Hacking Wireless Networks

Module 16

Hacking Wireless Networks

Wi-Fi is developed on IEEE 802.11 standards and is widely used in wireless communication. It provides wireless access to applications and data throughout a radio network.

Lab Scenario

Wireless network technology is becoming increasingly popular, but at the same time, it has many security issues. A wireless local area network (WLAN) allows workers to access digital resources without being tethered to their desks. However, the convenience of WLANs also introduces security concerns that do not exist in a wired world. Connecting to a network no longer requires an Ethernet cable. Instead, data packets are airborne and available to anyone with ability to intercept and decode them. Several reports have explained weaknesses in the Wired Equivalent Privacy (WEP) algorithm by 802.11x standard to encrypt wireless data.

To be an expert ethical hacker and penetration tester, you must have sound knowledge of wireless concepts, wireless encryption, and their related threats. As a security administrator, you must protect your company's wireless network from hacking.

Lab Objectives

The objective of this lab is to protect the wireless network from attackers.

In this lab, you will learn how to:

- Capture and Analyze Wireless Network Traffic
- Crack WEP by using various tools
- Crack WPA by using various tools

Lab Environment

In this lab, you will need a web browser with an Internet connection.

- Windows 10 running as virtual machine
- Kali Linux running as virtual machine

Lab Duration

Time: 35 Minutes

Overview of Wireless Network

"Wireless network" refers to any type of computer network commonly associated with telecommunications, whose interconnections between nodes are implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves such as radio waves for the carrier. The implementation usually takes place at the physical level or layer of the network.

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in Wireless Networks are:

- WiFi Packet Sniffing using **Microsoft Network Monitor** and **Wireshark**
- Cracking a WEP Network with **Aircrack-ng**
- Cracking a WPA Network with **Aircrack-ng**

Lab Requirements

Before you start performing any labs in this module, you have to configure your environment so that you can connect your machine to a wireless network. You will need a wireless network adaptor and an access point for demo purpose.

In this lab we have used **Linksys 802.11 g WLAN** adaptor and **CEHLabs** as the access point for demonstration purpose. CEHLabs access point has been configured with WEP and WPA encryption as per the lab requirements of Lab 2 and Lab 3.

- First log-in to **Windows 10** virtual machine and then plug in the WLAN adaptor. **Removable Devices** window pops up, click **OK** to proceed as shown in the screenshot.

FIGURE 1: Removable Devices pop-up window

- Now right-click your VM's tab in the vmware menu bar and click **Removable Devices → Linksys 802.11 g WLAN → Connect (Disconnect from Host)** as shown in the screenshot.

FIGURE 2: Connecting the wireless adaptor to the VM

- Now in your virtual machine, open **Network and Sharing Center** and click **Change adapter settings**.

  Note: You can find Network and Sharing Center option in the Control Panel.

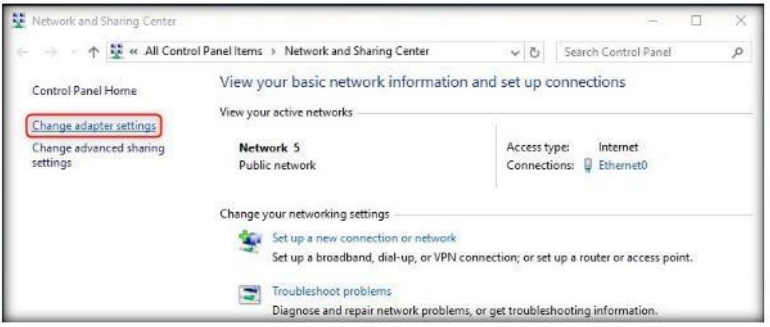

FIGURE 3: Network and Sharing Center window

- In the **Network Connections** window, first **disable** your wired network interface (here **Ethernet0**) by selecting the network interface, right-click on it and click **Disable**.

  Note: If a pop-up appears, click Yes.

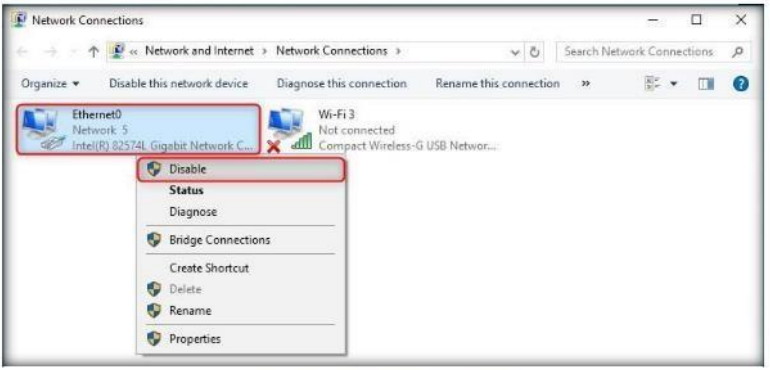

FIGURE 4: Network Connections window

- Now select your wireless interface (here **Wi-Fi 3**) and click **Connect To** button from the menu bar.

FIGURE 5: Connecting to the wireless network

- **Settings** window appears with **Wi-Fi** settings being shown as default, select your wireless interface and click **Connect** as shown in the screenshot.

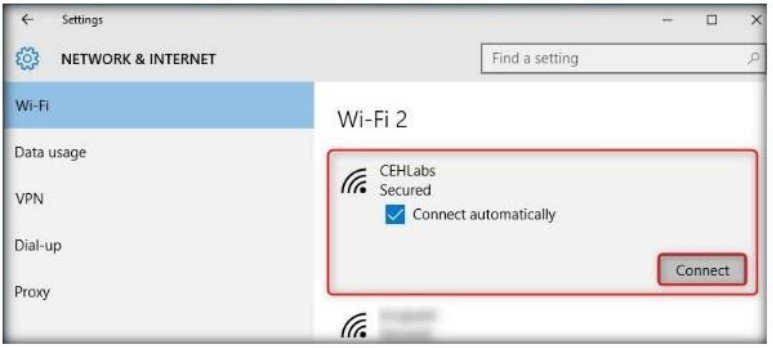

FIGURE 6: Connecting to the wireless network

- You will have to enter the network **security key** and click **Next** to connect.

FIGURE 7: Connecting to the wireless network

- The virtual machine connects to the wireless network interface as shown in the screenshot.

FIGURE 8 Wireless network connected

- In this way, you can connect a wireless network to your virtual machines. Repeat similar steps if you are using the wireless network with other virtual machine.

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

Lab Analysis

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

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

Lab 1

WiFi Packet Sniffing using Microsoft Network Monitor and Wireshark

Microsoft Network Monitor is a packet analyzer which enables capturing, viewing, and analyzing network data and deciphering network protocols.

Lab Scenario

Wireless networks can be open to active or passive attacks. These attacks include DoS, MITM, spoofing, jamming, war driving, network hijacking, packet sniffing, and many more. Passive attacks that take place on wireless networks are common and are difficult to detect since the attacker usually just collects information. Active attacks happen when a hacker has gathered information about the network after a successful passive attack. Sniffing is the act of monitoring the network traffic using legitimate network analysis tools. Hackers can use monitoring tools, including AiroPeek, Ethereal, TCPDump, or Wireshark, to monitor the wireless networks. These tools allow hackers to find an unprotected network that they can hack. Your wireless network can be protected against this type of attack by using strong encryption and authentication methods.

In this lab, we use Microsoft Network Monitor, a tool that can sniff network using a wireless adapter. Because you are the ethical hacker and a penetration tester of an organization, you need to check the wireless security and evaluate weaknesses present in your organization.

Lab Objectives

The objective of this lab is to capture and analyze wireless packets in a network.

Lab Environment

To execute this lab, you will need:

- Run this lab in **Windows 10** machine
- Administrative privileges to run tools
- A client connected to a wireless access point

Lab Duration

Time: 10 Minutes

Overview of Network Monitoring

A network monitoring system gives you a full overview of what's going on in your network at all times. A network monitor has the ability to manage multiple servers and can also manage data from multiple devices such as switches, routers, firewalls, etc. Learning to monitor your network is a great way to know the stress on your network infrastructure and to see what kind of demands it can handle from the users. By knowing about all the overview information, it helps you to troubleshoot your network and a good amount of data to build your future growth plan for your networking infrastructure.

Lab Tasks

1. Navigate to **Start → All Apps → Microsoft Network Monitor 3.4** and click **Microsoft Network Monitor 3.4** to launch the application. The application main window appears as shown in the screenshot.

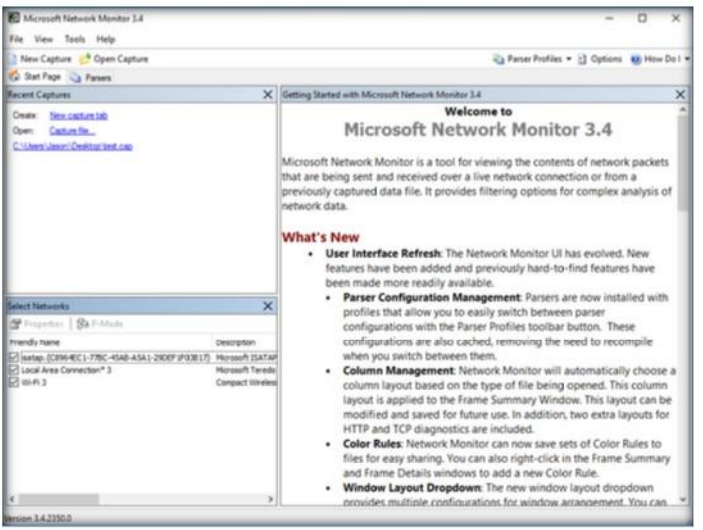

FIGURE 1.1: Microsoft Network Monitor 3.4 main window

2. In the **Select Networks** window on the bottom-left, check only the wireless interface (here **Wi-Fi 3**) and leave the other options unchecked.

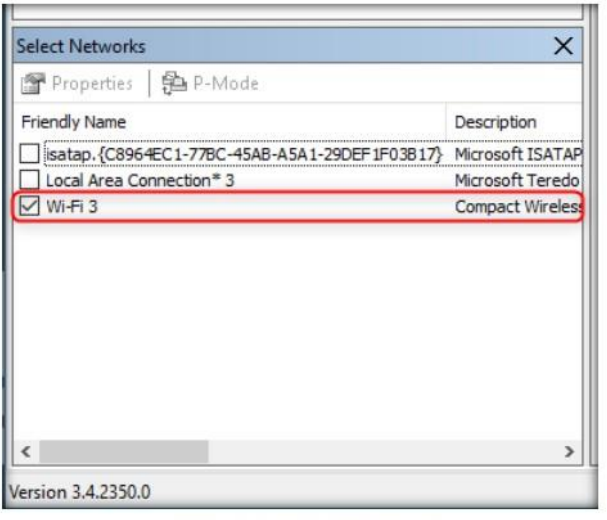

FIGURE 1.2: Selecting the network interface

3. Now click the **New Capture** button present in the menu bar, as shown in the screenshot.

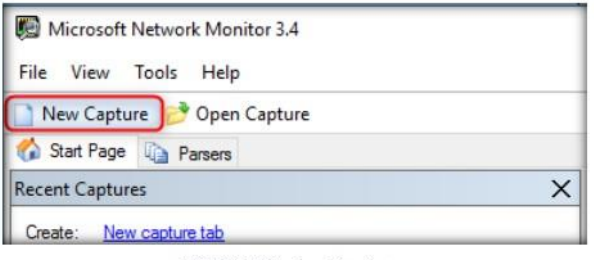

FIGURE 1.3: Opening a New Capture

4. Now click the **Capture Settings** button from the menu bar.

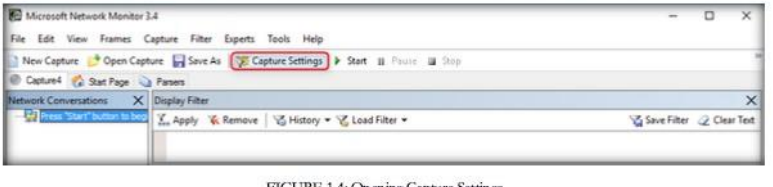

FIGURE 1.4: Opening Capture Settings

5. Capture Settings window opens, **double-click** on the wifi adapter (here **Wi-Fi 3**) in the **select network adapters to capture** section.

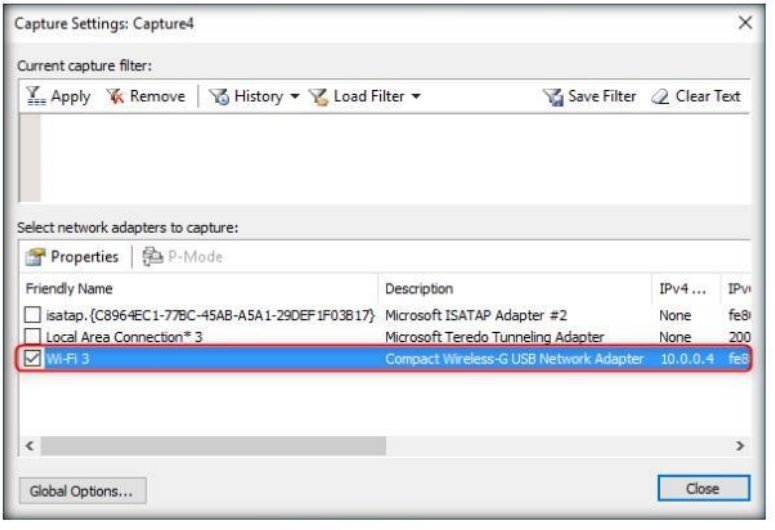

FIGURE 1.5: Capture Settings window

6. **Network Interface Configuration** window opens, click **Scanning Options** button.

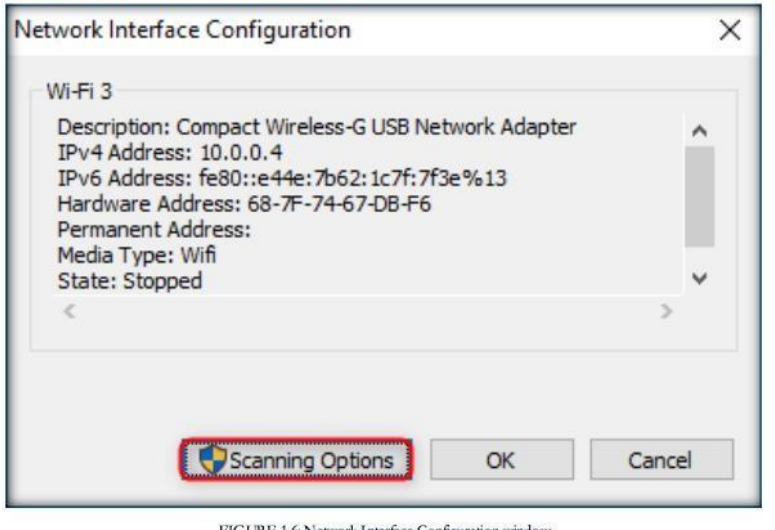

FIGURE 1.6: Network Interface Configuration window

7. **WiFi Scanning Options** window appears, tick the **Switch to Monitor Mode** checkbox and click **Apply** button as shown in the screenshot.

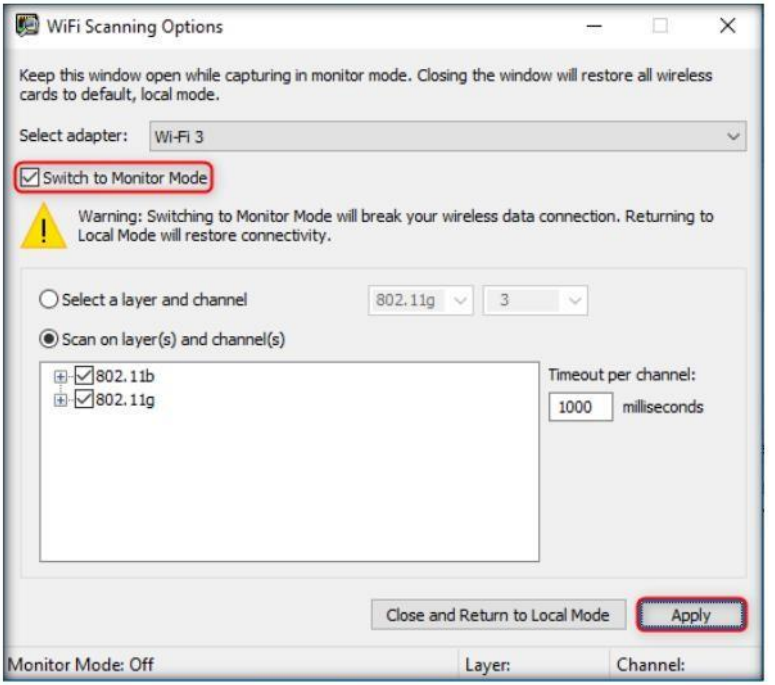

FIGURE 1.7: WiFi Scanning Options window

8. Now **close** the Scanning Options window by clicking the cross button on the title bar.

Note: Do **not** press the **Close and Return to Local Mode** button or your settings will be reset.

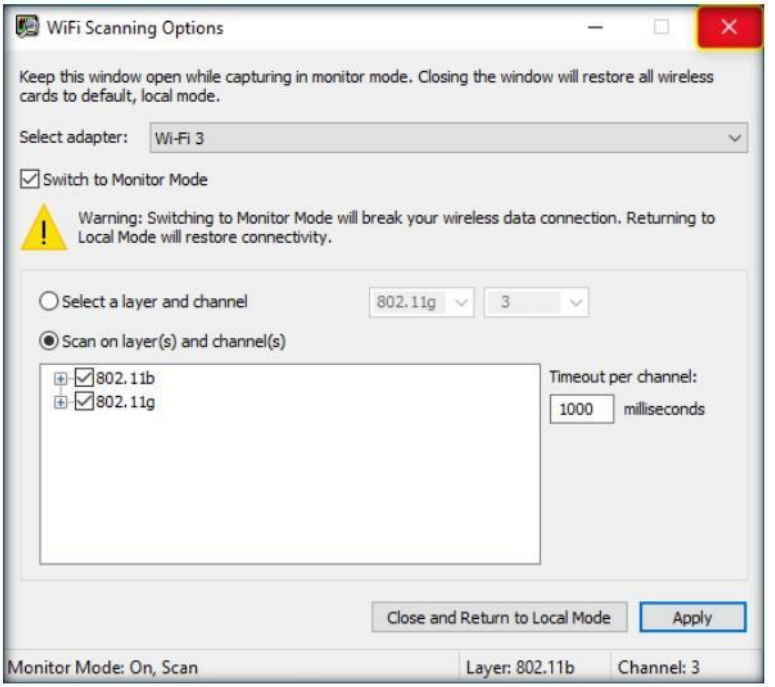

FIGURE 1.8: WiFi Scanning Options window

9. Close the **Network Interface Configuration** by clicking the **OK** button.

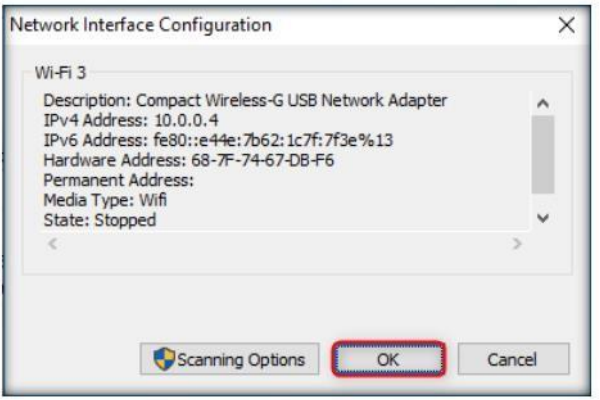

FIGURE 1.9: Network Interface Configuration window

10. Close the **Capture Settings** window by clicking the **Close** button as given in the screenshot.

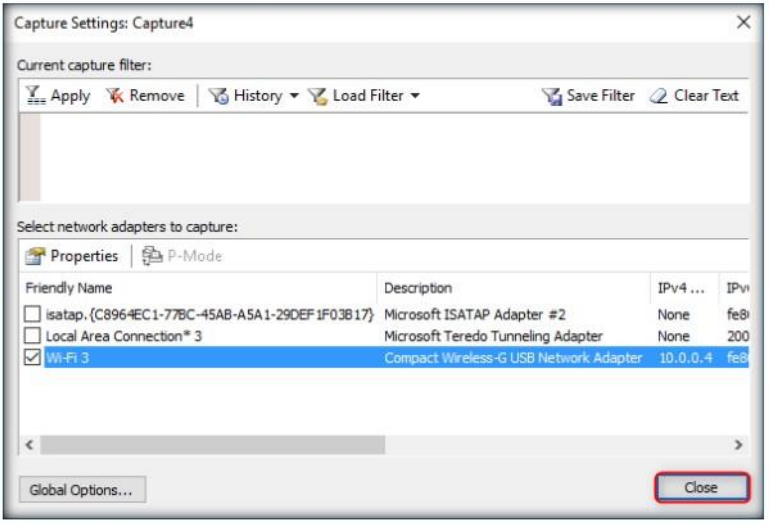

FIGURE 1.10: Capture Settings window

11. Click **Start** in the menu bar to begin your network monitoring.

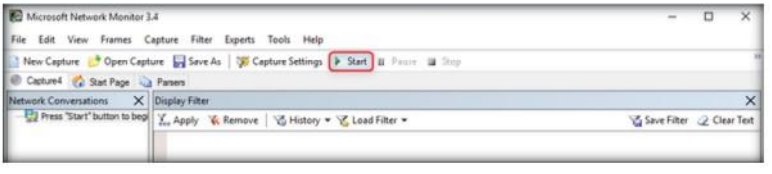

FIGURE 1.11: Starting the packet capture

12. The application starts capturing packets and displays them in the **Frame Summary** window. You can see the number of captured packets at the bottom as shown in the screenshot.

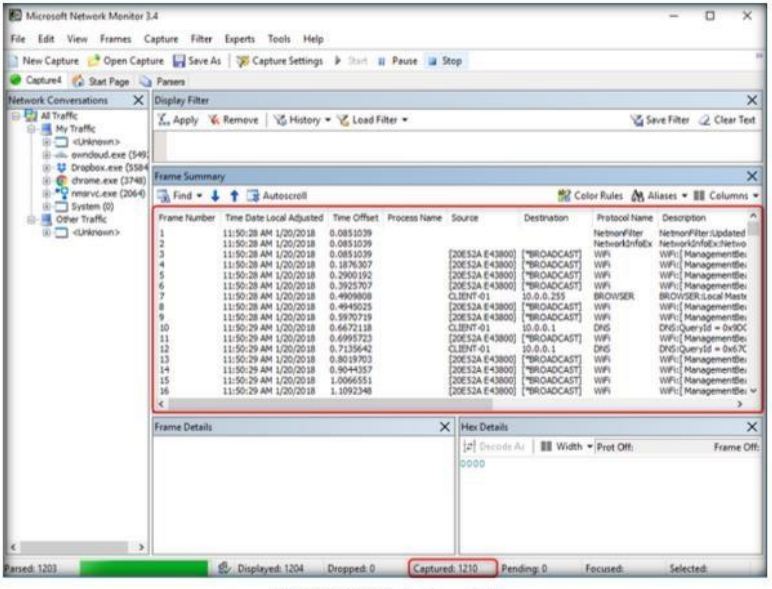

FIGURE 1.12: Packet capture started

13. Keep the packet capture running for a few minutes and then click the **Stop** button in the menu bar.

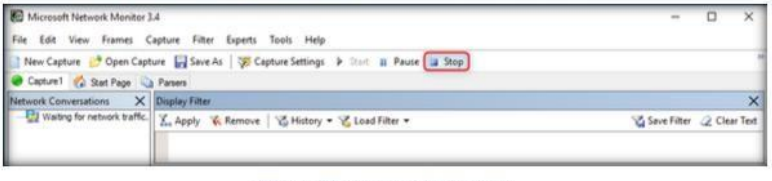

FIGURE 1.13: Stopping the packet capture

14. Now click the **Save As** button as shown in the screenshot.

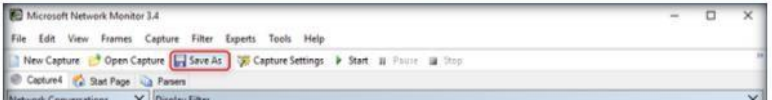

FIGURE 1.14: Saving the captured packets

15. **Save As** window appears, select a location and input the filename (here **Desktop** and **test**) and click the **Save** button.

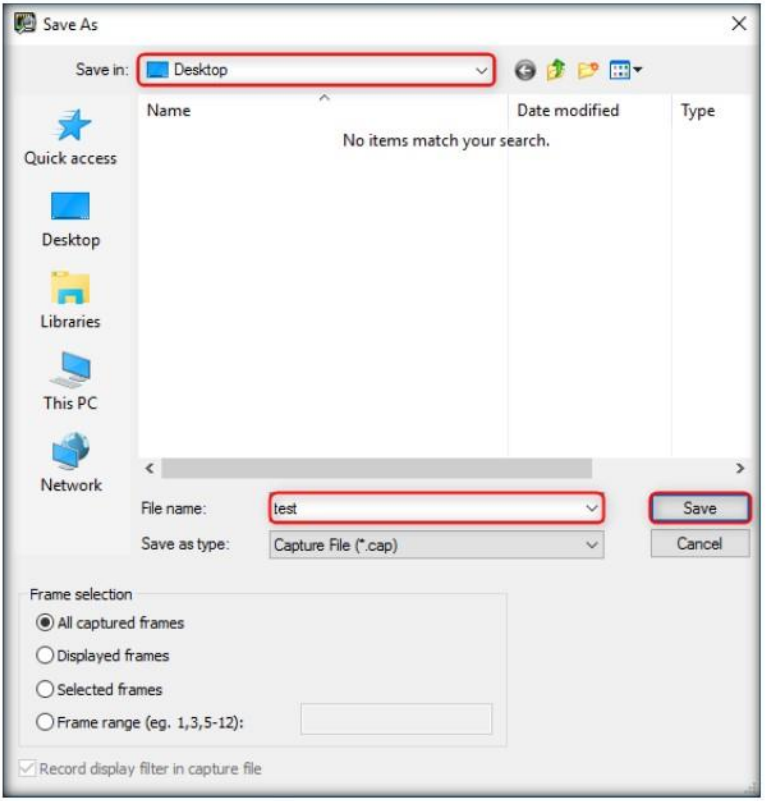

FIGURE 1.15: Saving the captured packets

16. Now launch **wireshark**. The wireshark main window appears, as shown in the following screenshot:

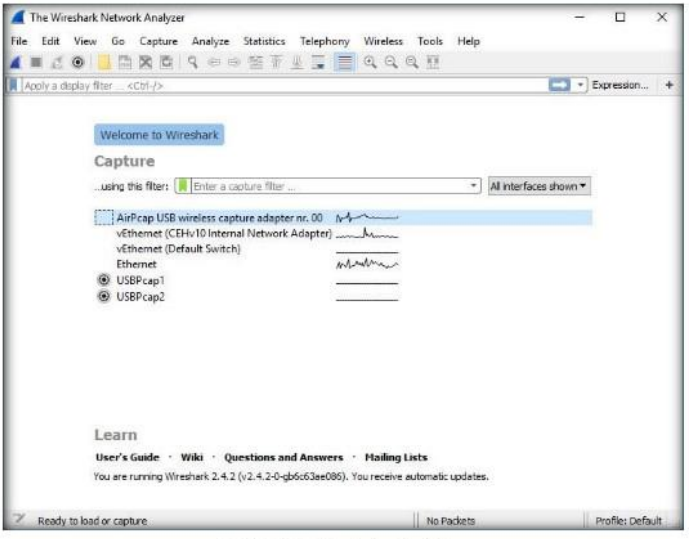

FIGURE 1.16: Wireshark main window

17. In the wireshark main window, click **File → Open** to view the saved packet capture file for analysis.

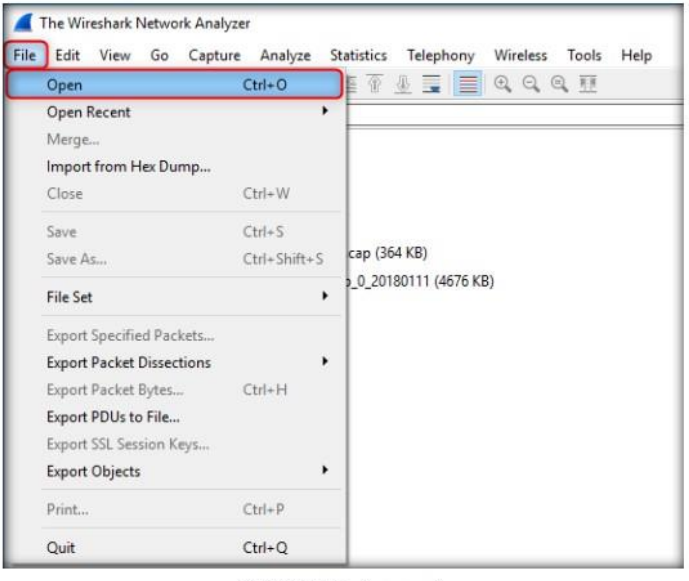

FIGURE 1.17: Opening test.cap file

18. **Wireshark: Open Capture File** window appears, select the **test.cap** file and click **Open**.

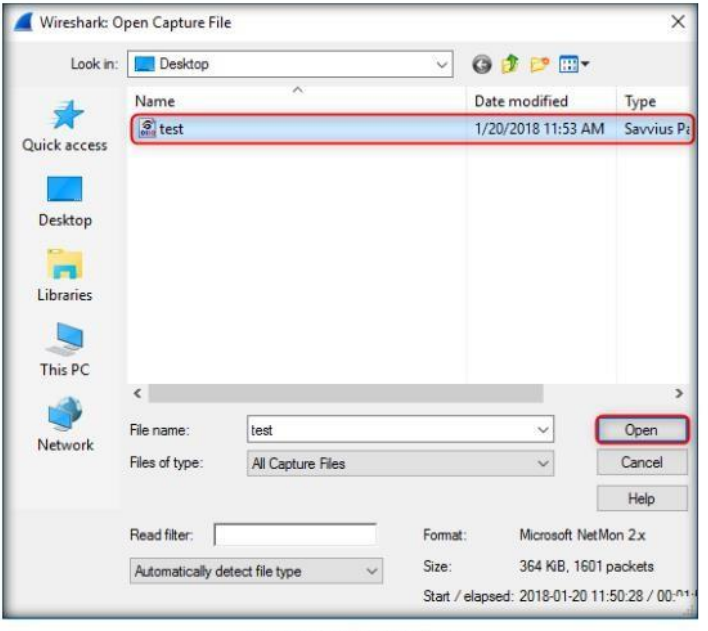

FIGURE 1.18: Opening test.cap file

19. The **test.cap** file opens in Wireshark window showing you the details of the packet for analysis. Here you can see the wireless packets captured which were otherwise masked to look like ethernet traffic.

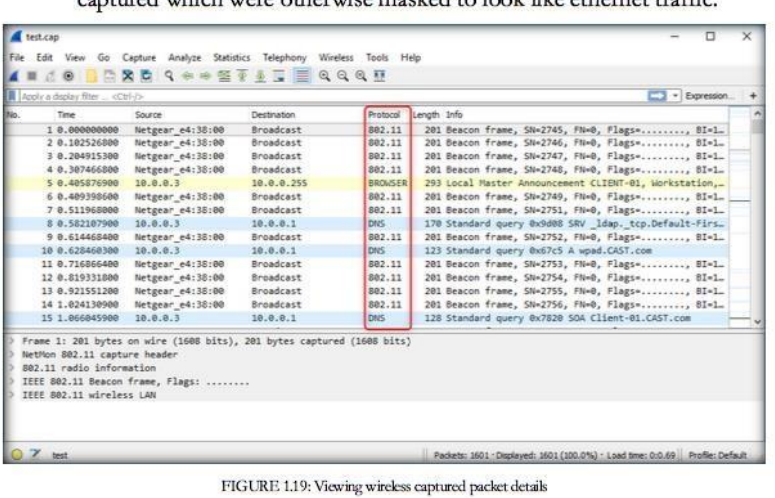

FIGURE 1.19: Viewing wireless captured packet details

20. You can access the saved packet capture file anytime, and by issuing packet filtering commands in the Filter field, you can narrow down the packet search in an attempt to find packets containing sensible information.
21. In real time, attackers enforce packet capture and packet filtering techniques to capture packets containing passwords (only for websites implemented on HTTP channel), perform attacks such as session hijacking, and so on.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

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

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

Lab

2

Cracking a WEP Network with Aircrack-ng

Aircrack-ng is an 802.11 WEP and WPA-PSK keys–cracking program that recovers keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, and the all-new PTW attack, thus making this attack much faster than those using other WEP cracking tools.

Lab Scenario

Network administrators can take steps to help protect their wireless network from outside threats and attacks. Most hackers will post details of any loops or exploits online, and if they find a security hole, attackers will descend in droves to test your wireless network with it.

WEP is used for wireless networks; always change your SSID from the default, before you actually connect the wireless router to the access point. If an SSID broadcast is not disabled on an access point, the use of a DHCP server to automatically assign IP address to wireless clients should not be used, because war-driving tools can easily detect your internal IP address if the SSID broadcasts are enabled and the DHCP is being used.

As an ethical hacker and penetration tester of an organization, your IT director will assign you the task of testing wireless security, exploiting the flaws in WEP, and cracking the keys present in your organization's WEP. In this lab, we discuss how WPA keys are cracked using standard attacks such as KoreK and PTW.

Lab Objectives

The objective of this lab is to protect wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Lab Environment

To execute this lab, you will need:

- A Windows 10 virtual machine running
- Kali Linux virtual machine
- **Before starting this lab make sure that the Wireless Access point is configured in WEP Encryption in Windows 10 machine**
- **This lab requires wireless network adapter installed on your machine. If you don't have this adapter, please do not proceed to the lab.**

Lab Duration

Time: 15 Minutes

Overview of WEP (Wired Equivalent Privacy) Encryption

WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of **security and privacy** comparable to a wired LAN. WEP **uses a 24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission. It has significant vulnerabilities and design flaws and **can be easily cracked**.

Lab Task

1. Launch a **Kali Linux** virtual machine and login as **root/toor**.
2. Open a **terminal** window from the taskbar.
3. In a terminal window type **airmon-ng** and press **Enter**. To find the wireless adapter

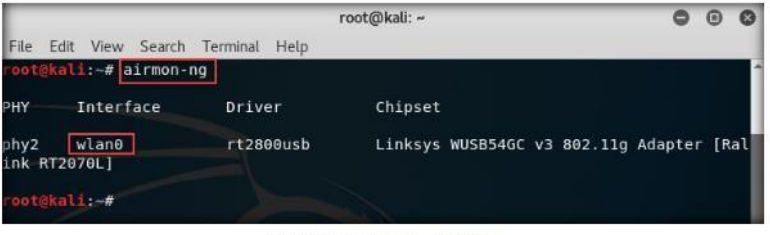

FIGURE 2.1: airmon-ng Identifying

4. Now put the wireless adapter into monitor or promiscuous mode, to do this type **airmon-ng start wlan0** and press **Enter**.

5. By issuing this command **airmon** will change the interface name as **wlan0mon** as shown in the screenshot.

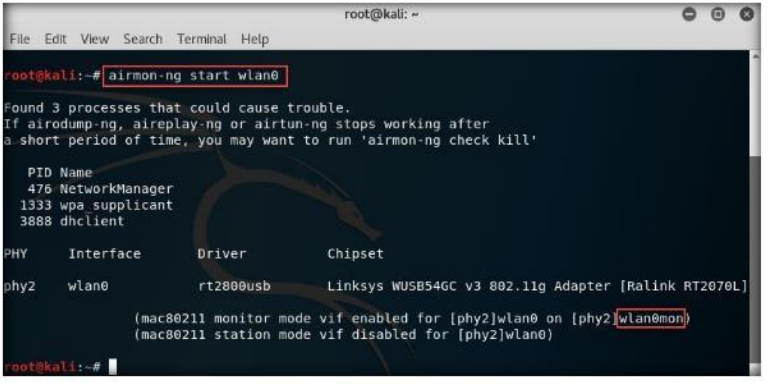

FIGURE 2.2: Starting airmon-ng in Monitor mode

6. Use **airodump-ng** to get the list of detected access points, and also a list of connected clients ("stations").

7. Type **airodump-ng wlan0mon** and press **Enter**. By issuing this command we can see all the available Access Points (APs) and clients within our range.

8. In this lab we are choosing CEHLabs to perform the WEP cracking.

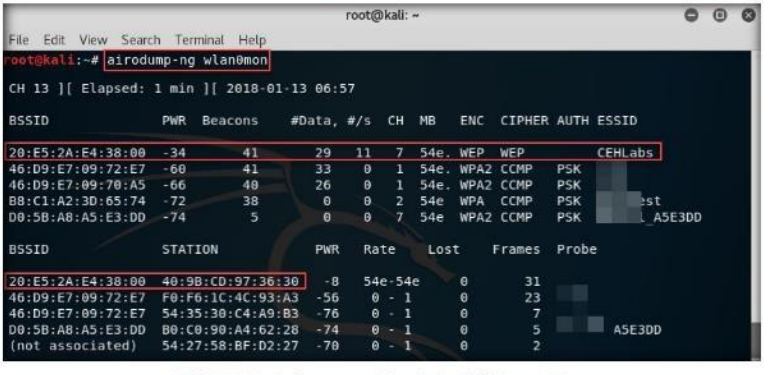

FIGURE 2.3: airodump-ng searching for Available Access Points

9. Before proceeding, check if the injection attack can be performed on the target AP.

10. Now, open a new terminal window and type **aireplay-ng -9 -e CEHLabs -a 20:E5:2A:E4:38:00 wlan0mon** and press **Enter**.

11. In the above command, where:
    a. **-9** is for Injection Test
    b. **-e CEHLabs** is Wirelesss Network Name
    c. **-a 20:E5:2A:E4:38:00** is the MAC address of the Access Point
    d. **wlan0mon** is the wireless interface name
12. While performing this process you should receive message as **Injection is working!** as shown in the screenshot.

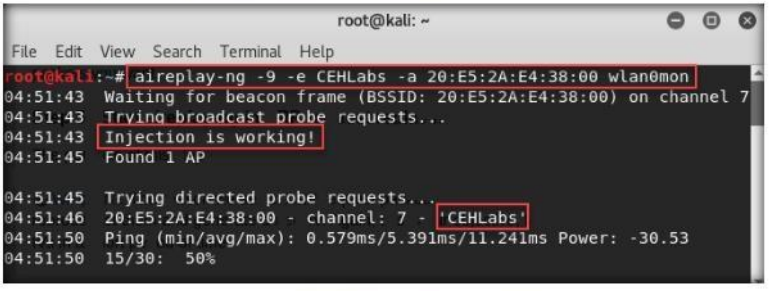

FIGURE 2.4: aireplay-ng performing injection attack

13. Next, start airodump-ng to capture the **Initialization Vector (IV)** from the AP.
14. By running this command airodump-ng will capture the IVs generated from the specific Access Point.
15. Open a new terminal window and type **airodump-ng --bssid 20:E5:2A:E4:38:00 -c 7 -w WEPcrack wlan0mon** and press **Enter**.
    a. **--bssid 20:E5:2A:E4:38:00** is the access point MAC address. This eliminates extraneous traffic.
    b. **-c 7** is the channel number for CEHLabs network
    c. **-w WEPcrack** is the name to be prefix for the file which contains the IVs.
    d. **wlan0mon** is the interface name.

FIGURE 2.5: airodump-ng capturing the IVs for selected Access Point

16. Next, we need to generate traffic between the AP and the station. Open another terminal type **aireplay-ng -3 -b 20:E5:2A:E4:38:00 -h 40:9B:CD:97:36:30 wlan0mon** and press **Enter**.

17. It will generate ARP traffic in the network. The reason for choosing the ARP request packets is because the Access Points will usually rebroadcast them and this will generate the new IV.

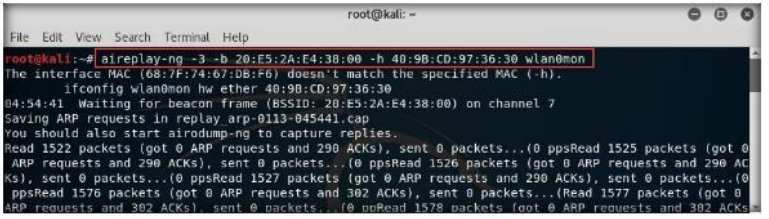

FIGURE 2.6: aireplay-ng generating traffic

18. The source MAC address should be associated with the access point in order to accept the packet. The source MAC address, which is used to inject the packets has no connection with the Access Point; so the AP usually ignores the packets and sends out a **DeAuthentication** packet in a clear text. In order to create a fake authentication, we need to associate it with the Access Point.

19. Next, use aireplay-ng to do a fake authentication with the access point, this will generate authentication packets in the traffic. Open a new terminal type **aireplay-ng -1 0 -e CEHLabs -a 20:E5:2A:E4:38:00 -h 40:9B:CD:97:36:30 wlan0mon** and press **Enter**.

    a. **-1** means fake authentication

    b. **0** reassociation timing in seconds

    c. **-e CEHLabs** is the wireless network name

    d. **-a 20:E5:2A:E4:38:00** is the access point MAC address

    e. **-h 40:9B:CD:97:36:30** is our card MAC address

    f. **wlan0mon** is the wireless interface name

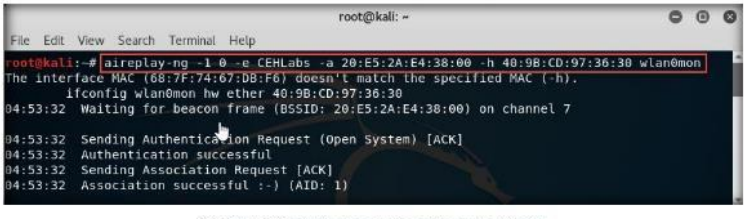

FIGURE 2.7: aireplay-ng creating a fake authentication

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

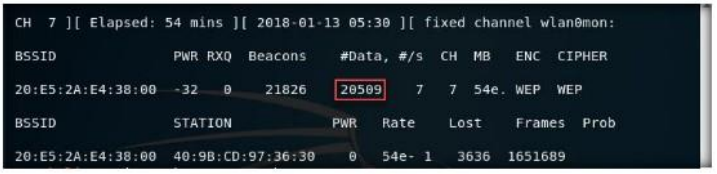

FIGURE 2.8: Stop capturing the packets in airodump-ng

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

22. By issuing the above command aircrack-ng will crack the WEP key of the CEHLabs as shown in the screenshot.

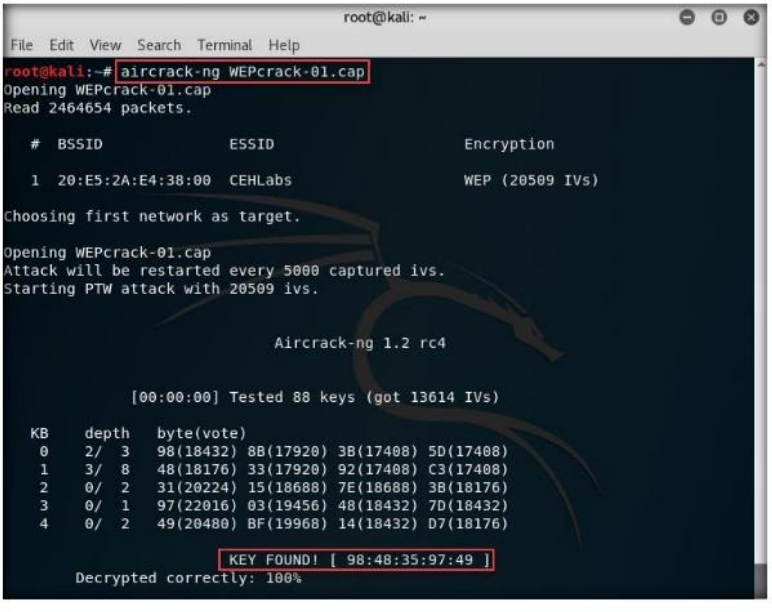

FIGURE 2.9: aircrack-ng recovering WEP key

23. Now we will be connecting the CEHLabs access point. To do this navigate to the top right-side corner of the desktop and click the down arrow icon as shown in the screenshot, and click Wi-Fi connectivity to search for available Access Points.

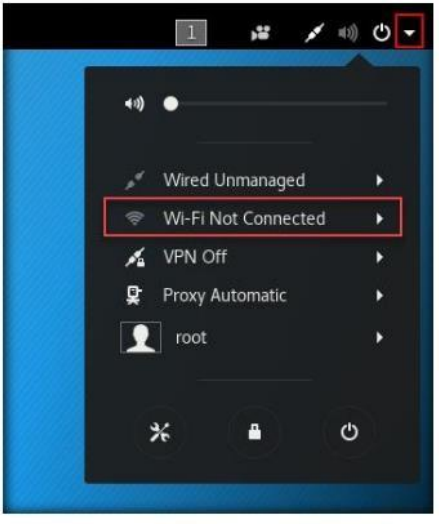

FIGURE 2.10: Connecting to CEHLabs Access Point

24. It will display the available Access Points, click CEHLabs access point from the list. As soon as you click on the CEHLabs Access point, it will prompt you for the Authentication pop-up.

25. Type the key that you have cracked in the **Task 5**, and click **Connect**.

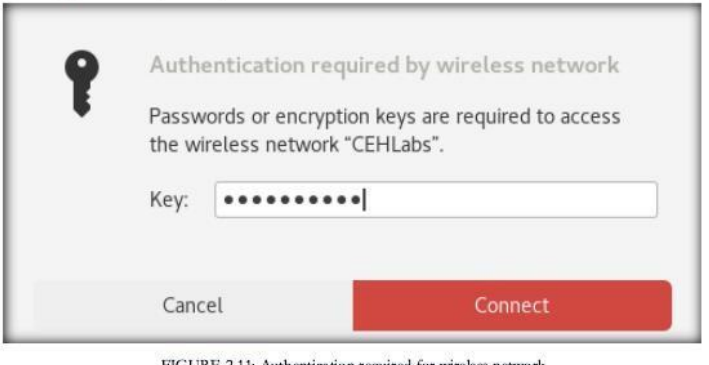

FIGURE 2.11: Authentication required for wireless network

26. Once you click Connect button on the Authentication required pop-up, you will be connected to the **CEHLabs** access point as shown in the screenshot.

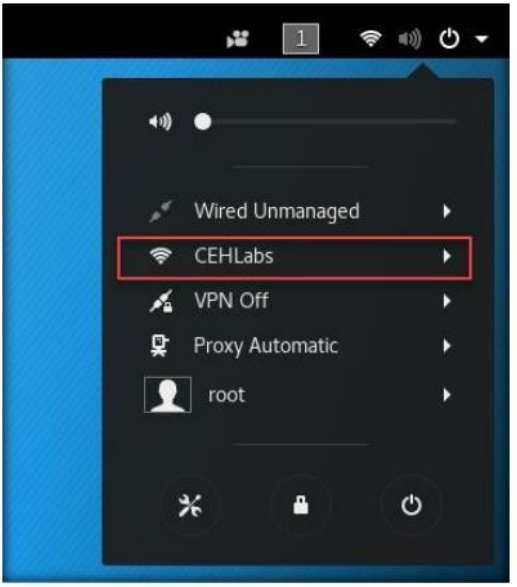

FIGURE 2.12: Connected to CEHLabs access point

27. An attacker uses this key to connect to the access point and then enters the respective network. Once he/she enters the network, he/she can use scanning tools to scan for open devices, perform vulnerability analysis, and then start exploiting them.

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Airecrack-ng attacks and their respective data packet generation rate.

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

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

Lab

3

Cracking a WPA Network with Aircrack-ng

Aircrack-ng is an 802.11 WEP and WPA-PSK keys–cracking program that recovers keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, and the all-new PTW attack, thus making this attack much faster than those using other WEP cracking tools.

Lab Scenario

Network administrators can take steps to help protect their wireless network from outside threats and attacks. Most hackers will post details of any loops or exploits online, and if they find a security hole, attackers will descend in droves to test your wireless network with it.

WEP is used for wireless networks; always change your SSID from the default before you actually connect the wireless router to the access point. If an SSID broadcast is not disabled on an access point, the use of a DHCP server to automatically assign IP address to wireless clients should not be used, because war-driving tools can easily detect your internal IP address if the SSID broadcasts are enabled and the DHCP is being used.

As an ethical hacker and penetration tester of an organization, your IT director will assign you the task of testing wireless security, exploiting the flaws in WEP, and cracking the keys present in your organization's WEP. In this lab, we discuss how WPA keys are cracked using standard attacks such as KoreK and PTW.

Lab Objectives

The objective of this lab is to protect wireless network from attackers.

In this lab, you will learn how to:

- Crack WPA using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Lab Environment

To execute this lab, you will need:

- A Windows 10 virtual machine running
- Kali Linux virtual machine
- **Before starting this lab make sure that the Wireless Access point is configured in WPA Encryption in Windows 10 machine**
- **This lab requires wireless network adapter installed on your machine. If you don't have this adapter, please do not proceed with the lab.**

Lab Duration

Time: 10 Minutes

Overview of WPA (Wi-Fi Protected Access) Encryption

WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes **the RC4 stream cipher encryption** with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption, and authentication. WPA uses TKIP to eliminate the weaknesses of WEP by including **per-packet mixing functions, message integrity checks, extended initialization vectors**, and **re-keying mechanisms**. 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 mode** with strong security.

Lab Task

1. Launch a **Kali Linux** virtual machine and login as **root/toor**.
2. Open a **terminal** window from the taskbar.
3. In a terminal window type **airmon-ng** and press **Enter**. To find the wireless adapter

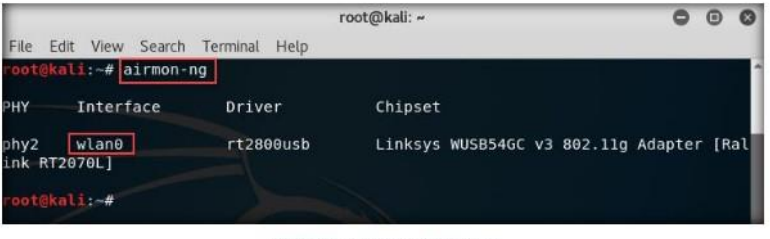

FIGURE 3.1: airmon-ng Identifying

4. Now put the wireless adapter into monitor or promiscuous mode, to do this type **airmon-ng start wlan0** and press **Enter**.

5. By issuing this command airmon will change the interface name as **wlan0mon** as shown in the screenshot.

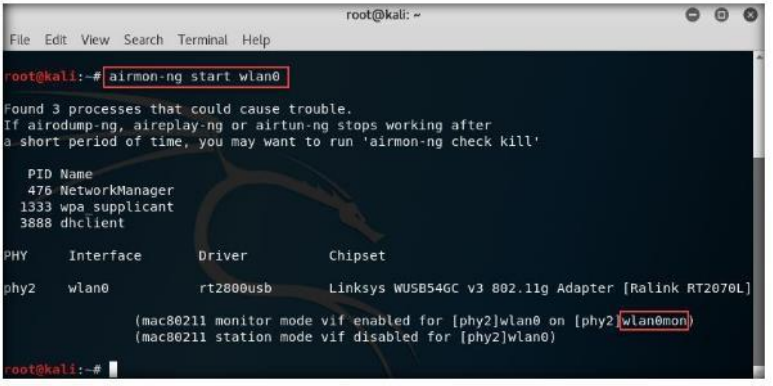

FIGURE 3.2: Starting airmon-ng in Monitor mode

6. Use **airodump-ng** to get the list of detected access points, and also a list of connected clients ("stations").
7. Type **airodump-ng wlan0mon** and press **Enter**. By issuing this command we can see all the available Access Points (APs) and clients with in our range.
8. In this lab we are choosing CEHLabs to perform the WEP cracking.

FIGURE 3.3: Launching airodump-ng

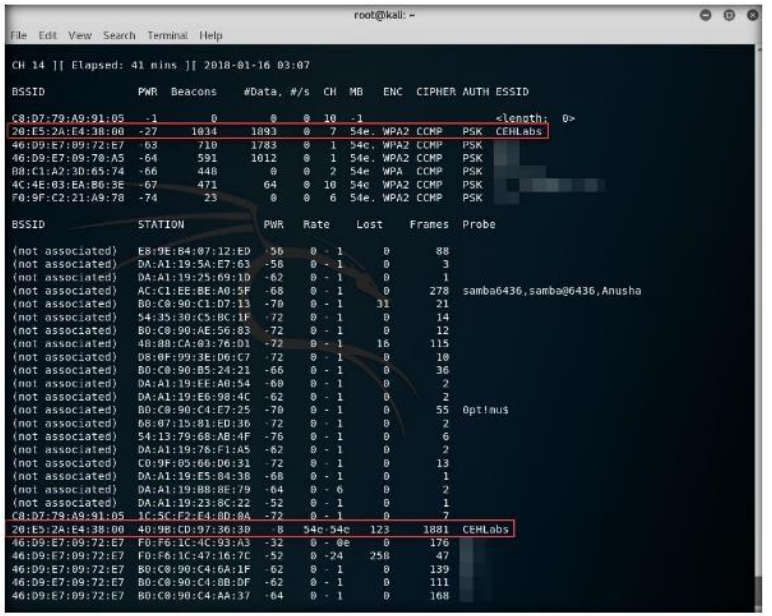

FIGURE 3.4: airodump-ng searching for Available Access Points

9. Next, start airodump-ng to capture the packets from the AP.
10. Now open a new terminal and type **airodump-ng --bssid 20:E5:2A:E4:38:00 -c 7 -w WPA2crack wlan0mon** and press **Enter**. Leave airodump-ng running.

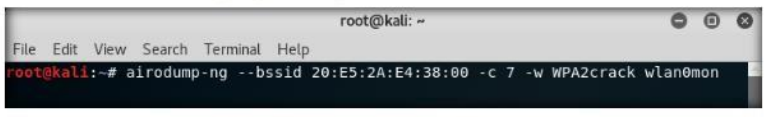

FIGURE 3.5: Starting airodump-ng to capture the packets

FIGURE 3.6: airodump-ng capturing the packets

11. Now, open a new terminal window and type **aireplay-ng –0 2 –a 20:E5:2A:E4:38:00 –c 40:9B:CD:97:38:00 wlan0mon** and press **Enter**.

12. In the above command:
    a. **-0** is the short-cut for the death mode
    b. **2** is the no.of deauth packets which need to be send
    c. **-a** is the access points bssid of the target network
    d. **-c** is the clients bssid
    e. **wlan0mon** is the monitor interface

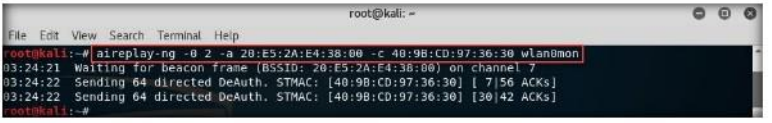

FIGURE 3.7: aireplay-ng generating traffic

13. Switch back to the **terminal** where airodum-ng is running and press **Ctrl+C** to stop the capture.

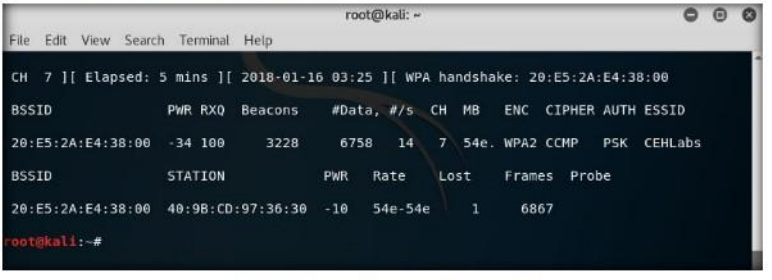

FIGURE 3.8: Stop airodump-ng traffic capture

14. Now open a new terminal window and type **aircrack-ng -a2 -b 20:E5:2A:E4:38:00 -w /usr/share/wordlists/2017 WPA2crack-01.cap** and press **Enter**.
    a. **-a** is the technique used to crack the handshake, 2=WPA technique.
    b. **-b** refers to bssid; replace with the BSSID of the target router.
    c. **-w** stands for wordlist; provide the path to a wordlist.

15. In this lab, we have already created a **wordlists** folder and placed in the above mentioned path.

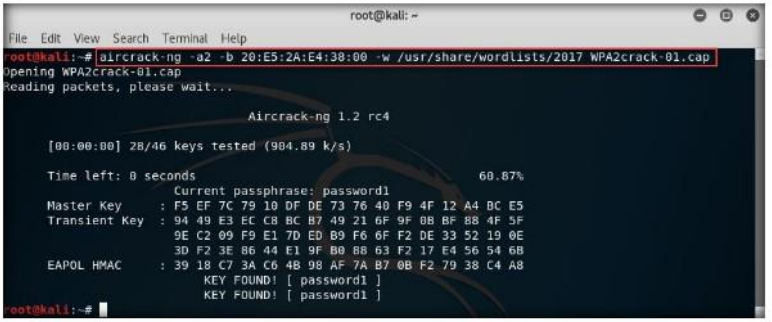

FIGURE 3.9: aircrack-ng WPA key cracked

16. An attacker uses this key to connect to the access point and then enters the respective network. Once he/she enters the network, he/she can use scanning tools to scan for open devices, perform vulnerability analysis, and then start exploiting them.

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Airecrack-ng attacks and their respective data packet generation rate.

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

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