Module 16: Hacking Wireless Networks

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.

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:

- Wi-Fi Packet Analysis
- Crack WEP and WPA2 Wi-Fi networks

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:

1. Perform wireless traffic analysis
    - Wi-Fi packet analysis using Wireshark
2. Perform wireless attacks
    - Crack a WEP network using Aircrack-ng
    - Crack a WPA2 network using Aircrack-ng

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

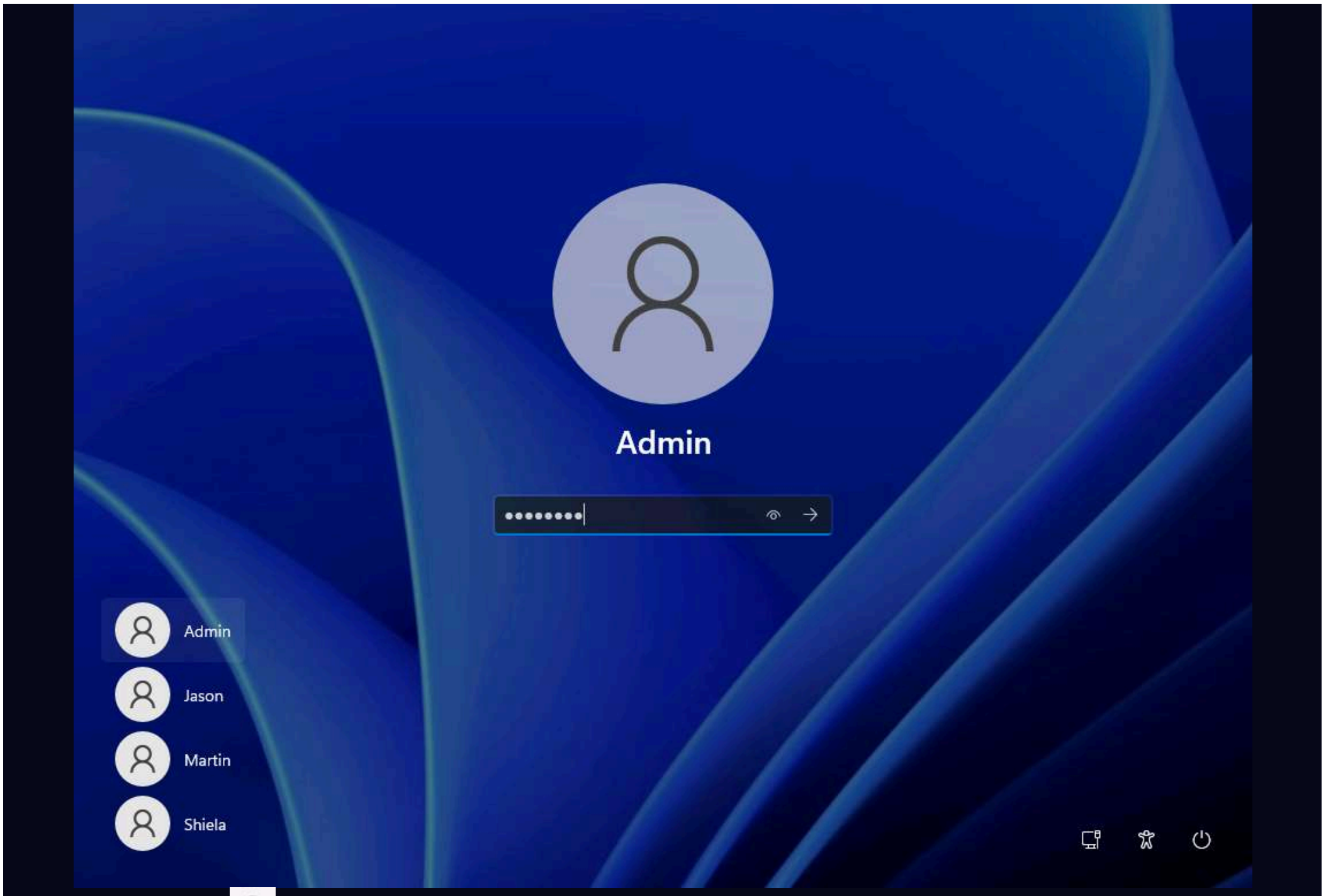
Wireshark is a network protocol sniffer and analyzer. It lets you capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark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

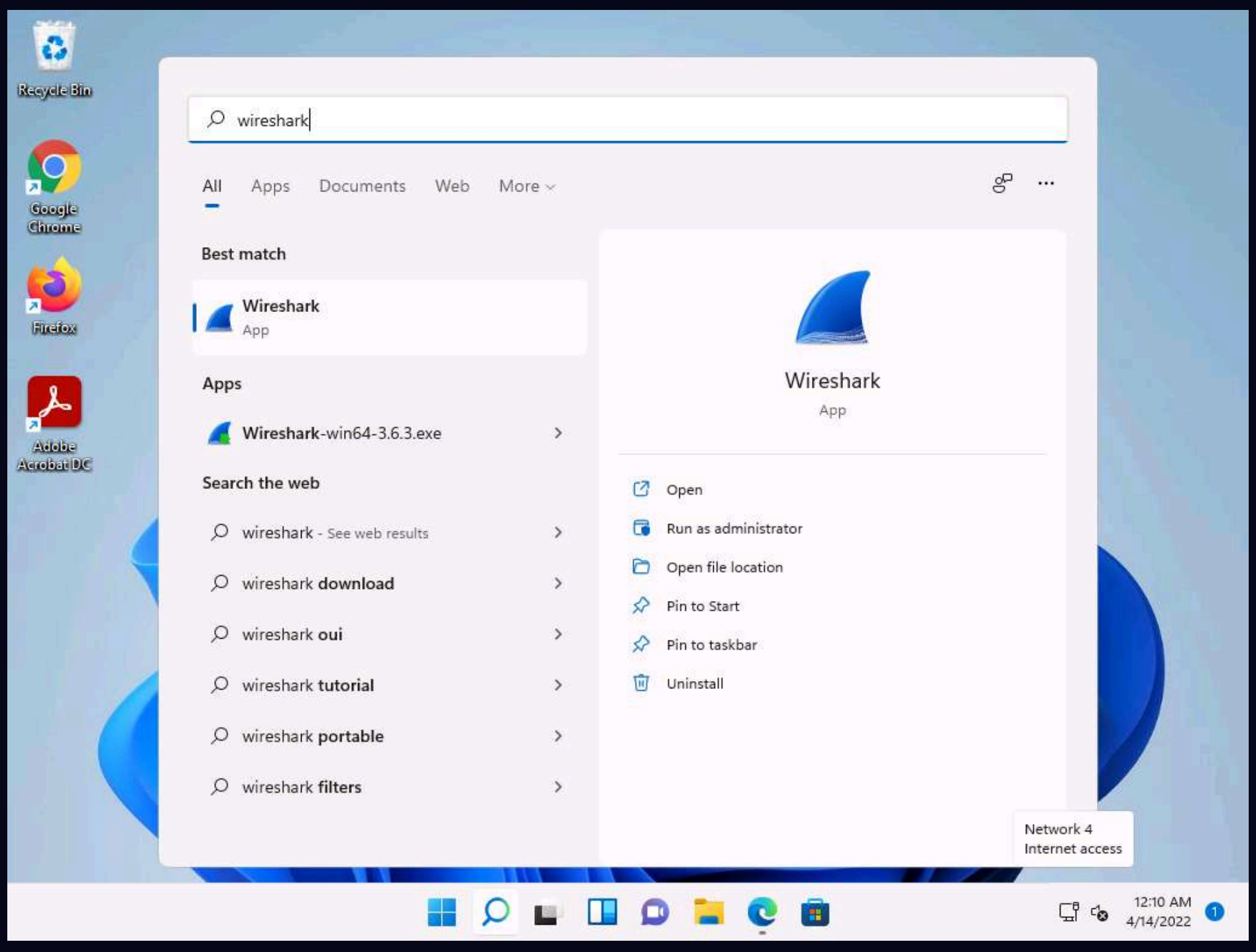
> Note: In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (**WEPcrack-01.cap**) to analyze wireless packets.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**.
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

> Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.
>
> Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

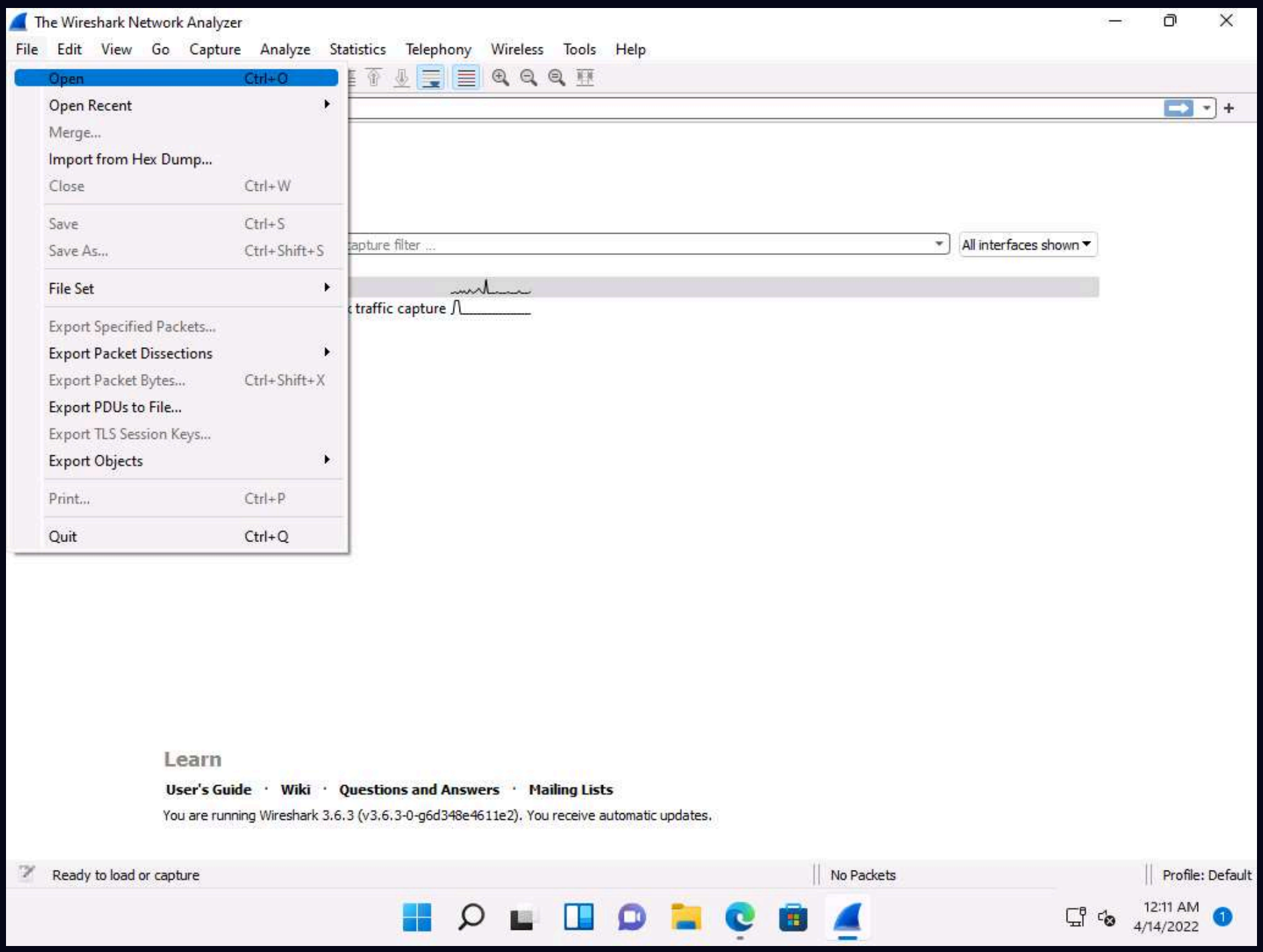


3. Click **search** icon on the **Desktop**. Type **wire** in the search field,the **Wireshark** appears in the results, click **open** to lanch it.

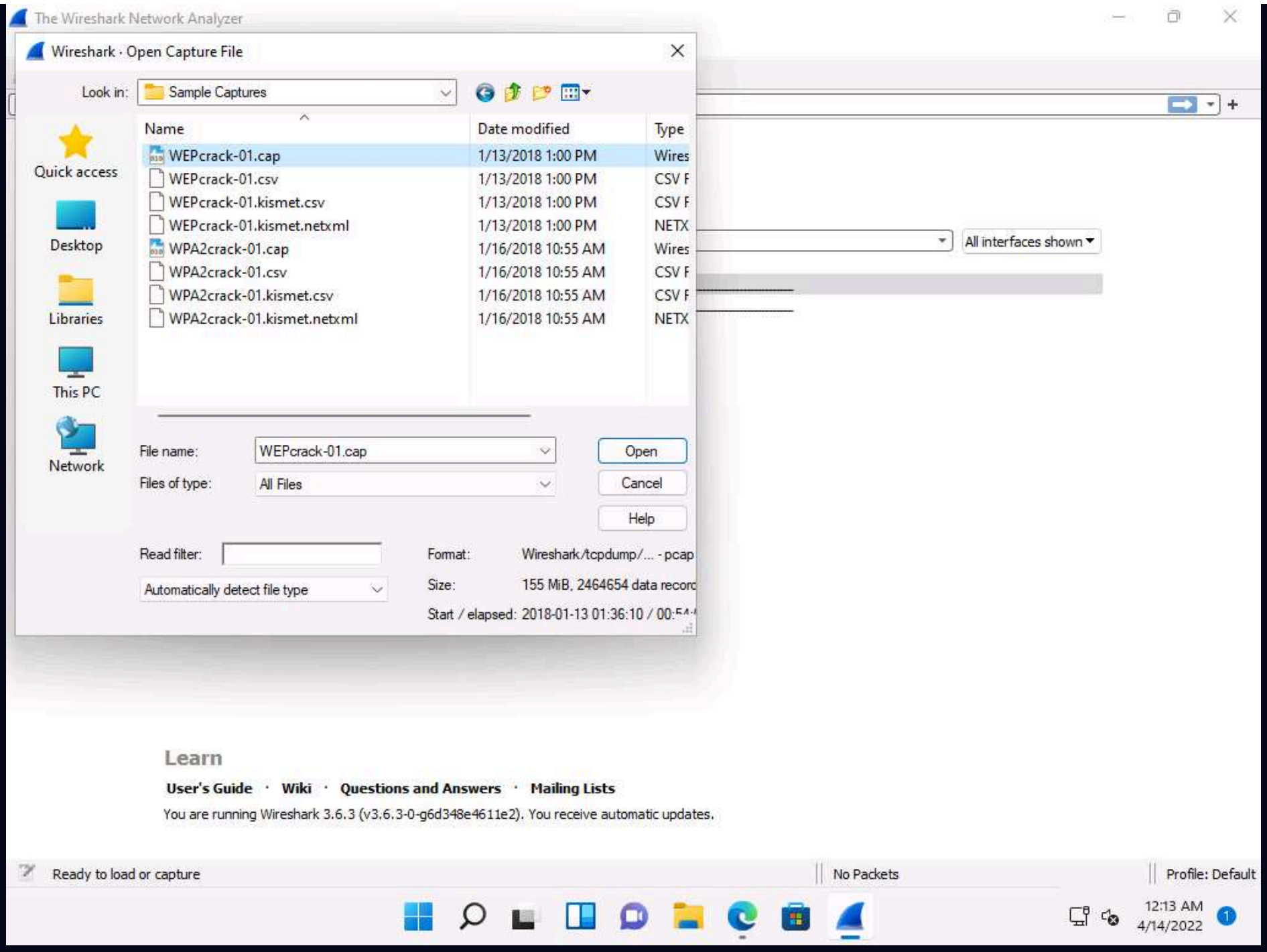


4. The **Wireshark Network Analyzer** window appears.

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



6. **Wireshark: Open Capture File** window appears, navigate to **E:\CEH-Tools\CEHv12 Module 16 Hacking Wireless Networks\Sample Captures**, select **WEPcrack-01.cap** and click **Open**.



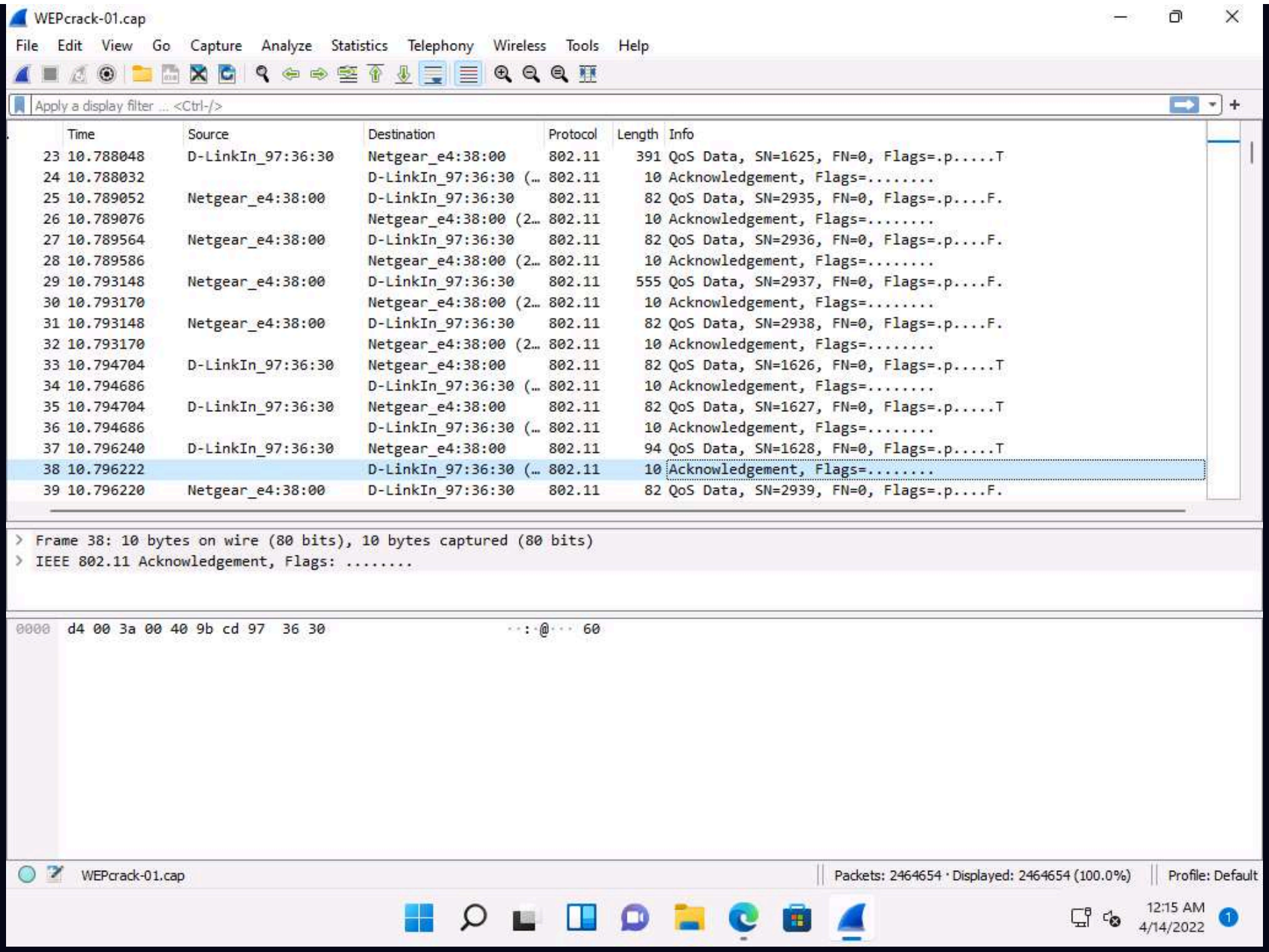
7. The **WEPcrack-01.cap** file opens in Wireshark window showing you the details of the packet for analysis. Here you can see the wireless packets captured which were otherwise masked to look like **ethernet** traffic.

   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.

Note: Similarly you can also analyze the **WPA2crack-01.cap** file for WPA packets.



8. This concludes the demonstration of how to analyze Wi-Fi packets using Wireshark.
9. Close all open windows and document all the acquired information.
10. 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.

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 (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

- Crack a WEP network using Aircrack-ng
- 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

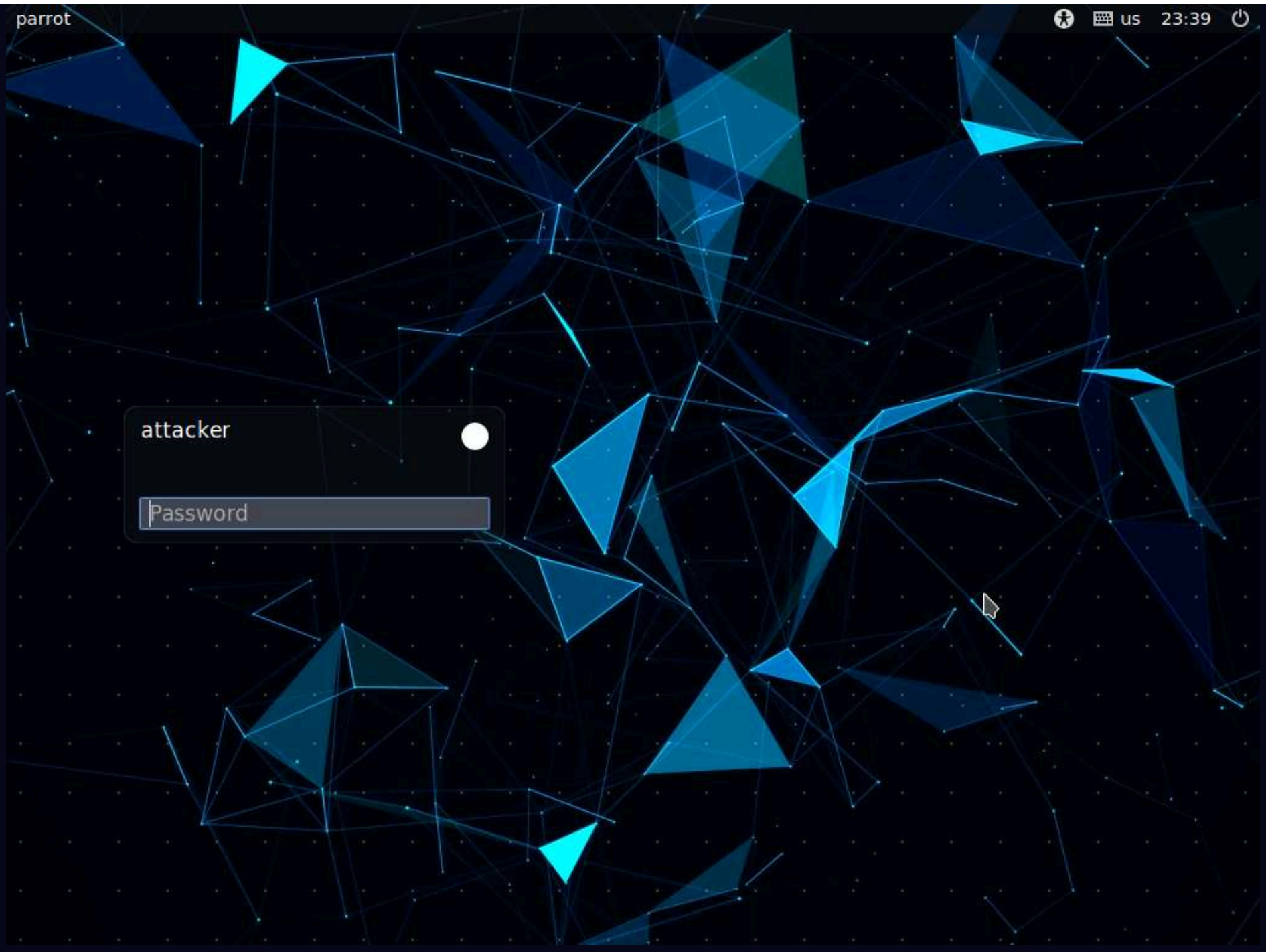
Task 1: Crack a WEP network using Aircrack-ng

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.

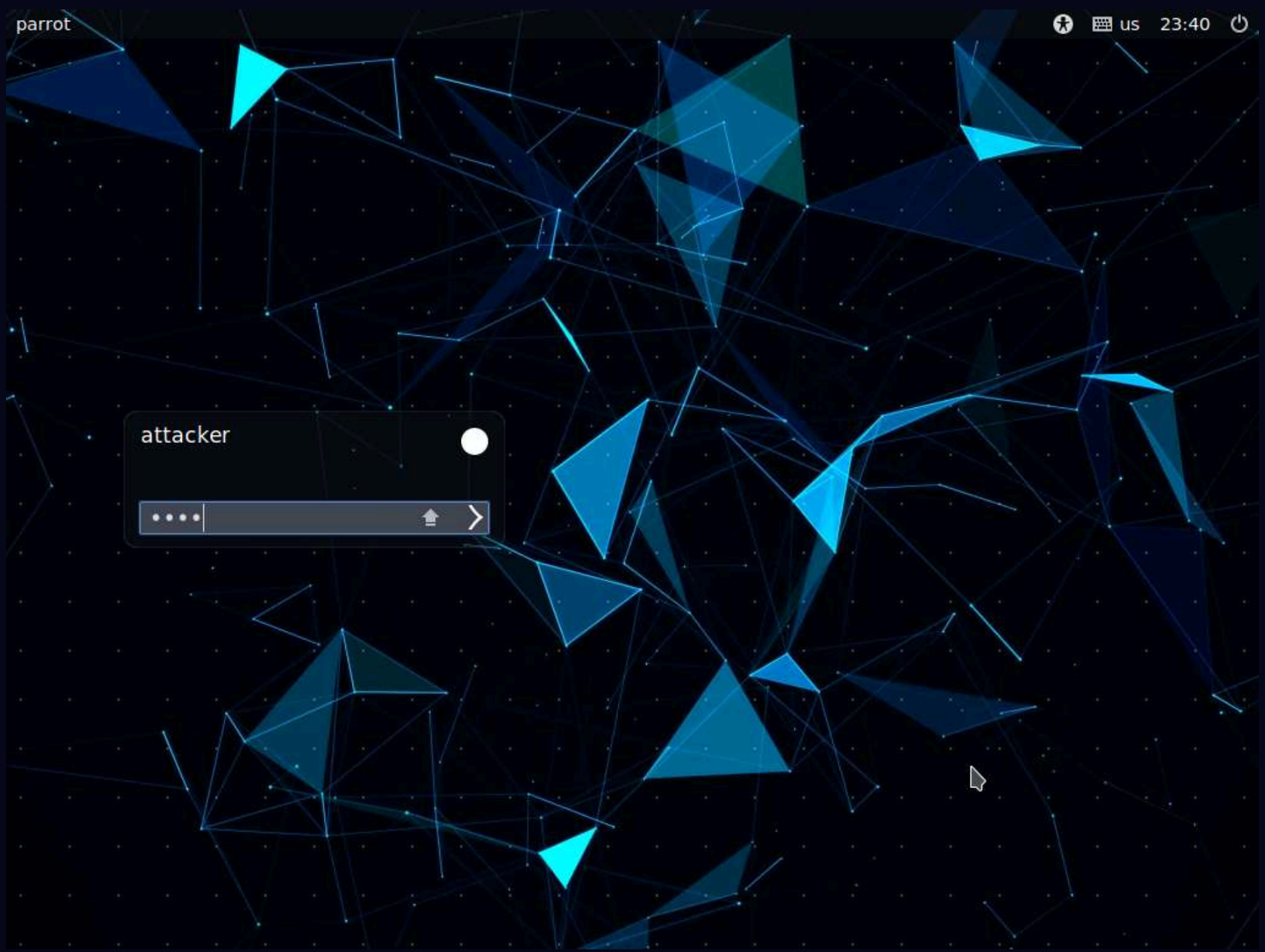
In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

> Note: 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 (**WEPcrack-01.cap**) to crack WEP key.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

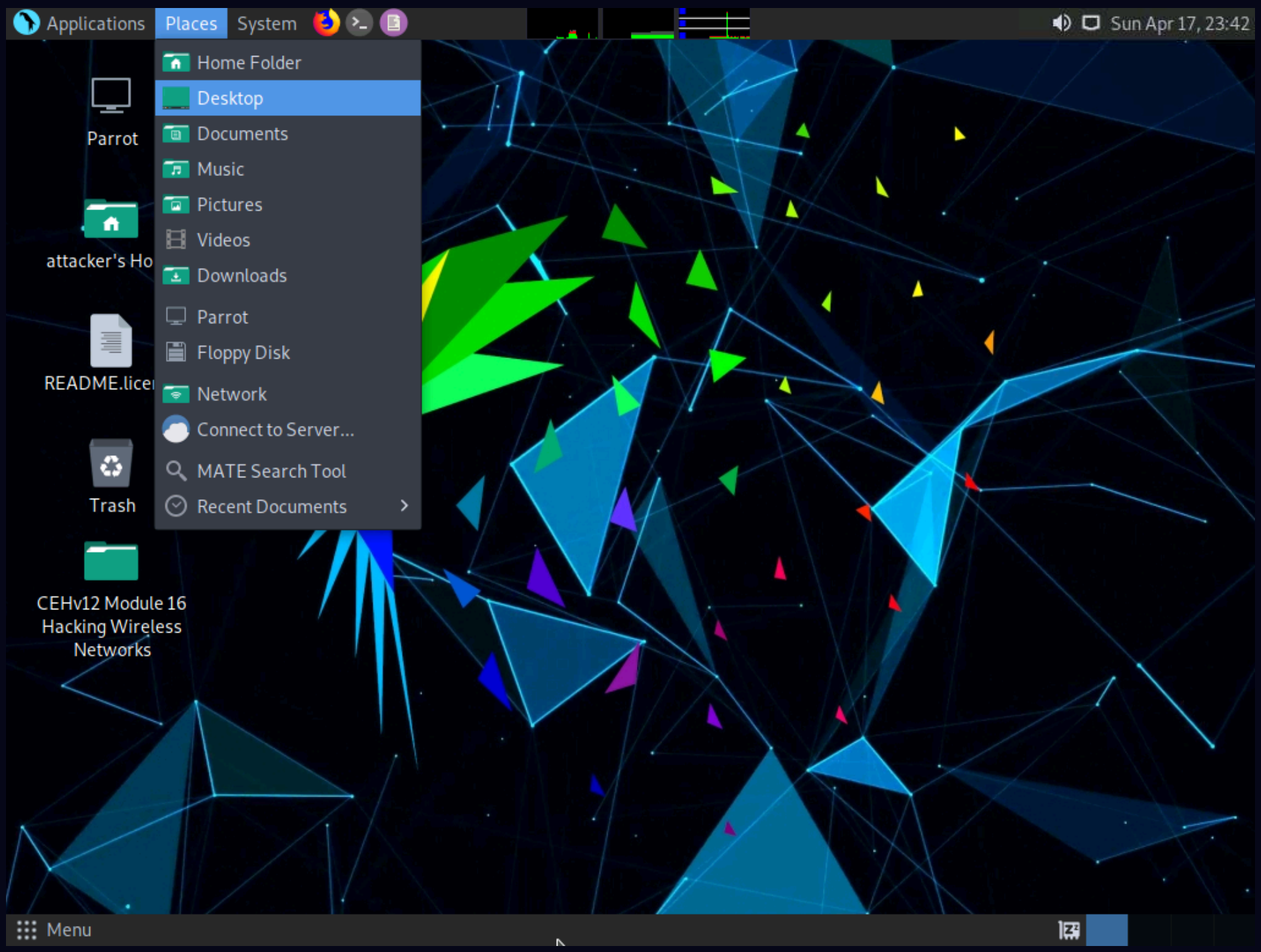


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



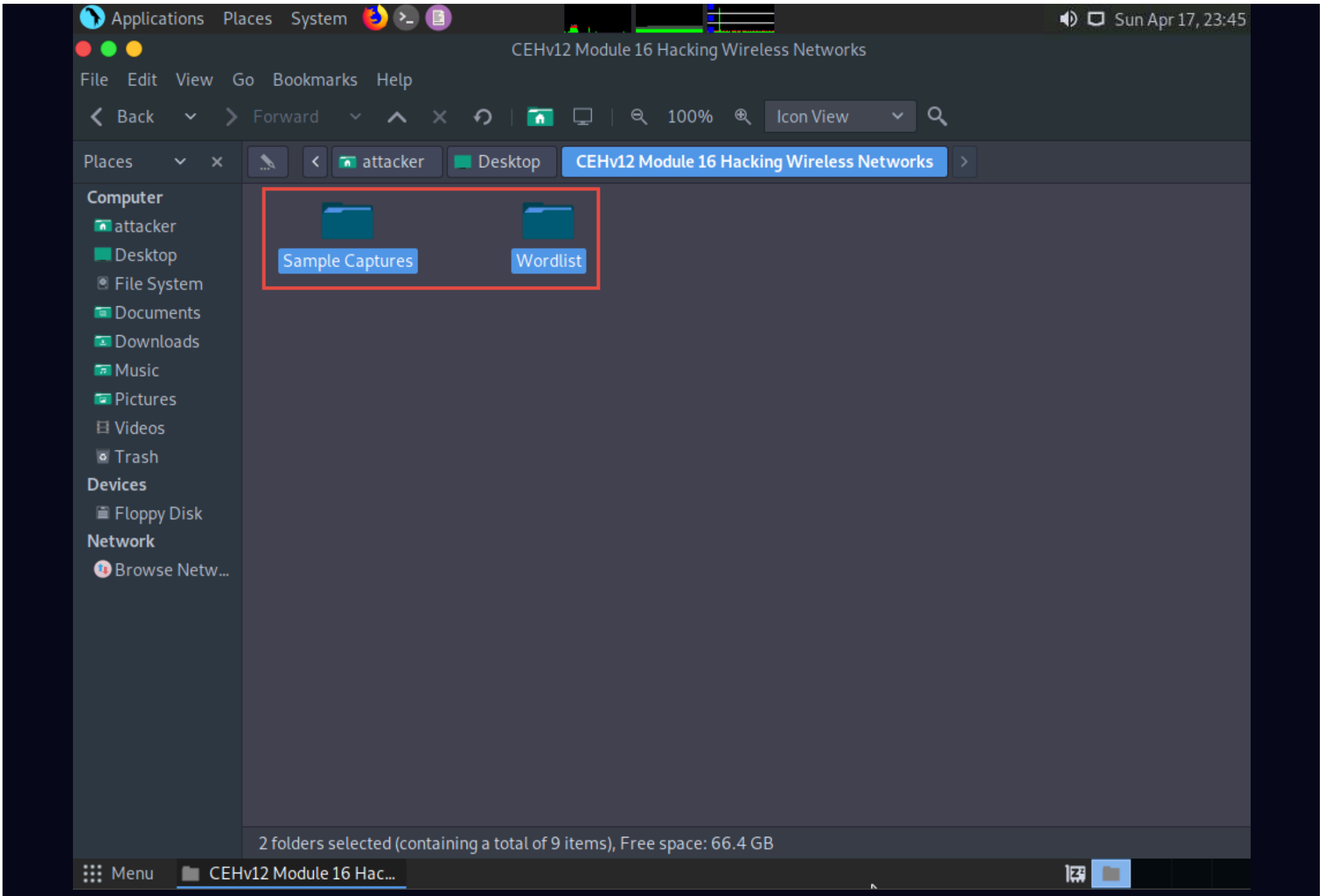
3. Navigate to the **Places** in the top-section of the window and click **Desktop** from the drop-down list.

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

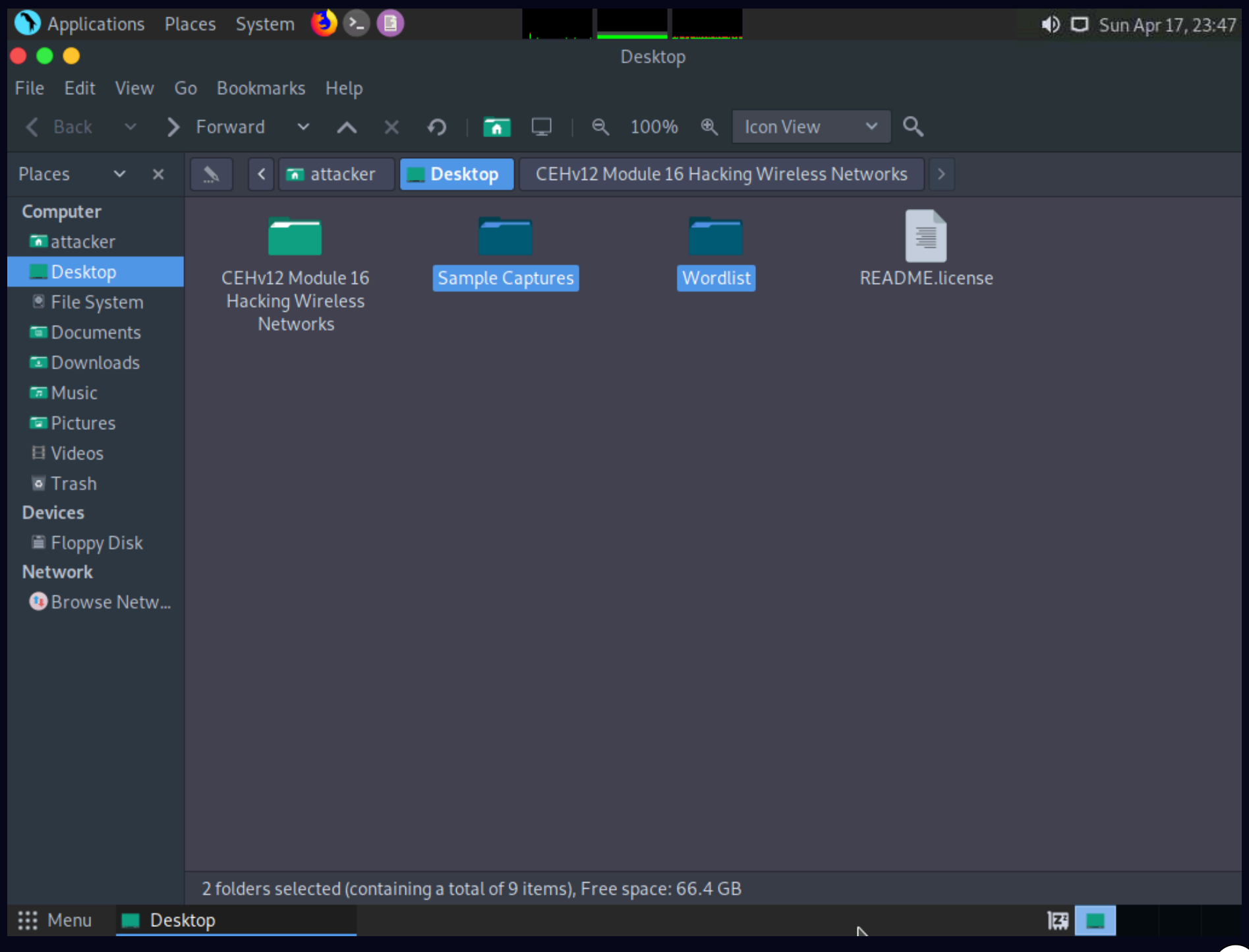


4. The **Desktop** window appears, navigate to the **CEHv12 Module 16 Hacking Wireless Networks** folder and copy **Sample Captures** and **Wordlist** folders.

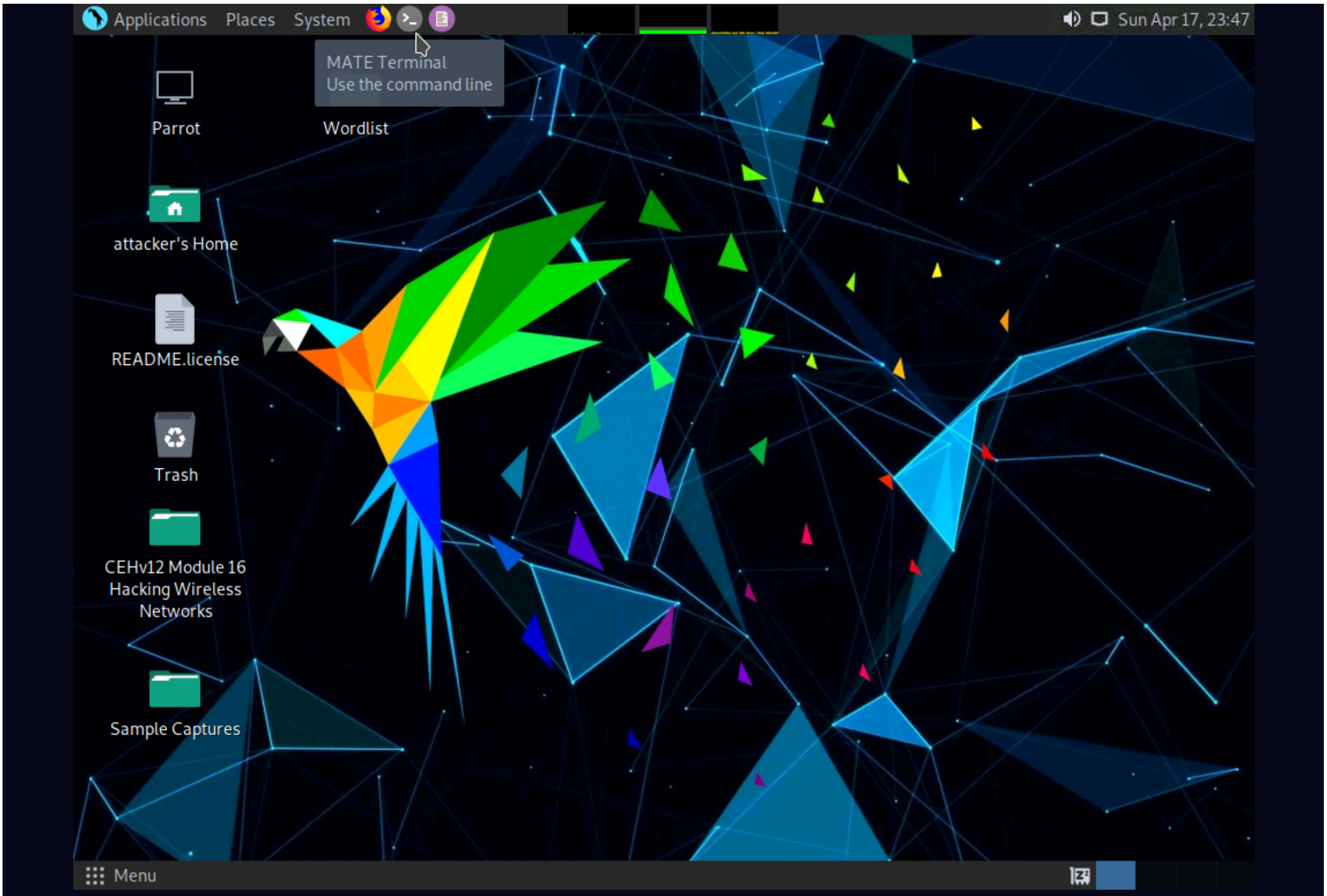
Note: To copy the folders, firstly select both the folders and then press **Ctrl+C**.



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



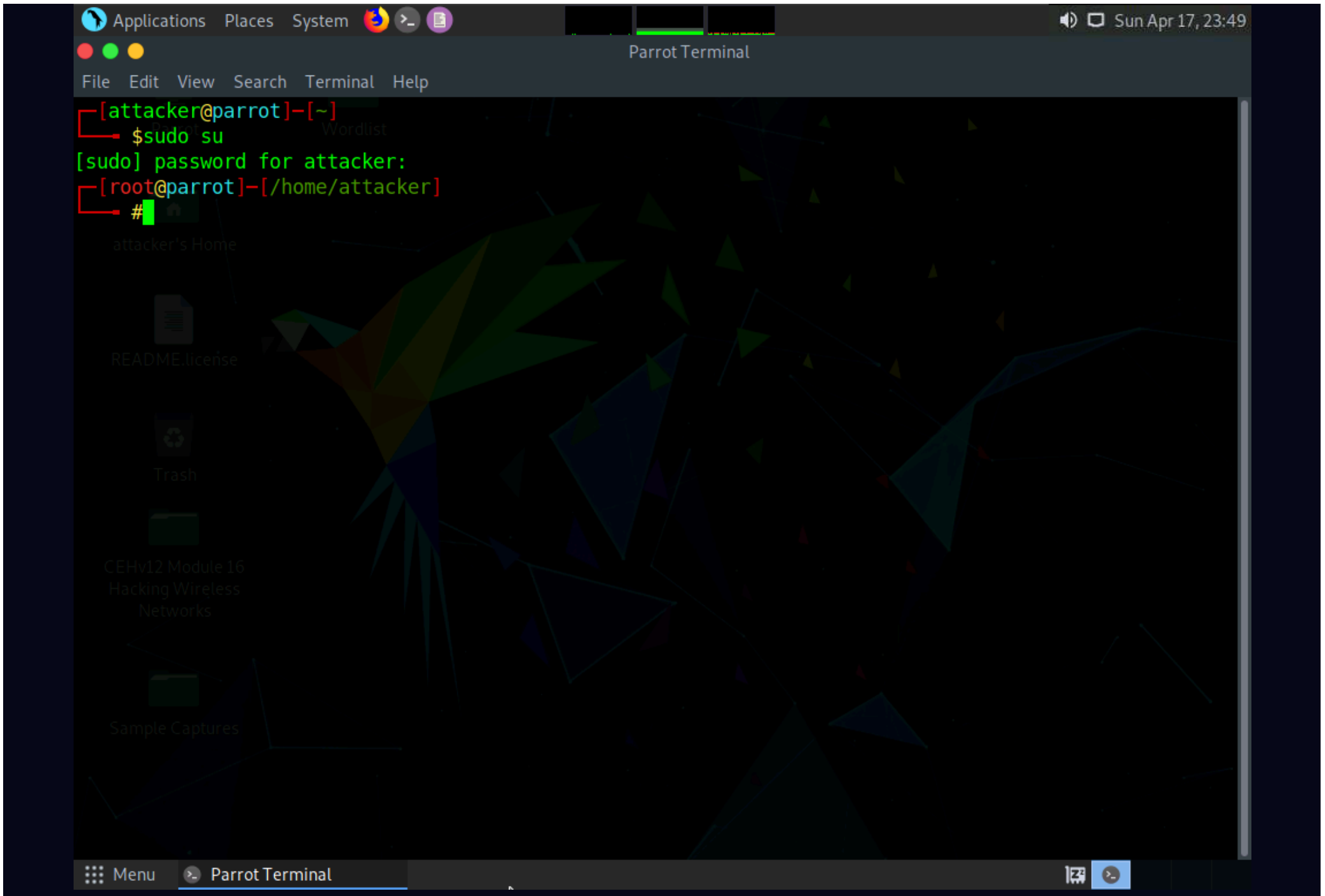
6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



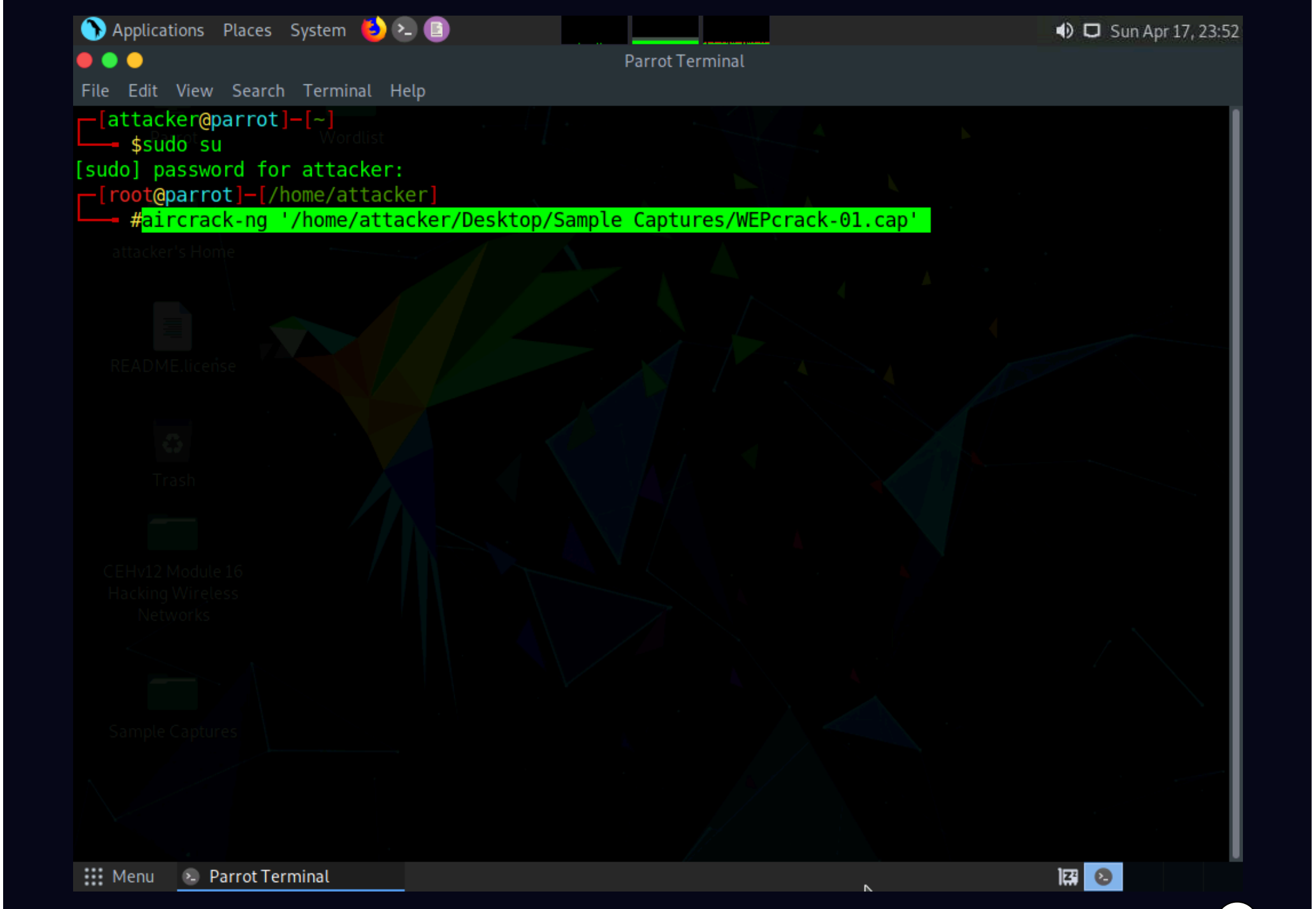
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

8. 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.

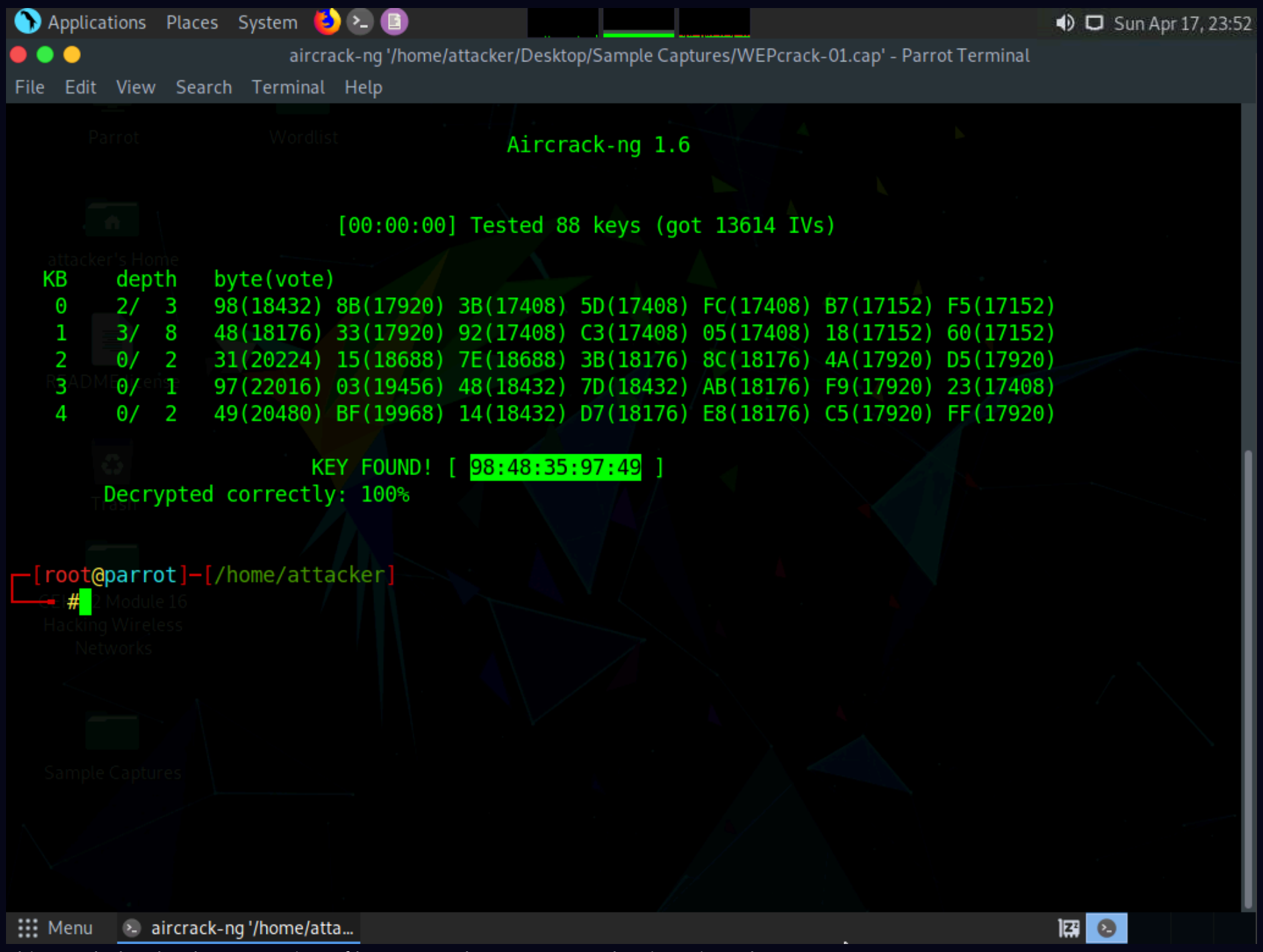


9. In the **Parrot Terminal** window, type **aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'** and press **Enter**.



10. By issuing the above command **aircrack-ng** will crack the WEP key of the **CEHLabs** 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.



11. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.

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

Task 2: 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.

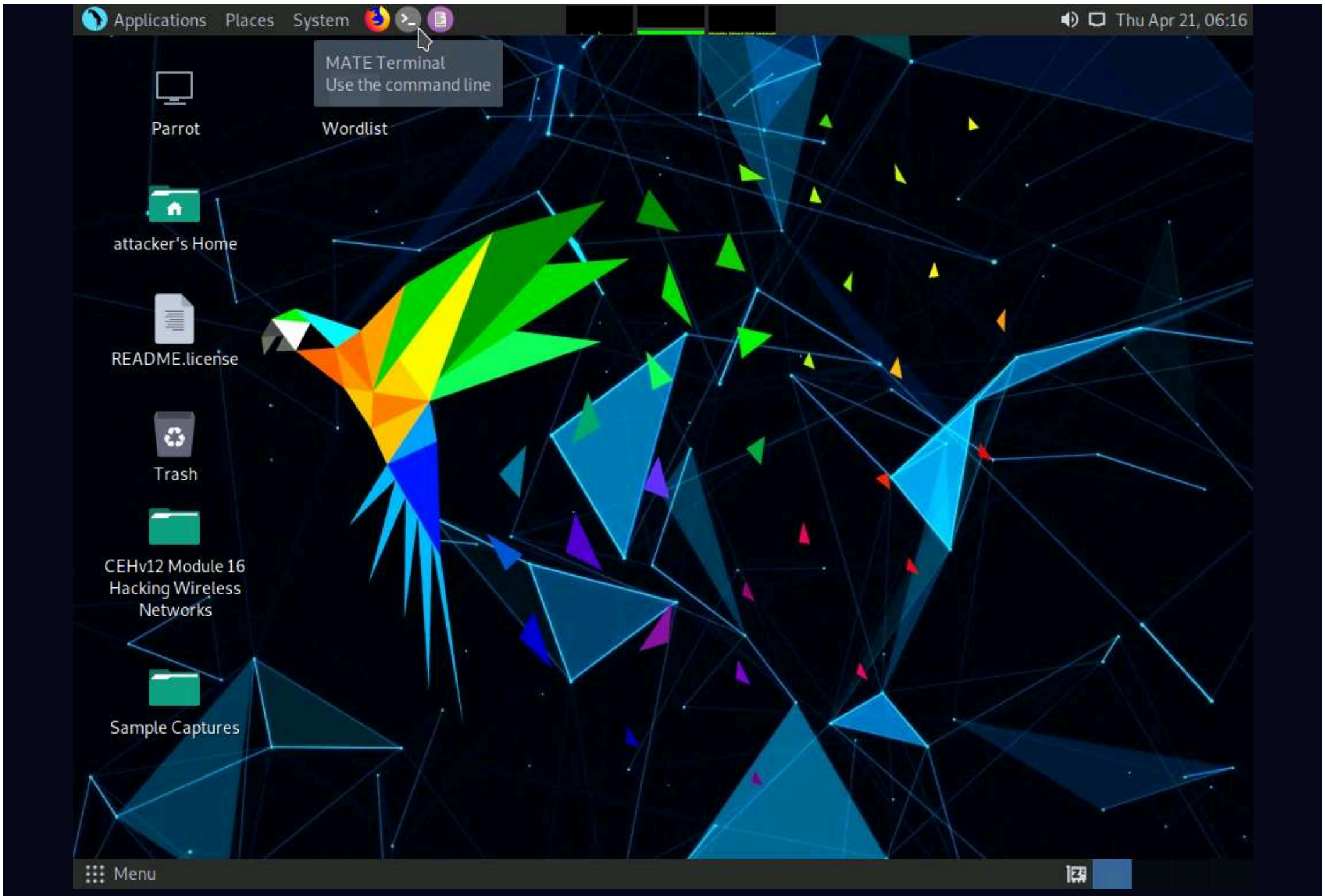
In this task, we will use the Aircrack-ng suite to crack a WPA2 network.

Note: Before starting this task, you need to configure your access point router (**CEHLabs**) 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**.

Note: 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.

Note: Ensure that **Sample Captures** and **Wordlist** folders are present at the location **home/attacker/Desktop** which we copied in the previous task. If not, then navigate to the **CEHv12 Module 16 Hacking Wireless Networks** folder on the **Desktop**, copy the **Sample Captures** and **Wordlist** folders and paste them at the location **home/attacker/Desktop**.

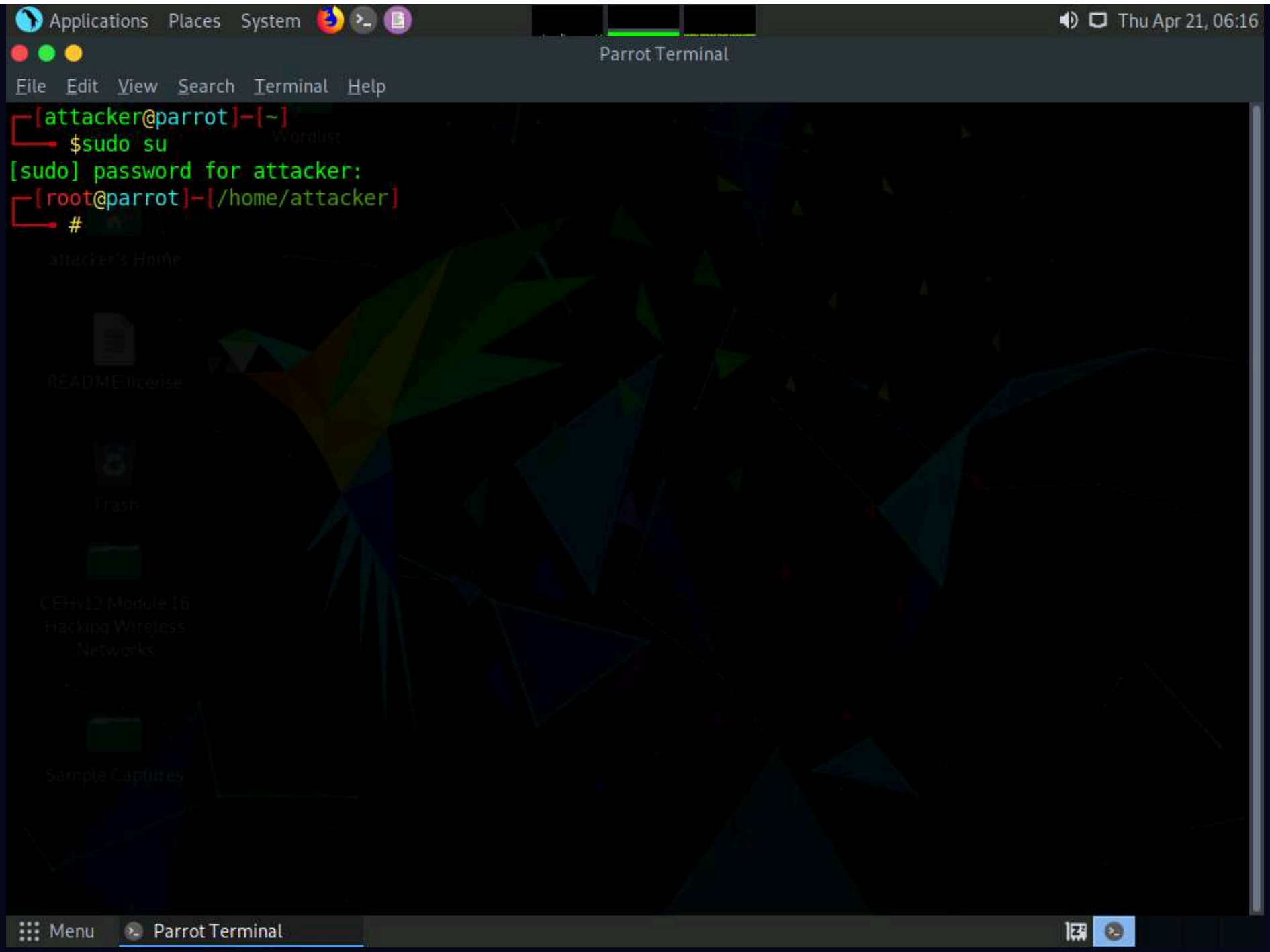
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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

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

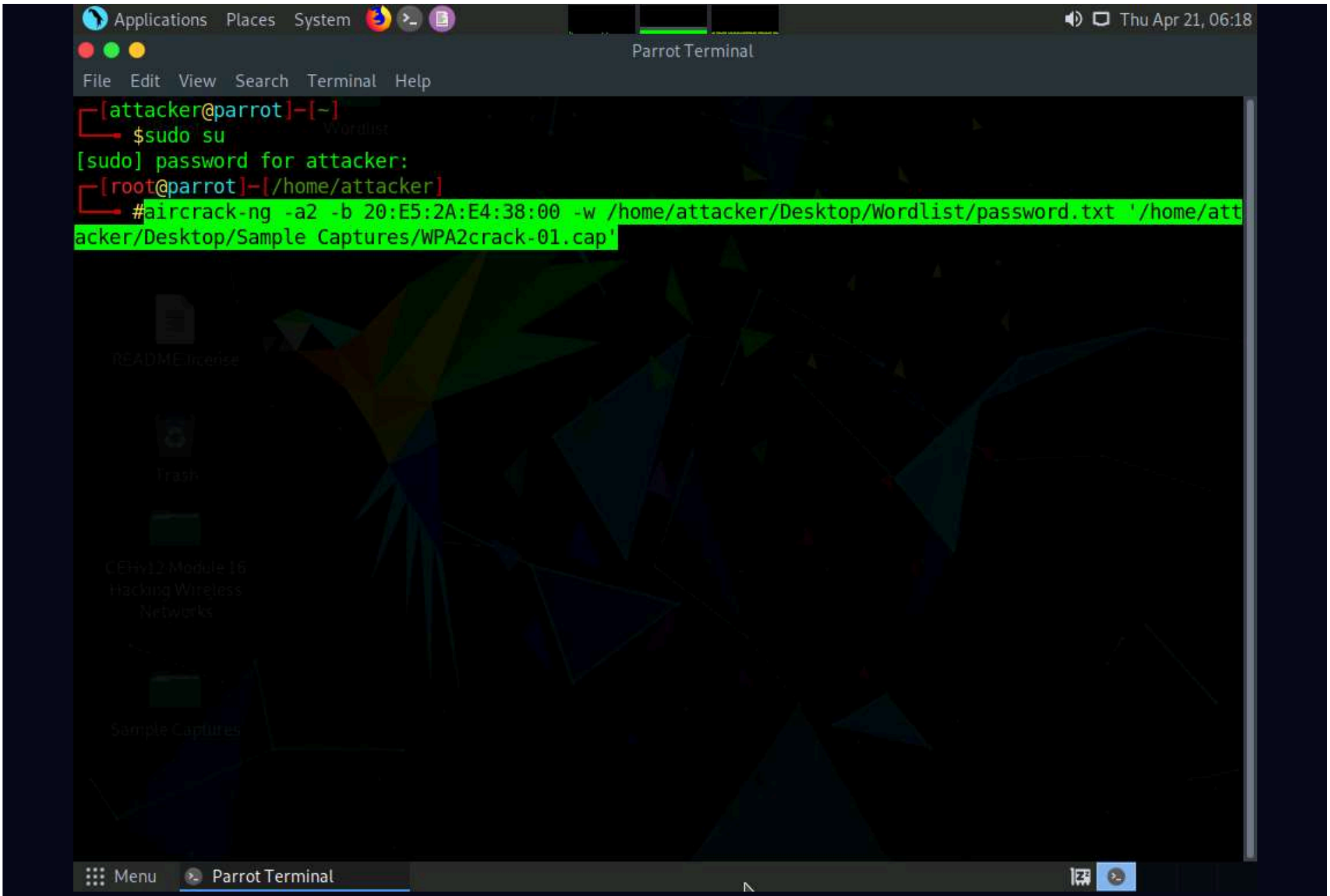
Note: The password that you type will not be visible.



4. In the **Parrot Terminal** window, type **aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'** and press **Enter**. Here, the BSSID of the target is **20:E5:2A:E4:38:00**.

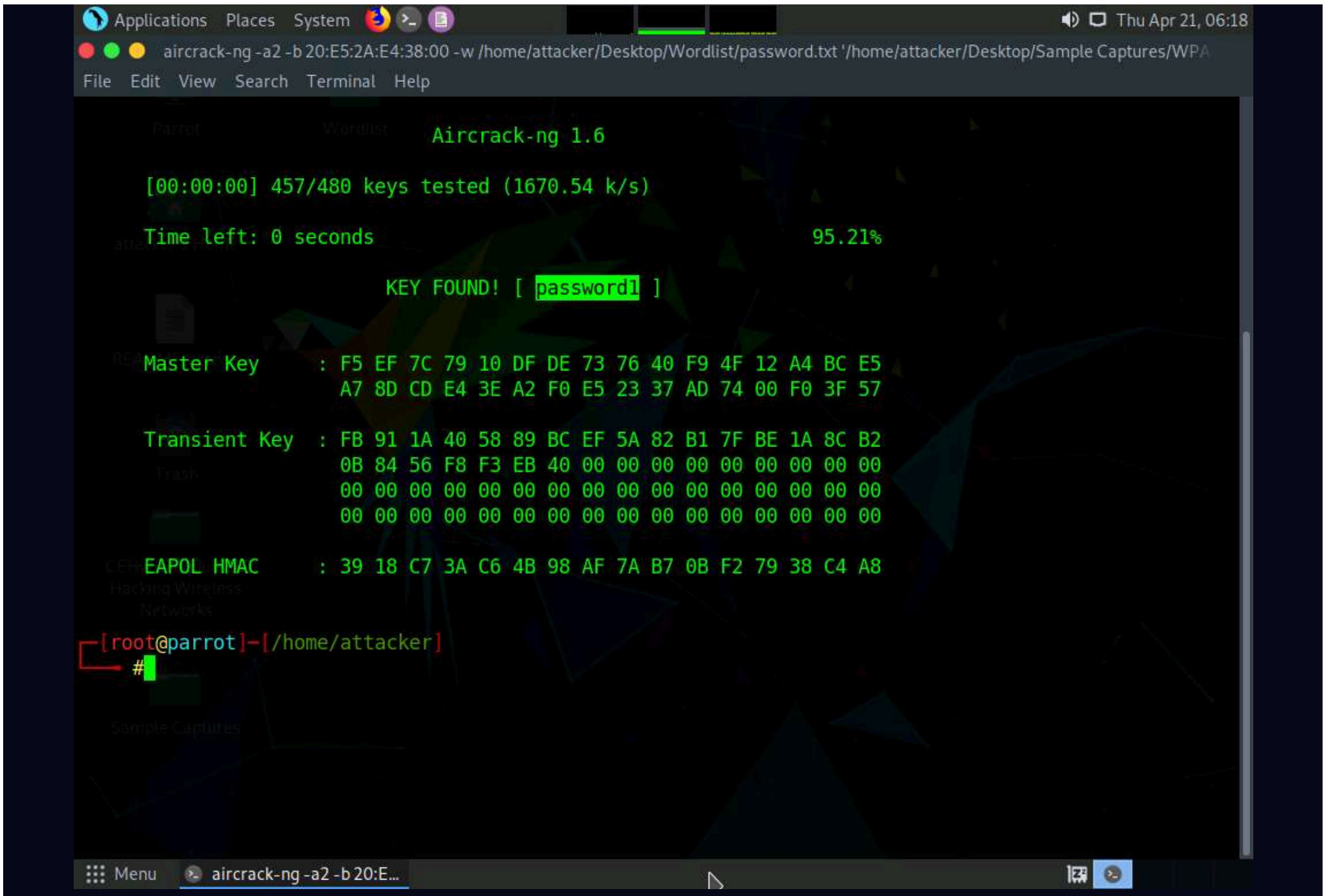
Note: - **-a** is the technique used to crack the handshake, **2**=WPA technique.

- **-b** refers to bssid; replace with the BSSID of the target router.
- **-w** stands for wordlist; provide the path to a wordlist.



5. 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.



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

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

8. 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.