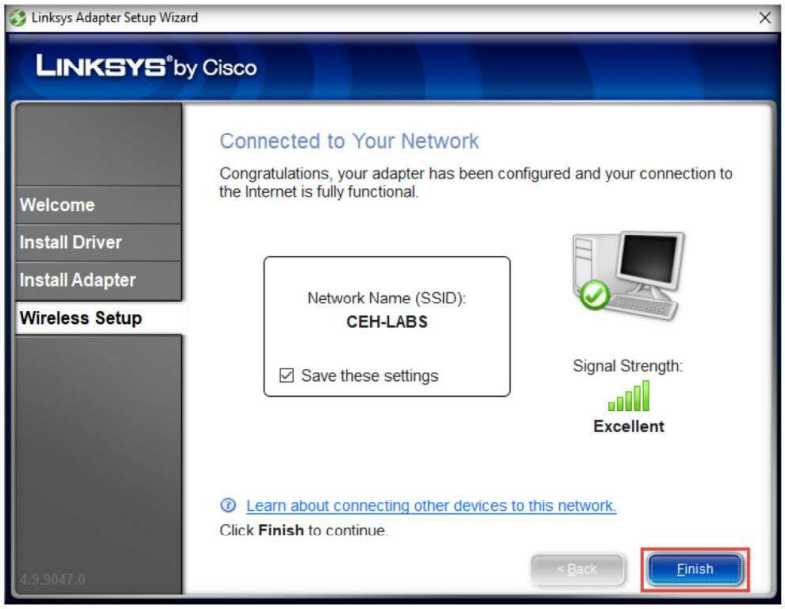
18. Select **CEH-LABS** and click the **Connect** button.

19. In the **Quickly Connect Using Push Button** wizard, click **Skip**.

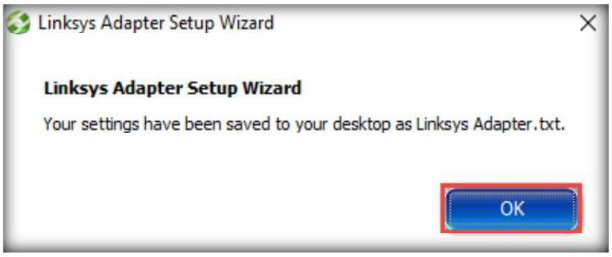
20. In the **Connect to a Wireless Network** wizard, type the password of wireless network **CEH-LABS** (in this example, **password1**) in the **Your network requires a security key. Enter it here:** field, and click **Next**.



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

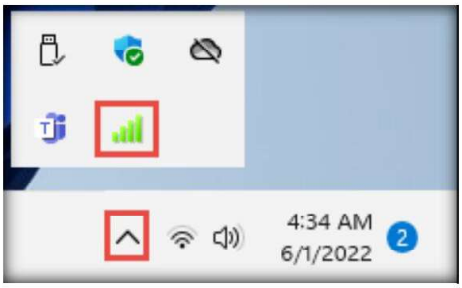


23. When the **Linksys Adapter Setup Wizard** notification appears, click **OK**.



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

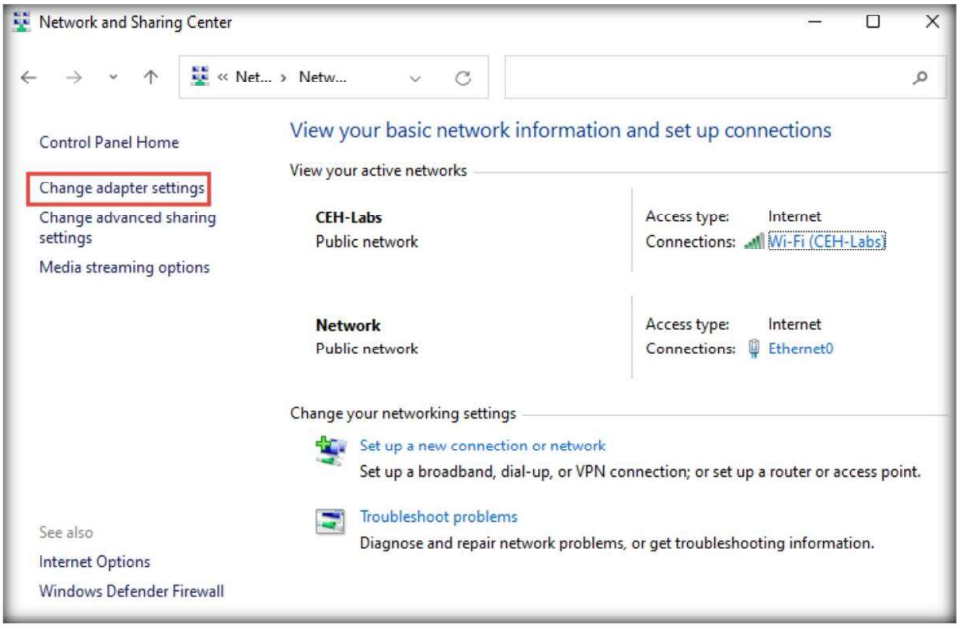
25. Close all windows and click **Show hidden icons** ( ) from the bottom-right corner of **Desktop**. You can observe the **Wireless Network Connection** icon ( ), as shown in the screenshot.
26. You can double-click the **Wireless Network Connection** icon ( ) to manage wireless network connections.



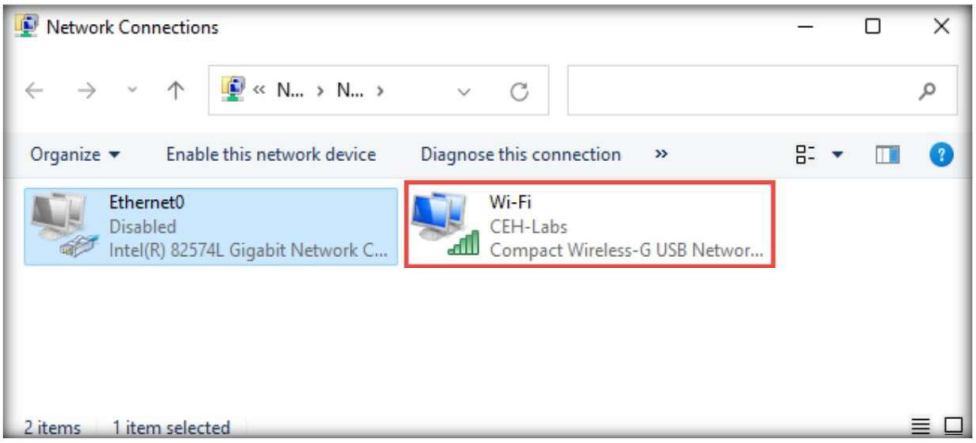
27. Your **Linksys 802.11 g WLAN** adapter has been configured successfully.
28. In this way, you can connect your virtual machines to a wireless network. Repeat these steps if you wish to connect to the wireless network with another virtual machine.

    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:
29. In the **Windows 11** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
30. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.



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



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

Lab Analysis

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

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

Lab 1

Footprint a Wireless Network

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

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 11 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\CEHv12 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

Lab Tasks

Task 1: Find Wi-Fi Networks in Range using NetSurveyor

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.

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

1. Turn on the **Windows 11** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

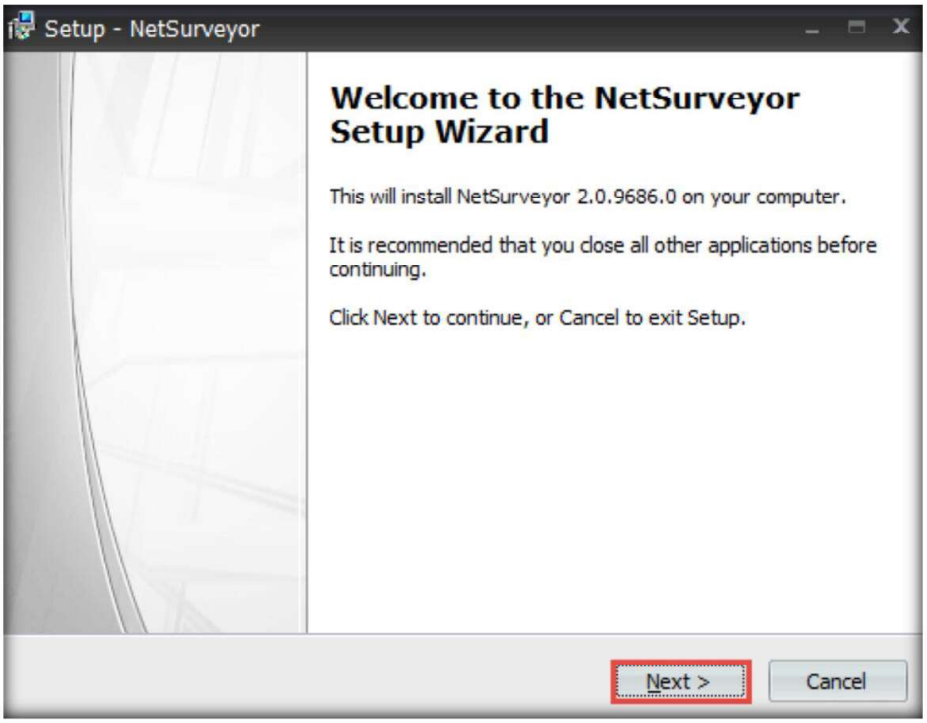
   Note: Ensure that the **Linksys 802.11 g WLAN** adapter is plugged in and connected to the **Windows 11** virtual machine.

   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 11**; click **OK**.

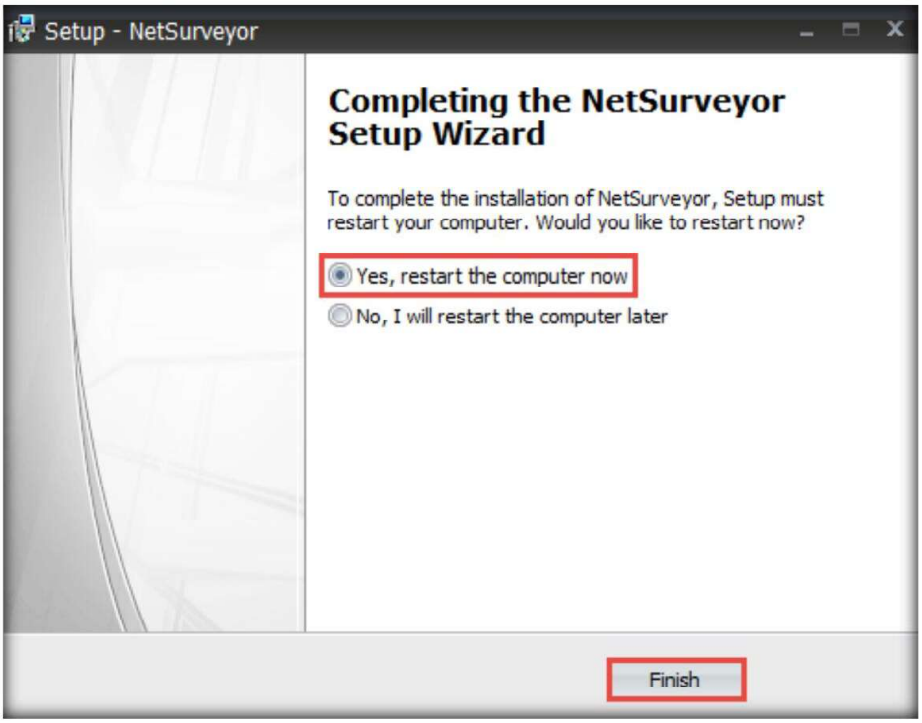
2. Navigate to **E:\CEH-Tools\CEHv12 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor** and double-click **NetSurveyor-Setup.exe**.

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

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



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**.



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 11** virtual machine.

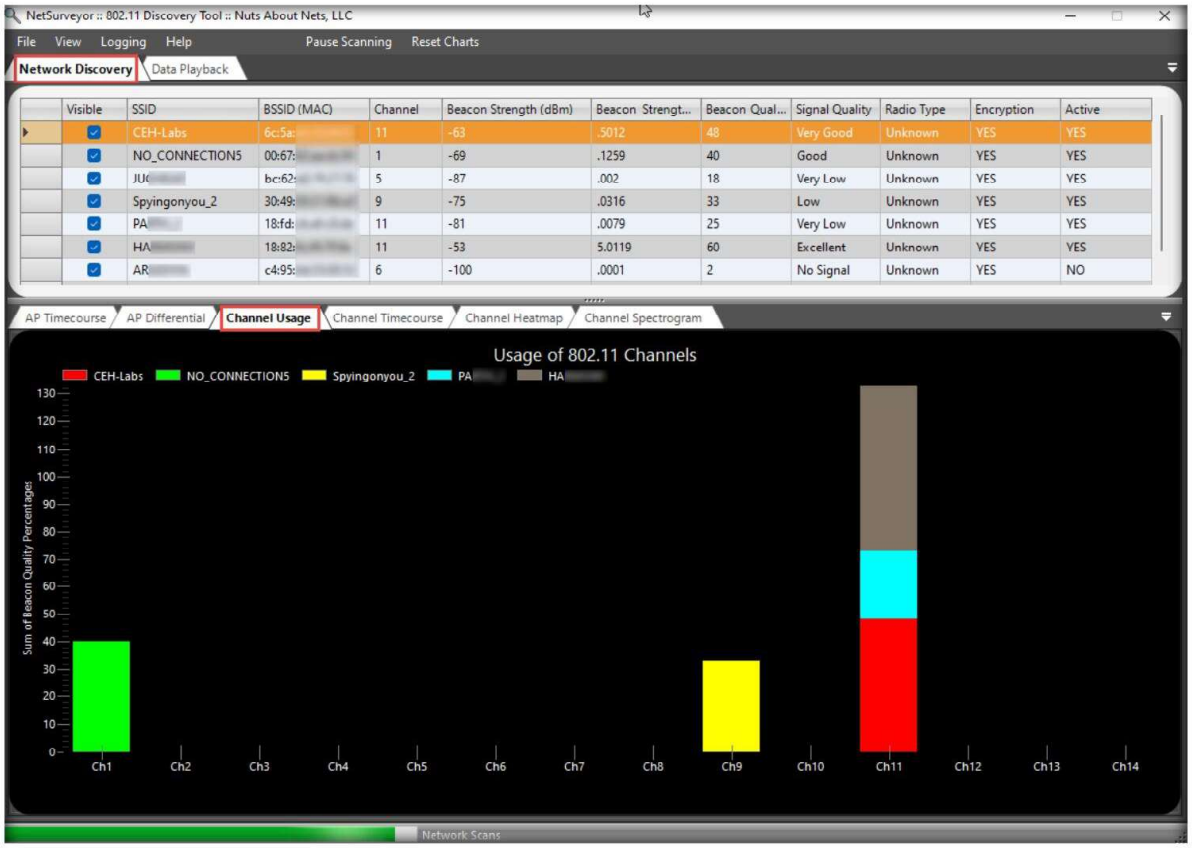
   If the adapter is not connected, unplug and plug it in again. A **New USB Device Detected** window appears, select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 11**; click **OK**.

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

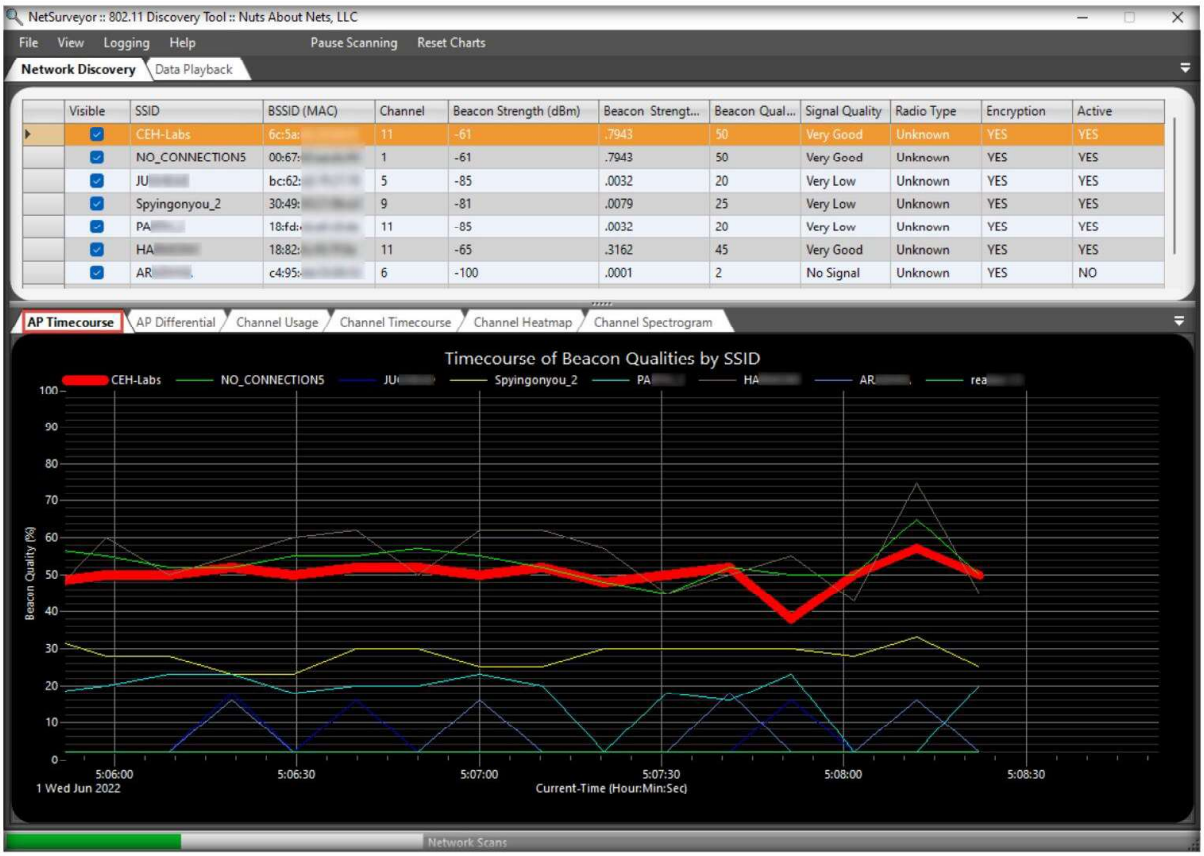
   Note: If a **User Account Control** pop-up appears, click **Yes**.

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.

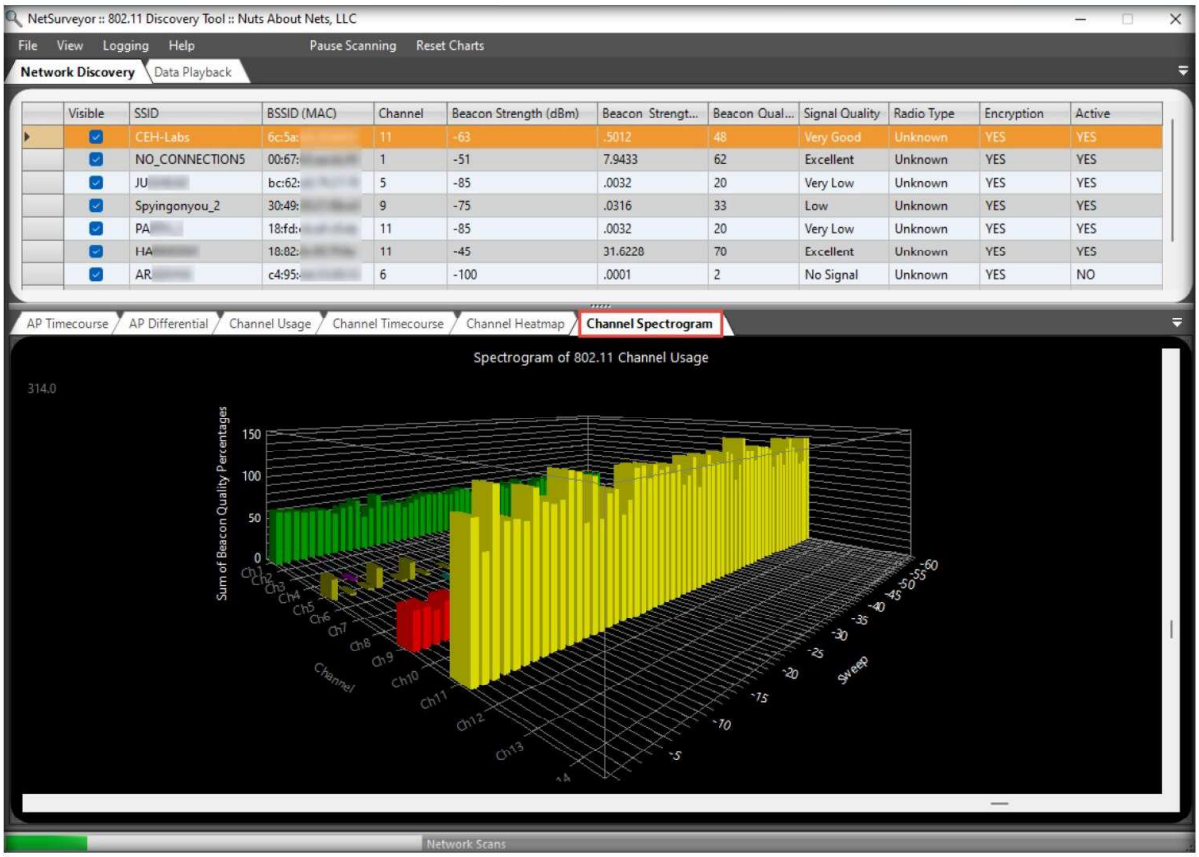
9. In the lower section of the window, the **Channel Usage** tab displays a graphical view of the usage of 802.11 channels by discovered access points.



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.

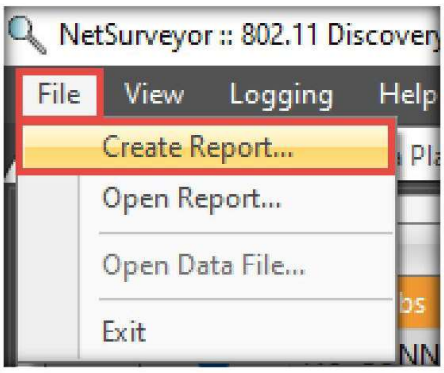


11. Click the **Channel Spectrogram** tab to view the spectrogram of the 802.11 channel usage. This information can be used to perform spectrum analysis, actively monitor spectrum usage in a particular area, and detect the spectrum signal of the target network.

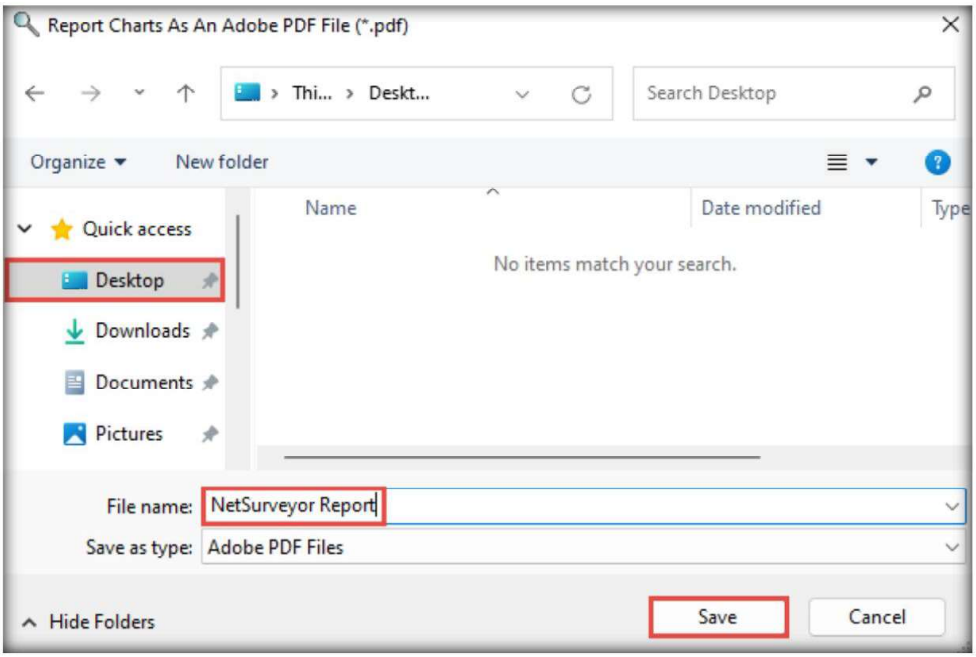


12. Similarly, you can gather detailed information about the discovered access points with other graphical diagnostic views by navigating to different tabs in the lower section. Information you can discover includes differential beacon qualities by SSID, the timecourse of 802.11 channel usage, and a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

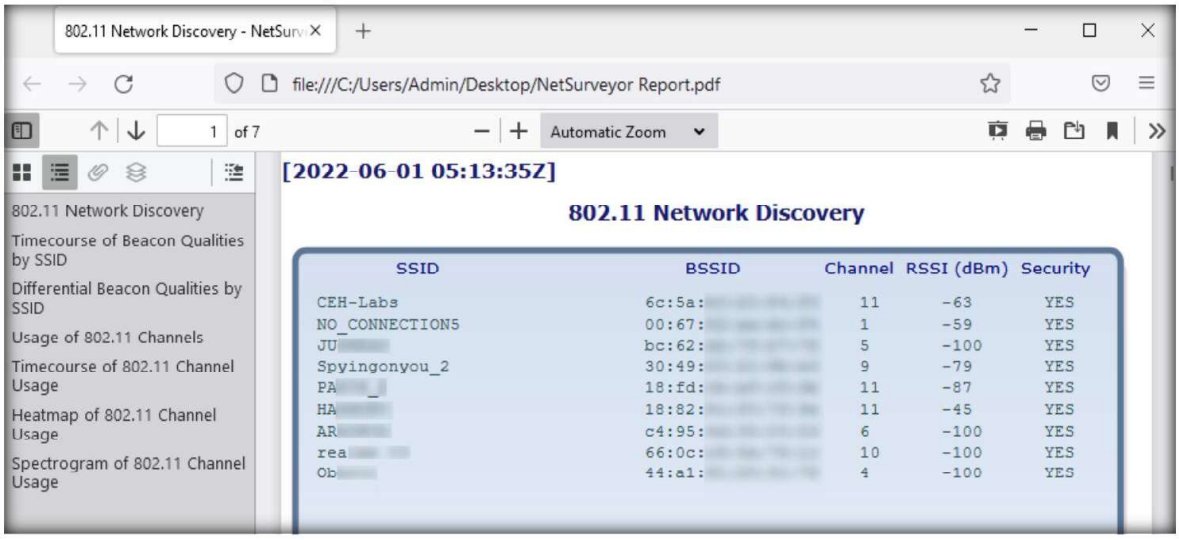
13. To save the gathered information in a report, click **File** from the menu bar and select Create **Report…** from the options.

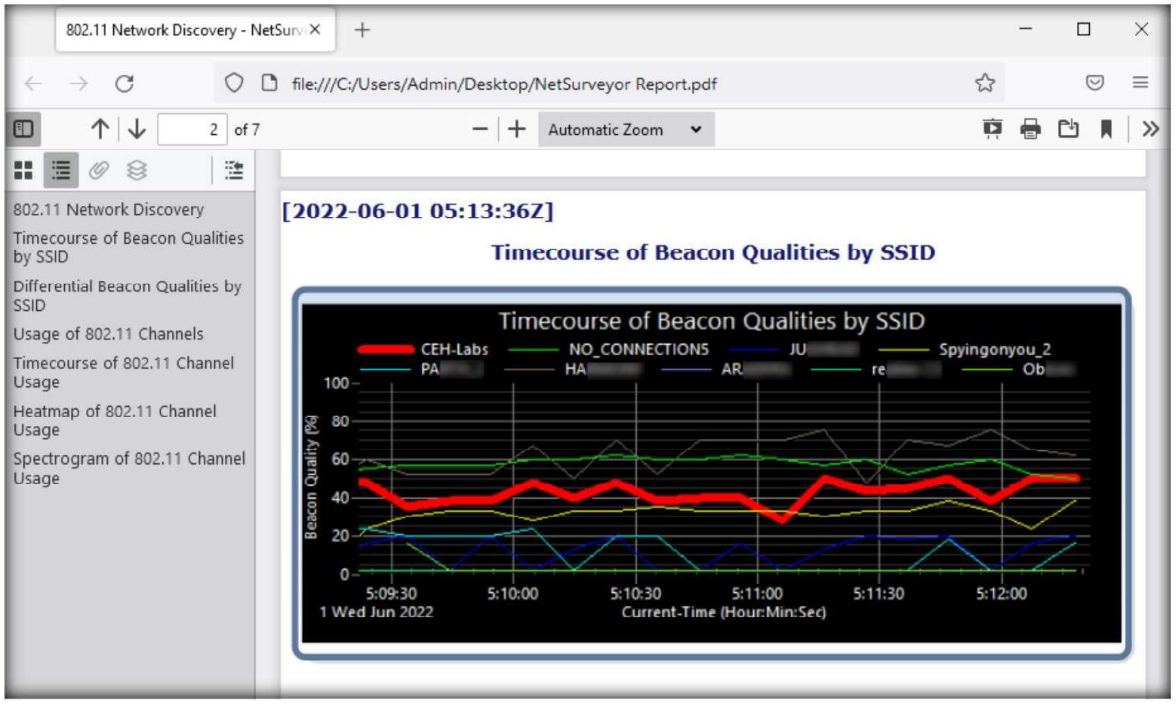


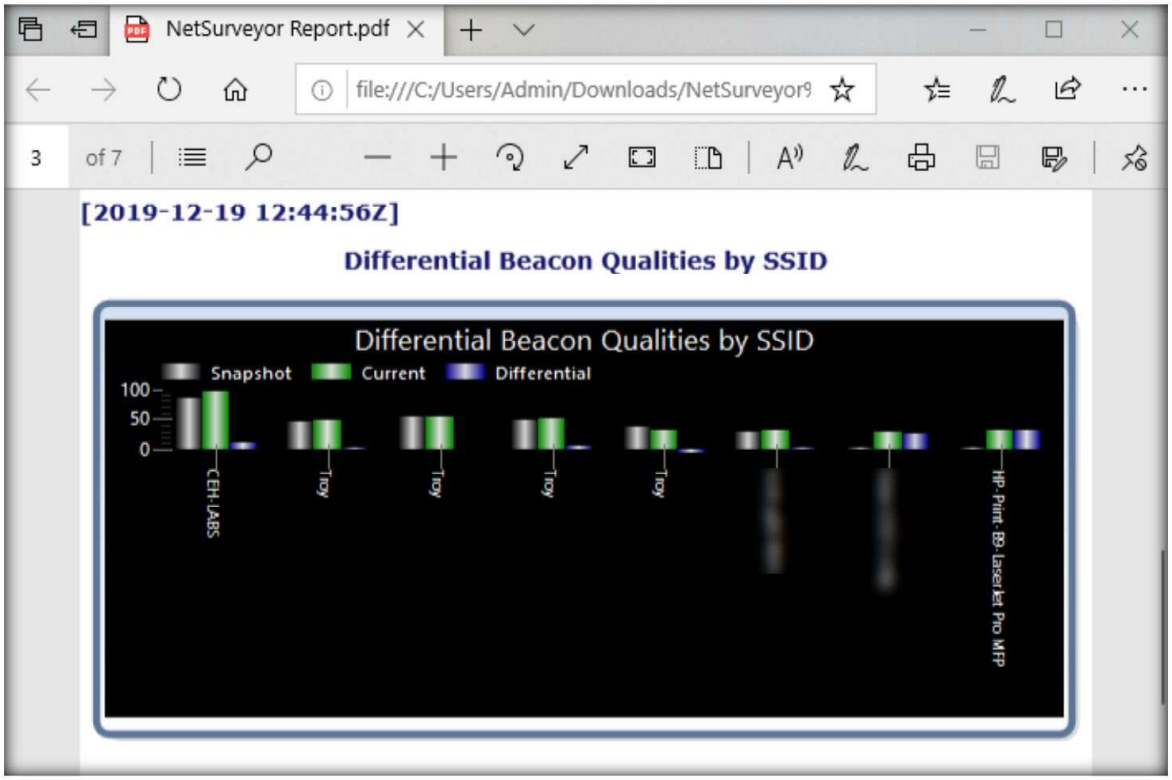
14. The **Report Charts As An Adobe PDF File (*.pdf)** window appears. Navigate to the location where you want to save the file (in this case, **Desktop**), ensure the **File name** is **NetSurveyor Report**, and click **Save**.



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.







17. This concludes the demonstration of how to find Wi-Fi networks in range using Wi-Fi discovery tools.
18. 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.

19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 11** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

Lab 2

Perform Wireless Traffic Analysis

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

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.

Lab Tasks

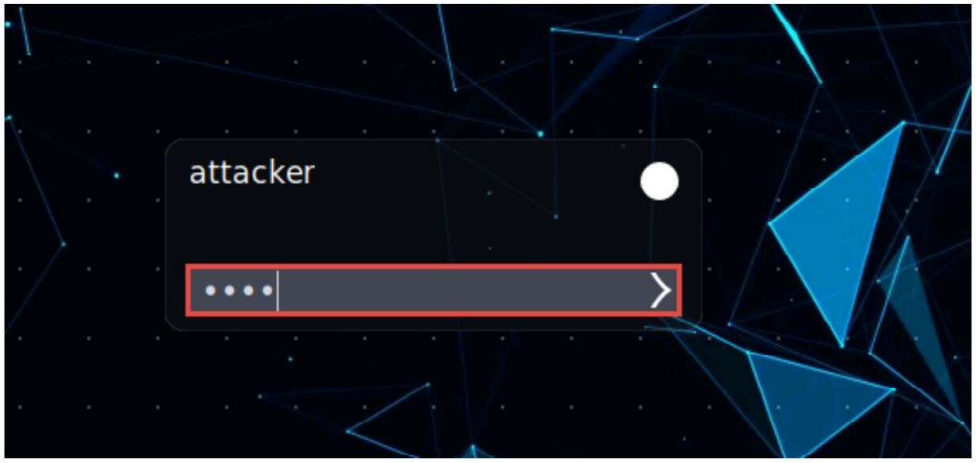
Task 1: Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark

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.

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.

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

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.

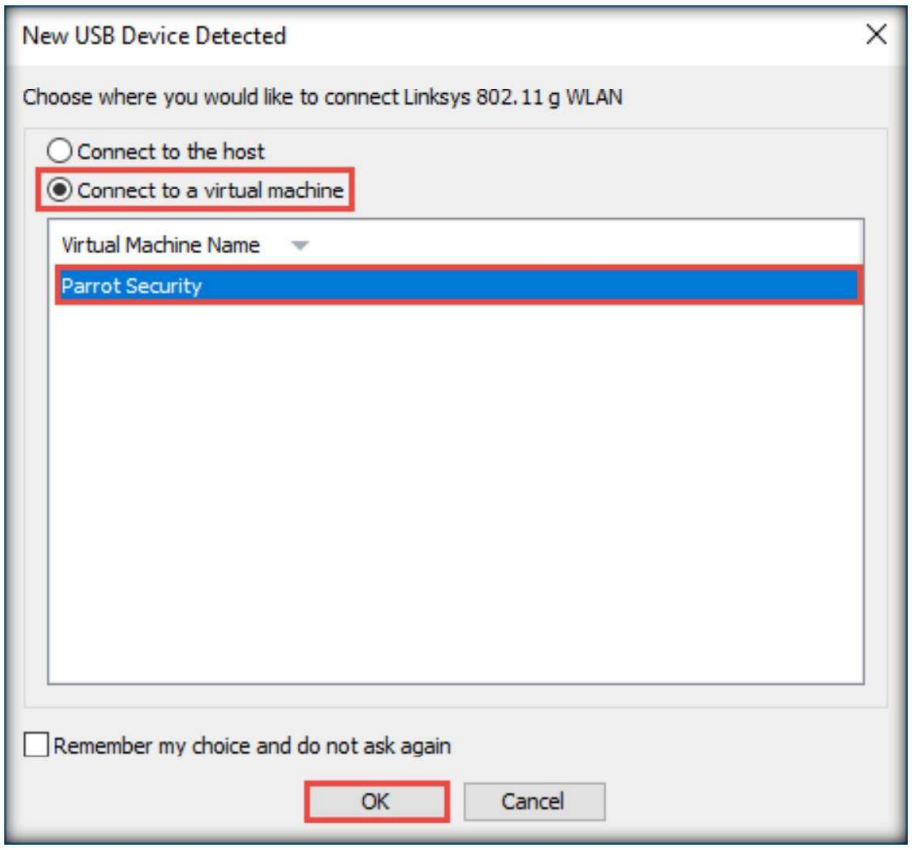


Note:

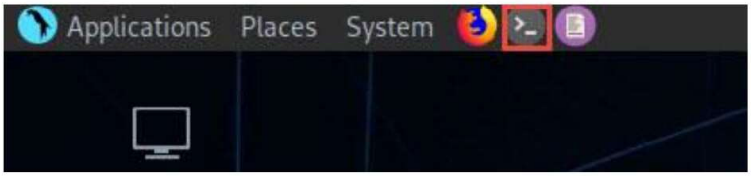
- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

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**.

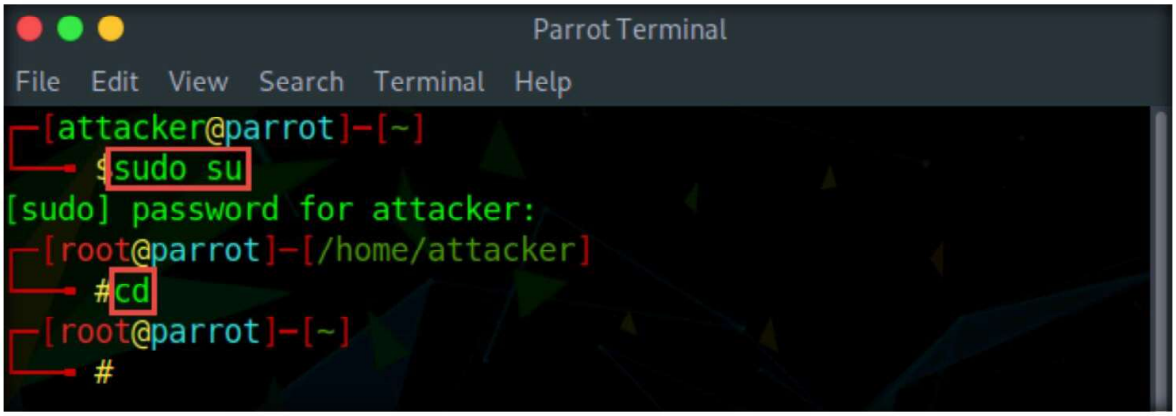


4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



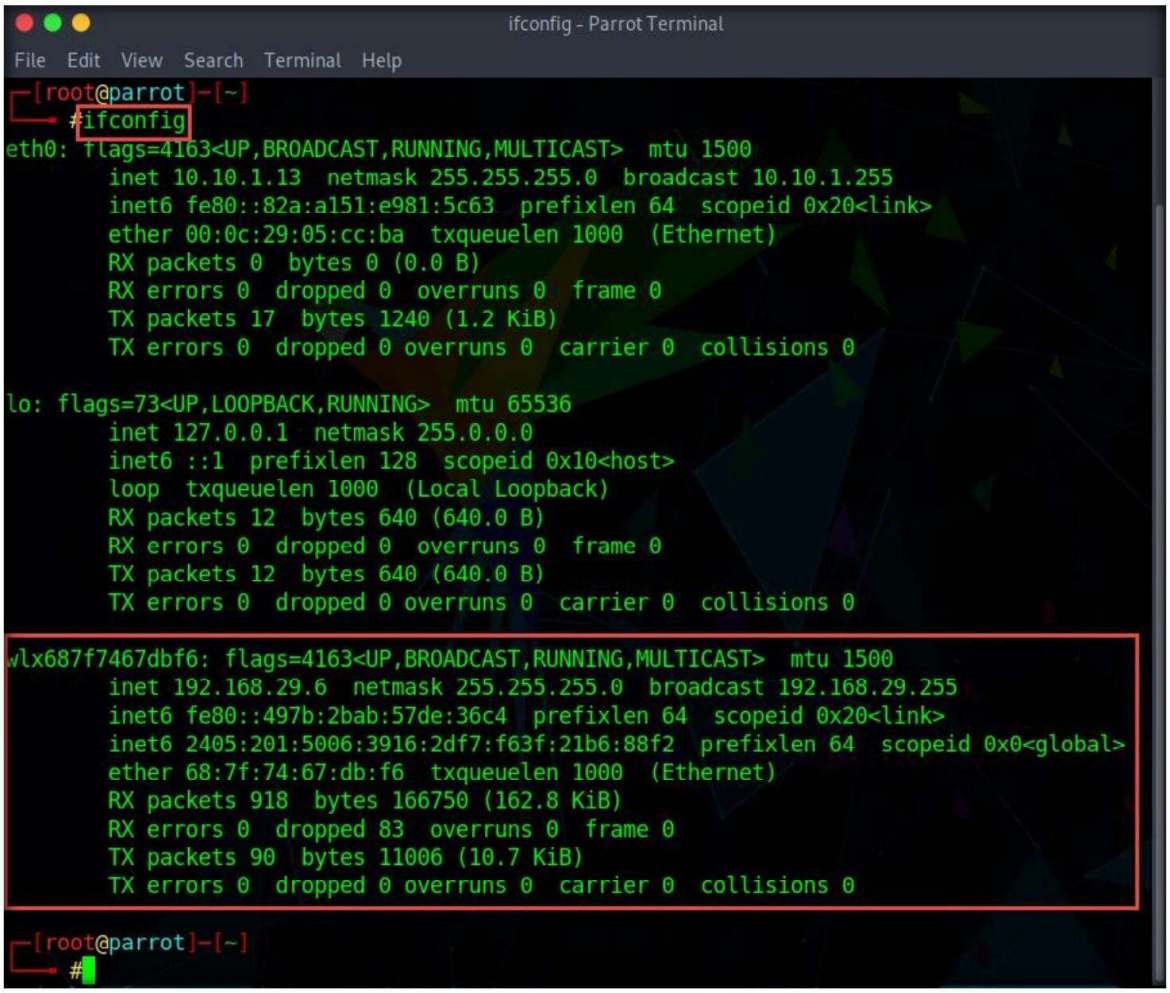
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

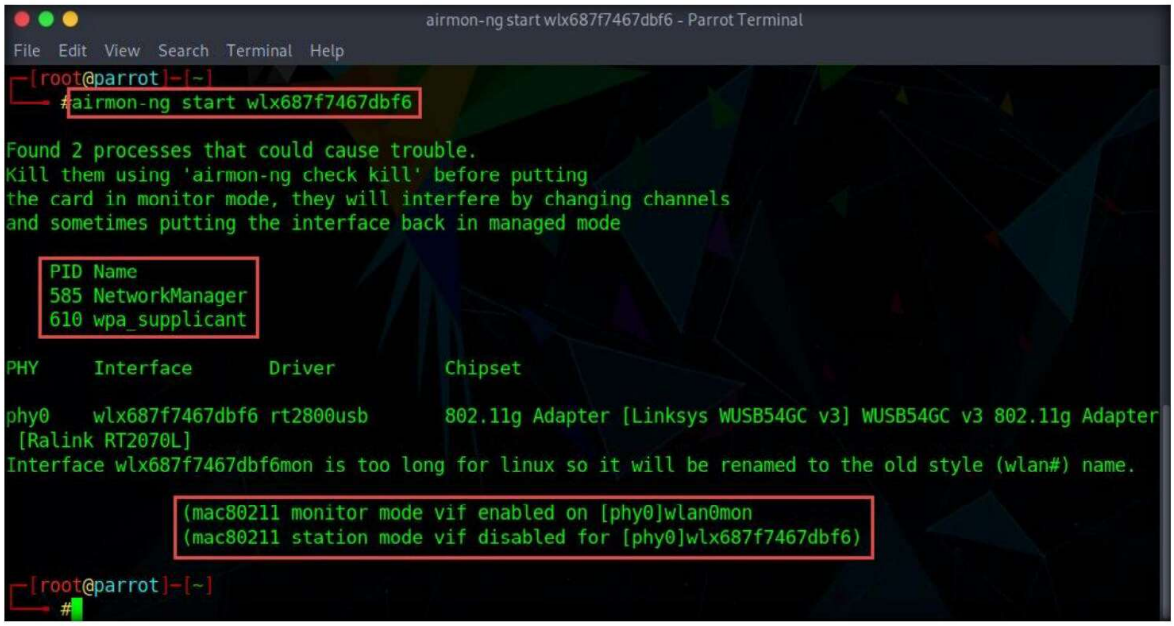


8. In the Parrot Terminal window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

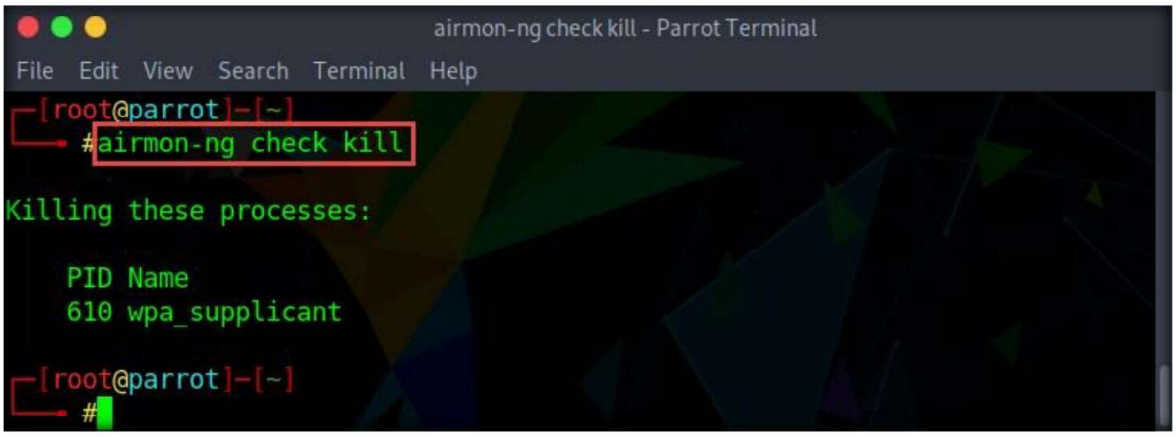
   Note: The name of wireless interface might vary in your lab environment.



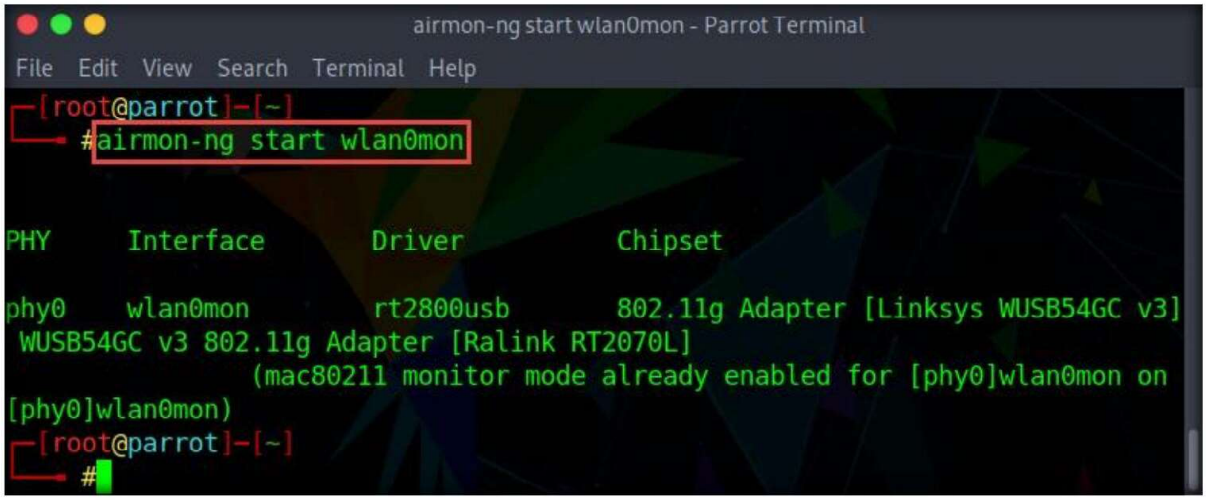
9. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface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



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



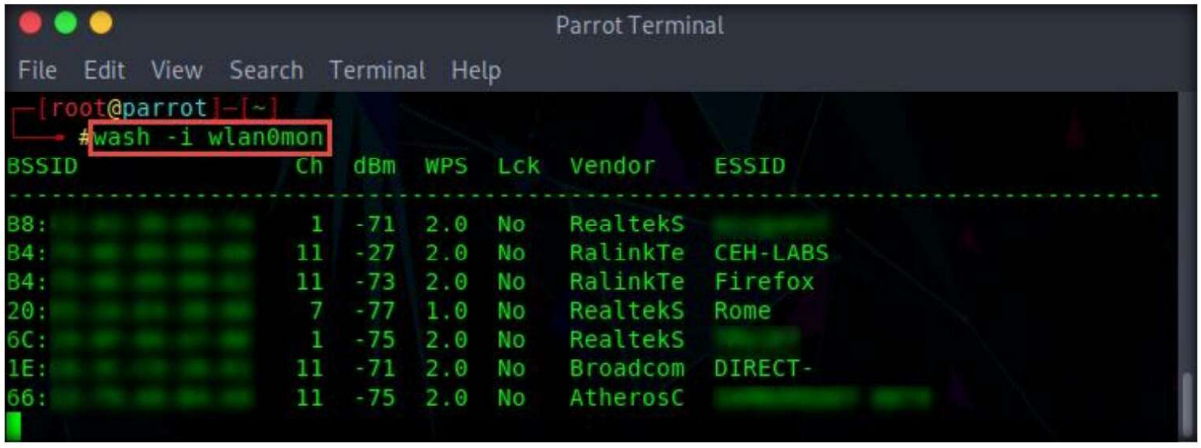
13. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
14. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.



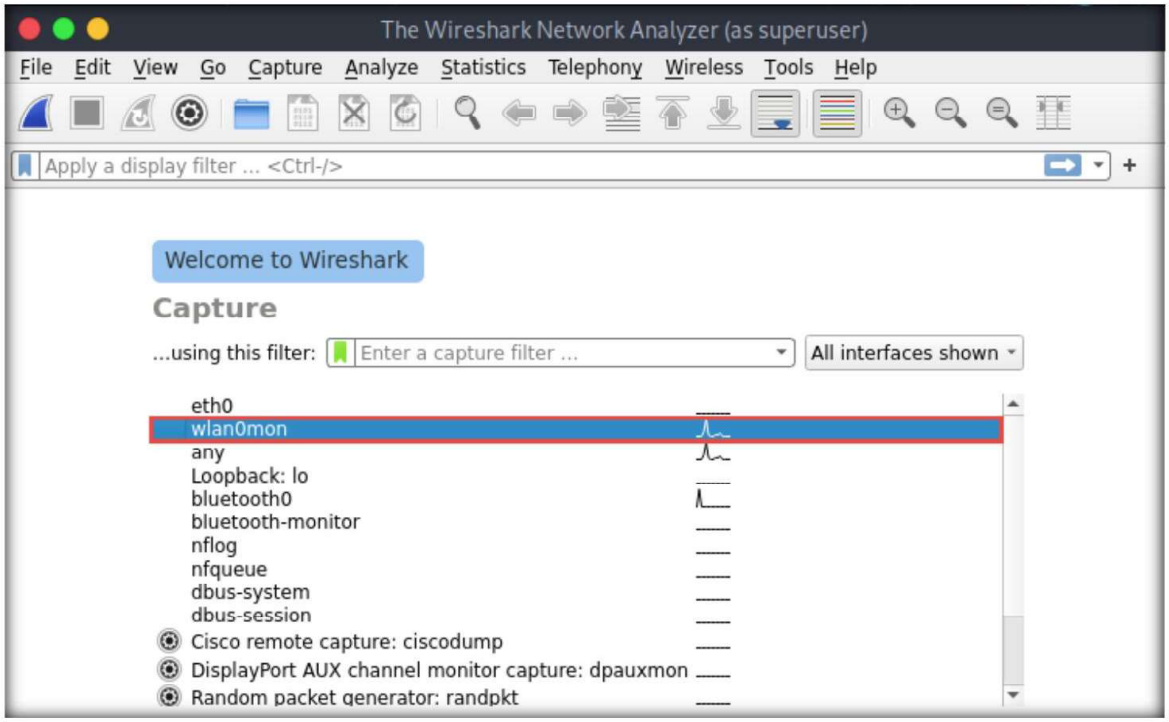
15. Now, we shall find Wi-Fi networks (access points) by using the wireless interface **wlan0mon**.
16. Type **wash -i wlan0mon** and press **Enter** to detect WPS-enabled devices.

    Note: The command **-i**, **--interface=<iface>** specifies the interface to capture the packets.
17. The results appear, displaying the discovered Wi-Fi access points, as shown in the screenshot.

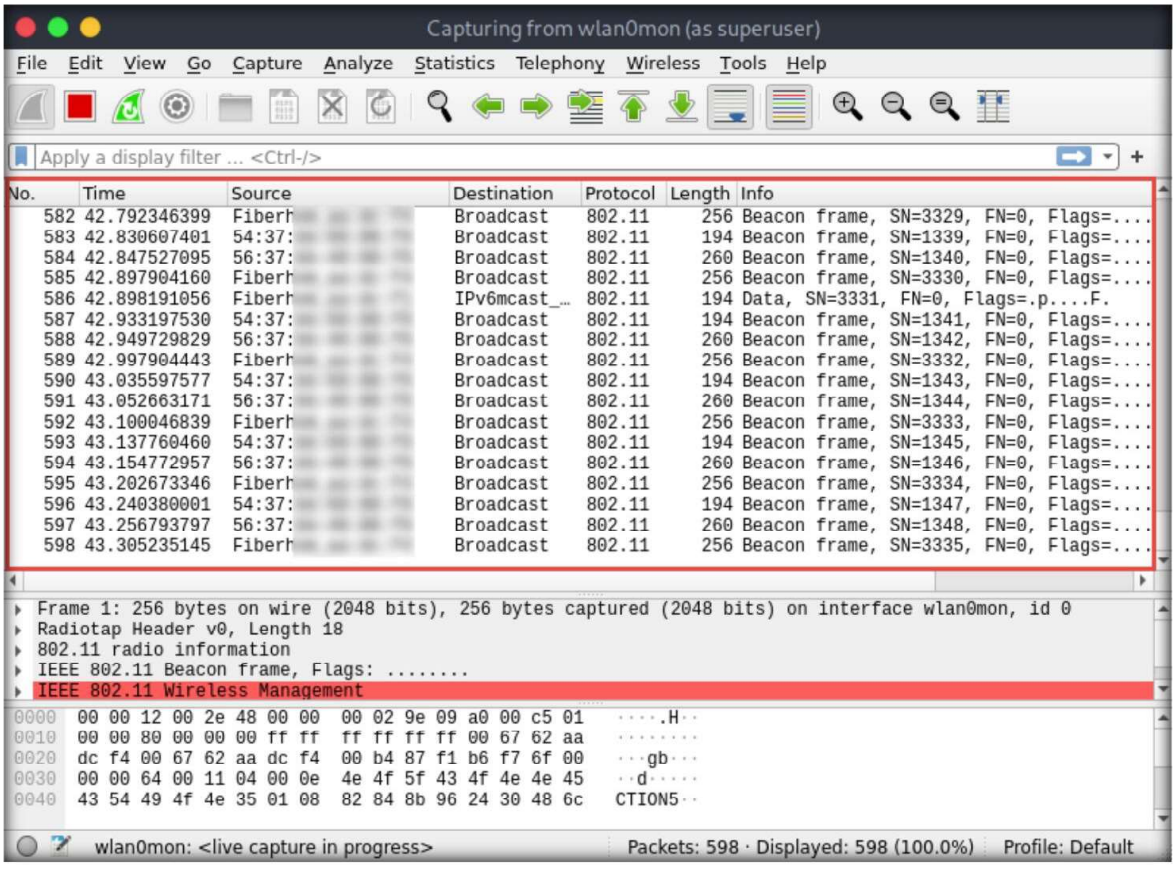
    Note: If no results appear, restart the **Parrot Security** virtual machine and perform **Steps 1 - 8**, type **wash -i wlan0mon** in the **Terminal** window, and press **Enter**.



18. Now, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
19. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
20. The **Wireshark Network Analyzer** window appears; double-click the wireless network interface (in this case, **wlan0mon**) to start capturing network traffic.



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



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.

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

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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.

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

Lab Environment

To carry out this lab, you need:

- Windows 11 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: 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

Lab Tasks

Task 1: Crack a WEP network using Aircrack-ng

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.

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

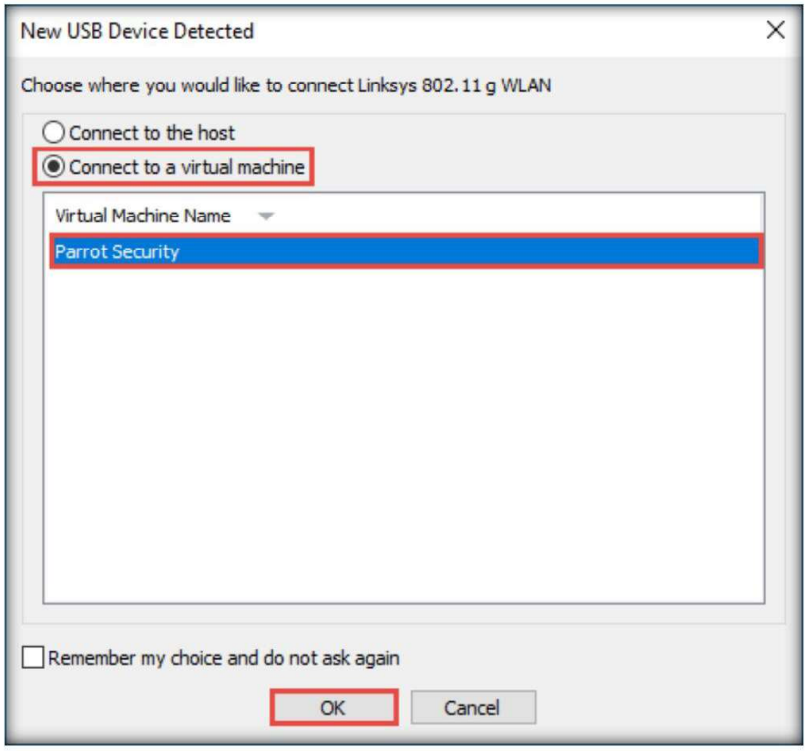
Note: Before starting this task, configure the target access point (**CEH-LABS**) with WEP encryption and a hidden SSID.

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

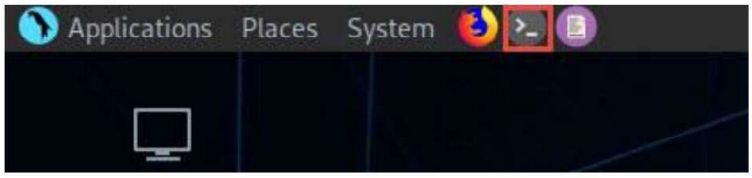
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   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**.

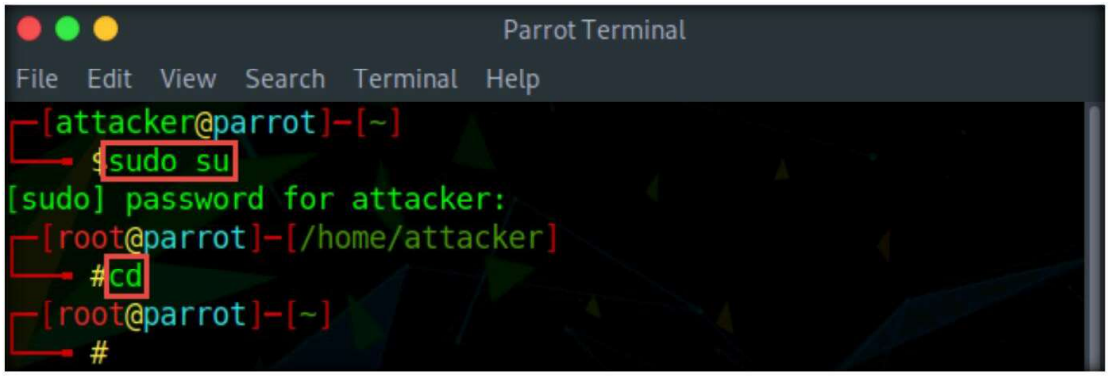


5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



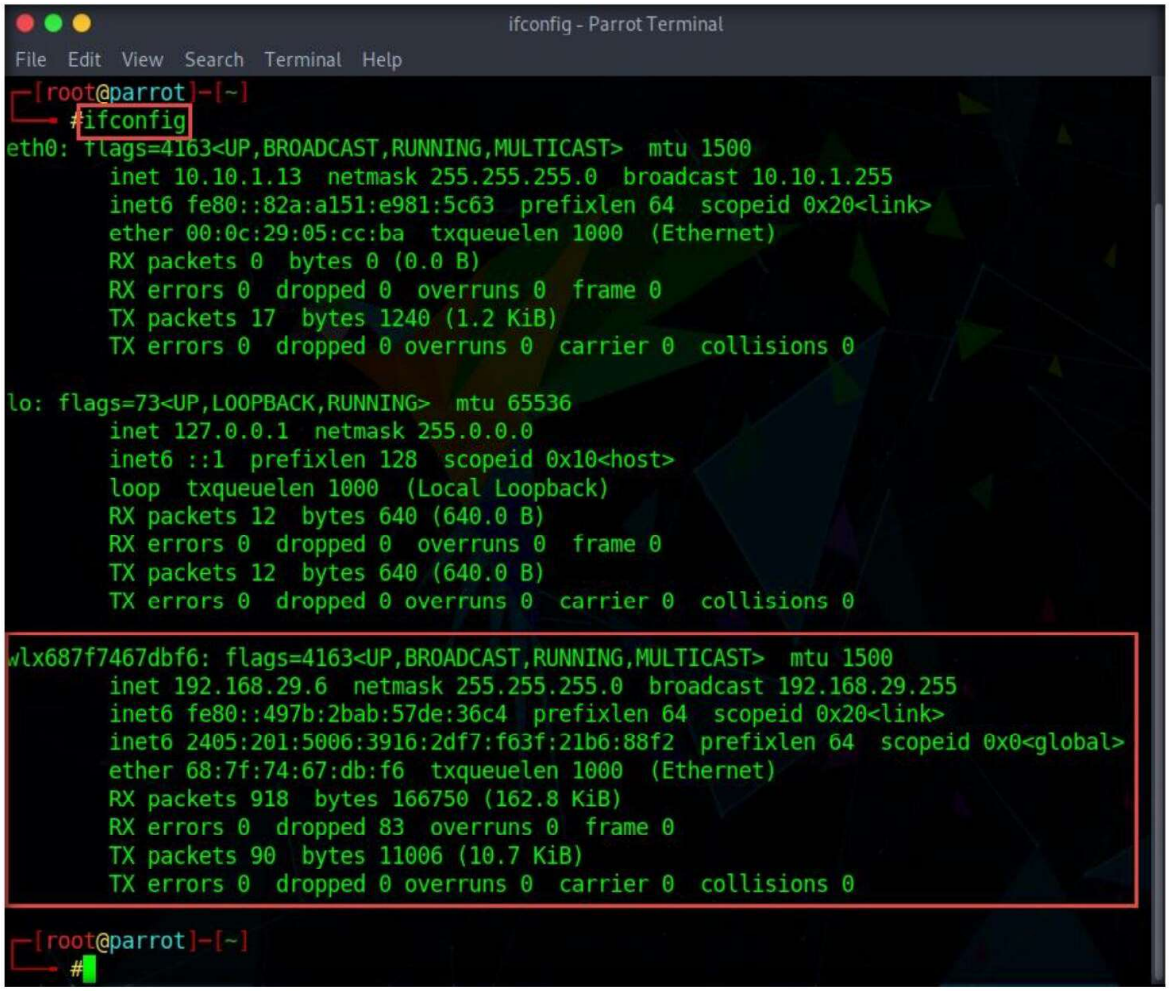
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

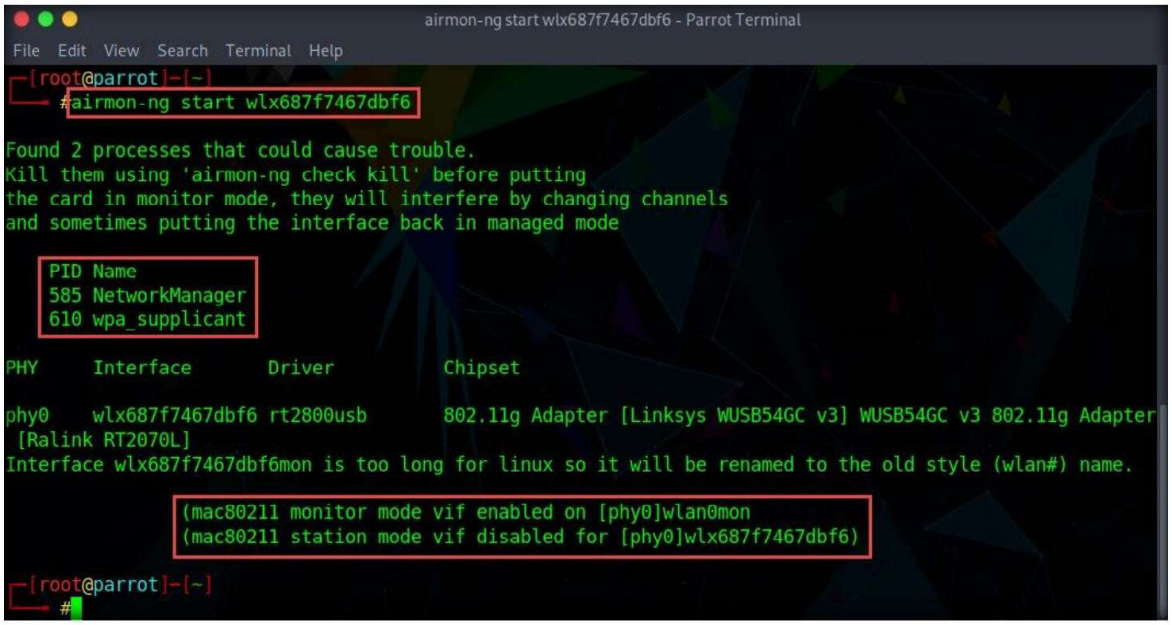


9. In the **Parrot Terminal** window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

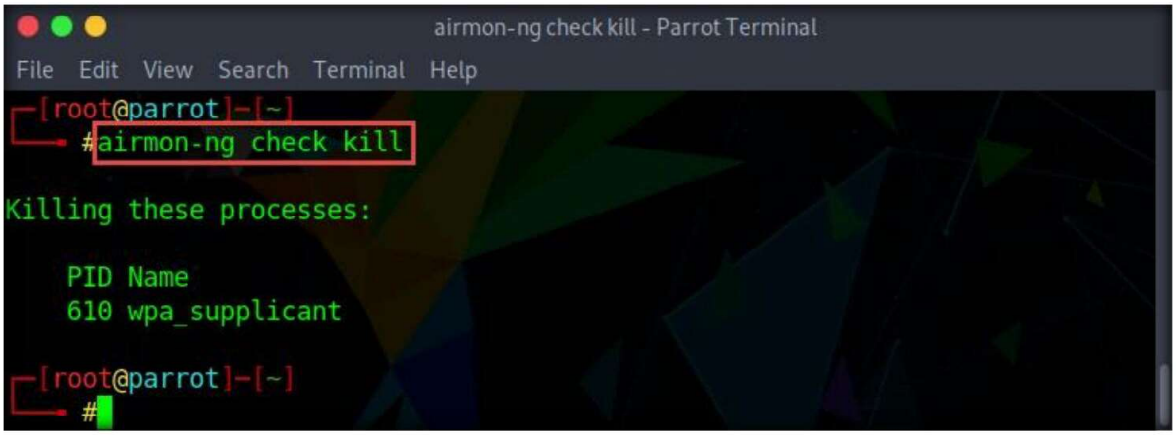
   Note: The name of wireless interface might vary in your lab environment.



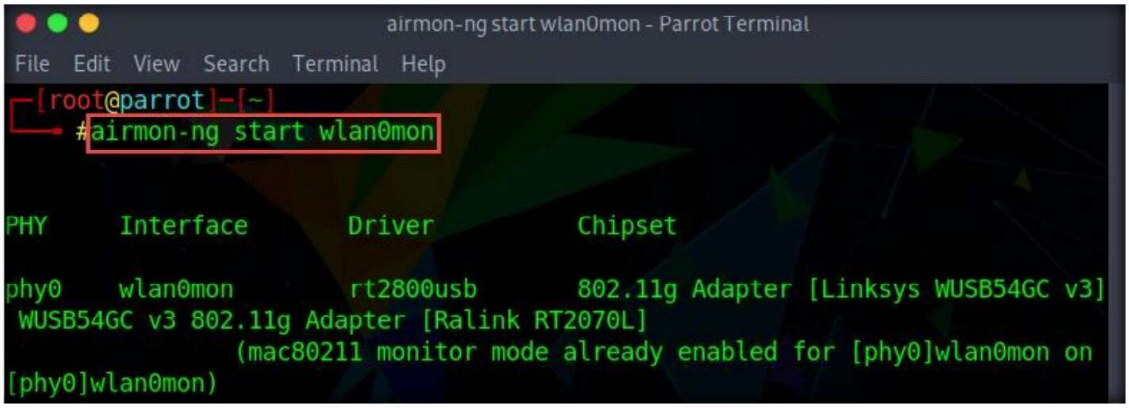
10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface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



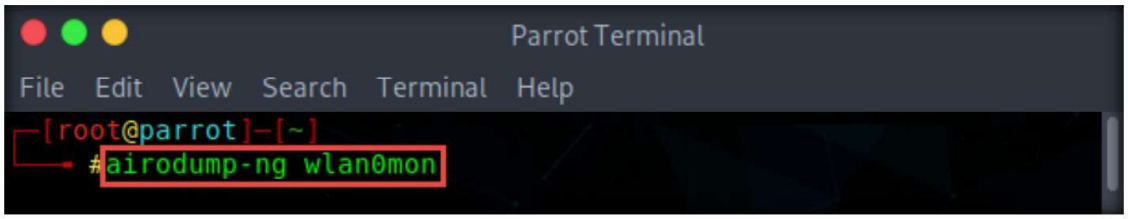
13. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



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



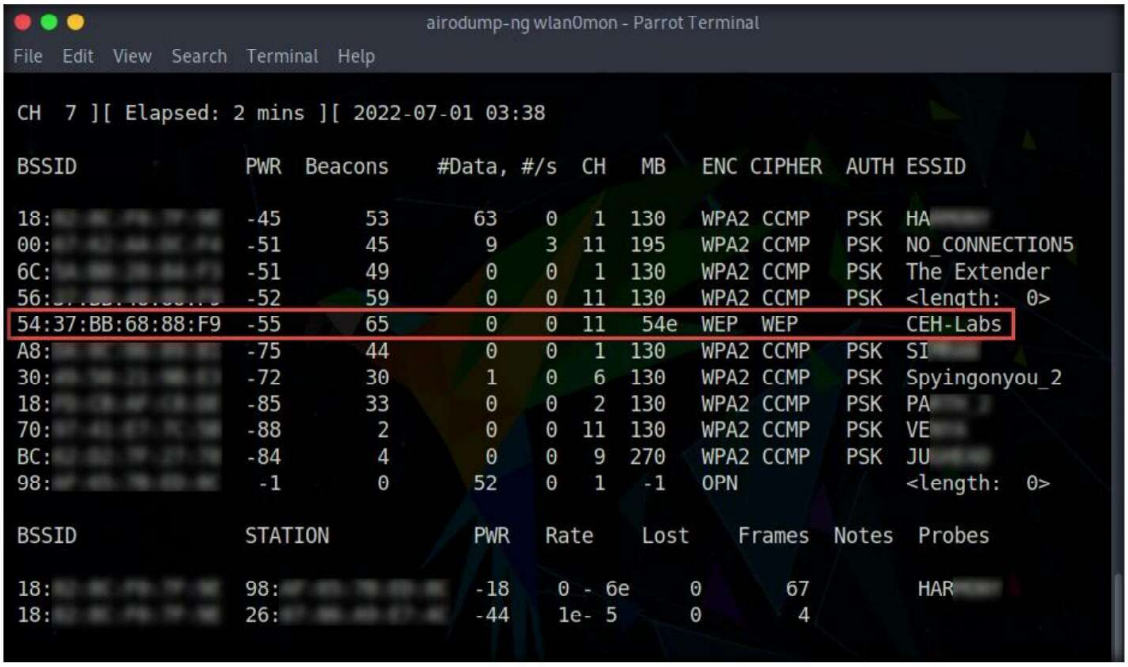
16. Type **airodump-ng wlan0mon** and press **Enter**. This command requests a list of detected access points, and connected clients ("stations").



17. The result appears, displaying the available access points. Note the hidden ESSID associated with BSSID: **54:37:BB:68:88:F9**.

    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.

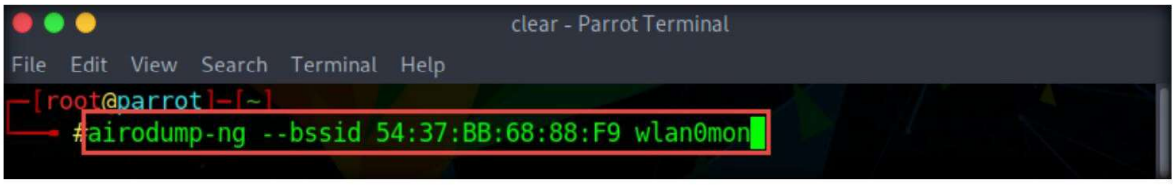


18. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
19. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and **press** Enter to run the programs as a root user.
20. In the **[sudo] password for attacker** 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.
22. In the terminal window, type **airodump-ng --bssid 54:37:BB:68:88:F9 wlan0mon** and press **Enter**.

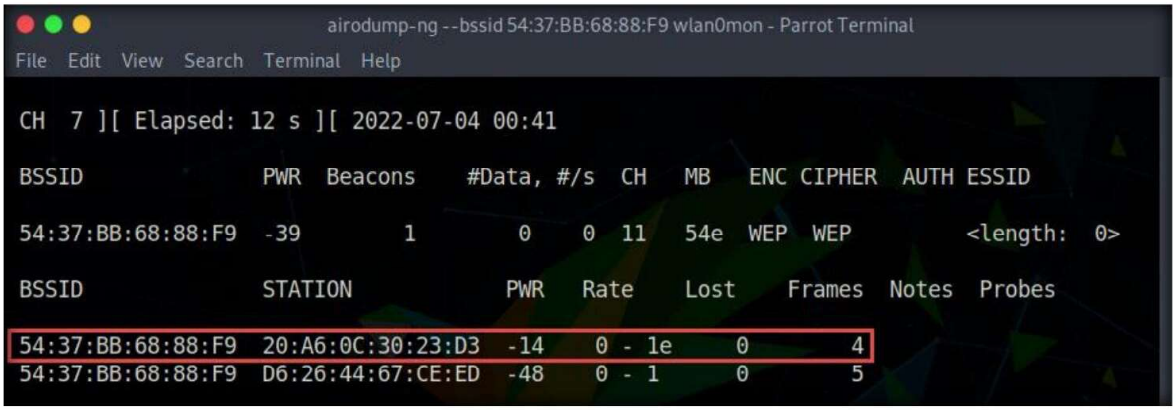
    Note: In this command,

    - **--bssid**: MAC address of the target access point (in this example, **54:37:BB:68:88:F9**).
    - **wlan0mon**: Wireless interface



23. Airodump-ng starts capturing the Initialization Vector (IV) from the target AP, as shown in the screenshot.
24. The list of connected clients ("stations") appears. You can observe that there are two clients connected to the target access point (**54:37:BB:68:88:F9**). 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.



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

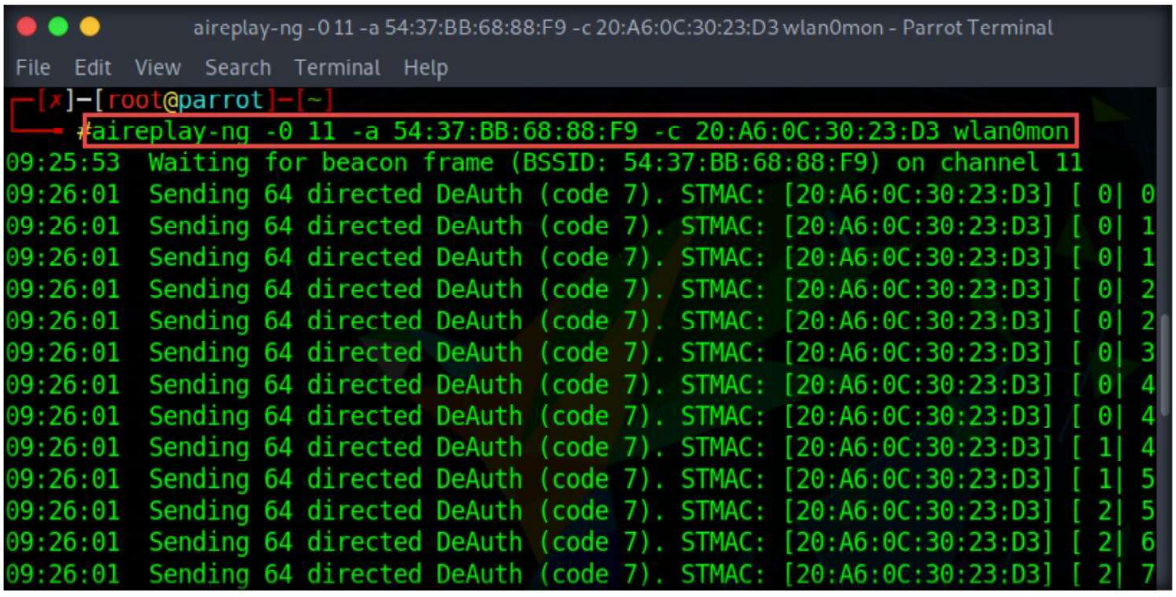
26. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
27. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
28. Now, type **cd** and press **Enter** to jump to the root directory.
29. In the new terminal window, type **aireplay-ng -0 11 -a 54:37:BB:68:88:F9 -c 20:A6:0C:30:23:D3 wlan0mon** and press **Enter** to generate de-authentication packets.

    Note: In this command,

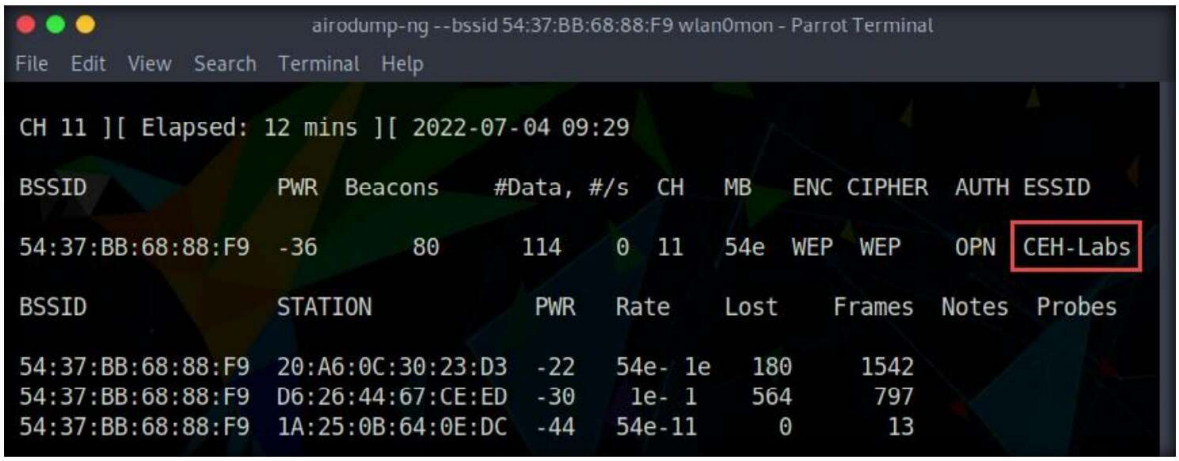
    - **-0**: Activates deauthentication mode
    - **11**: Number of deauthentication packets to be sent
    - **-a**: Sets the access point MAC address
    - **-c**: Sets the destination MAC address
    - **wlan0mon**: Wireless interface

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



30. 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.

31. Switch back to the terminal window where airodump-ng is running. You will observe that the hidden SSID associated with **BSSID 54:37:BB:68:88:F9** appears under ESSID as **CEH-LABS**, as shown in the screenshot.



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.

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

Task 2: Crack a WEP Network using Wifiphisher

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. 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.

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.

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 iPhone). 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.

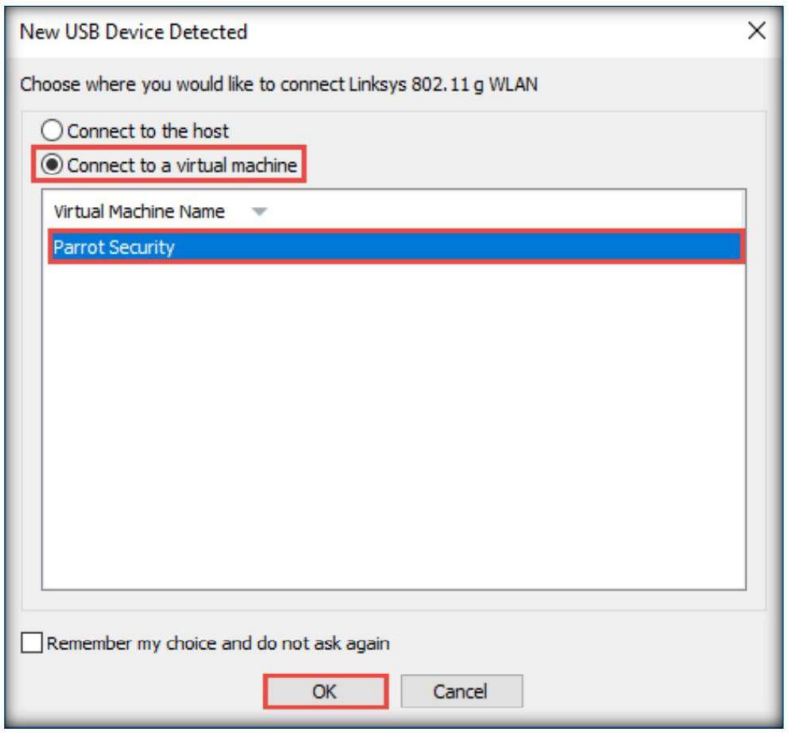
1. Turn on the **Parrot Security** virtual machine.

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.

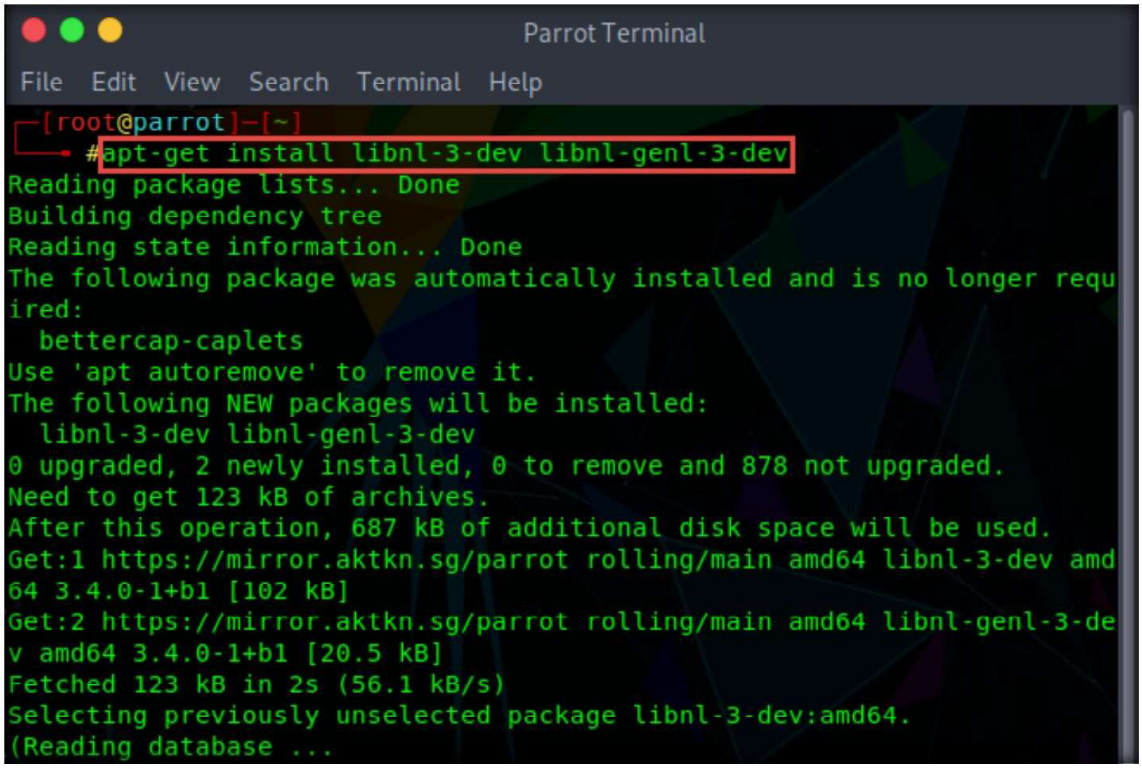
3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



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

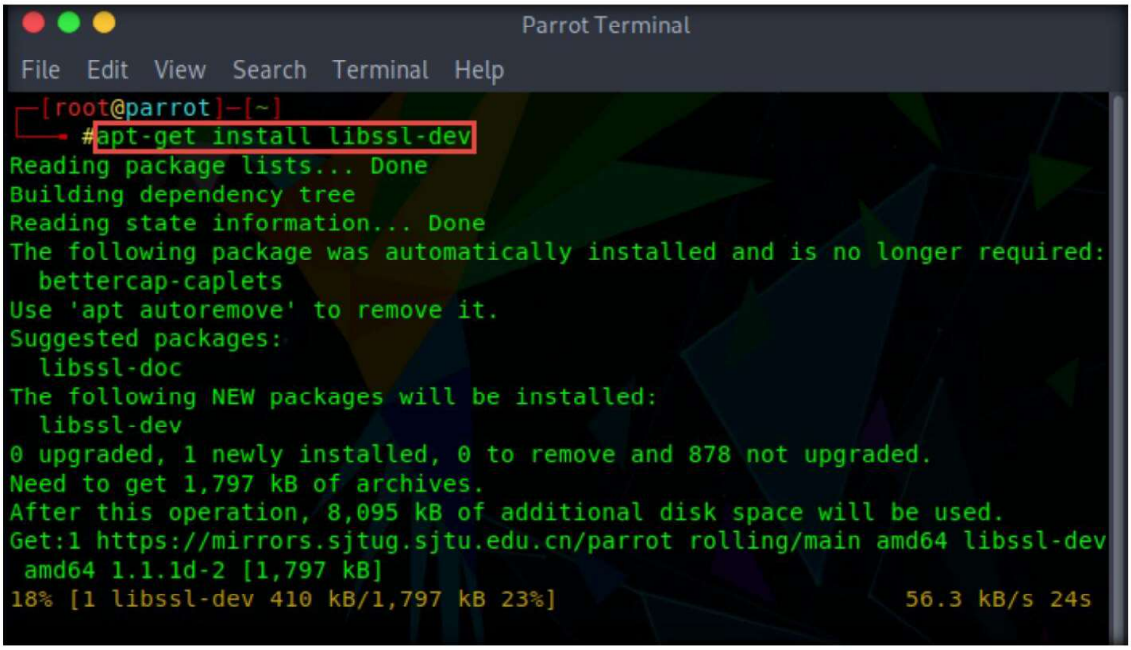
   Note: The password that you type will not be visible.

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



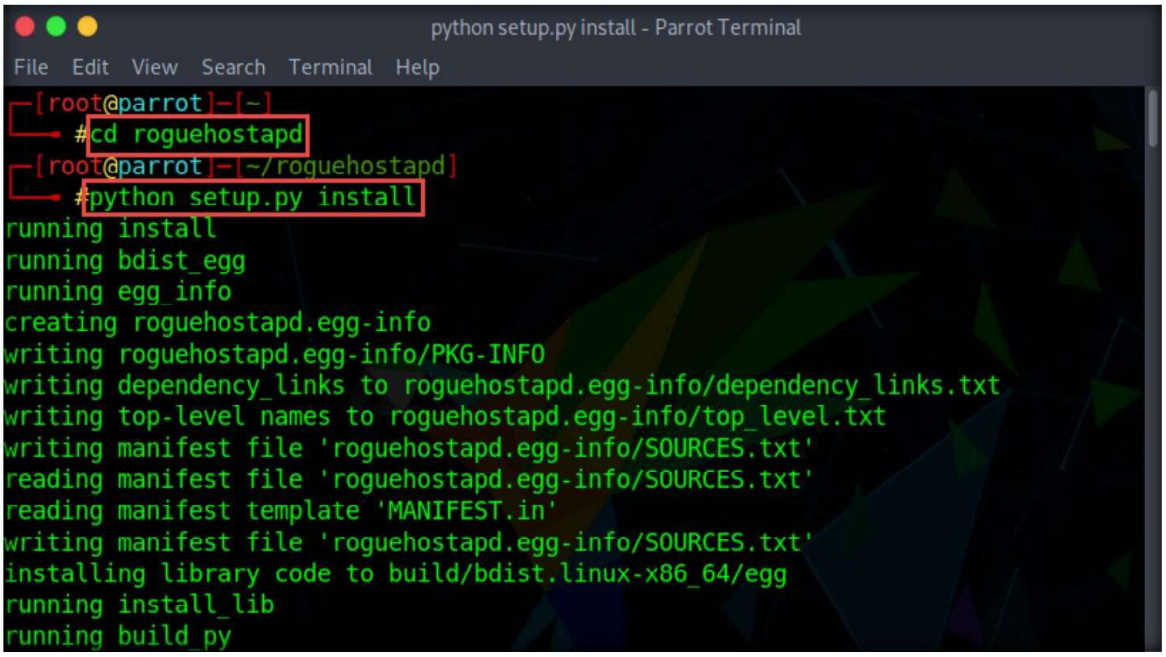
10. Once the installation has finished, type **apt-get install libssl-dev** in the terminal window and press **Enter** to install the **libssl-dev** dependency.

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

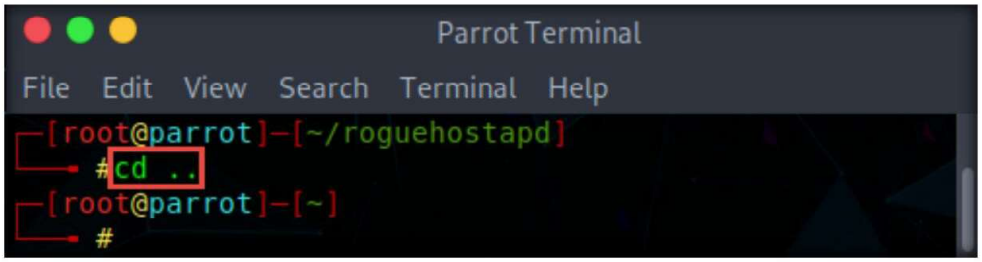


11. Once the update is complete, type **cd roguehostapd** and press **Enter** to navigate to the cloned repository.
12. Now, type **python setup.py** install and press **Enter** to install the roguehostapd application.

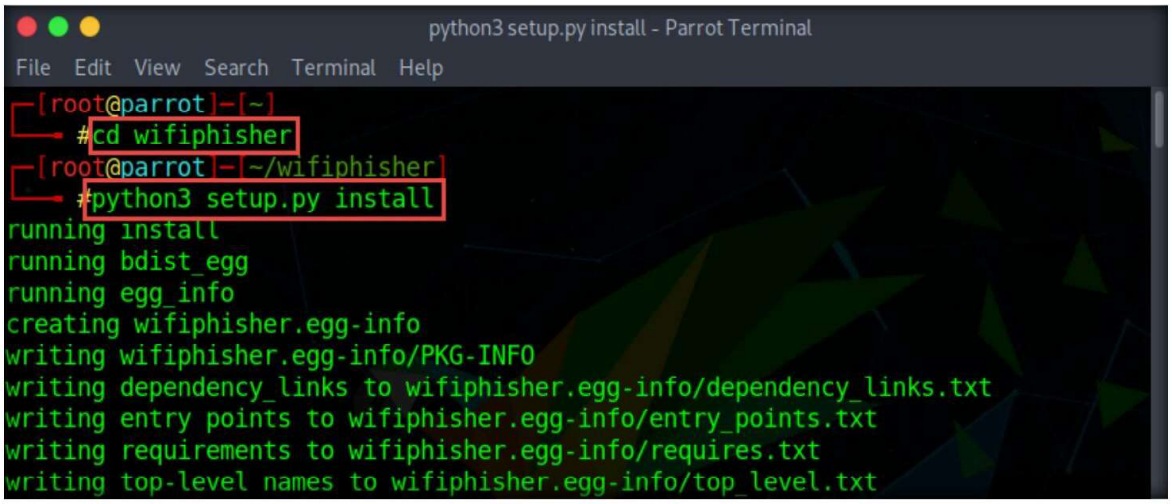
    Note: Roguehostapd is a fork of hostapd, the famous user space software access point. It provides Python ctypes bindings and a number of additional attack features. It was primarily developed for use in the Wifiphisher project.



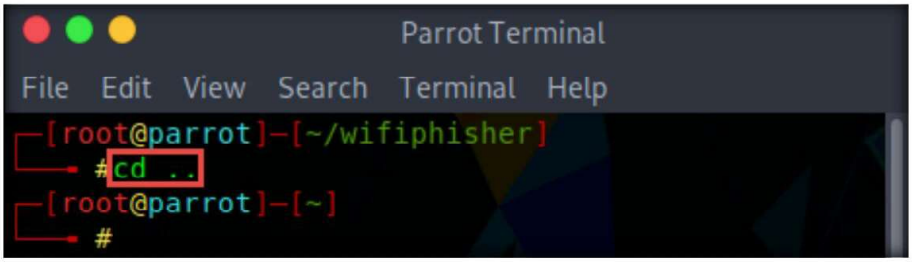
13. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the root directory.



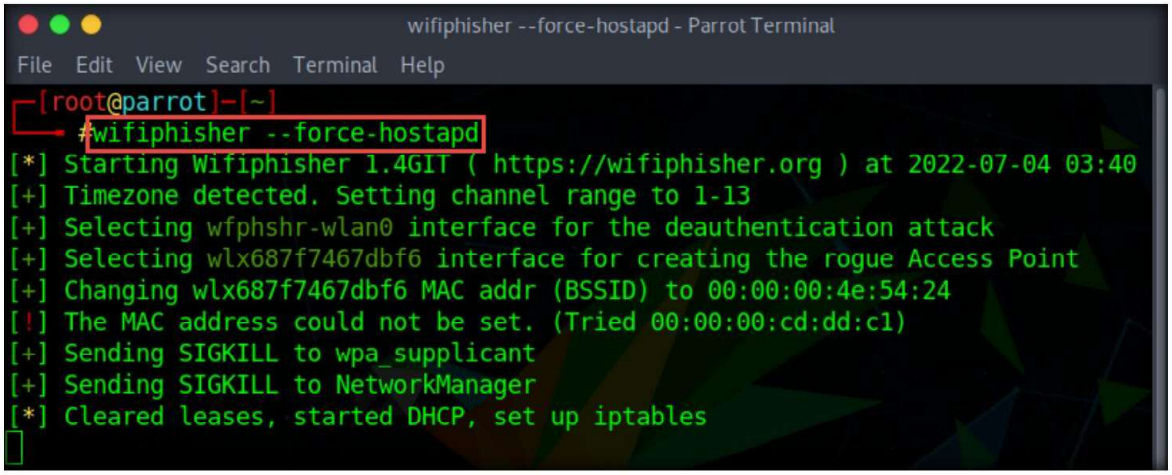
14. Now, type **cd wifiphisher** and press **Enter** to navigate to the Wifiphisher repository.
15. Type **python3 setup.py** install and press **Enter** to install Wifiphisher.



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

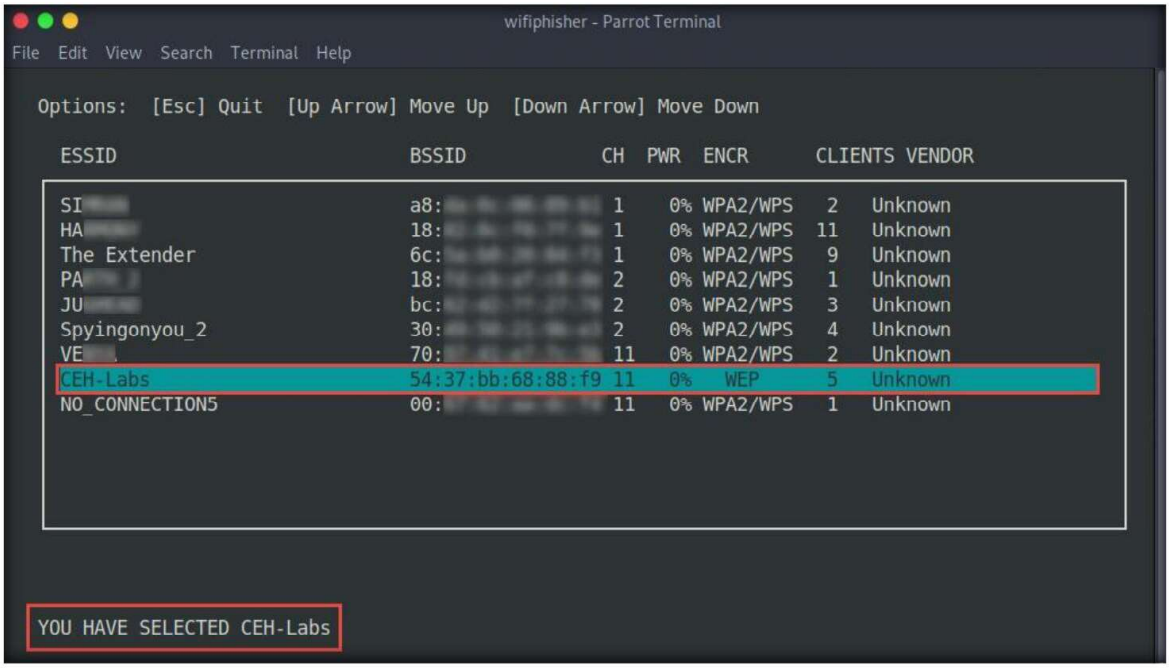


17. Type **wifiphisher --force-hostapd** and press **Enter** to launch the Wifiphisher application.



18. Wifiphisher initializes and appears in the **Parrot Terminal** window.
19. It scans the network for available access points and displays them, as shown in the screenshot.

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

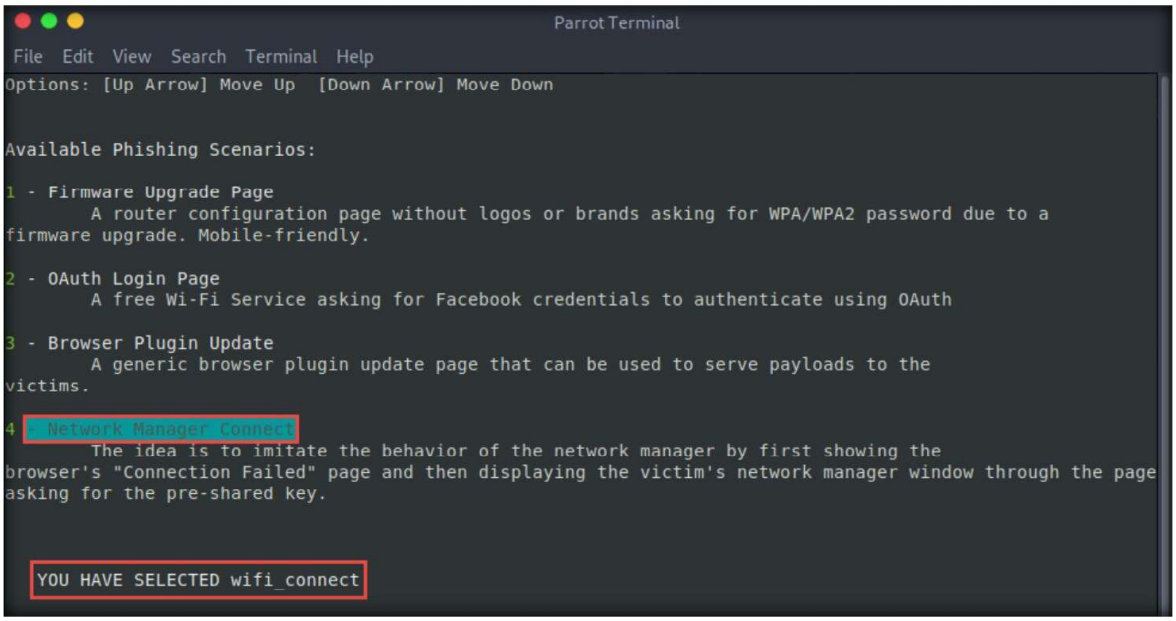


22. The **Available Phishing Scenario** wizard appears. Use the **Down Arrow** key to navigate to **Network Manager Connect** and press **Enter** to select the option.

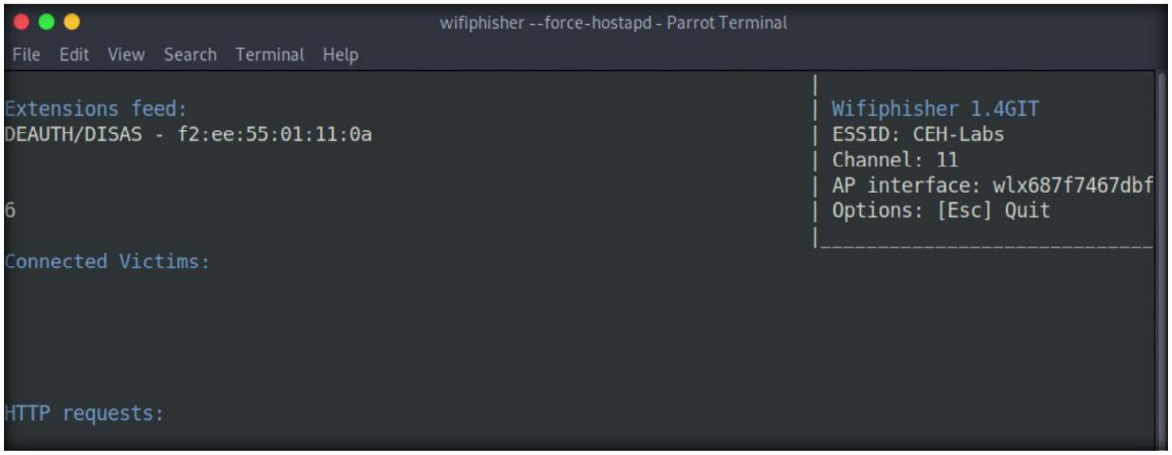
    Note: In this task, we are selecting the **Network Manager Connect** option. However, you can use any of the other available phishing options (**Firmware Upgrade Page**, **OAuth Login Page**, or **Browser Plugin Update**).

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

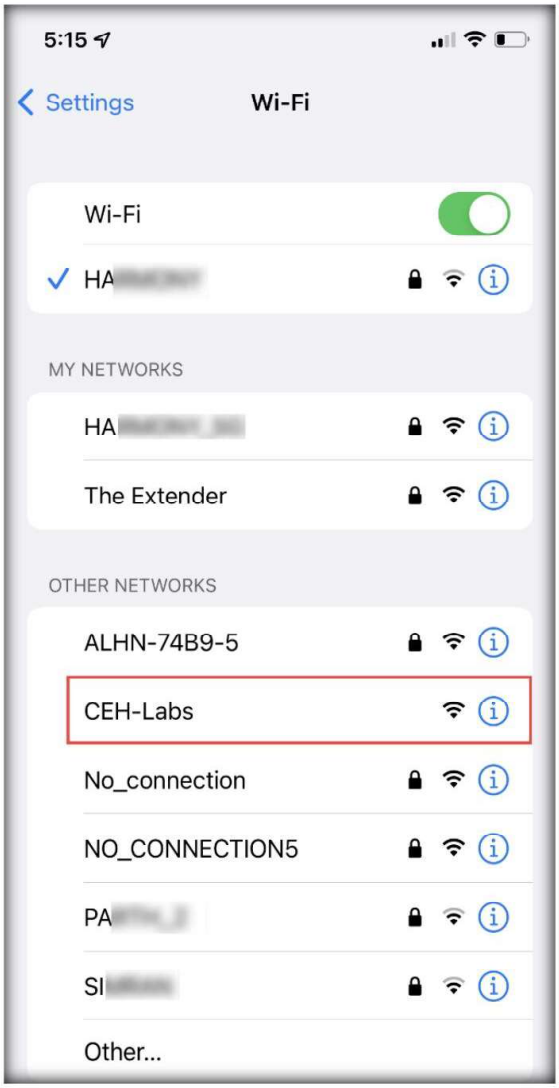
23. After selecting **Network Manager Connect**, you will observe a **YOU HAVE SELECTED wifi_connect** notification in the lower section of the window, as shown in the screenshot.



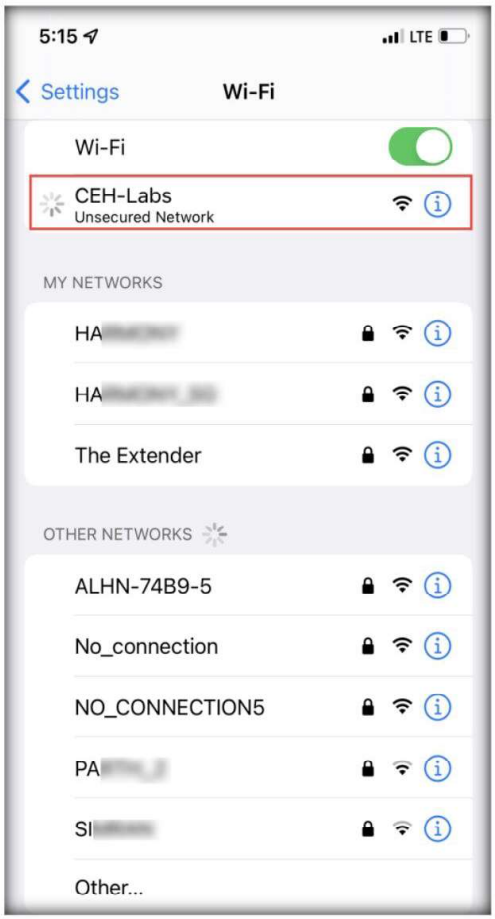
24. A window appears, displaying the fake network that we have created under **Extensions feed**. Note that deauth (deauthentication) packets are sent to the all the connected devices.



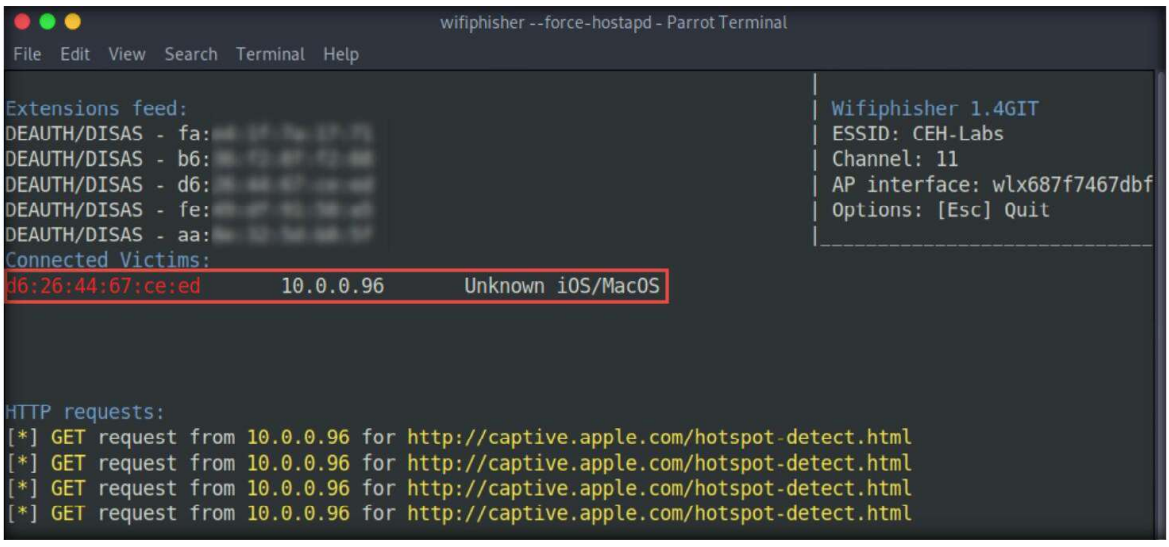
25. Now, switch to your "victim" mobile device. Note that a rogue access point with the name **CEH-LABS** has been created along with the original CEH-LABS access point, as shown in the screenshot.
26. Observe that the rogue access point does not have any security enabled.



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

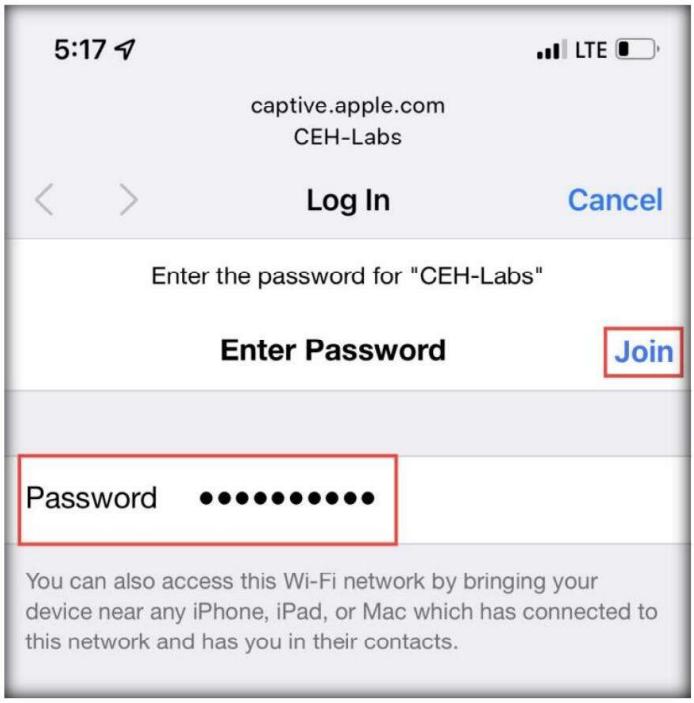


28. Now, switch back to the **Wifiphisher** window running in the **Parrot Security** virtual machine. You can see the connected device under the **Connected Victims** section, as shown in the screenshot.

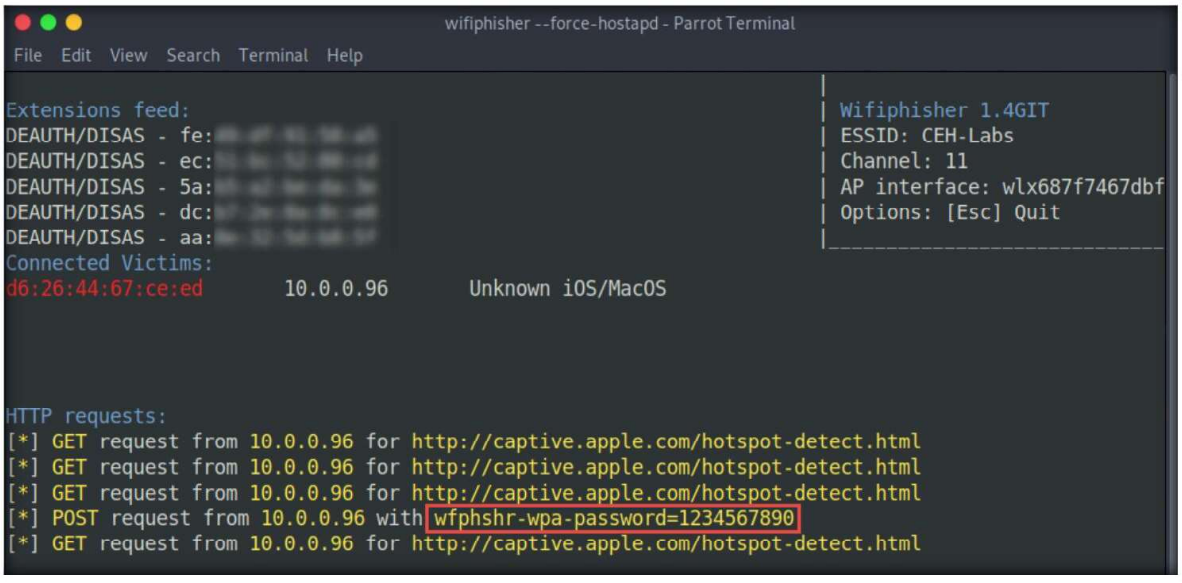


29. The **Enter the password for "CEH-LABS"** screen appears. Under **Enter Password**, type the pre-shared key in the **Password** field and click **Join**.

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



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



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

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

Task 3: Crack a WEP Network using Aircrack-ng

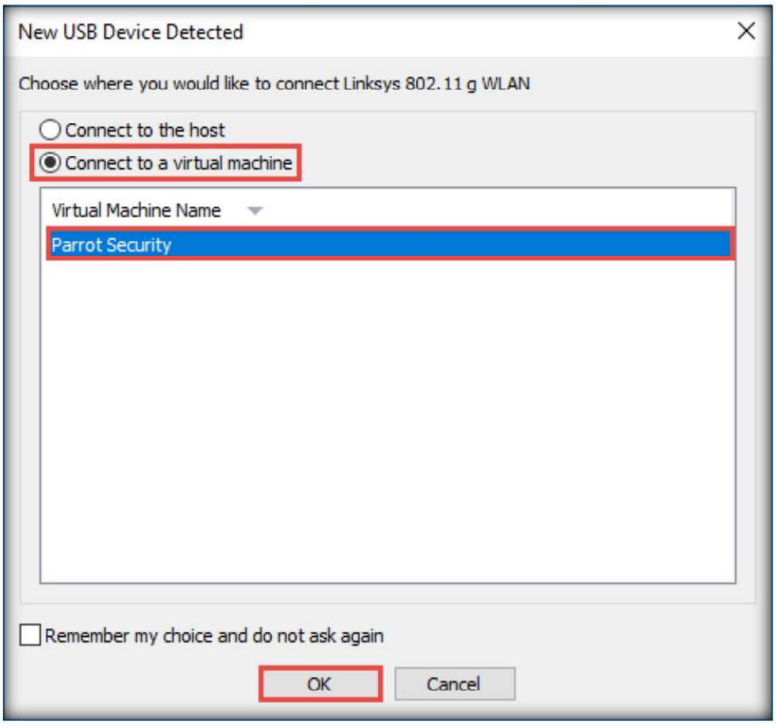
In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

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

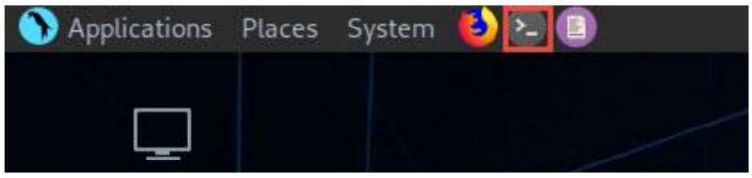
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note:

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



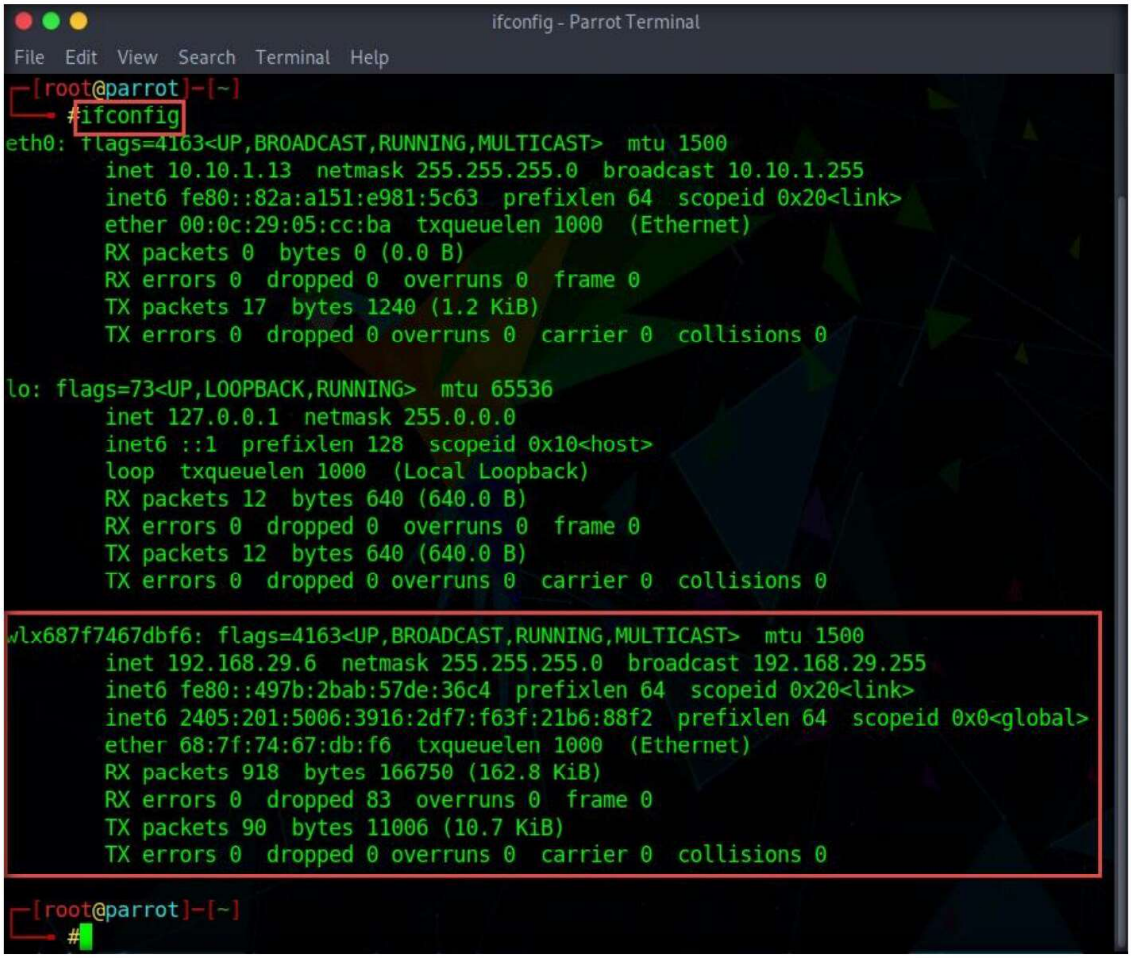
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



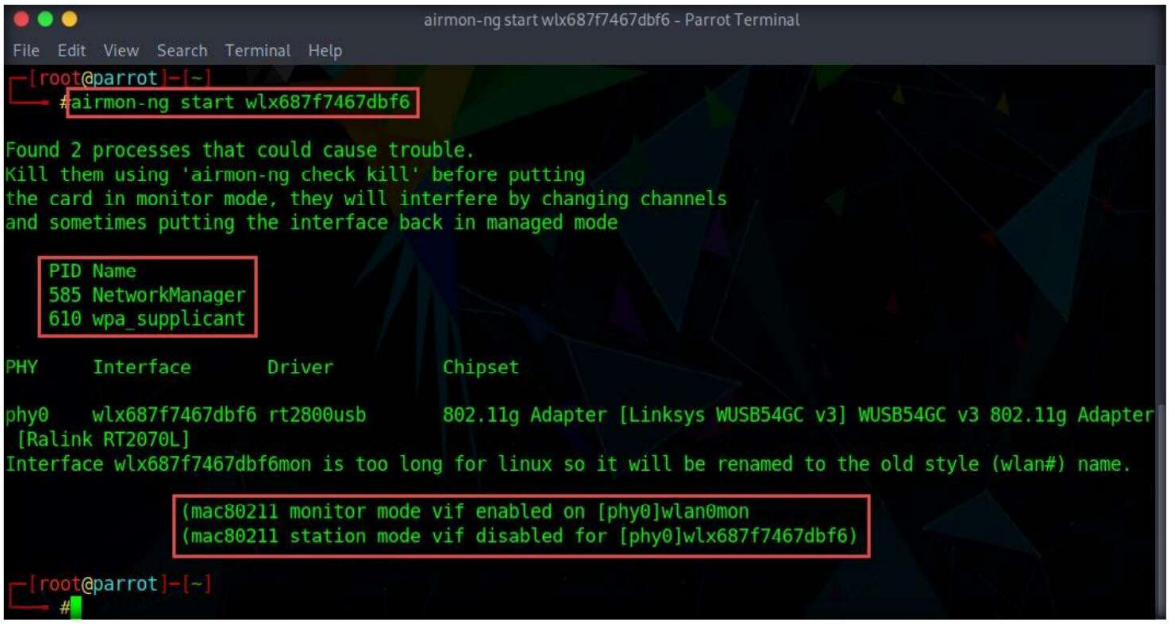
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

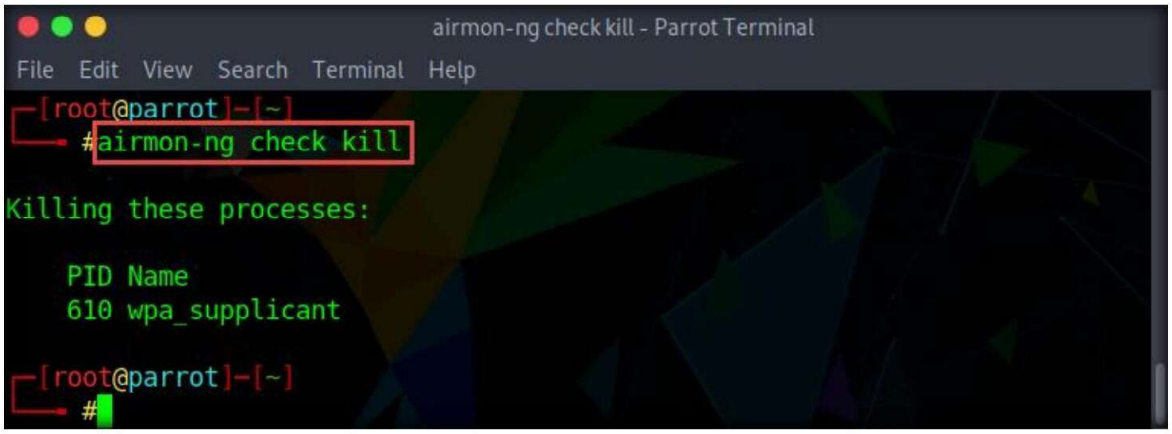
   Note: The name of wireless interface might vary in your lab environment.



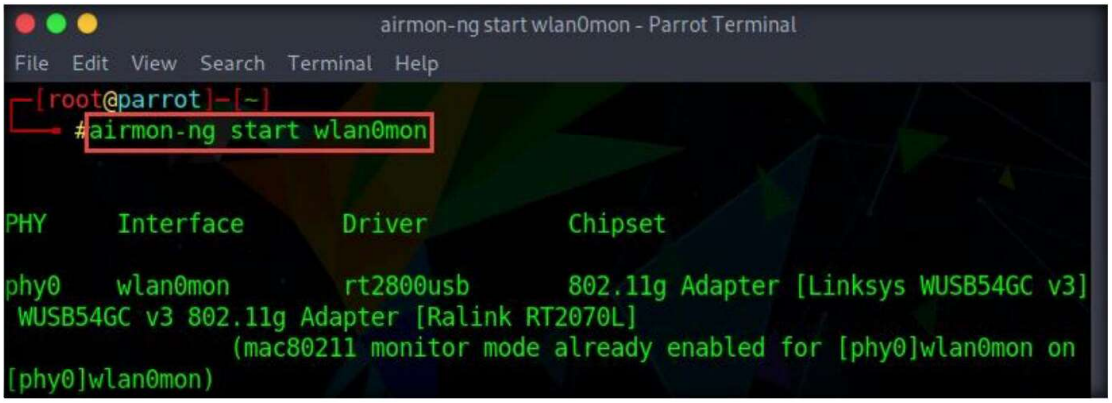
10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface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



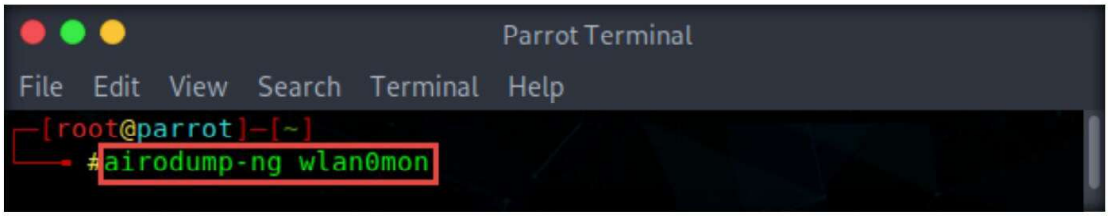
13. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

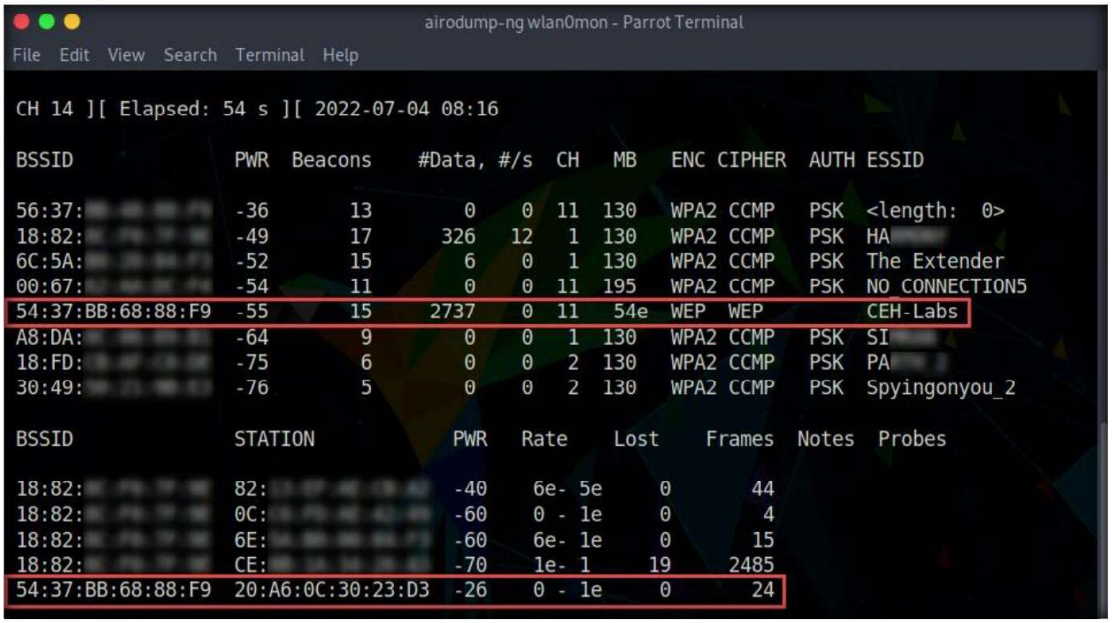


14. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
15. Note that **Linksys WUSB54GC v3 802.11g** Adapter is now running in monitor mode on the wlan0mon interface, as shown in the screenshot.



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



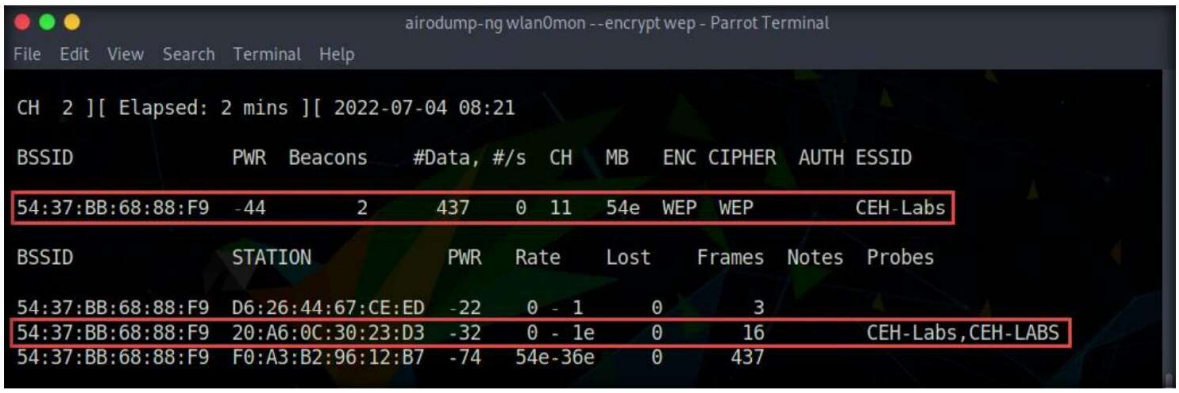


Note: In this lab, we will crack **CEH-LABS**.

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

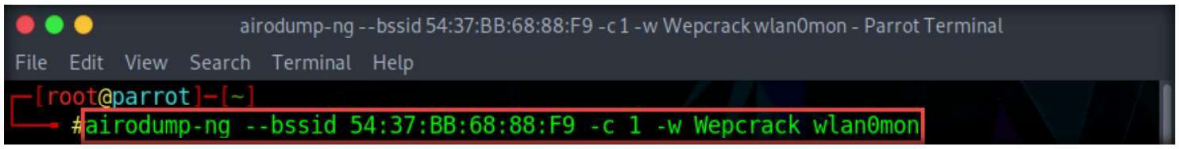
Note: airodump-ng hops from channel to channel and shows all the access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

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

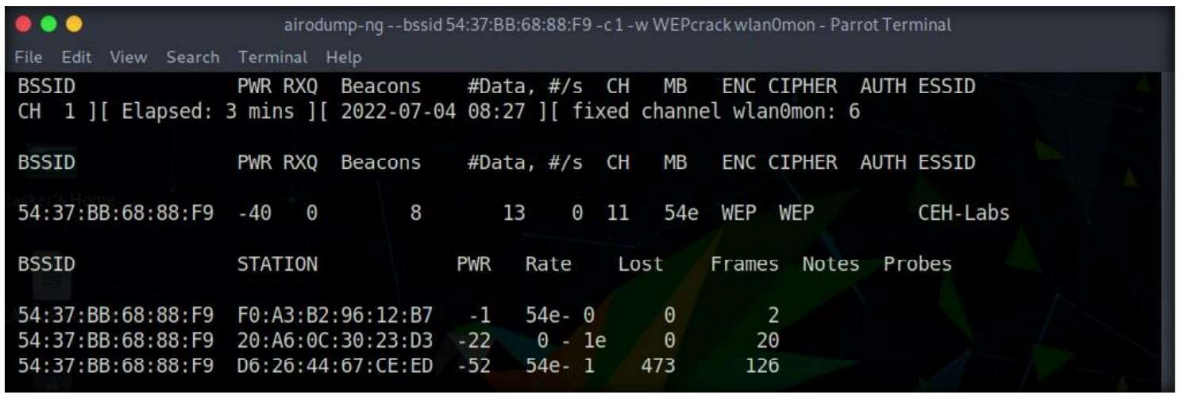


19. Now, you must instruct airodump-ng to begin capturing the Initialization Vector (IV) from the access point. To do so, in the terminal window, type **airodump-ng --bssid 54:37:BB:68:88:F9 -c 1 -w WEPcrack wlan0mon** and press **Enter**. Leave airodump-ng running.

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



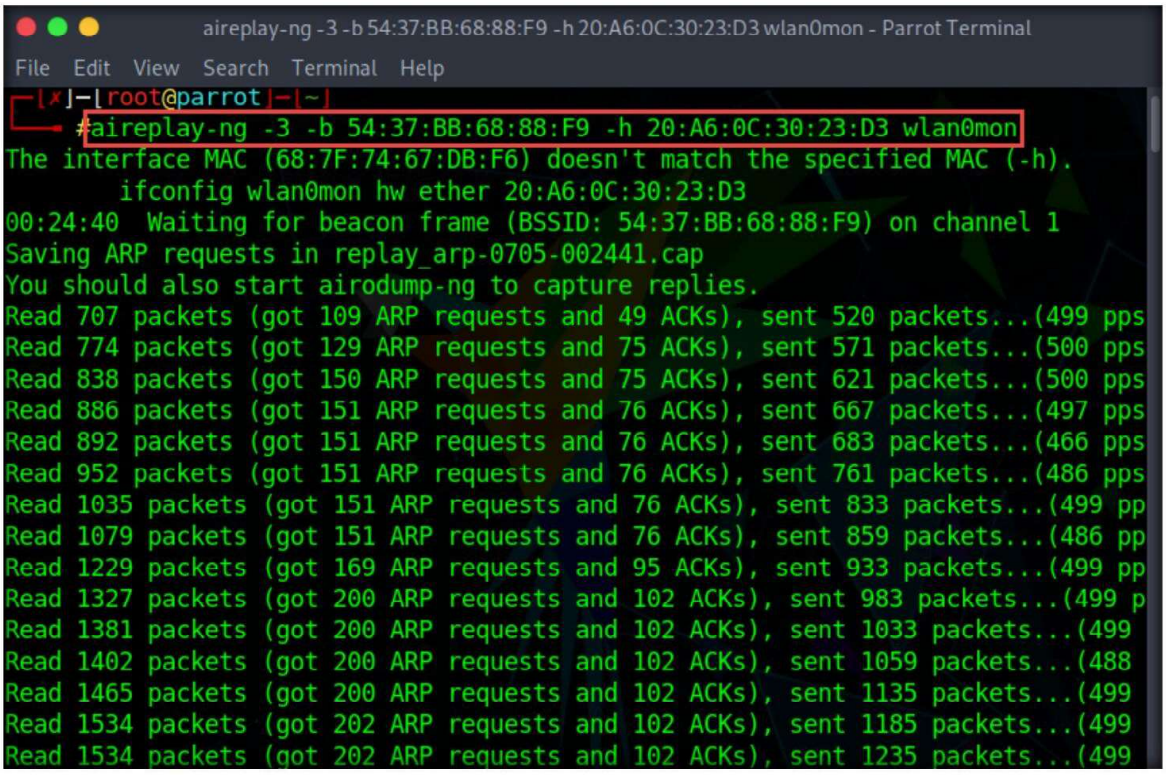
20. Airodump-ng will capture the IVs generated from the target access point, as shown in the screenshot.



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

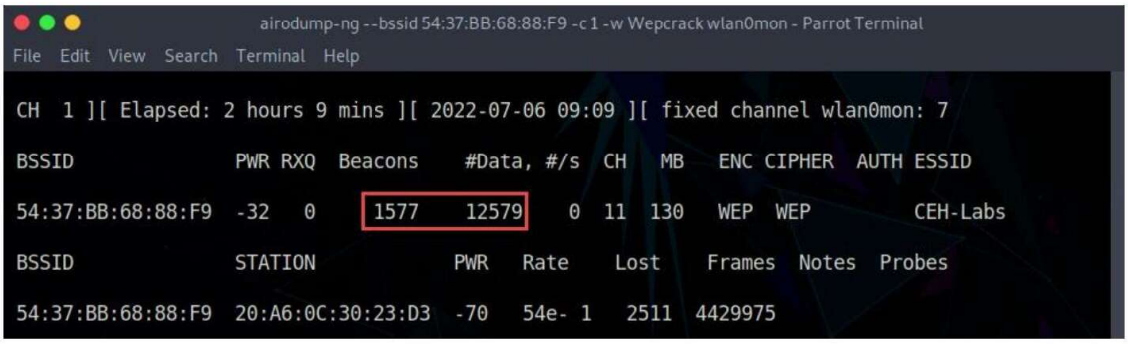
    Note: The password that you type will not be visible.
24. Now, type **cd** and press **Enter** to jump to the root directory.
25. In this new terminal window, type **aireplay-ng -3 -b 54:37:BB:68:88:F9 -h 20:A6:0C:30:23:D3 wlan0mon** and press **Enter**. This command will generate ARP traffic in the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

    Note: Reissue this command until it runs successfully.



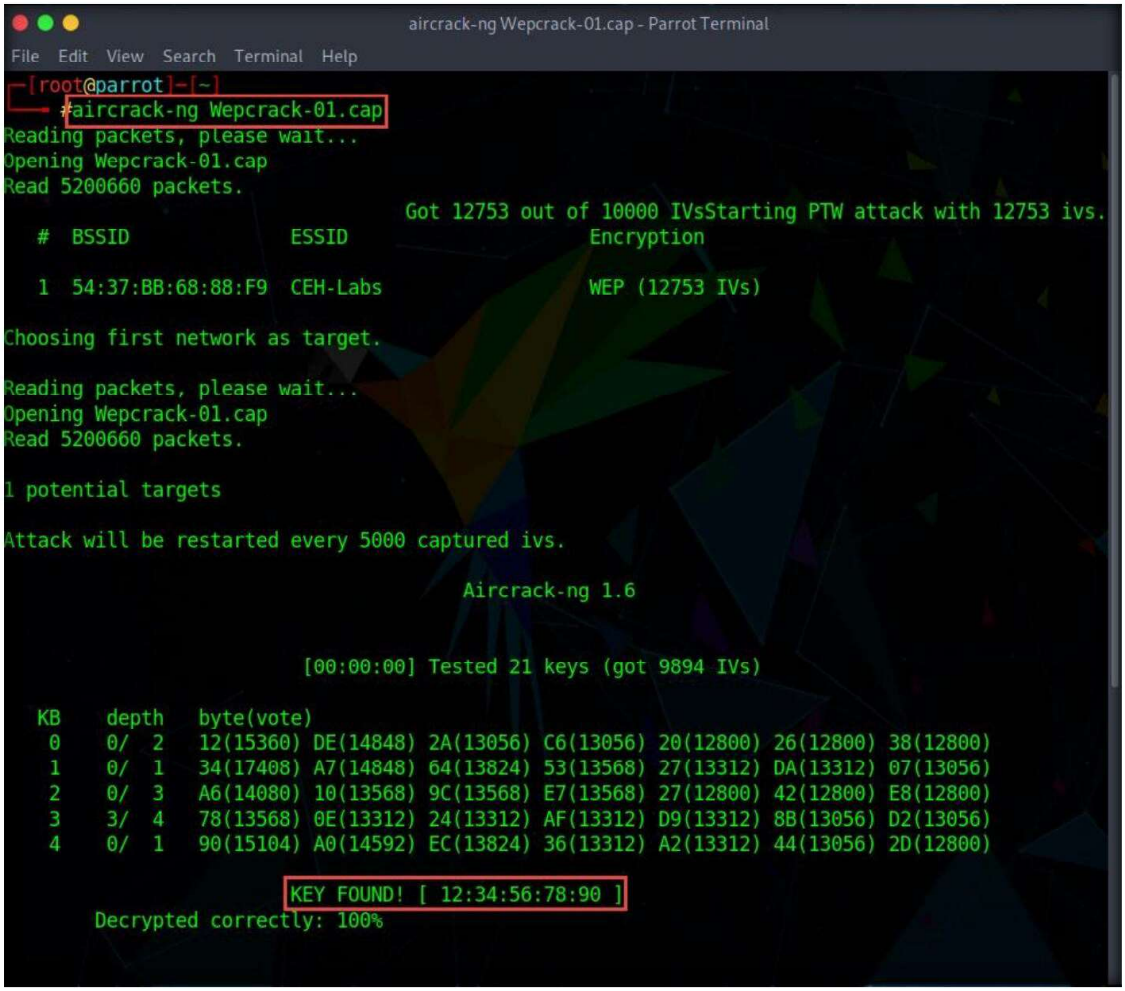
26. Wait until the number of send ARP packets reaches the range of 10,000–20,000, and then press **Ctrl+C** to stop generating ARP traffic in the network.

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

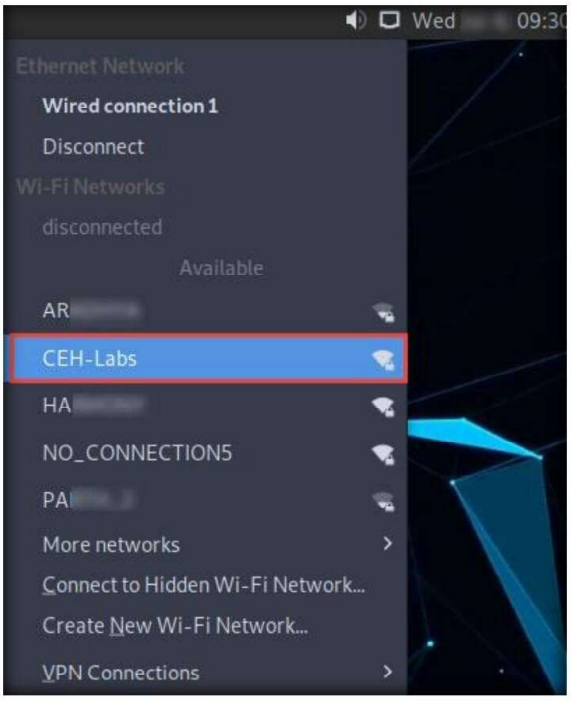


28. Now, launch aircrack-ng to recover the WEP key from the capture file. Type **aircrack-ng Wepcrack-01.cap** and press **Enter**.

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

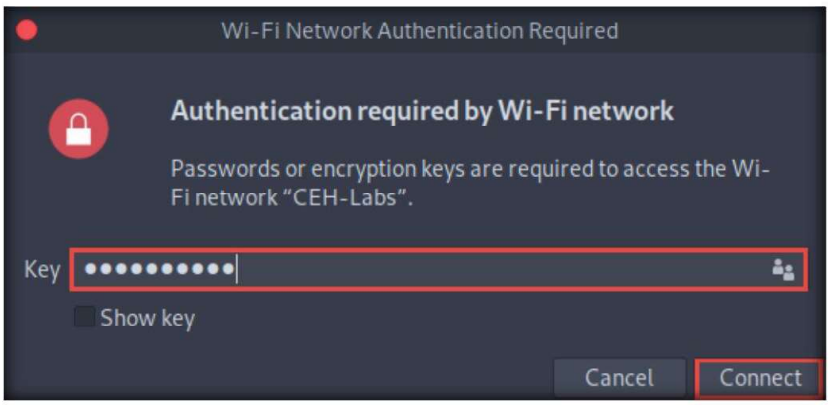


30. Close all the open windows and reboot the **Parrot Security** machine.
31. After the machine reboots, in the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
32. Now, we will connect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

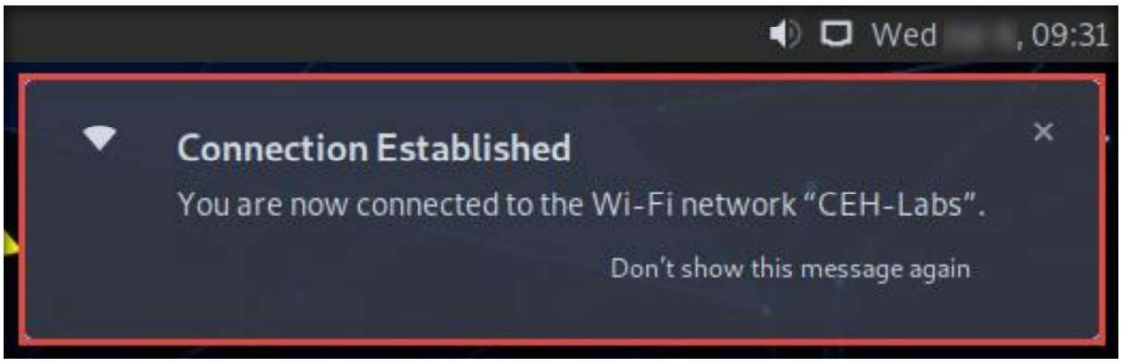


34. A **Wi-Fi Network Authentication** Required pop-up appears; type the cracked key and click the **Connect** button.

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



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



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

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

Task 4: Crack a WPA Network using Fern Wifi Cracker

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

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

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

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

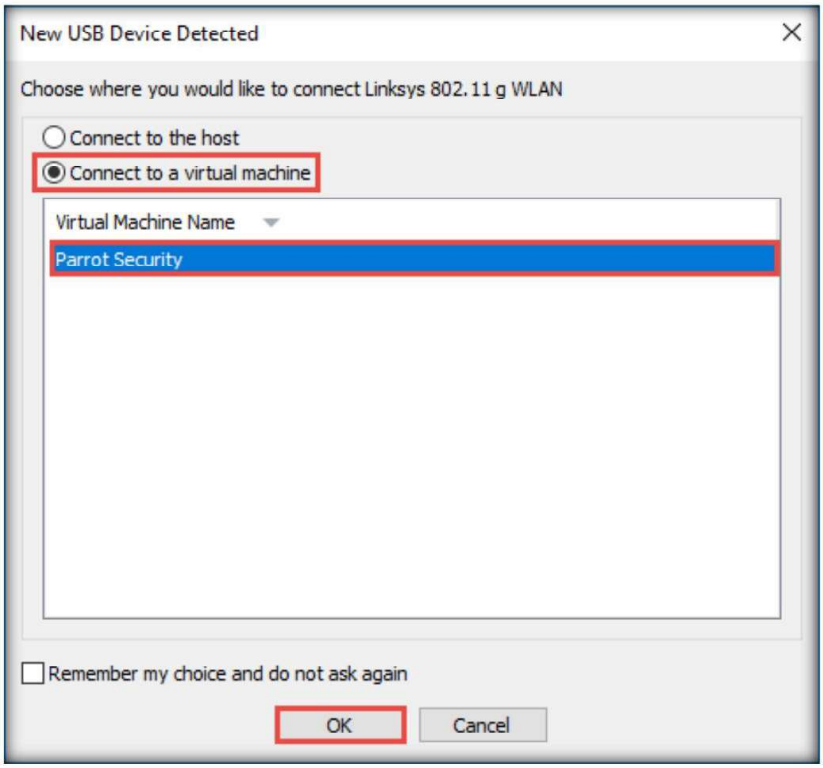
Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

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

Note:

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

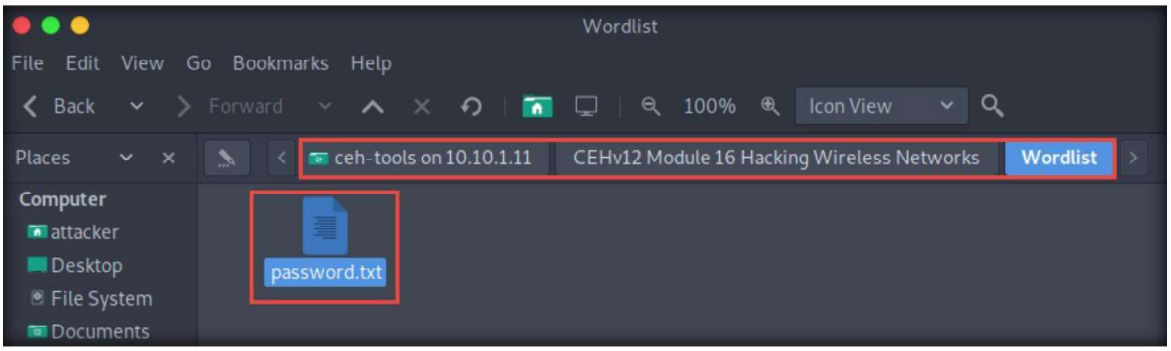
3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



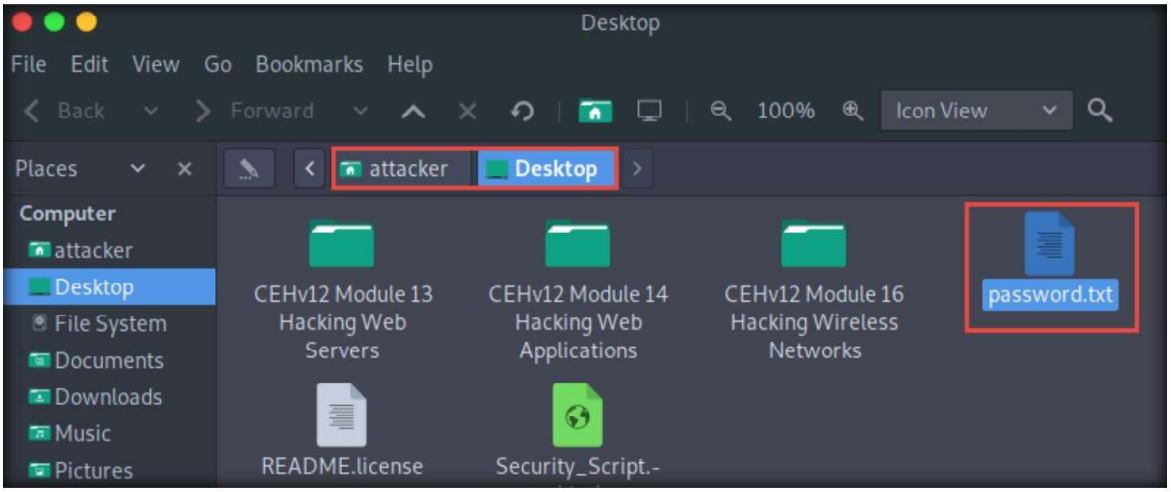
Note: In this task, we will use a sample password file (**password.txt**) containing a list of passwords to crack the target WPA network.

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

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

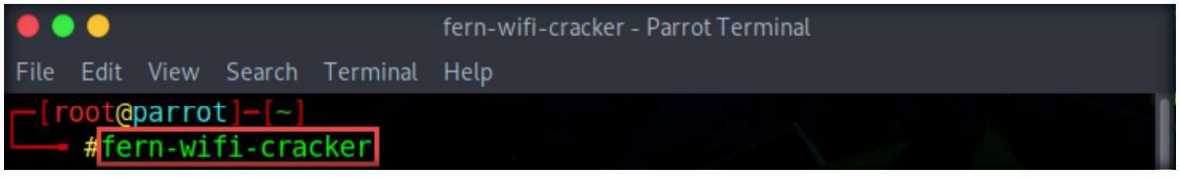


10. Paste **password.txt** on the **/attacker/Desktop**.



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

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



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

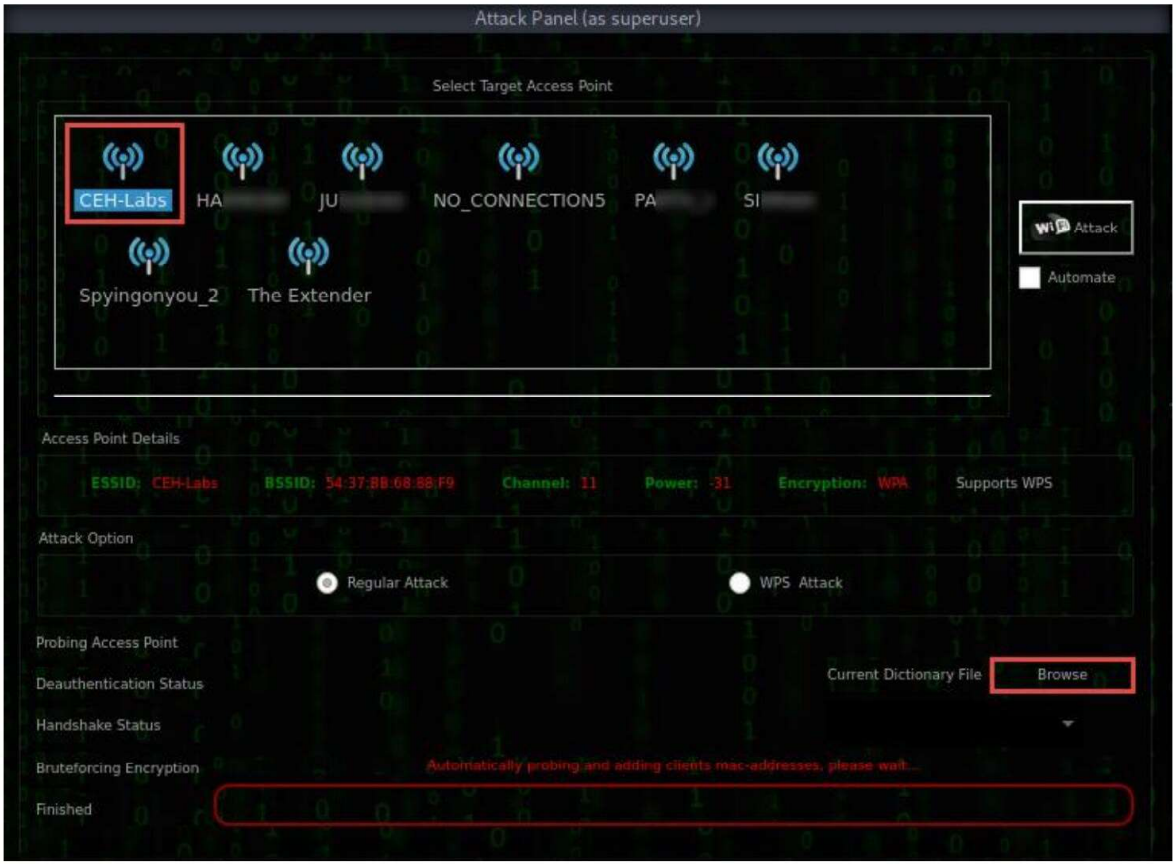
16. Click **Select Interface** and from the drop-down list, select the **wlx687f7467dbf6** interface.
17. A **Tips - Scan** settings pop-up appears, click **OK**.
18. The selected adapter (**wlx687f7467dbf6**) loads, and the notification Monitor Mode Enabled on wlan0mon appears in the selected network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

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

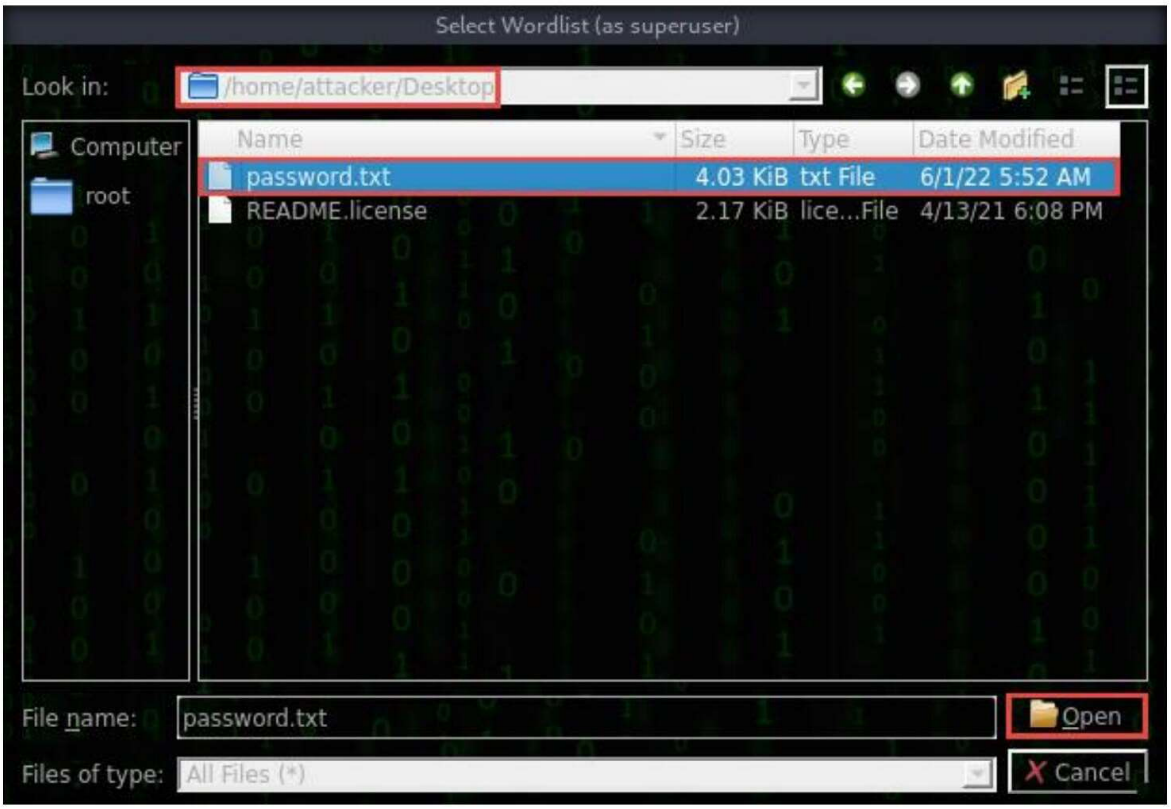
    Note: The number of detected WPA networks will differ in your lab environment.

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

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



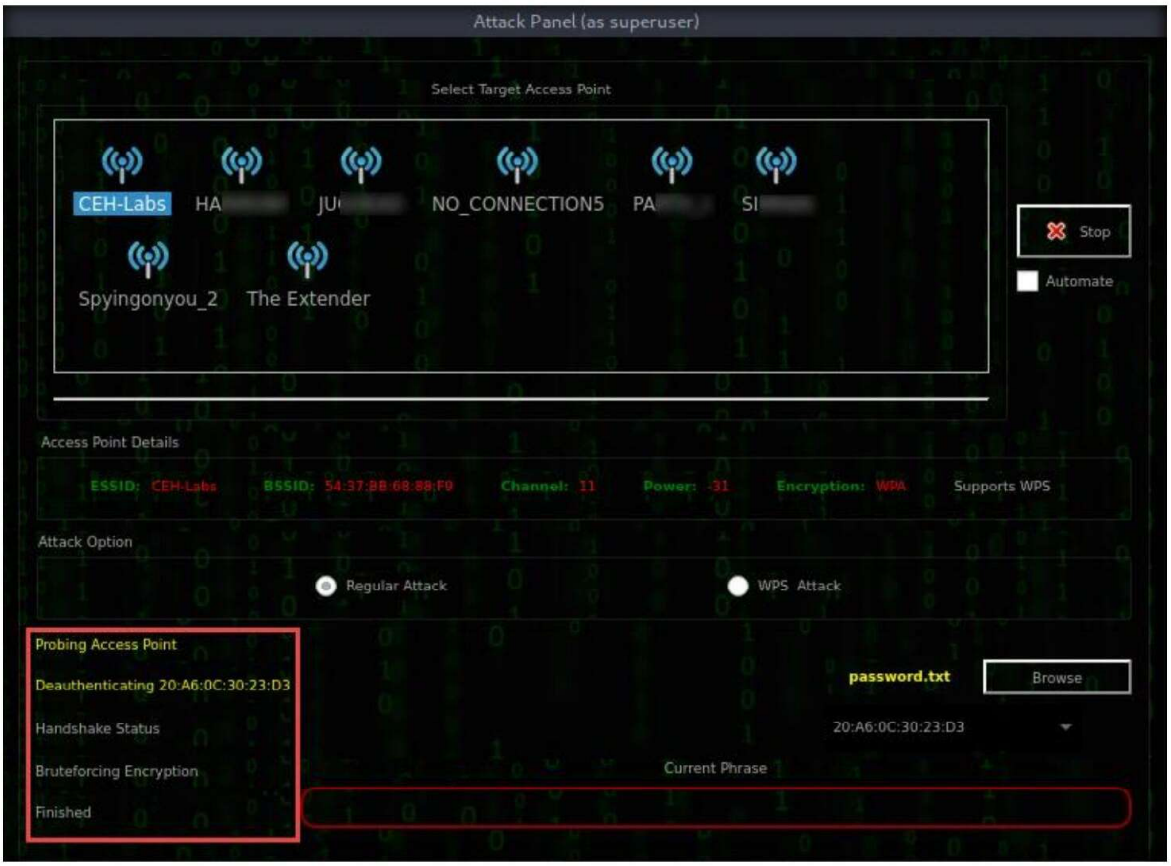
24. The **Select Wordlist** window appears. Navigate to the location **/home/attacker/Desktop**, and select **password.txt**. Click **Open**.



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

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

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

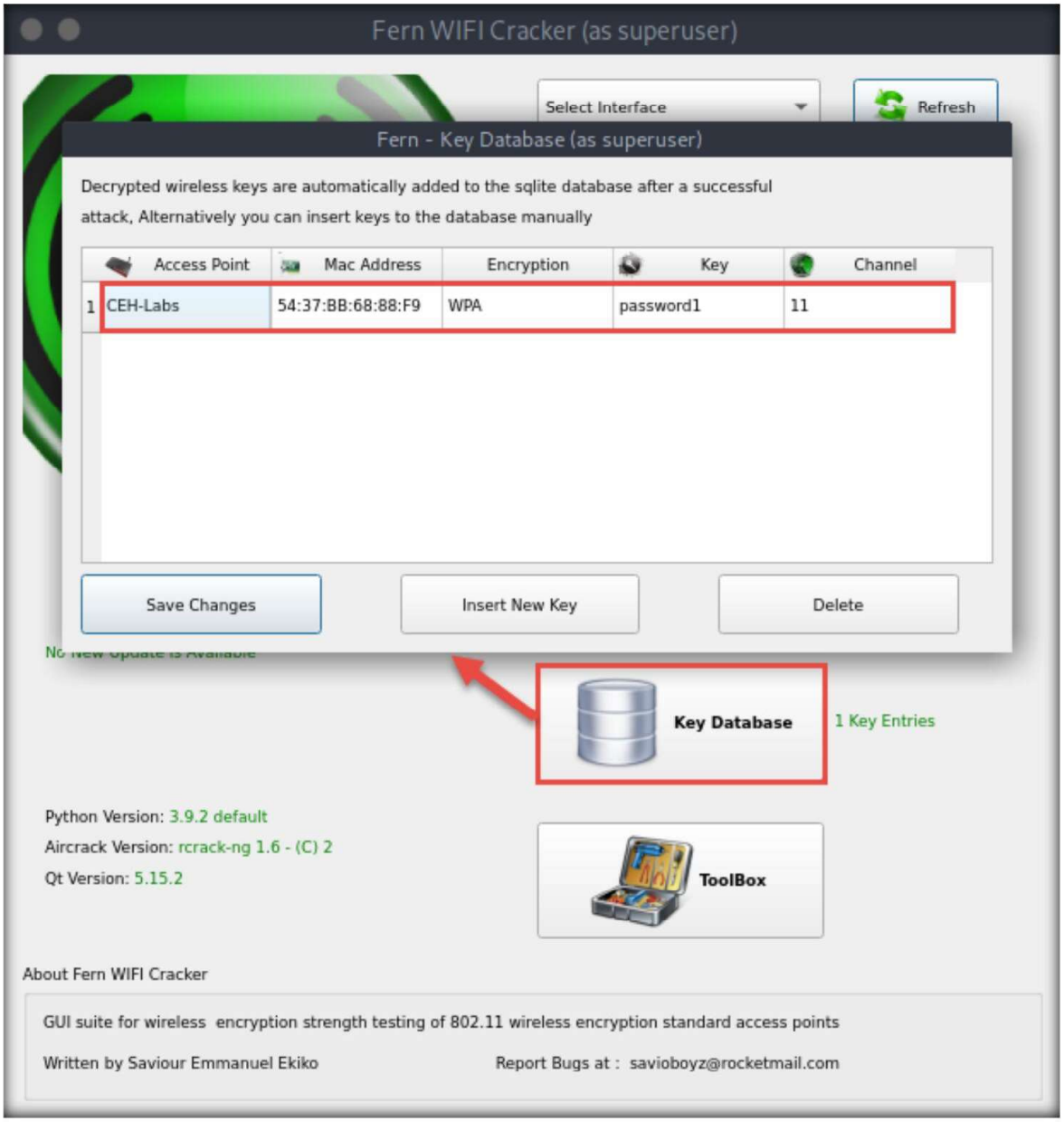


27. After the completion of the **Current Phrase** bar, the cracked **WPA KEY** appears, as shown in the screenshot.

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

    Or

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



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

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

Task 5: Crack a WPA2 Network using Aircrack-ng

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

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

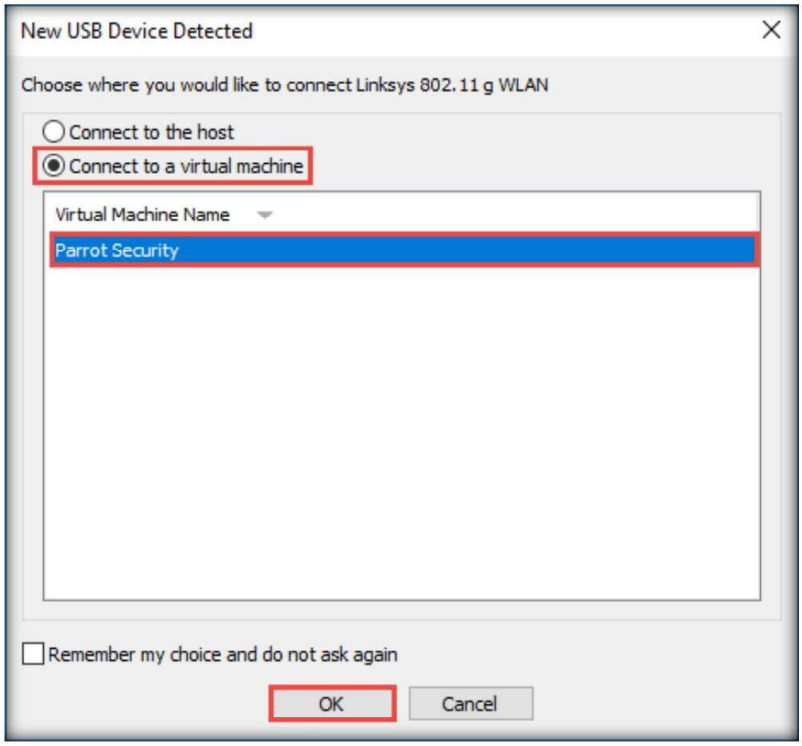
In this task, we will use the Aircrack-ng suite to crack a WPA2 network.

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

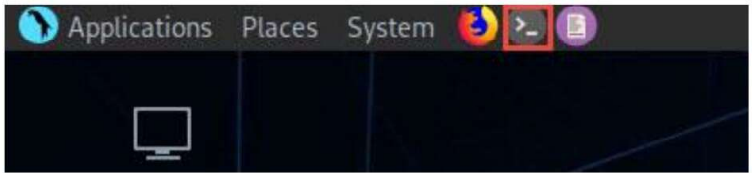
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note:

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

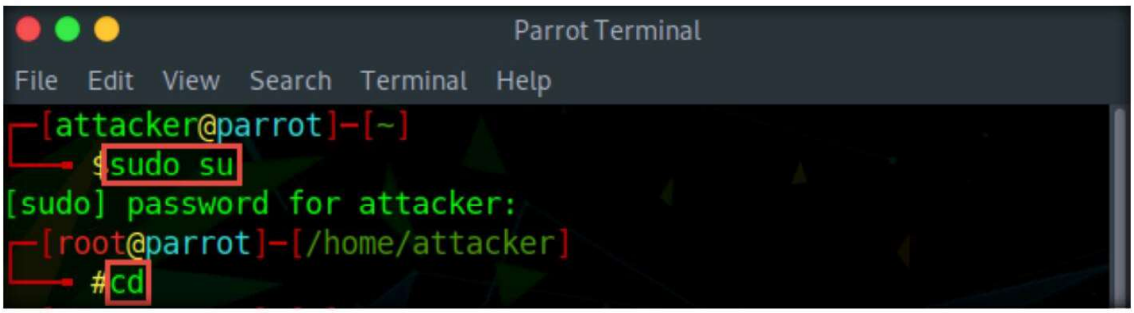


5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



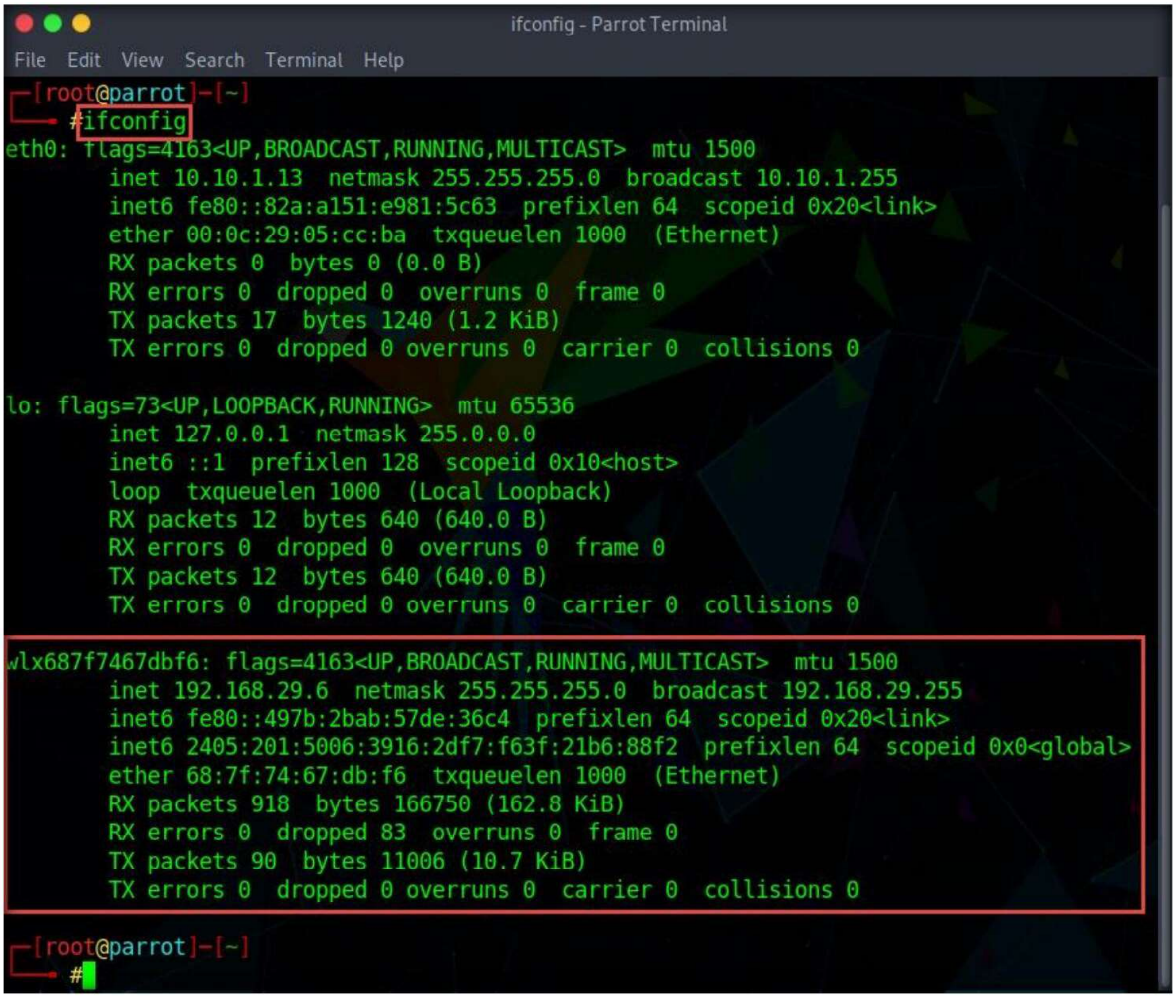
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

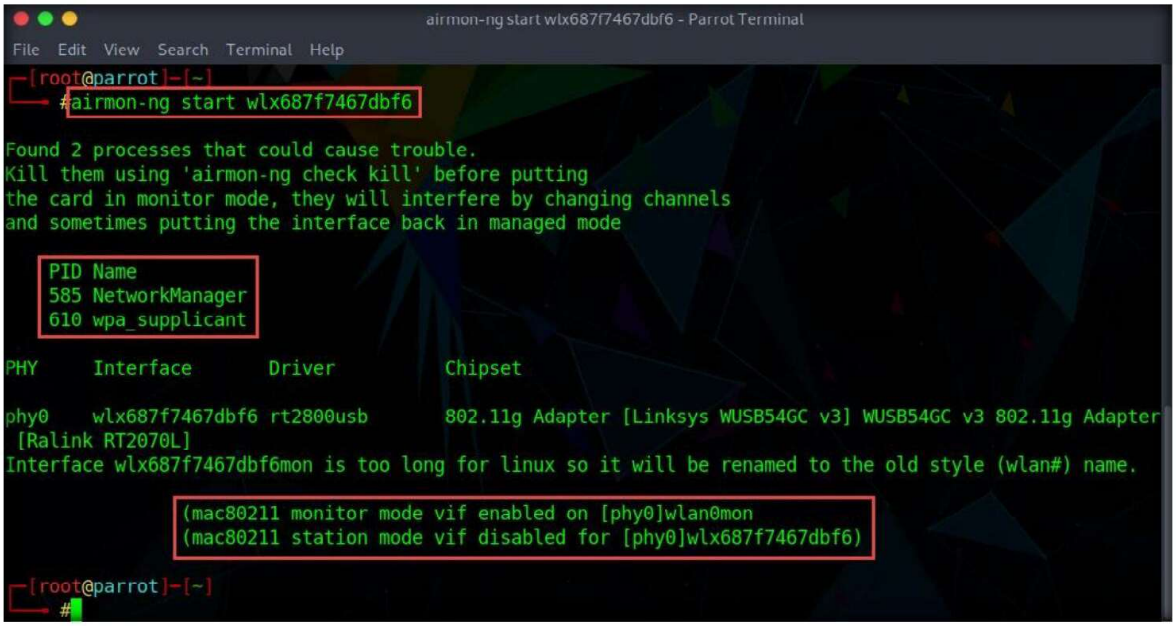


9. In the Parrot Terminal window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

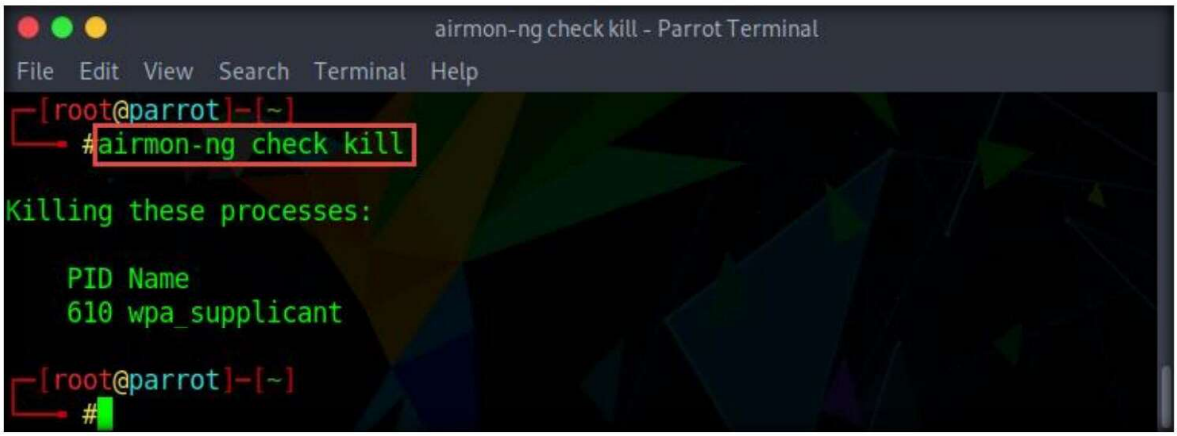
   Note: The name of wireless interface might vary in your lab environment.



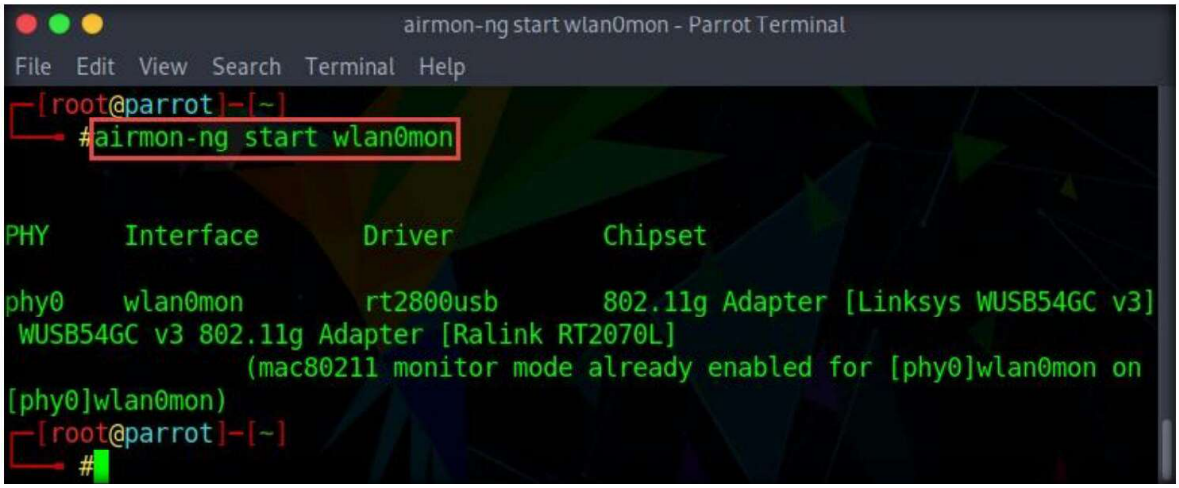
10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface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



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

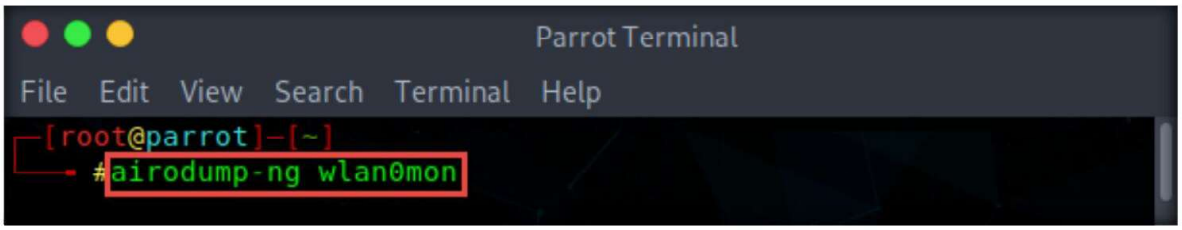


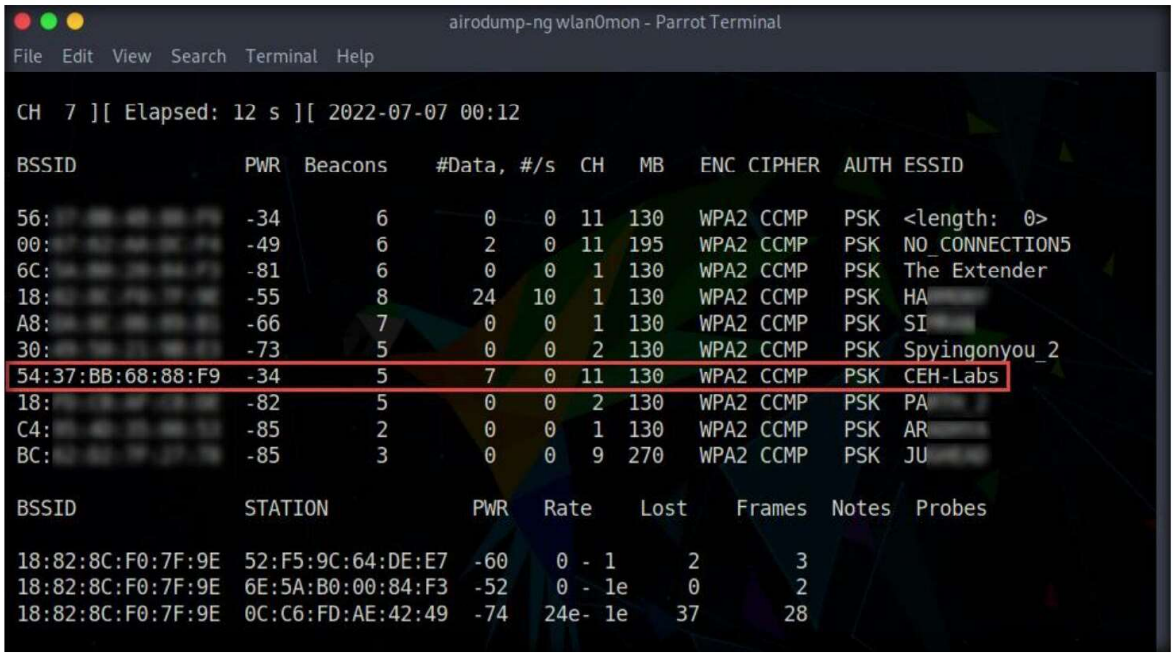
14. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
15. Note that **Linksys WUSB54GC v3 802.11g** Adapter is now running in monitor mode on the wlan0mon interface, as shown in the screenshot.



16. 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.

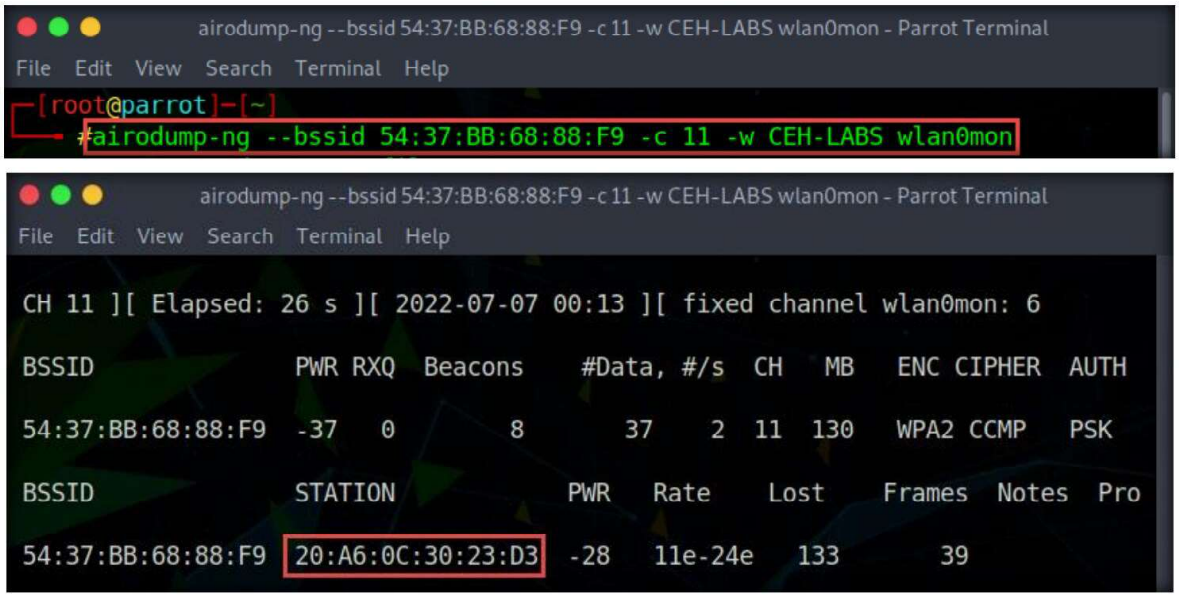




17. In this task, we will target the access point **CEH-LABS** to perform WPA2 cracking.
18. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
19. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter**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

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

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

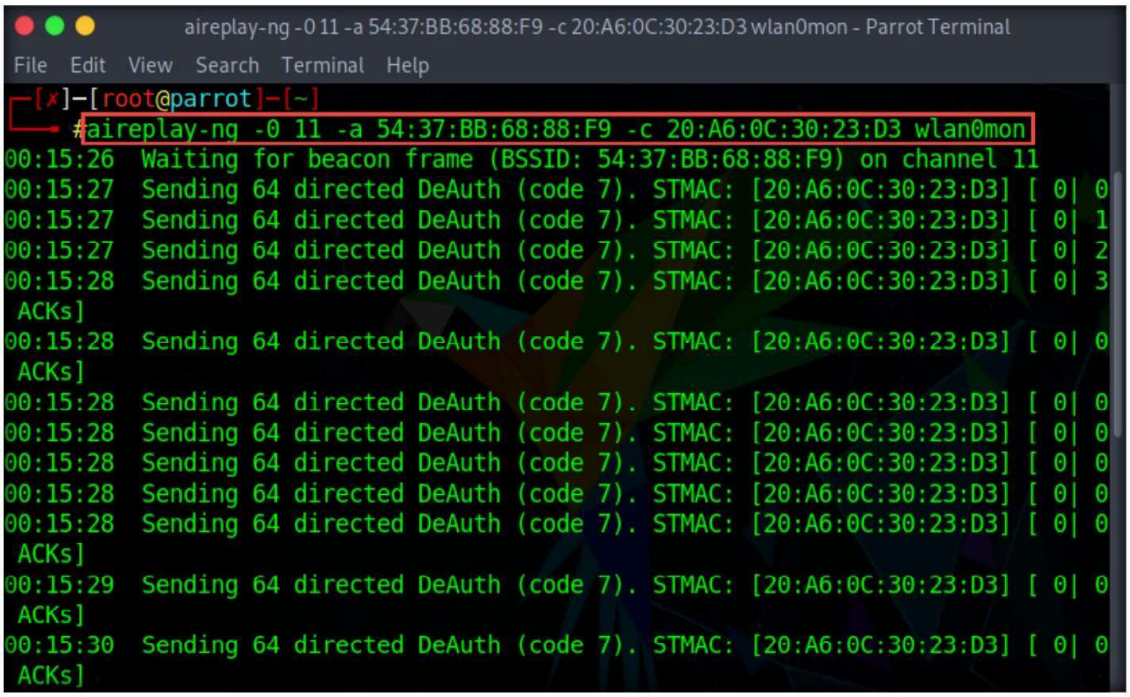


23. Now, open another terminal by clicking the **MATE Terminal** icon ( ) at the top of the **Desktop** window.
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
25. In the **[sudo] password for attacker** field,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

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

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

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



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

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

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

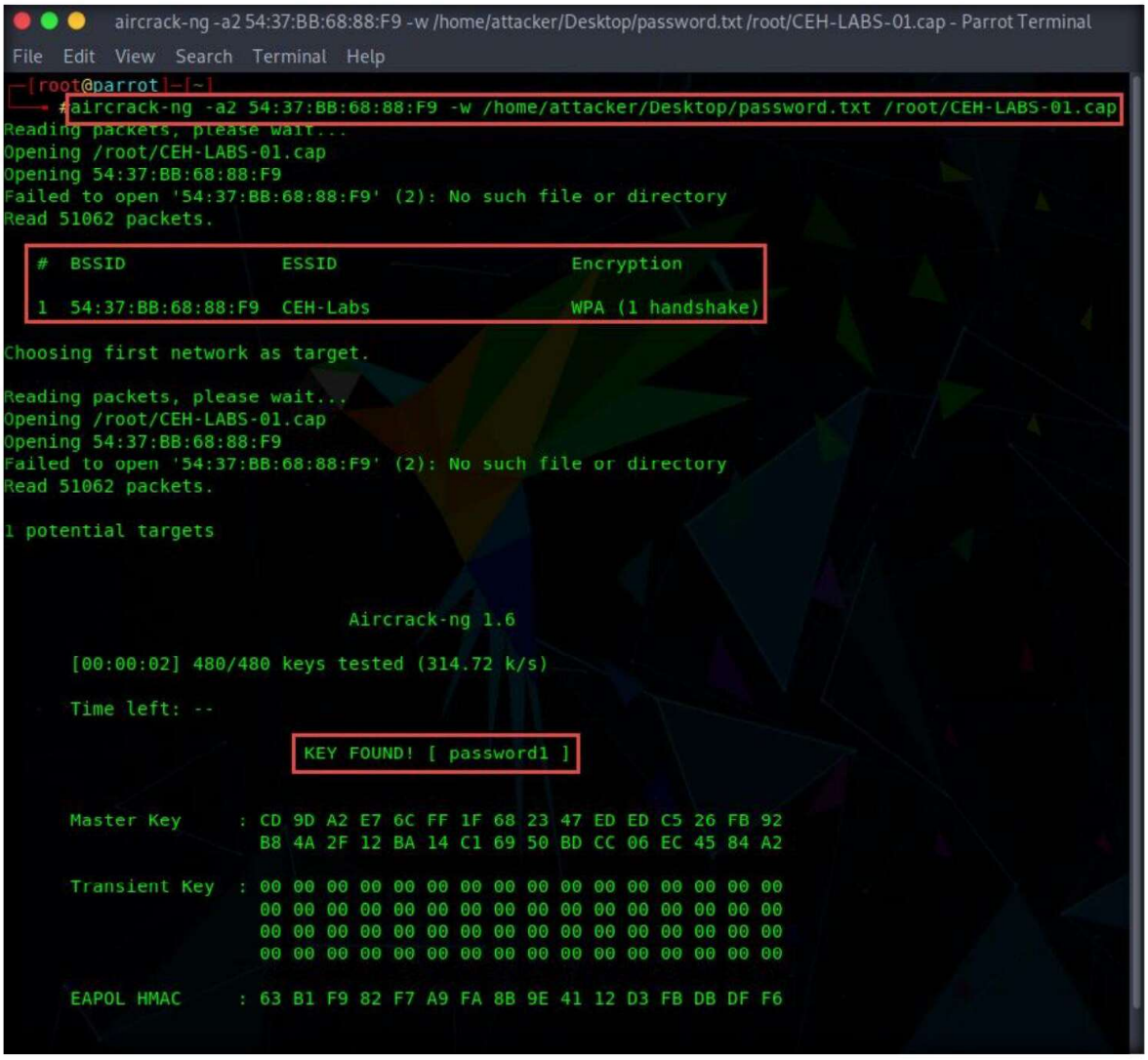
    Note: The password that you type will not be visible.

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

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

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

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



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

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

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

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

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

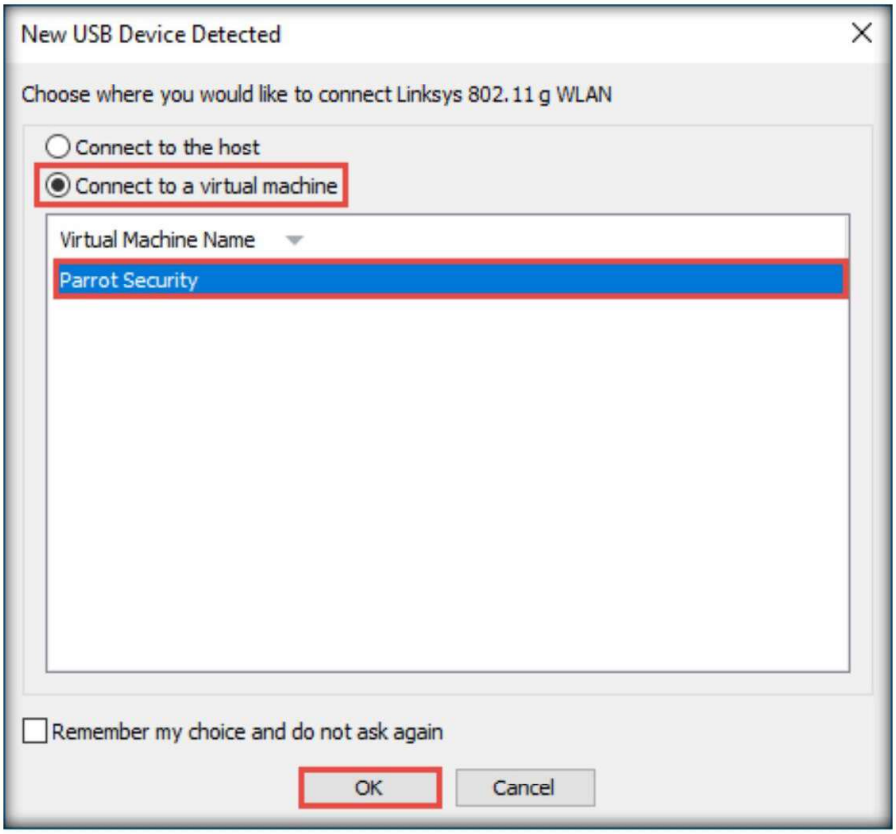
Here, we will use create_ap tool to create a rogue access point and capture data packets using Bettercap.

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

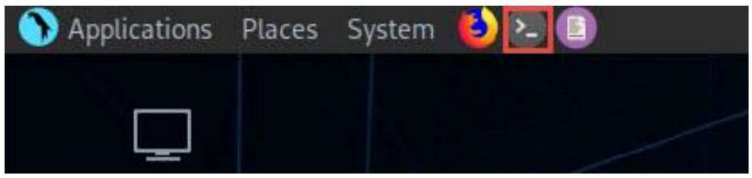
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note:

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

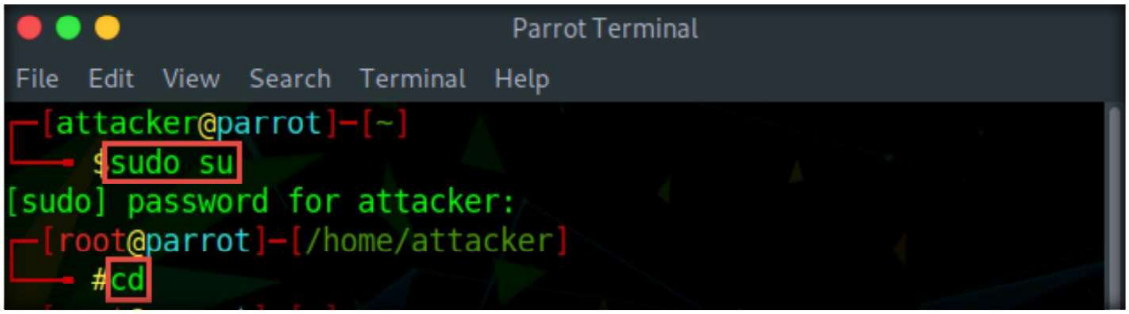


5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

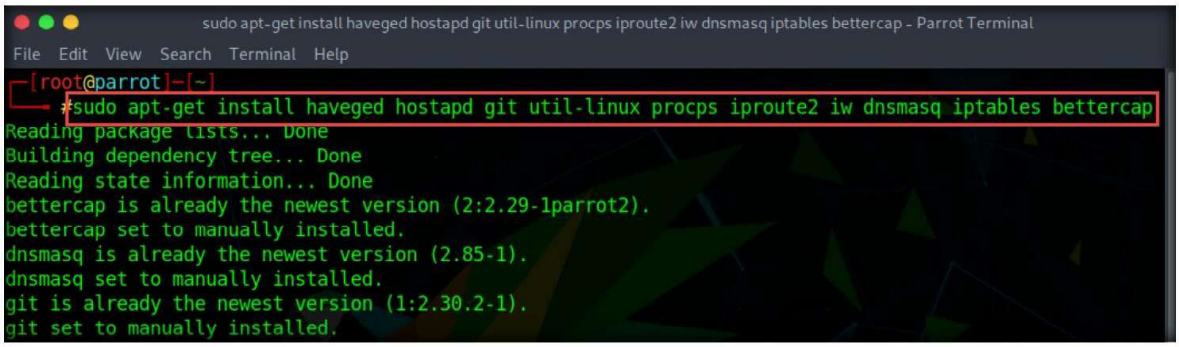


6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

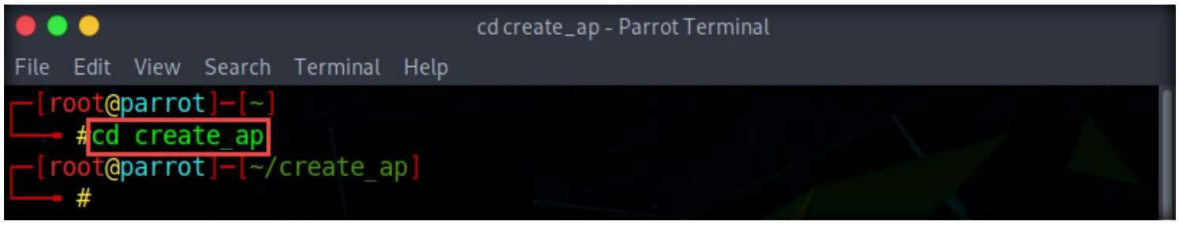
   Note: The password that you type will not be visible
8. Now, type **cd** and press **Enter** to jump to the root directory.



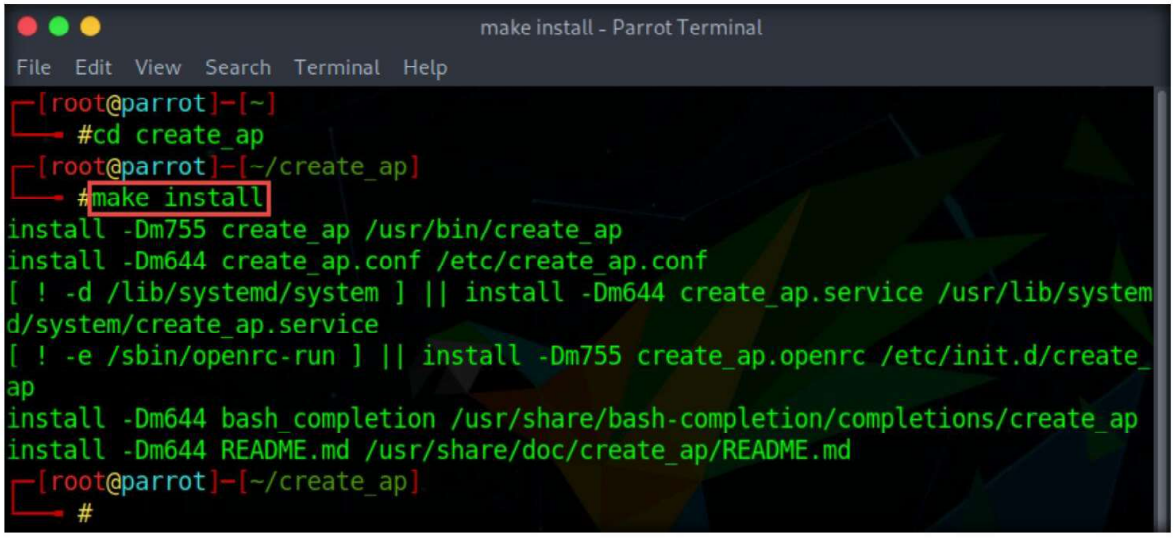
9. In the terminal window, type **apt-get install haveged hostapd git util-linux procps iproute2 iw dnsmasq iptables bettercap** and press **Enter**.



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



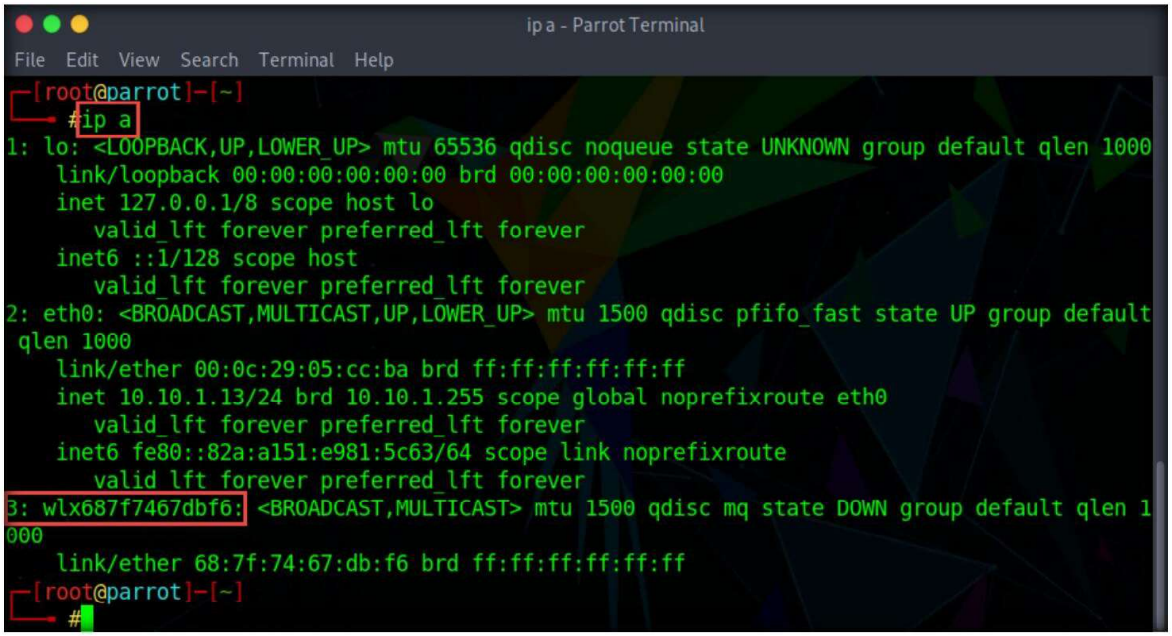
11. Type **make install** and press **Enter** to install the create_ap.



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

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

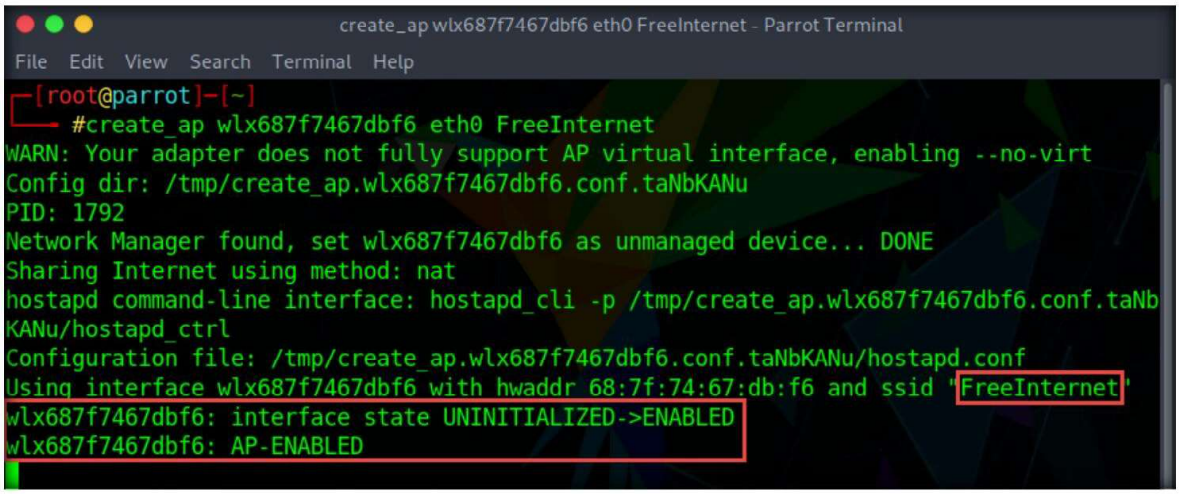
    Note: The name of wireless interface might vary in your lab environment.



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

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

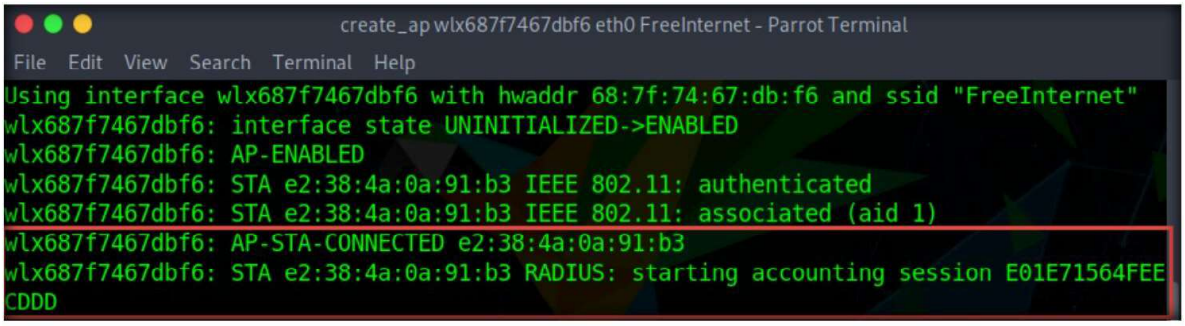
15. You can observe that an access point "**FreeInternet**" has been enabled, as shown in the screenshot.



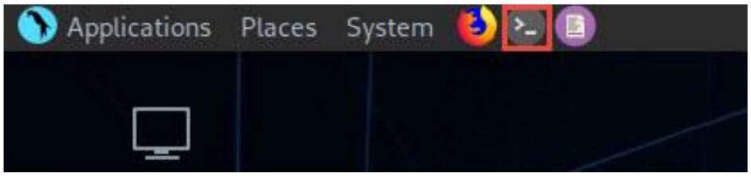
16. Now, switch to your mobile device and turn it on.
17. Turn on Wi-Fi and navigate to **Wi-Fi Settings**.
18. On the **Wi-Fi** screen, you should see an access point with the SSID **FreeInternet** under **MY NETWORKS** section.

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

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



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

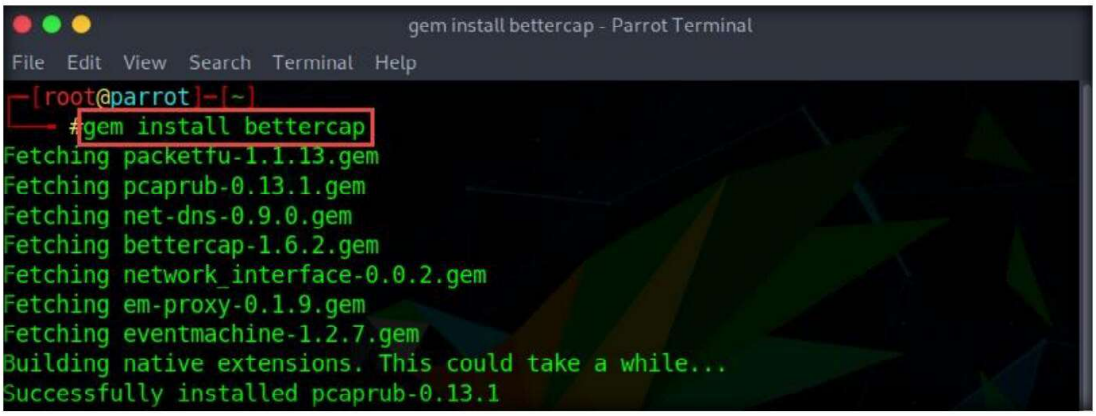


23. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
24. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible

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

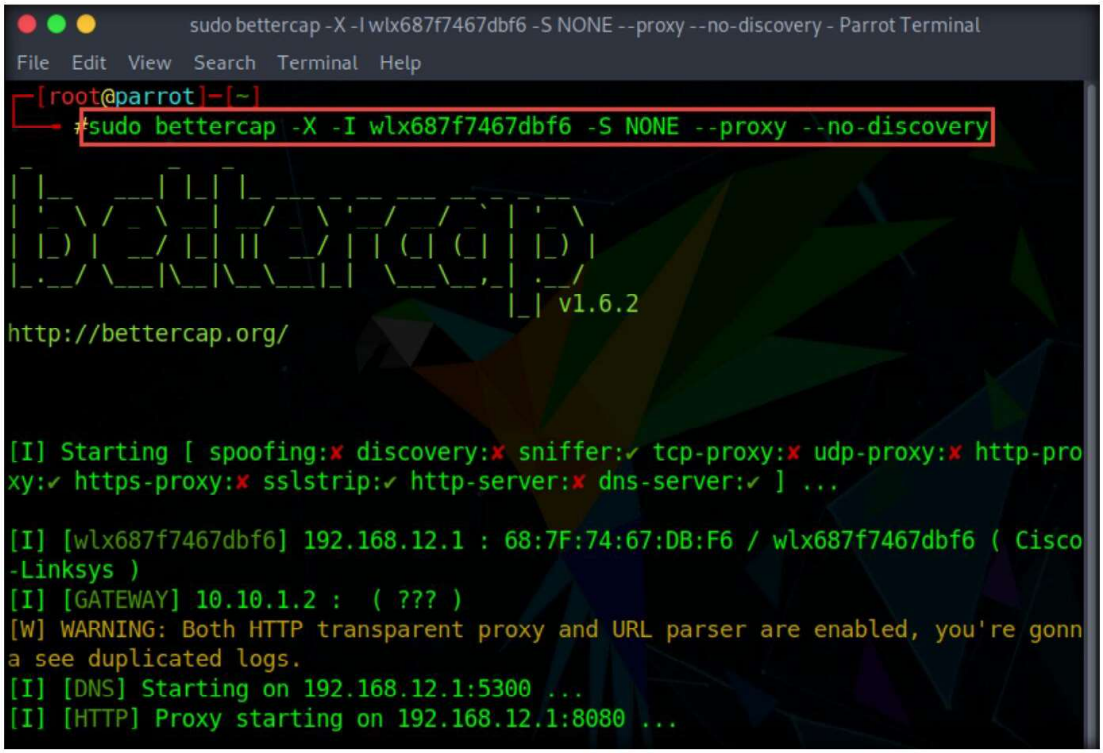
26. In the **Parrot Terminal** window, type **gem install bettercap** and press **Enter** to install Bettercap.



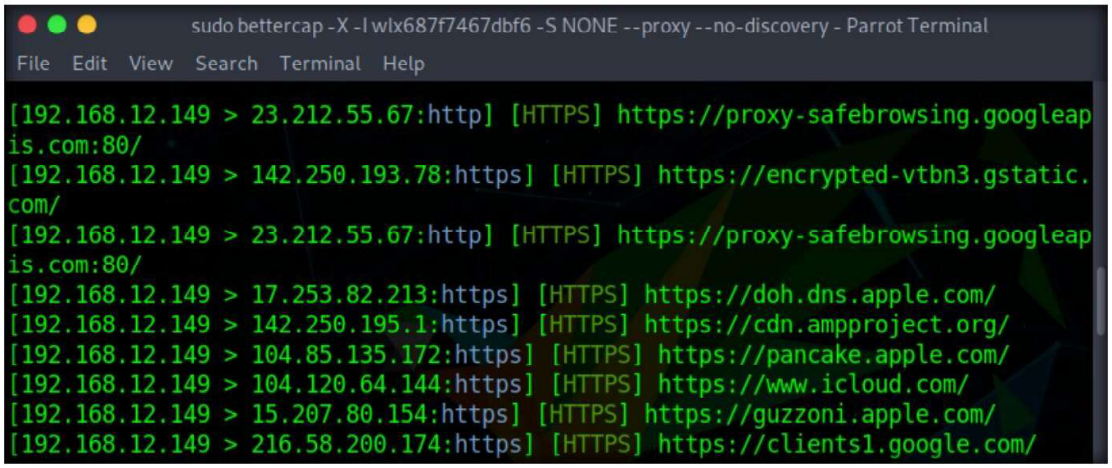
27. Now, we will capture the traffic from the victim's device using Bettercap. To do so, type **sudo bettercap -X -I wlx687f7467dbf6 -S NONE --proxy --no-discovery** and press **Enter**.

Note:

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



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



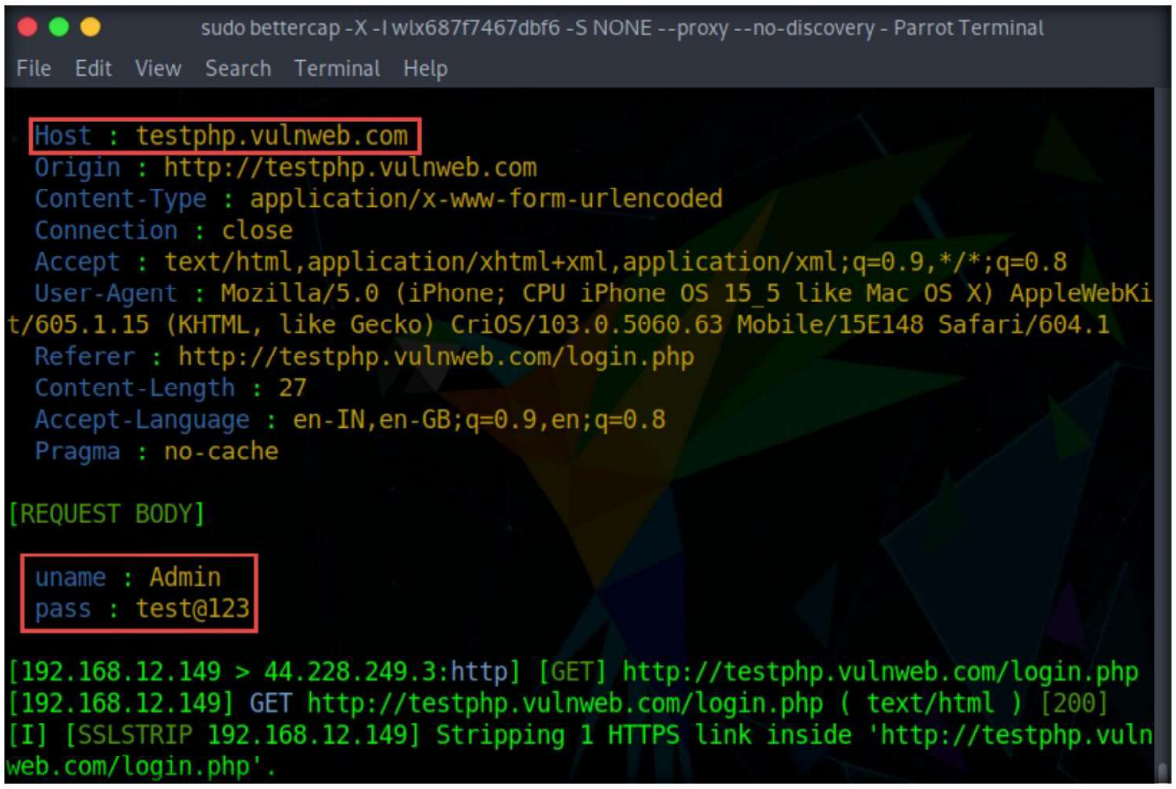
29. Now, switch to the mobile device (victim's device) and open any web browser app.
30. In the browser, type **http://testphp.vulnweb.com/login.php** in the address bar and press **Enter**.
31. The **Acunetix Web Vulnerability Scanner** webpage appears, enter random **Username** and **Password** values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

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

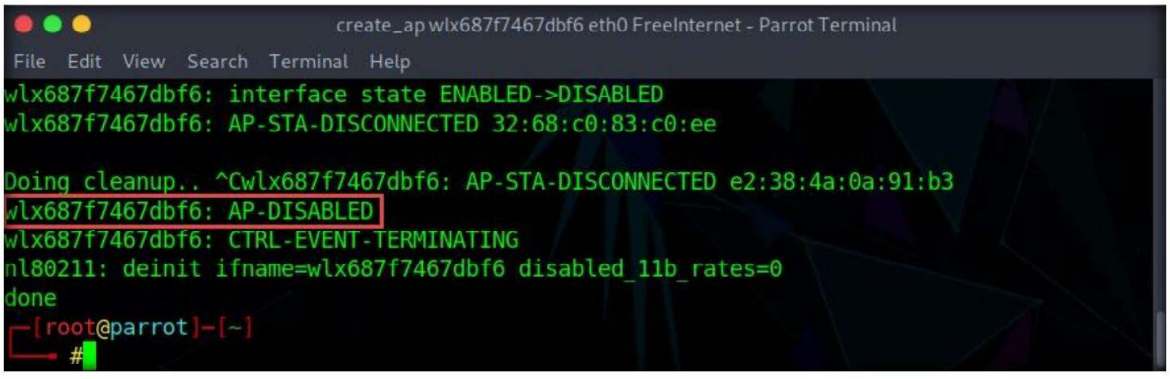
    Note: You may use any HTTP website of your choice to capture user credentials. However, if you decide to use an HTTPS website, you must enable Bettercap to capture HTTPS traffic.

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

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

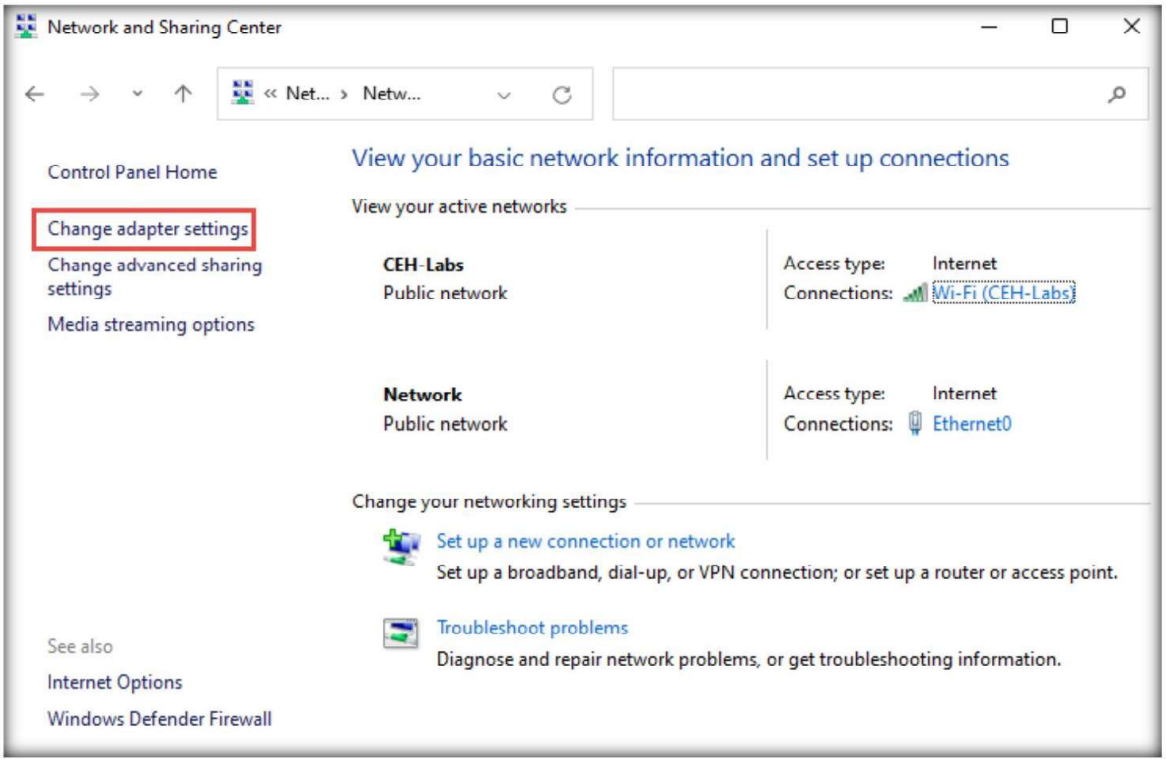


34. The captured credentials can be further used to gain unauthorized access to the victim's account.
35. Close the **Terminal** window and switch back to the previously opened **Terminal** window.
36. Type **Ctrl+C** and press **Enter** to disable the rogue access point (**FreeInternet**).

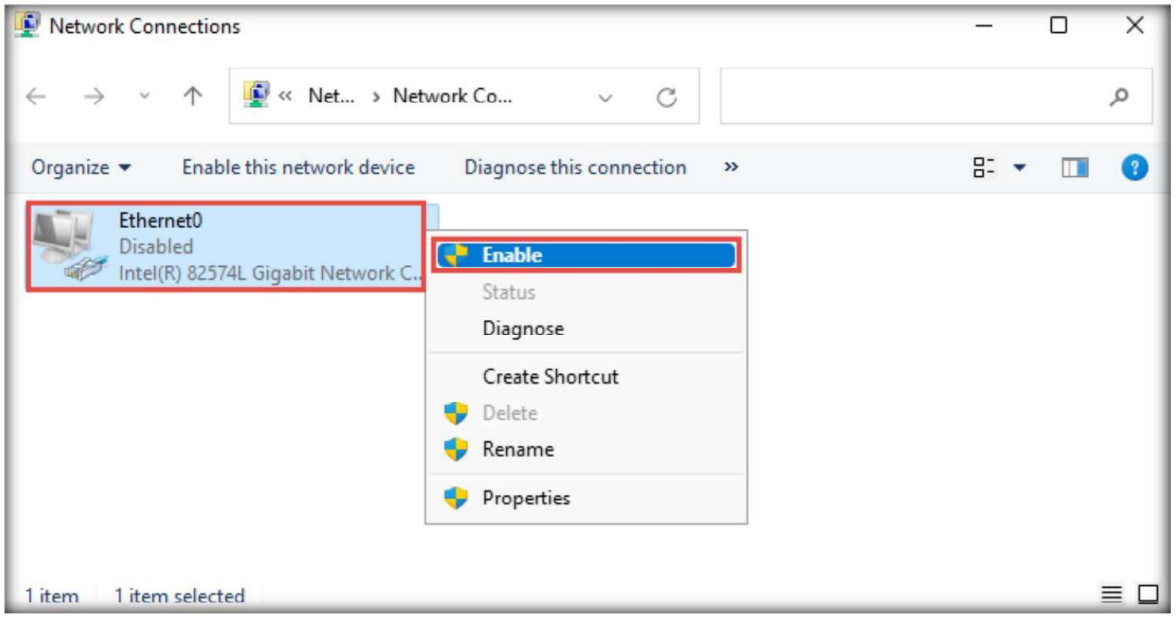


37. This concludes the demonstration of how to create a rogue access point and capture traffic using Bettercap.
38. Close all open windows and document all the acquired information.

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



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



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

Lab Analysis

Analyze and document the results of this lab exercise.

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

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