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

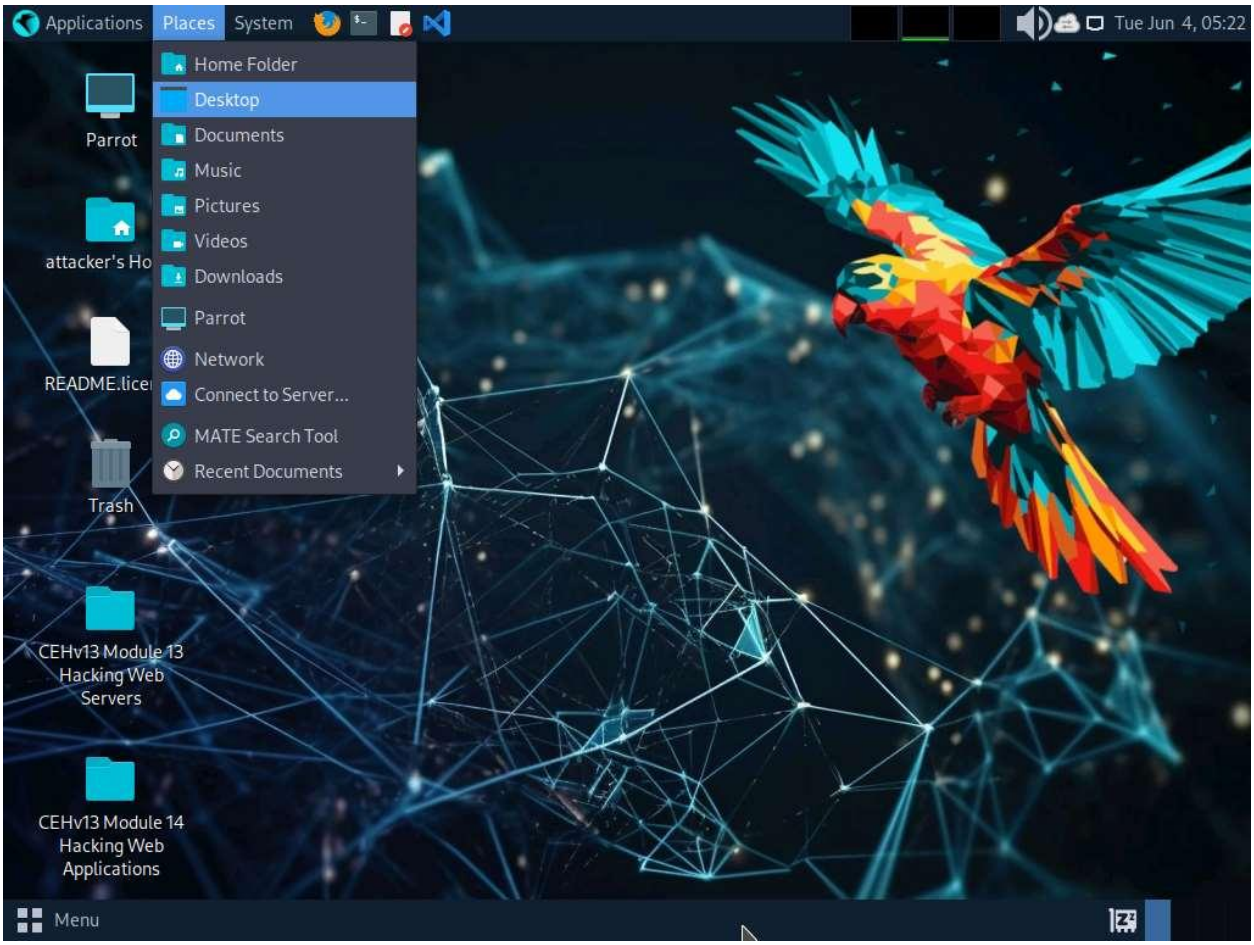
WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security. WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both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

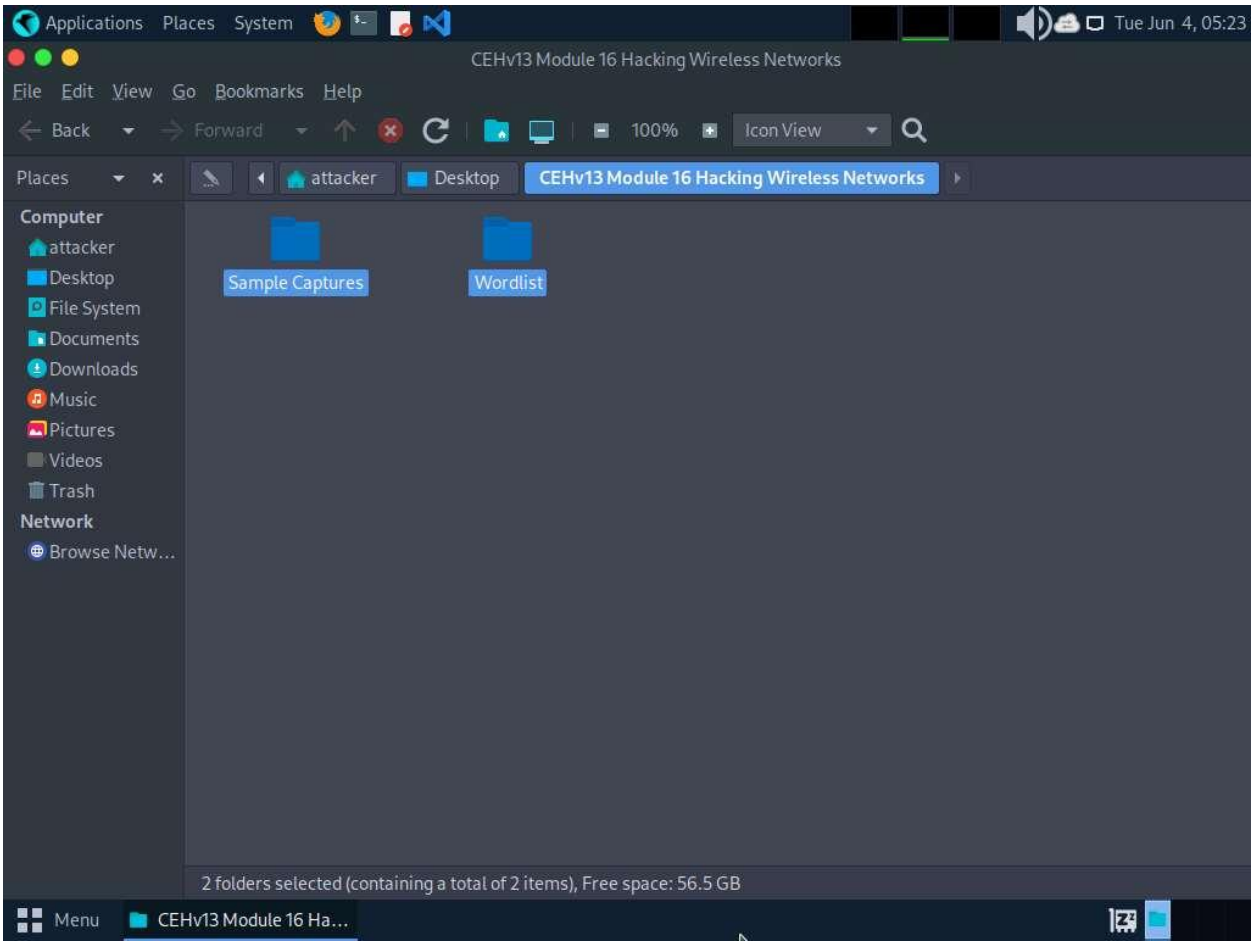
In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (**WPA2crack-01.cap**) to crack WPA key.

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.

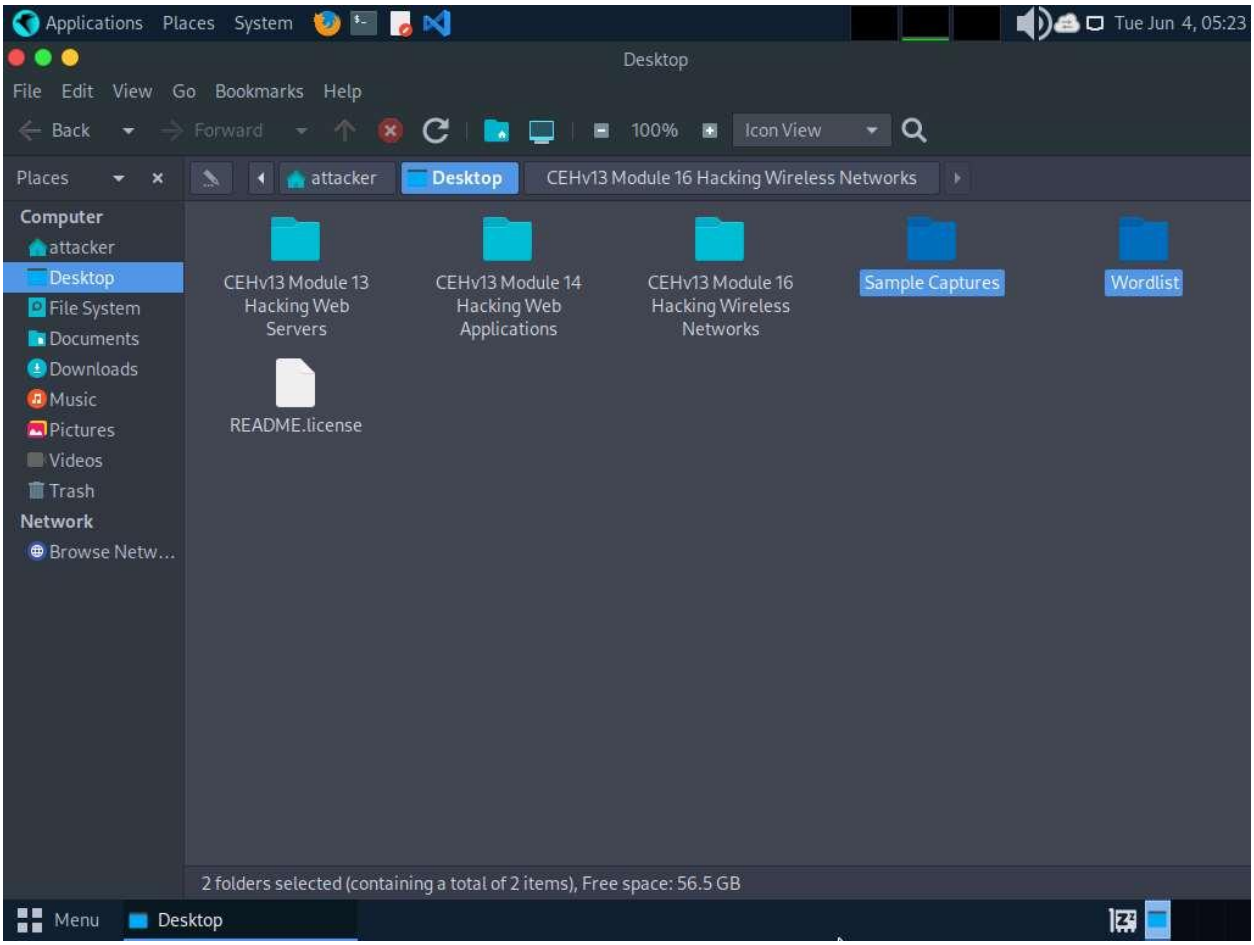


3. The **Desktop** window appears, navigate to the **CEHv12 Module 16 Hacking Wireless Networks** folder and copy **Sample Captures** and **Wordlist** folders.

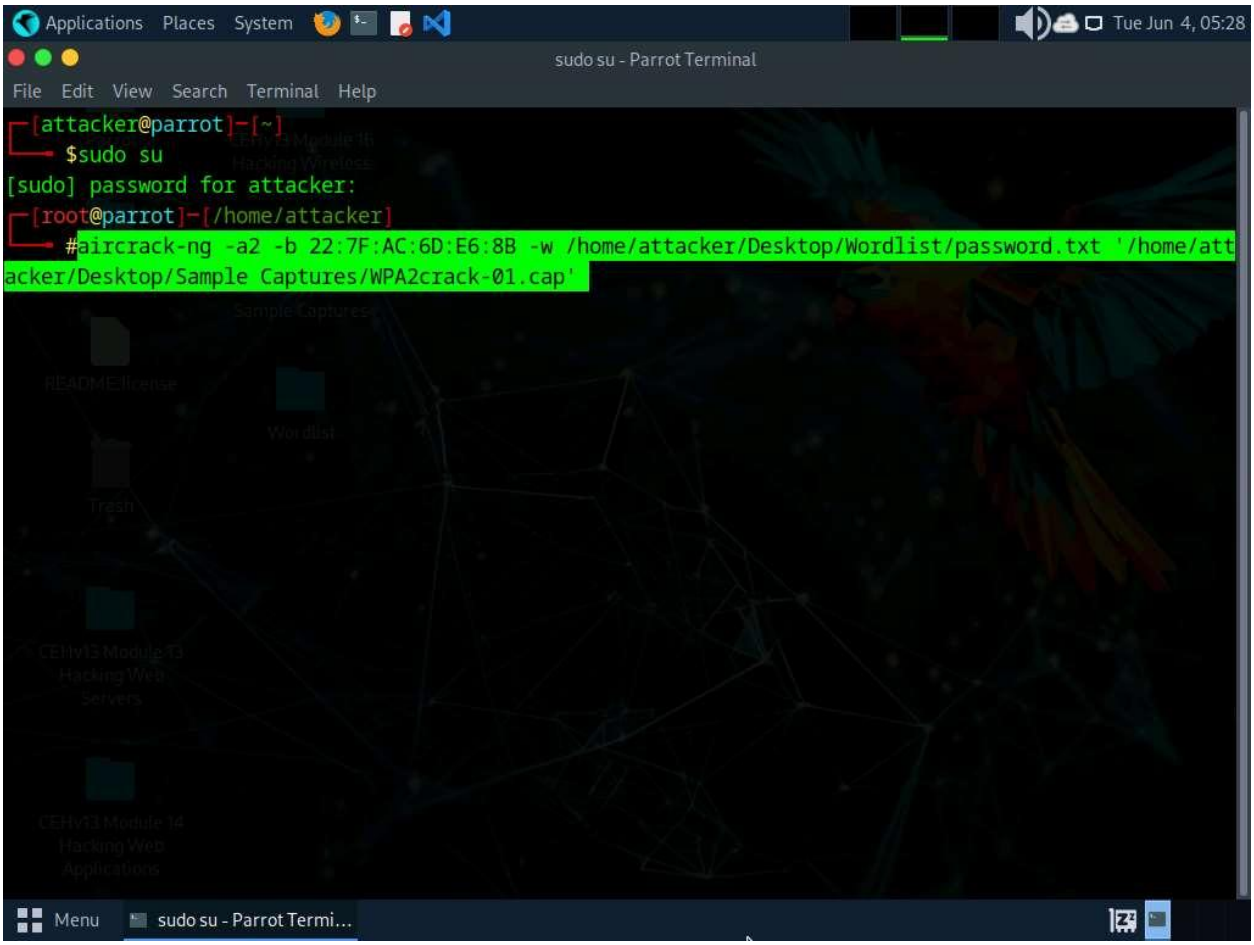
To copy the folders, firstly select both the folders and then press **Ctrl+C**.



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

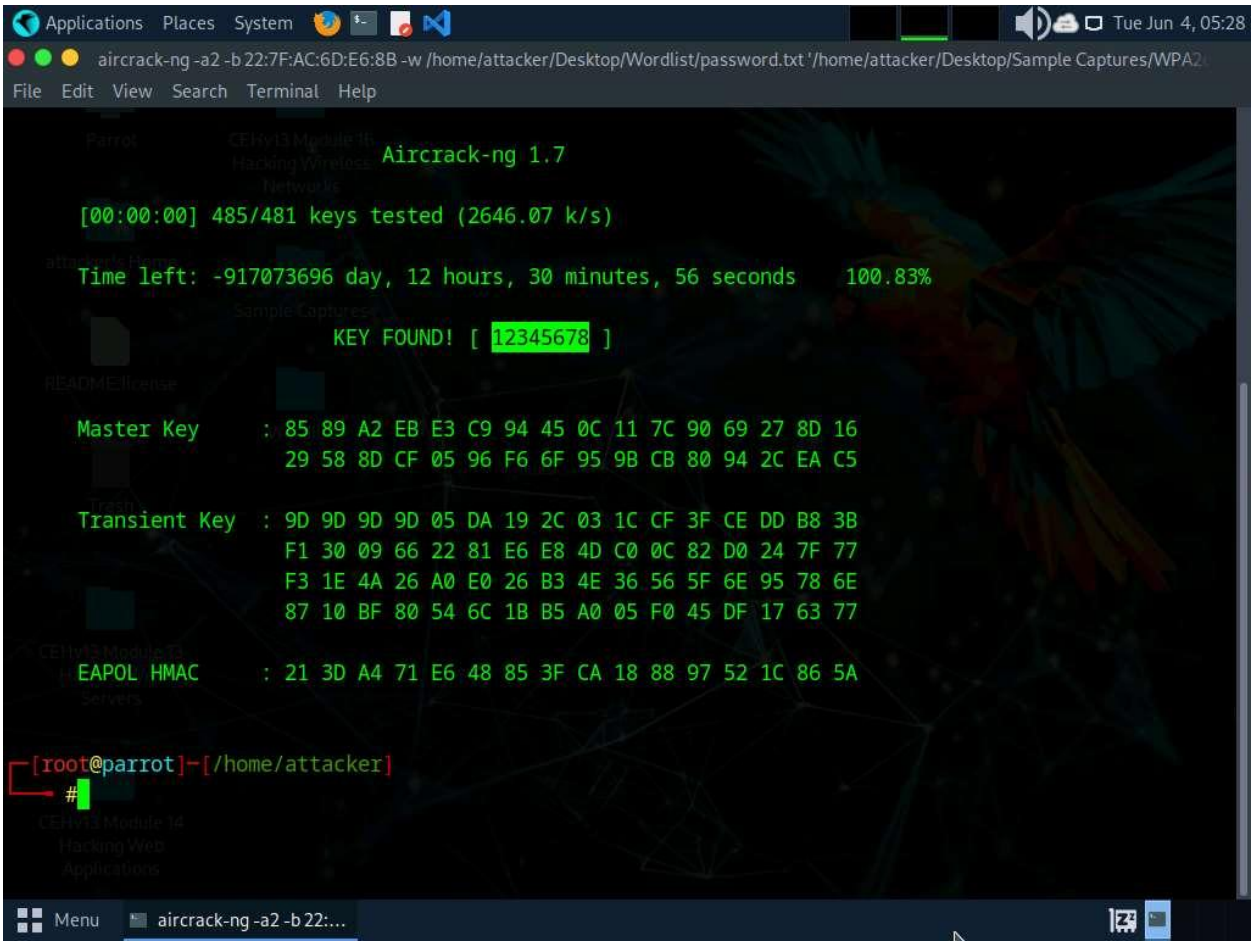


5. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
6. In the **Parrot Terminal** window, run **aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'**. 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.



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.



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