Cryptography

Lab 2 |Rajesh Avala | R11772787

# Experiment Steps:

The Experiment involves launching an attack on WPA2- protected Wi-Fi network.

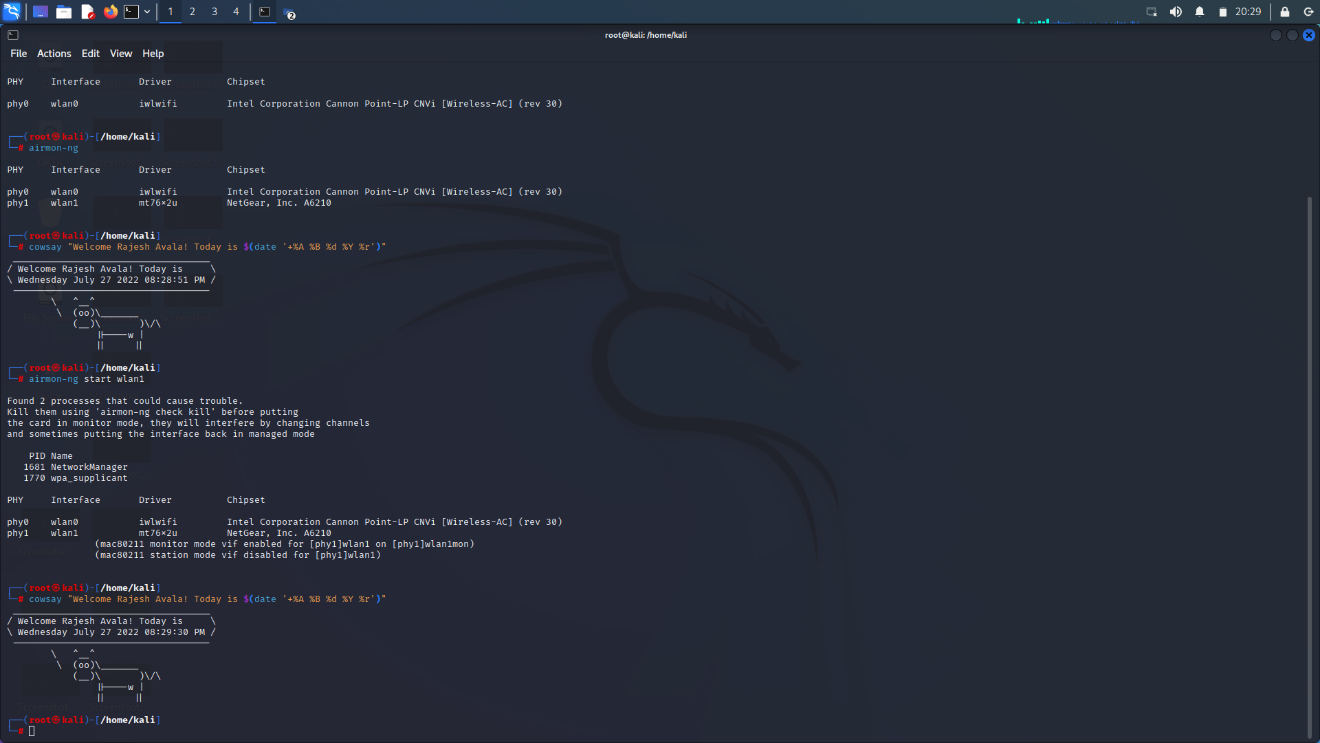
This can be done using the following options

* Dual Boot OS option
* Using virtual box
* Using live USB
* In this experiment I’ve used Live USB kali Linux with cowsay for date and time stamp, aircrack-ng for cracking the protected key.

## part-1:

**Step-1:** To verify whether the wireless adapter has been detected by live kali Linux I’ve used. It is also used to switch the transition from monitor to managed mode. Executing it without any parameters shows the status of interfaces.

**Command:** *airmon-ng*

****

It can be observed that kali has detected the wireless adapter with all the specifications.

**Step-2:** Now the detected adapter has been kept in monitor mode as shown below.

The snapshot shows that it has detected two error process and has to be killed and switch back to monitor mode again.

**Command:** *airmon-ng start wlan1*

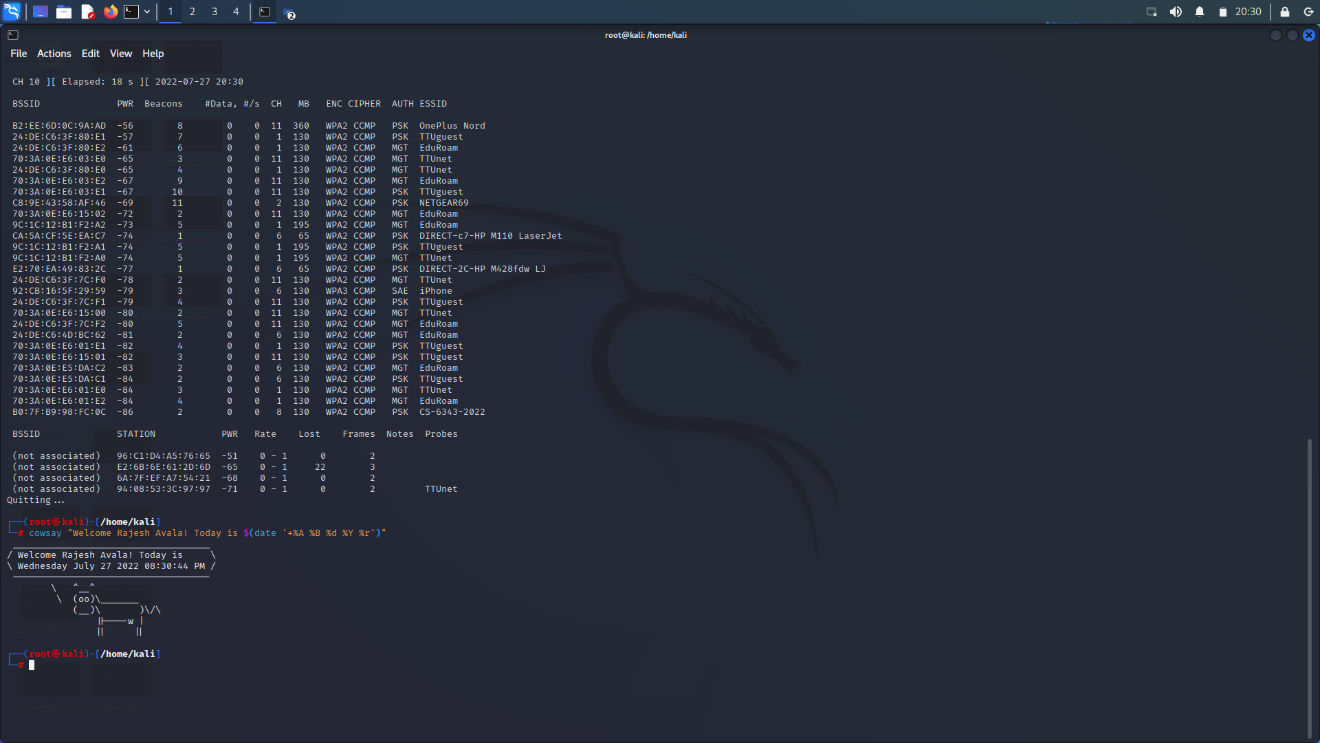
**

The snapshot shows that it has detected two error process and has to be killed and switch back to monitor mode again using.

**Command:** *airmon-ng check kill*

**Step-3:** Displaying wireless networks information that are detected by Wi-Fi adapter. In addition, airodump-ng creates a text file that contains information about all of the access points and clients it encounters.

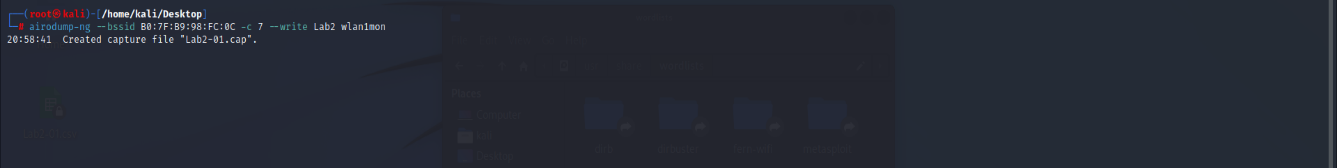
**Command:** *airodump-ng wlan1mon*

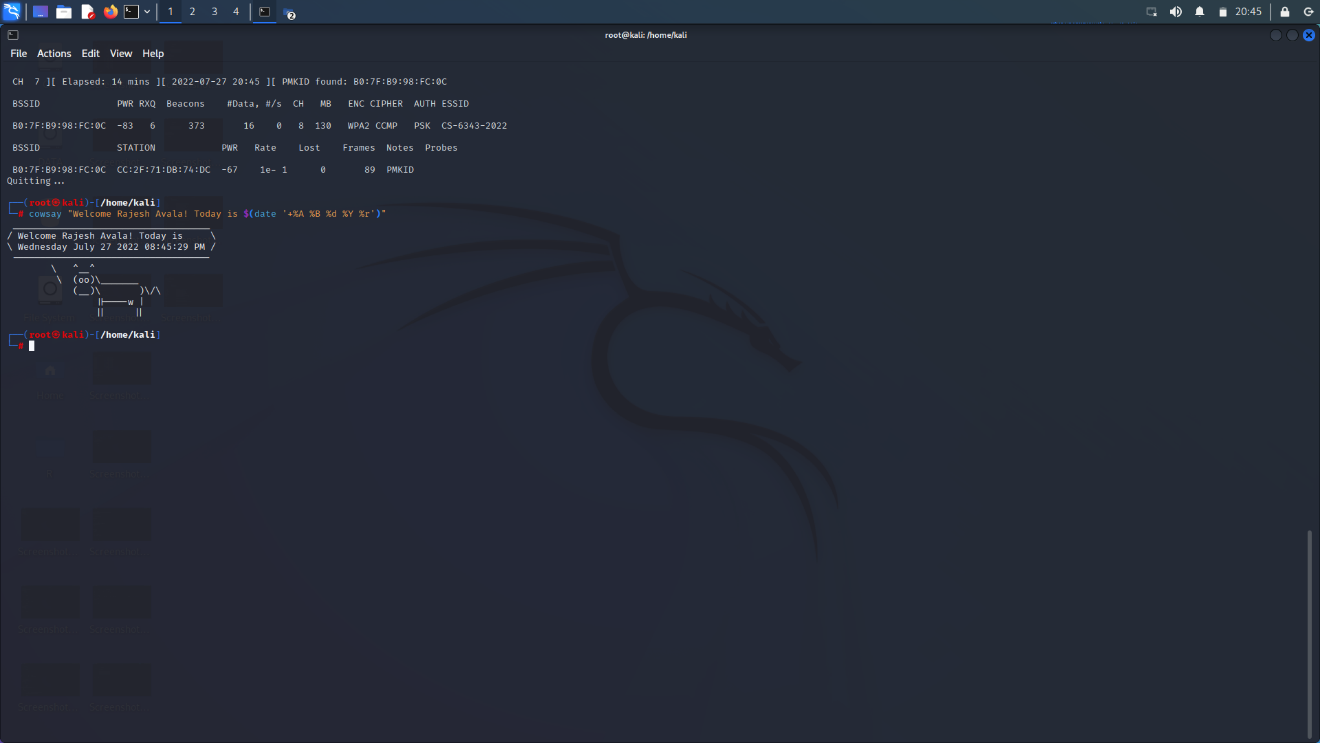
****

We have identified the desired wireless network (Access point) **CS-6343-2022** which is assigned for the lab as highlighted with blue arrow in the above snapshot. Hence quitting the adapter from detecting the other networks.

**Step-4:** Now we identify the network traffic to capture the date by using the access point obtained above.

**Command:** *airodump-ng --bssid B0:7F:B9:98:FC:0C -c 7 –write Lab2 wlan1mon*

**

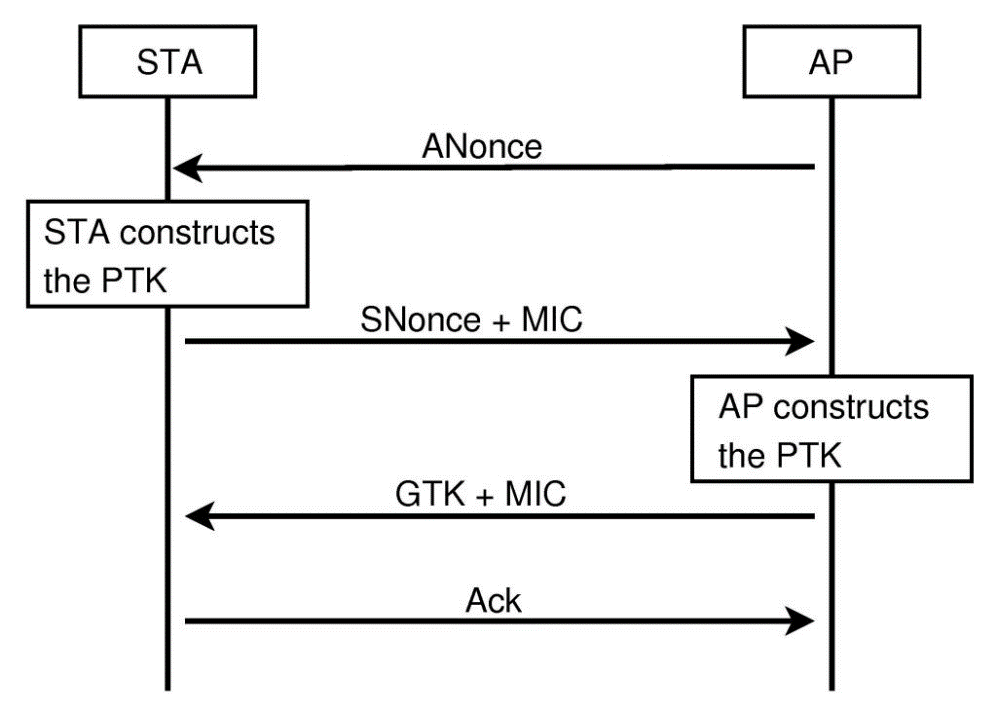
**

Here the given BSSID of CS-6343-2022 and –c is the channel of SSID Lab2 is the file created to save the captured data and wlan1mon is the interface wlan1 in monitor mode.

This will create the cap file in the directory we followed in above command and we need to extract the file.

The handshake was successful and we have found the PMKID: B0:7F:B9:98:0C which is elapsed for 14 min in channel 7.

CC:2F:71:DB:74:DC is the client MAC address connected to the Access point.



**Step-5:**

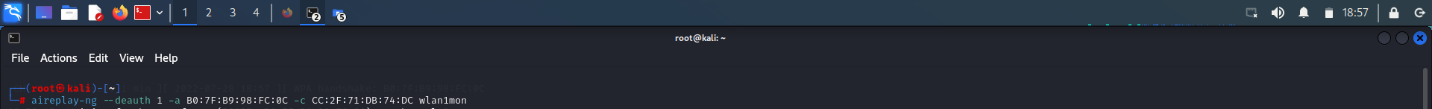
4 way WPA handshake:

* AP sends a ANONCE to client. Here the client has every requirement to create PTK because he got ANONCE as it was only thing missing.
* Client replies to Access point with SNONCE and MIC. Main function of MIC is that AP recognizes as it was from original client. After the confirmation from AP it will create the PTK.
* Now, the AP replies to the client with the GTK as it will be a new client itself and install the GTK.
* Finally, Client sends the ACKNOWLEDGEMENT saying everything is ok.

**Step-6:**

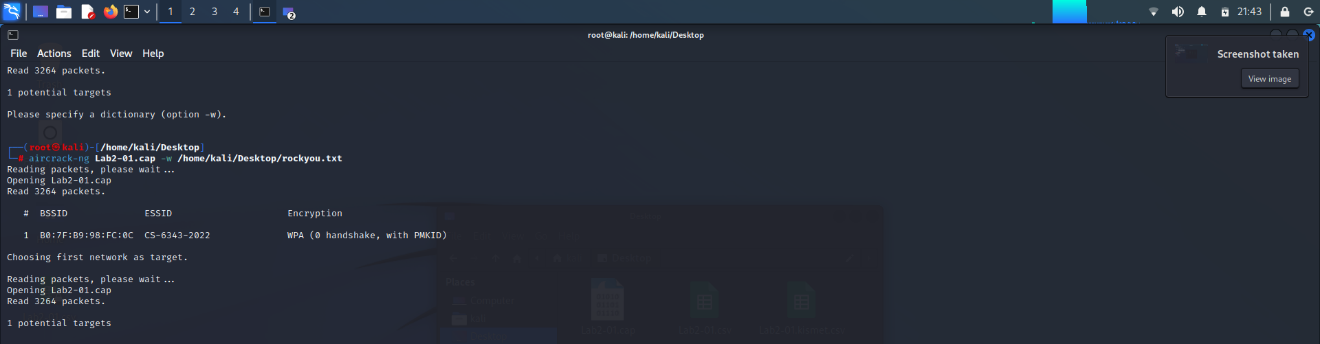
**Command:** *aireplay-ng -- deauth 1 –a B0:7F:B9:98:FC:0C –c CC:2F:71:DB:67:17 wlan0mon*

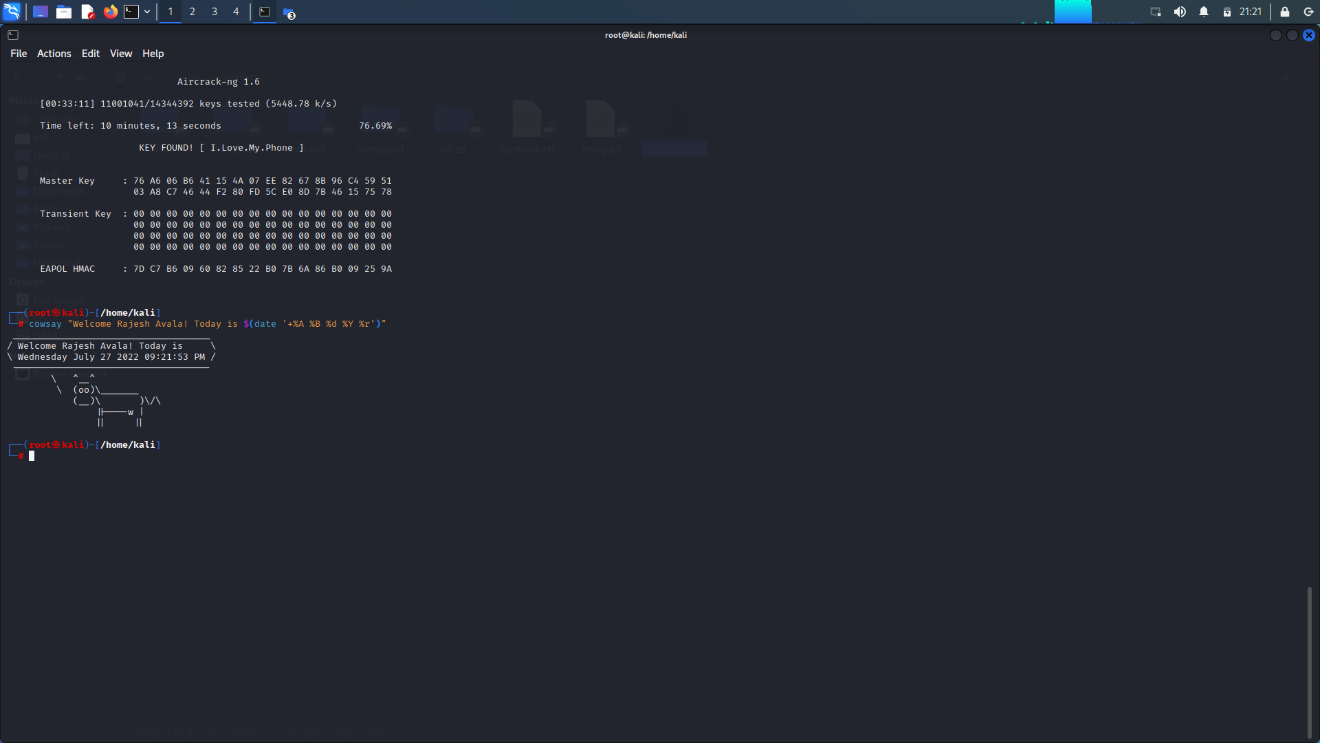
After running the above command, WPA handshake is captured once it is executed.

****

**Step-7:** Aircrack –ng is a set of tools which is used for detecting the flaws in Wi-Fi networks it will execute a brute-force on a target network and find the password for the network.

**Command:** *aircrack-ng*

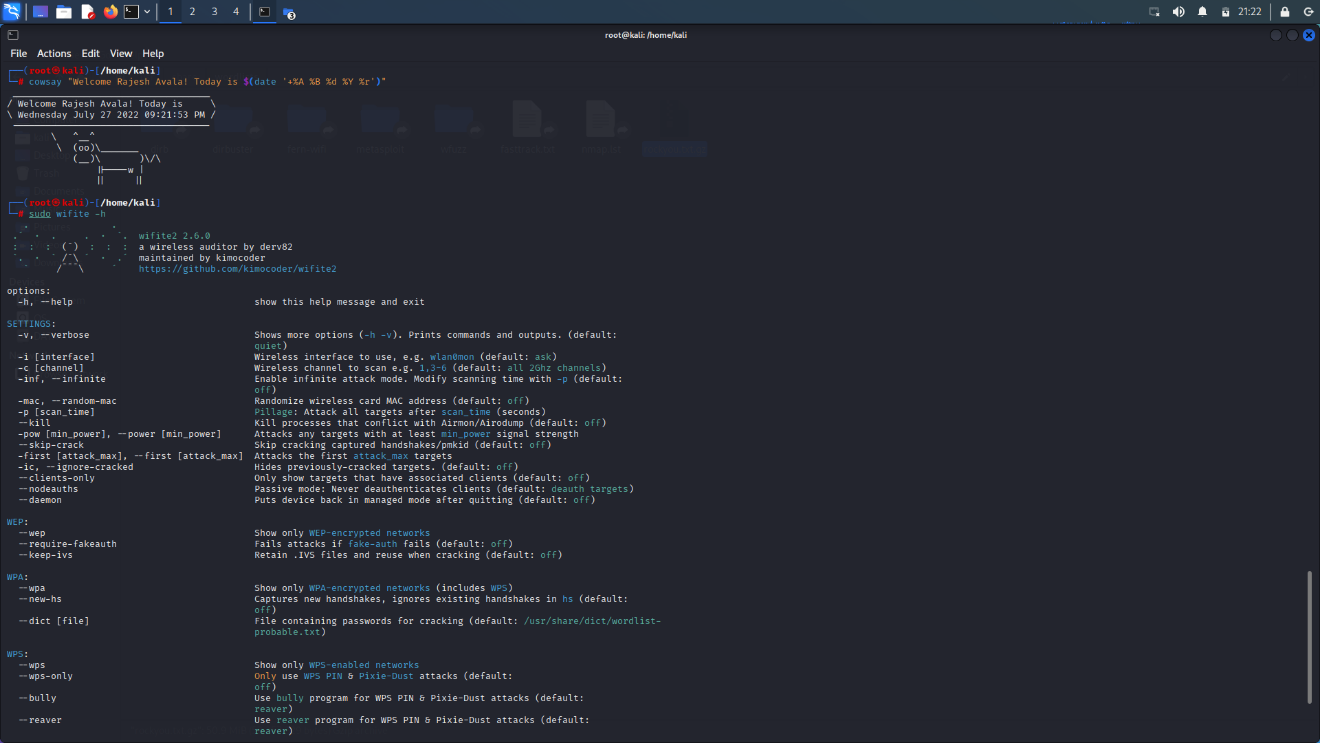


By executing the above command it will do the brute force attack on the target network and find the password (PSK) of the network.****

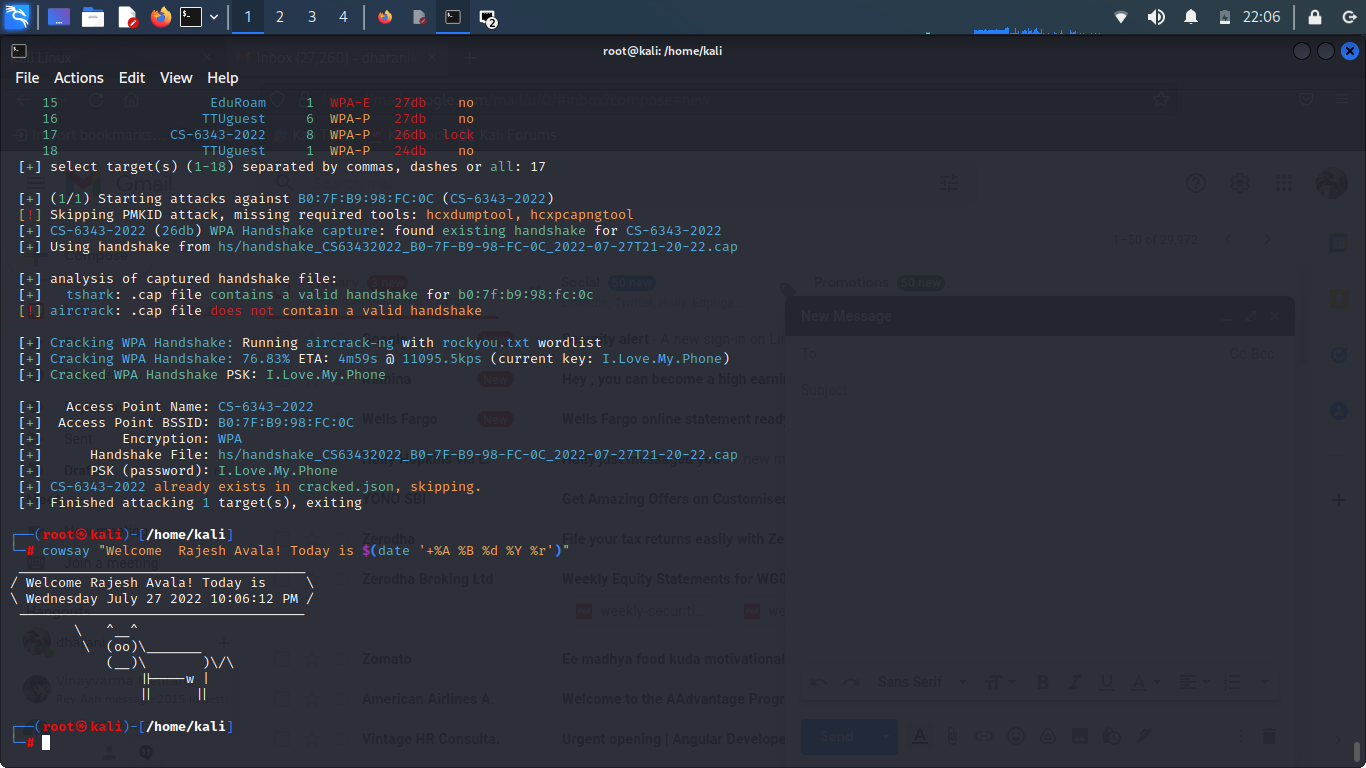
**Part-2:**

As instructed, ive used Wifite2 tool to run the attack again.

**Command:** *sudo wifite –h*

****

**Command:** sudo wifite –dict/home/kali/Desktop/rockyou.txt

****

We can observe from the above snapshot we got the same PSK: *I.Love.My.Phone.*

aireplay-ng -- deauth 1 –a B0:7f:B9:98:fC:0C –c CC:2F:71:DB:74:DC wlan1mon

In the sixth step, we separated the Message Integrity Code from the other parameters that comprise the Pairwise Transit Key with the broadcast command (PTK).

PTK is the technique of encryption utilized between the client and the access point. However, for encryption between client and access point, many factors such as Pairwise Master Key, ANONCE, SNONCE, MAC (access point), and MAC (client) are necessary (client). PMK + ANONCE + SNONCE + MAC (access point) + MAC = PTK (client). This command determines if the Message Integrity Code obtained from the combination corresponds to the original MIC. This is a time-consuming technique.

$ aircrack-ng Lab2-01.cap –w /home/Desktop/rockyou.txt

The seventh step aircrack command is a dictionary attack that operates in the CPU and requires a passcode list. If the network password isn't in the list, we can't hack. This assignment includes the password that we hacked.

Q3: How WPA2 be protected from this brute-force attack

1. To avoid this sort of attack, use strong and unique passwords with long passwords that are difficult to brute force.

2. Because the attacker must first be authorized, using access-list helps to safeguard your network.

3. Keep your device patched and up to date, which means updating the operating system on all client devices to improve WPA2 security and ensuring the most recent upgrades.

4. Prevent remote access to your router, i.e., restrict access over Wi-Fi so that updates can only be done by connecting in through an Ethernet cable to guarantee that your router configuration cannot be tampered with via a wireless connection.

5. To view router settings using a web browser, enter the IP address.

6. To completely remove the risk of this attack, use WPA-PSK (don't forget to use AES-CCM encryption). In this attack, WPA-PSK will not include the field used to validate the password.

7. The ability to prevent sending PMKID in WPA2-PSK handshake message 1. Disabling it will also protect your network from this type of attack. RouterOS versions 6.40.9, 6.42.7, and 6.43 support this option (from rc56).

8. Using a secure VPN such as Norton Secure VPN, the web traffic is encrypted and protected from interception.