Module 16: Hacking Wireless Networks

Lab 1: Perform Wireless Traffic Analysis

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

- Wi-Fi packet analysis using Wireshark

Overview of Wireless Traffic Analysis

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

Task 1: Wi-Fi Packet Analysis using Wireshark

Wireshark is a network protocol sniffer and analyzer. It lets you capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting. Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

Here, we will use Wireshark to analyze captured Wi-Fi packets.

In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (**WPA2crack-01.cap**) to analyze wireless packets.

1. By default, **Windows 11** machine selected, click Ctrl+Alt+Delete and login with **Admin/Pa$$w0rd**.

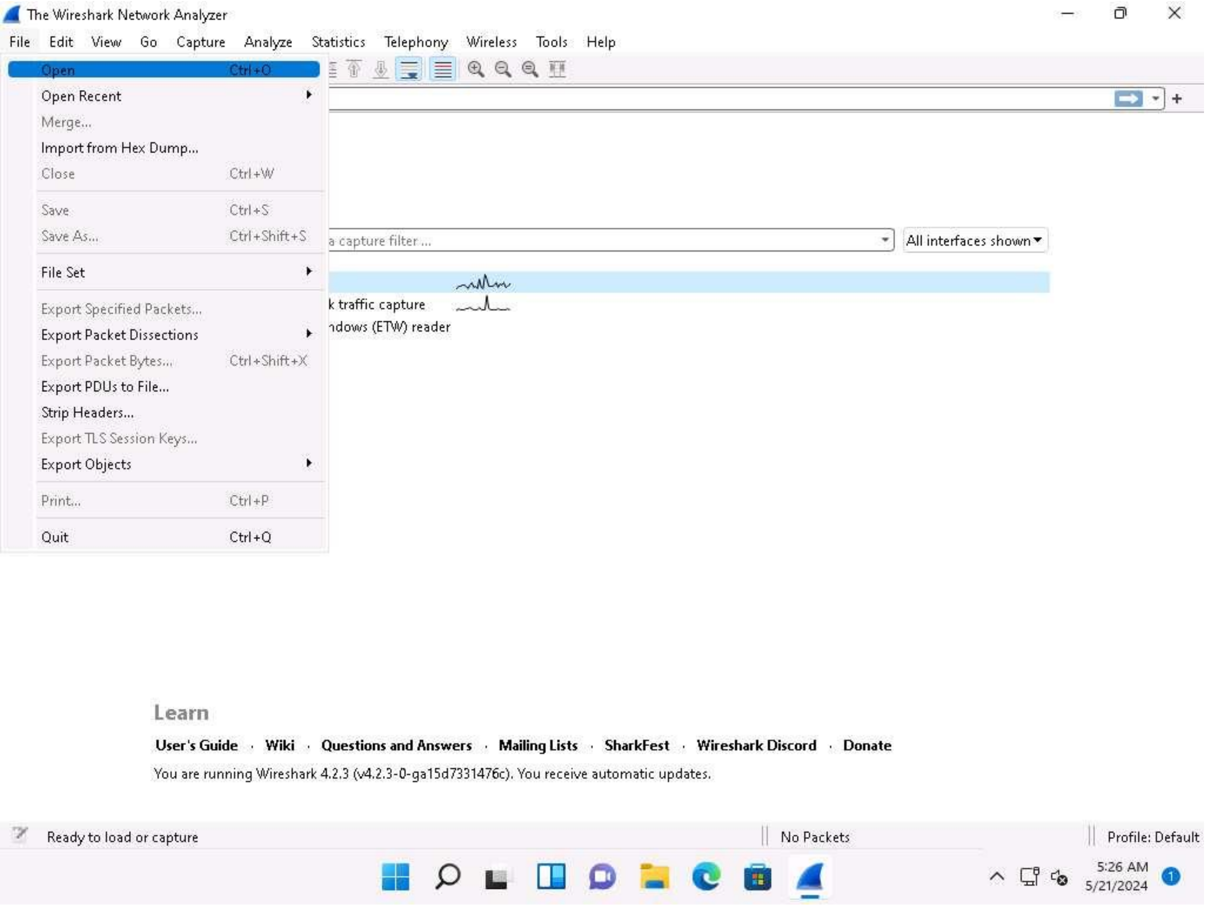
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

2. Click windows **Search** icon on the **Desktop**, search for **Wireshark** in the search bar and launch it.

3. The **Wireshark Network Analyzer** window appears.

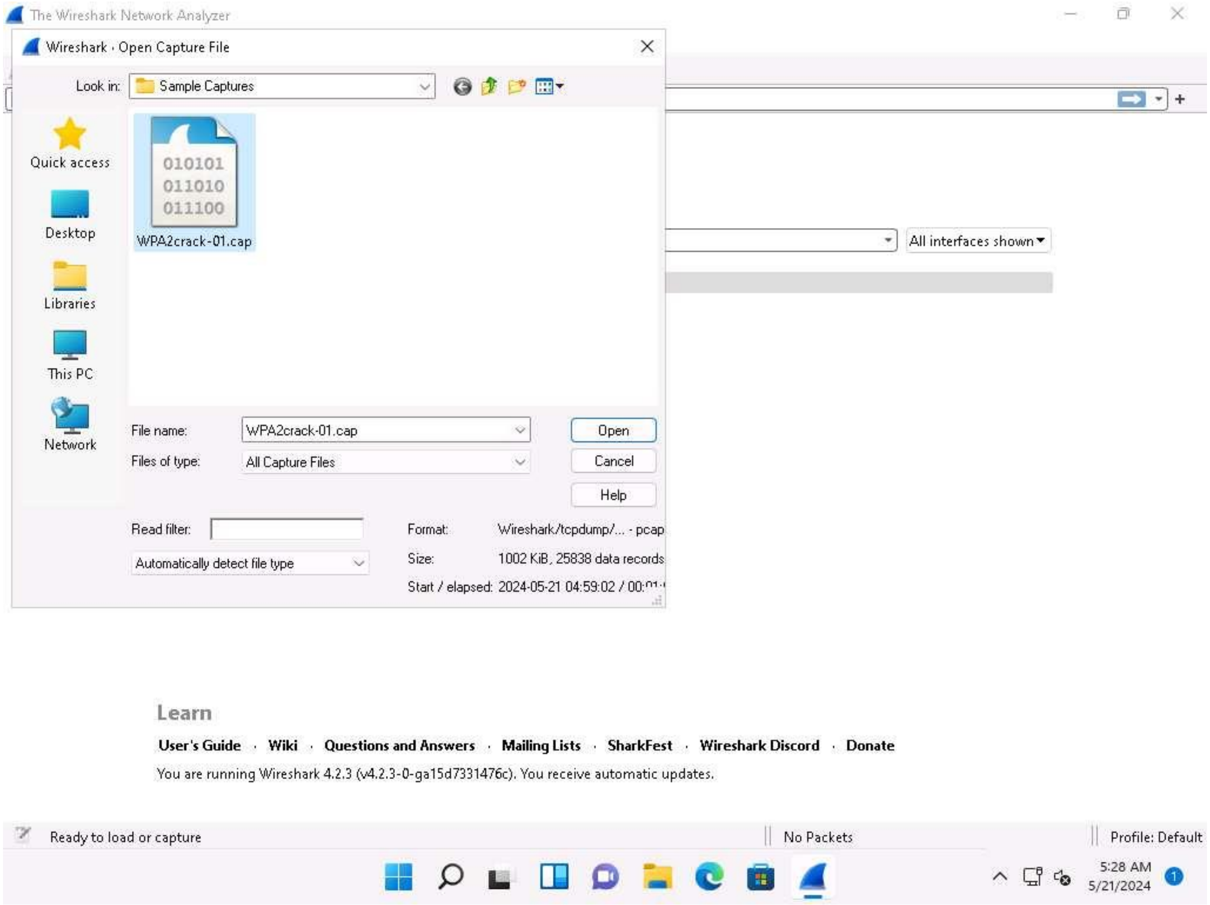
   If **Software Update** window appears, click **Skip this version** to close it.

4. In the menu bar, click **File** and click **Open** option from the drop-down list.



You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.

5. **Wireshark: Open Capture File** window appears, navigate to **E:\CEH-Tools\CEHv13 Module 16 Hacking Wireless Networks\Sample Captures**, select **WPA2crack-01.cap** and click **Open**.


The Wireshark Network Analyzer
Wireshark · Open Capture File
Quick access
Desktop
Libraries
This PC
Network
Open
Cancel
Help
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default
5:28 AM
5/21/2024

Look in: Sample Captures

WPA2crack-01.cap

File name: WPA2crack-01.cap

Files of type: All Capture Files

Read filter:

Automatically detect file type

Format: Wireshark/tcpdump/... - pcap

Size: 1002 KiB, 25838 data records

Start / elapsed: 2024-05-21 04:59:02 / 00:01:

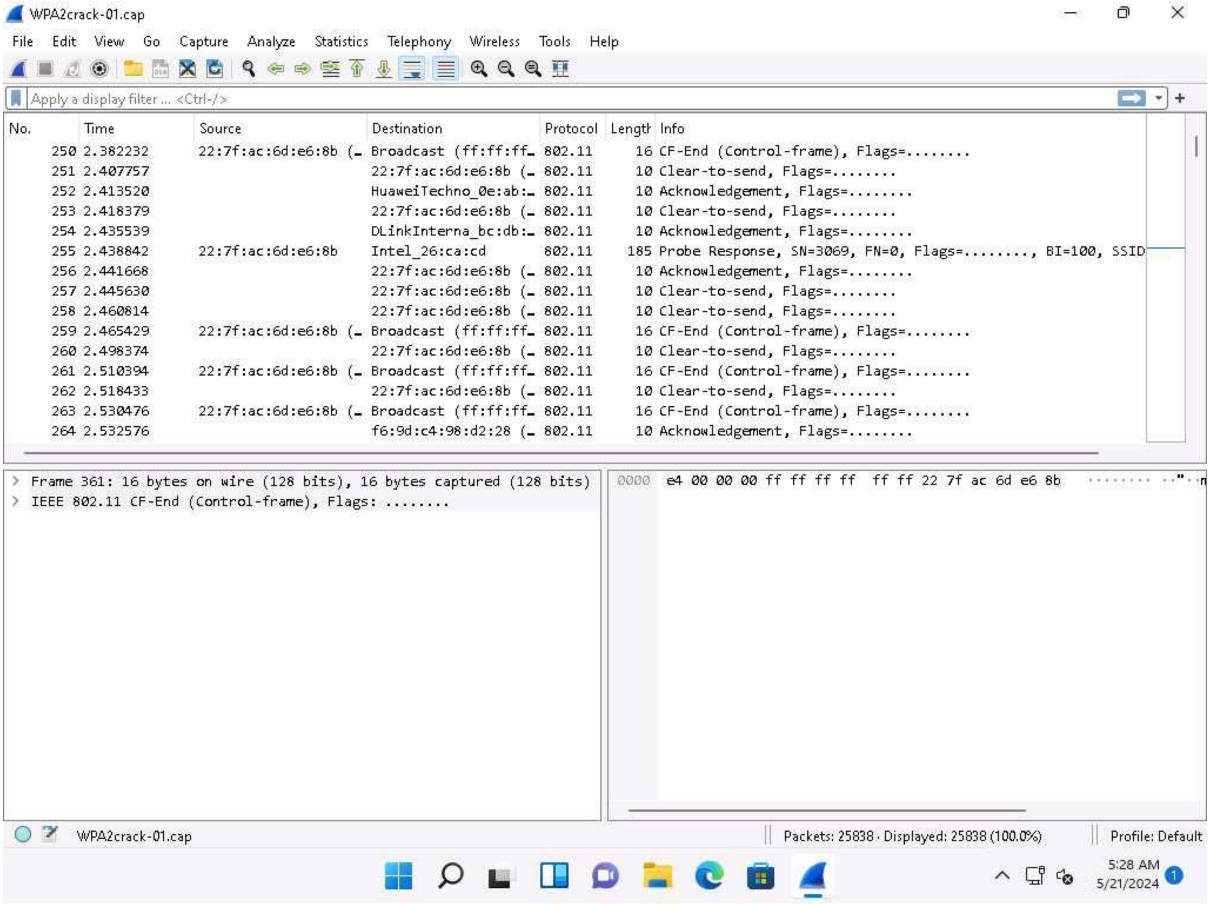
You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.

6. The **WPA2crack-01.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.

   Here 802.11 protocol indicates wireless packets.

   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.

   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.



```
No.   Time        Source               Destination          Protocol Length Info
  250 2.382232    22:7f:ac:6d:e6:8b (… Broadcast (ff:ff:ff… 802.11     16 CF-End (Control-frame), Flags=........
  251 2.407757                         22:7f:ac:6d:e6:8b (… 802.11     10 Clear-to-send, Flags=........
  252 2.413520                         HuaweiTechno_0e:ab:… 802.11     10 Acknowledgement, Flags=........
  253 2.418379                         22:7f:ac:6d:e6:8b (… 802.11     10 Clear-to-send, Flags=........
  254 2.435539                         DLinkInterna_bc:db:… 802.11     10 Acknowledgement, Flags=........
  255 2.438842    22:7f:ac:6d:e6:8b    Intel_26:ca:cd       802.11    185 Probe Response, SN=3069, FN=0, Flags=........, BI=100, SSID
  256 2.441668                         22:7f:ac:6d:e6:8b (… 802.11     10 Acknowledgement, Flags=........
  257 2.445630                         22:7f:ac:6d:e6:8b (… 802.11     10 Clear-to-send, Flags=........
  258 2.460814                         22:7f:ac:6d:e6:8b (… 802.11     10 Clear-to-send, Flags=........
  259 2.465429    22:7f:ac:6d:e6:8b (… Broadcast (ff:ff:ff… 802.11     16 CF-End (Control-frame), Flags=........
  260 2.498374                         22:7f:ac:6d:e6:8b (… 802.11     10 Clear-to-send, Flags=........
  261 2.510394    22:7f:ac:6d:e6:8b (… Broadcast (ff:ff:ff… 802.11     16 CF-End (Control-frame), Flags=........
  262 2.518433                         22:7f:ac:6d:e6:8b (… 802.11     10 Clear-to-send, Flags=........
  263 2.530476    22:7f:ac:6d:e6:8b (… Broadcast (ff:ff:ff… 802.11     16 CF-End (Control-frame), Flags=........
  264 2.532576                         f6:9d:c4:98:d2:28 (… 802.11     10 Acknowledgement, Flags=........
```

```
> Frame 361: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
> IEEE 802.11 CF-End (Control-frame), Flags: ........
```

```
0000  e4 00 00 00 ff ff ff ff  ff ff 22 7f ac 6d e6 8b   ........ .."..m
```

```
WPA2crack-01.cap          Packets: 25838 · Displayed: 25838 (100.0%)     Profile: Default
```

7. This concludes the demonstration of how to analyze Wi-Fi packets using Wireshark.

8. Close all open windows and document all the acquired information.

9. 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), and **CommView for Wi-Fi** (https://www.tamos.com) to analyze Wi-Fi traffic.

Question 16.1.1.1

Use the Wi-Fi packet-sniffing tool Wireshark to analyze captured Wi-Fi packets (WPA2crack-01.cap). Enter the protocol that indicates the wireless packets. Note: sample captured Wi-Fi packets are available at E:\CEH-Tools\CEHv13 Module 16 Hacking Wireless Networks\Sample Captures.

Lab 2: Perform Wireless Attacks

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 (WPA2), fragmentation, MAC spoofing, DoS, and ARP poisoning attacks.

As an ethical hacker and pen tester of an organization, you must test its wireless security, exploit WPA2 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

- Crack a WPA2 network using Aircrack-ng

Overview of Wireless Attacks

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

These include:

- **Fragmentation attack**: When successful, such attacks can obtain 1,500 bytes of PRGA (pseudo random generation algorithm)
- **MAC spoofing attack**: The attacker changes their MAC address to that of an authenticated user in order to bypass the access point's MAC-filtering configuration
- **Disassociation attack**: The attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the access point and client
- **Deauthentication attack**: The attacker floods station(s) with forged deauthentication packets to disconnect users from an access point
- **Man-in-the-middle attack**: An active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers
- **Wireless ARP poisoning attack**: An attack technique that exploits the lack of a verification mechanism in the ARP protocol by corrupting the ARP cache

maintained by the OS in order to associate the attacker's MAC address with the target host

- **Rogue access points**: Wireless access points that an attacker installs on a network without authorization and that are not under the management of the network administrator

- **Evil twin**: A fraudulent wireless access point that pretends to be a legitimate access point by imitating another network name

- **Wi-Jacking attack**: A method used by attackers to gain access to an enormous number of wireless networks

Task 1: Crack a WPA2 Network using Aircrack-ng

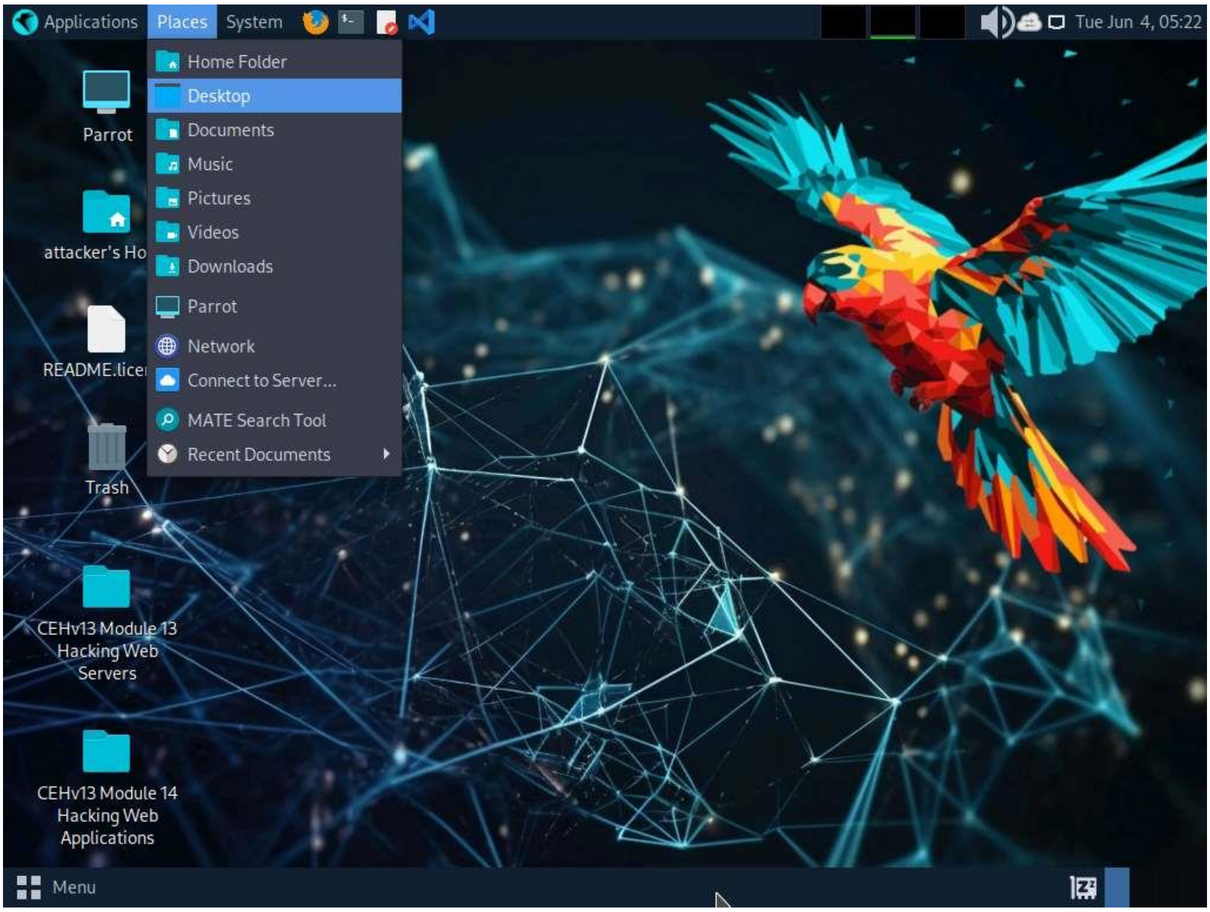
WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security. WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both 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.

Before starting this task, you need to configure your access point router (**ECC 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 to WPA2-PSK, with the password as **12345678**.
In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (**WPA2crack-01.cap**) to crack WPA key.

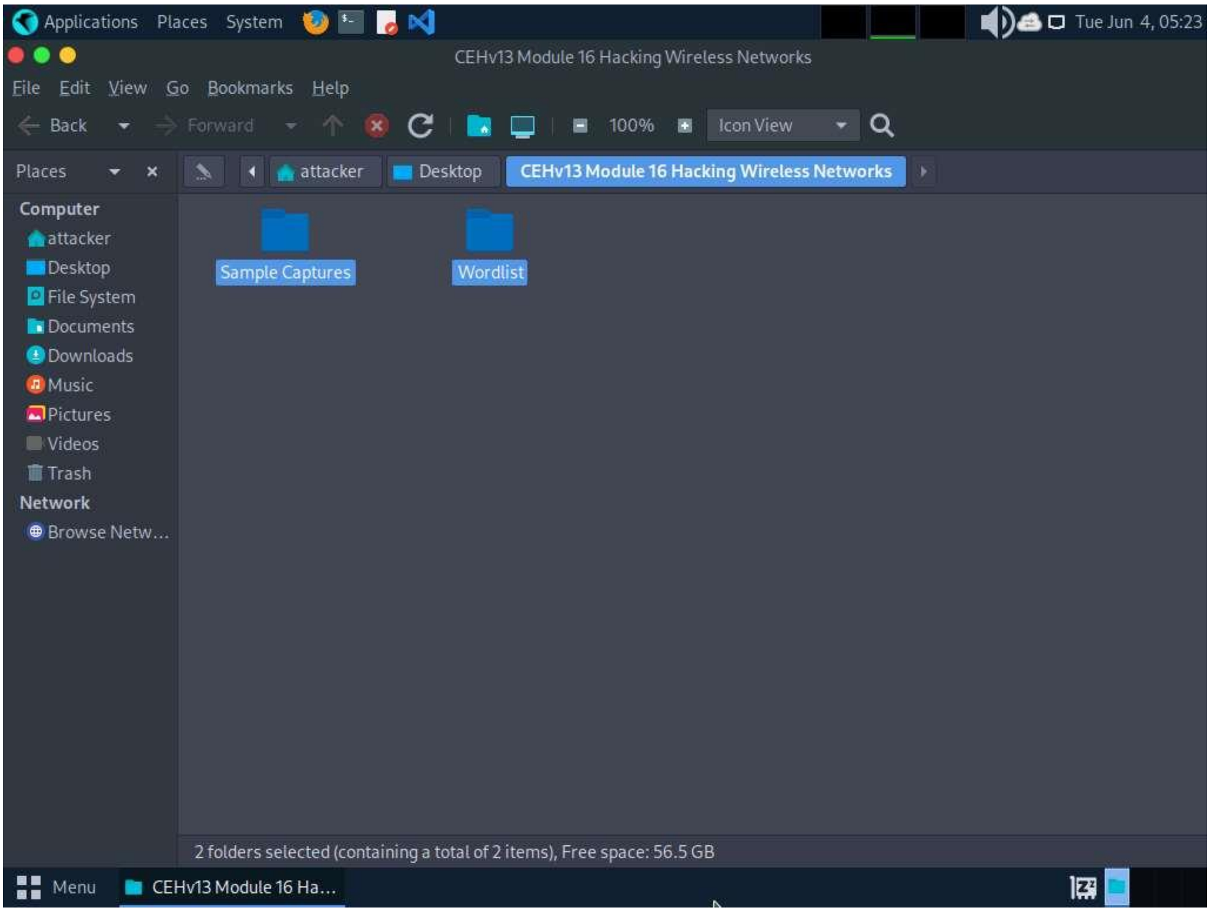
1. Click Parrot Security to switch to the **Parrot Security** machine and login with **attacker**/**toor**.

2. Navigate to the **Places** in the top-section of the window and click **Desktop** from the drop-down list.



3. The **Desktop** window appears, navigate to the **CEHv12 Module 16 Hacking Wireless Networks** folder and copy **Sample Captures** and **Wordlist** folders.

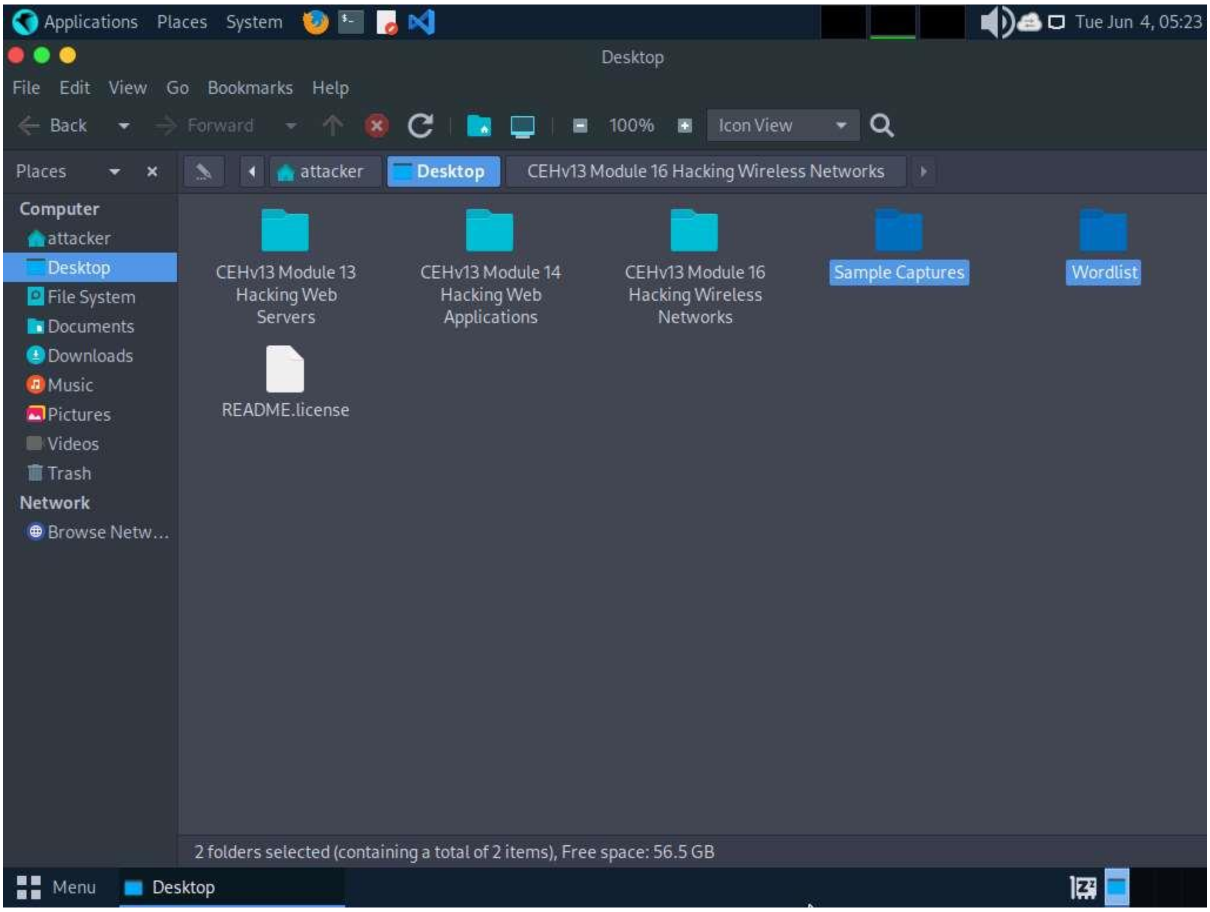
   To copy the folders, firstly select both the folders and then press **Ctrl+C**.



Applications Places System
Tue Jun 4, 05:23
CEHv13 Module 16 Hacking Wireless Networks
File Edit View Go Bookmarks Help
Back Forward 100% Icon View
Places
attacker Desktop CEHv13 Module 16 Hacking Wireless Networks
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Browse Netw…
Sample Captures
Wordlist
Menu
CEHv13 Module 16 Ha…

2 folders selected (containing a total of 2 items), Free space: 56.5 GB

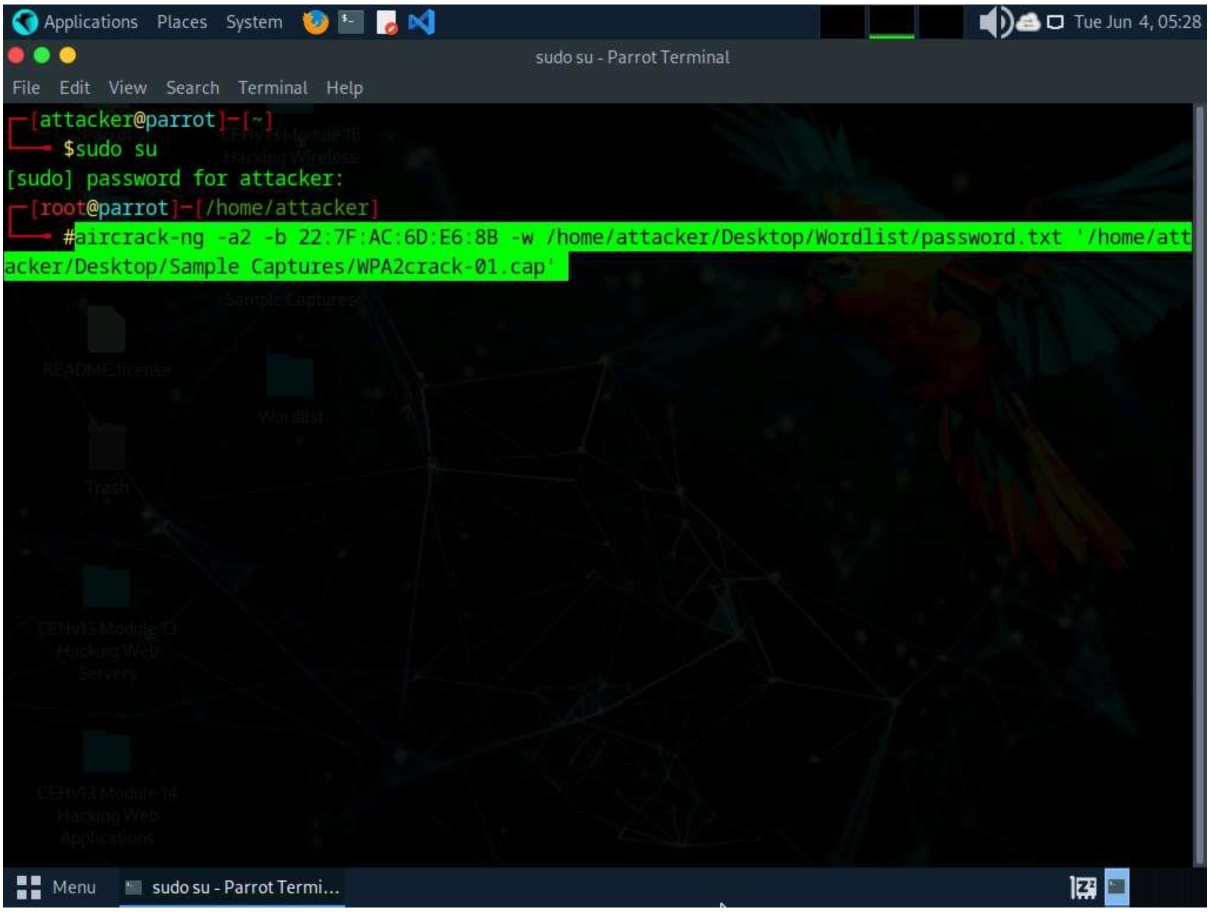
4. Now, navigate to the **Desktop** and press **Ctrl+V** to paste the copied folders (**Sample Captures** and **Wordlist**). Close the **Desktop** window.


Applications Places System
Tue Jun 4, 05:23
Desktop
File Edit View Go Bookmarks Help
Back Forward 100% Icon View
Places
attacker Desktop CEHv13 Module 16 Hacking Wireless Networks
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Browse Netw...
CEHv13 Module 13 Hacking Web Servers
CEHv13 Module 14 Hacking Web Applications
CEHv13 Module 16 Hacking Wireless Networks
Sample Captures
Wordlist
README.license
2 folders selected (containing a total of 2 items), Free space: 56.5 GB
Menu
Desktop

5. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

6. In the **Parrot Terminal** window, run **aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'**. Here, the BSSID of the target is **22:7F:AC:6D:E6:8B**.

   - **-a** is the technique used to crack the handshake, **2**=WPA technique.
   - **-b** refers to bssid; replace with the BSSID of the target router.
   - **-w** stands for wordlist; provide the path to a wordlist.

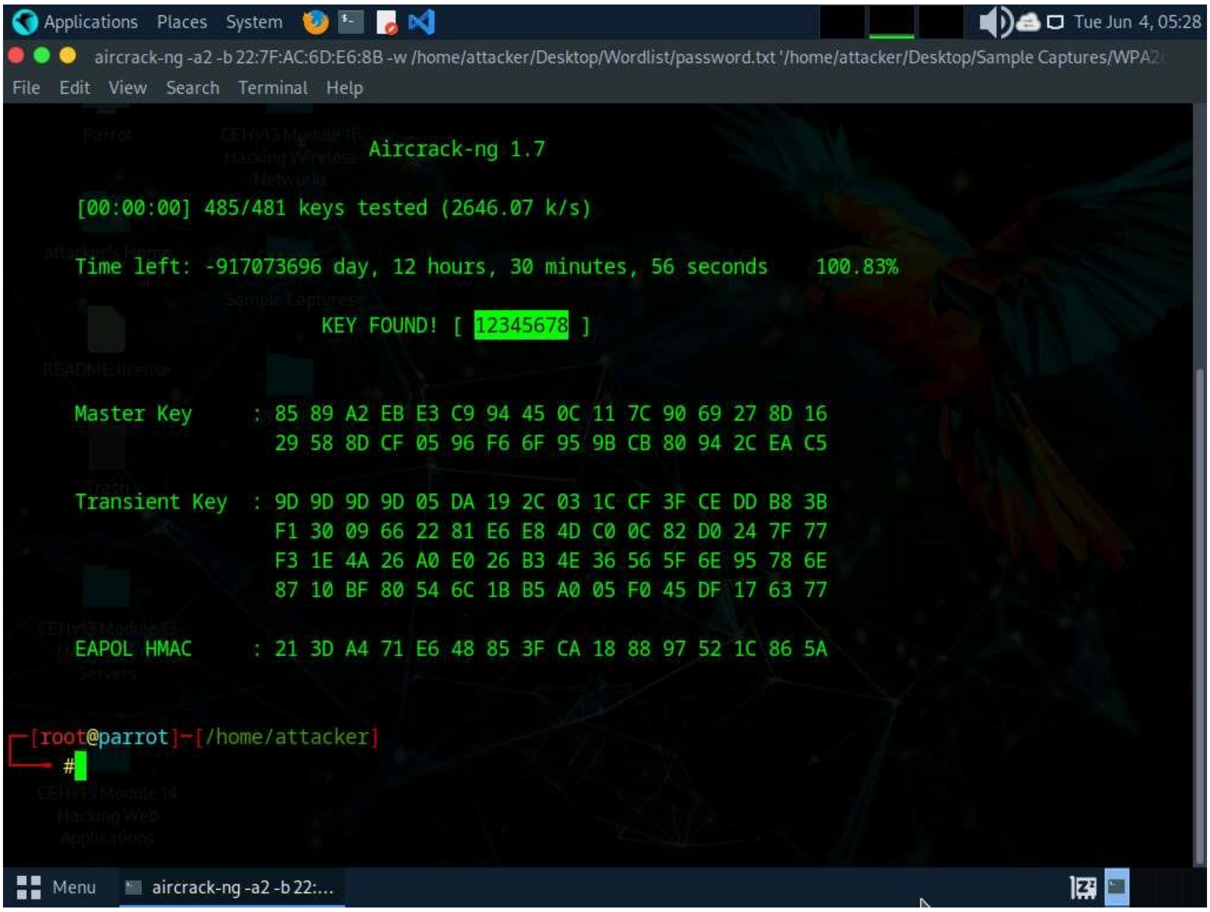


Applications Places System
Tue Jun 4, 05:28
sudo su - Parrot Terminal
File Edit View Search Terminal Help
Menu
sudo su - Parrot Termi...

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #aircrack-ng -a2 -b 22:7F:AC:6D:E6:8B -w /home/attacker/Desktop/Wordlist/password.txt '/home/att
acker/Desktop/Sample Captures/WPA2crack-01.cap'
```

7. 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.

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



```
aircrack-ng -a2 -b 22:7F:AC:6D:E6:8B -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2

                               Aircrack-ng 1.7

      [00:00:00] 485/481 keys tested (2646.07 k/s)

      Time left: -917073696 day, 12 hours, 30 minutes, 56 seconds    100.83%

                           KEY FOUND! [ 12345678 ]


      Master Key     : 85 89 A2 EB E3 C9 94 45 0C 11 7C 90 69 27 8D 16
                       29 58 8D CF 05 96 F6 6F 95 9B CB 80 94 2C EA C5

      Transient Key  : 9D 9D 9D 9D 05 DA 19 2C 03 1C CF 3F CE DD B8 3B
                       F1 30 09 66 22 81 E6 E8 4D C0 0C 82 D0 24 7F 77
                       F3 1E 4A 26 A0 E0 26 B3 4E 36 56 5F 6E 95 78 6E
                       87 10 BF 80 54 6C 1B B5 A0 05 F0 45 DF 17 63 77

      EAPOL HMAC     : 21 3D A4 71 E6 48 85 3F CA 18 88 97 52 1C 86 5A


┌─[root@parrot]─[/home/attacker]
└──╼ #
```

8. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng.

9. Close all open windows and document all the acquired information.

10. You can also use other tools such as **hashcat** (https://hashcat.net), **Portable Penetrator** (https://www.secpoint.com), **WepCrackGui** (https://sourceforge.net) to crack WEP/WPA/WPA2 encryption.

Question 16.2.1.1

Use the Aircrack-ng suite to crack a WPA2 network. Enter the key found in this exercise.
Note: sample captured Wi-Fi packets and wordlist are available at
/home/attacker/Desktop/CEHv13 Module 16 Hacking Wireless Networks