**QUESTIONS**

1. record screenshots for each stage of the experiment and give brief descriptions of the meanings of the content seen in each screenshot.

**Ans**: All the below screenshots and explanation answers this question.

1. using your knowledge of the WPA2 handshake/setup, explain what is happening in Steps 6-7.

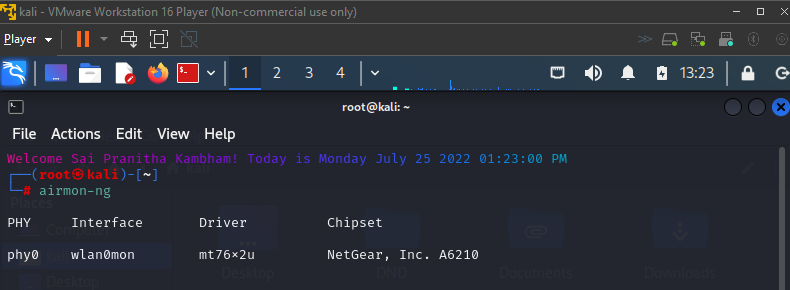
**Ans**: This is the command **aireplay-ng -- deauth 1 –a B0:7F:B9:98:FC:0C –c CC:2F:71:DB:67:03 wlan0mon**, we used in step-6. Here we are capturing the 4-way handshake that is sent from the client with MAC **CC:2F:71:DB:67:03** to access point with MAC **B0:7F:B9:98:FC:0C**. In the step-7, using the rockyou.txt file which contains millions of passwords are being encrypted and compared with the file that captured handshakes which is an offline process. This is how we crack the password of the router/ Access point.

1. In your opinion, how could WPA2 be protected from this attack? Discuss as many ideas as possible.

**Ans:** Now, when used a core-i3 processor, it is taking around 2-3 hours to brute force the key present in the wordlist (rockyou.txt). May be the passwords that contain special characters can help as I have observed there are one or two special characters in this wordlist. We can also use VPN for extra encryption.

**PART-I**

1. After installation of kali linux and required setup, I have typed the command **airmon-ng** to determine if wireless adapter is seen by Kali Linux. It has displayed the interface, chipset, and driver as below.



1. I have used the airmon-ng to put your wireless adapter in monitor mode. This will require a command of the form **airmon-ng start wlanxx**.  
   wlanxx is **wlan0mon** (as per the above image)

Text

Description automatically generated

1. The below page has been displayed as soon as I used the command **airodump-ng wlan0mon** (as per the first image). Critical information about the wireless networks is being seen by the wireless adapter as below.

Graphical user interface, text

Description automatically generated

I could see the SSID CS-6343-2022 network (read third from last) and the BSSID, channel number etc., in the above image.

I have captured and saved traffic associated with the channel and BSSID identified in the above step.

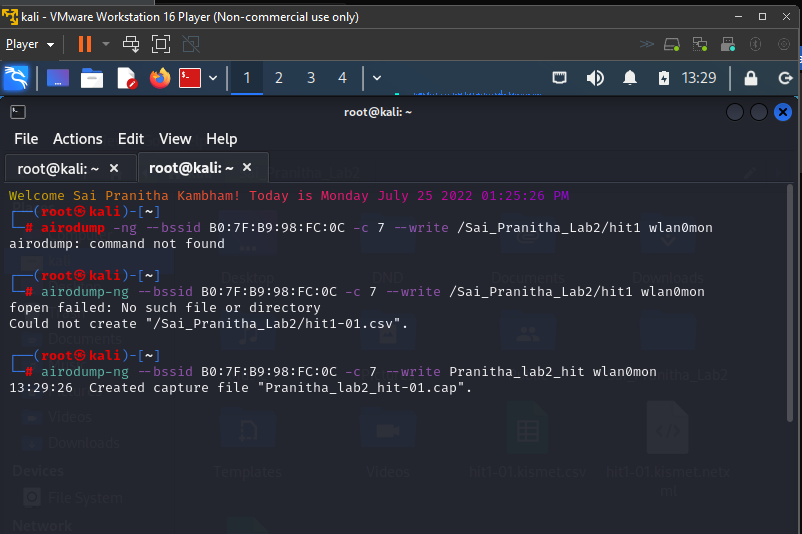
1. From above image,

**B0:7F:B9:98:FC:0C** is the BSSID,  
**7** is the channel,

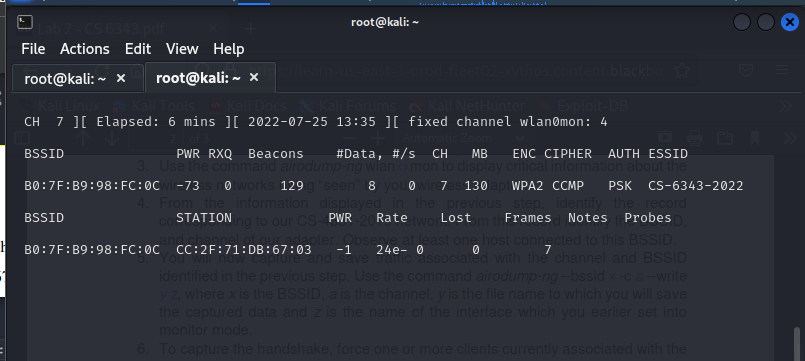
1. I used the command

**airodump-ng --bssid B0:7F:B9:98:FC:0C -c 7 --write /Sai\_Pranitha\_Lab2/hit1 wlan0mon**,

where,  
  
/Sai\_Pranitha\_Lab2/hit1 is the file name to which I have saved the captured data   
wlan0mon is the name of the interface which you earlier set into monitor mode.



After execution, we could see some client ID’s displaying.

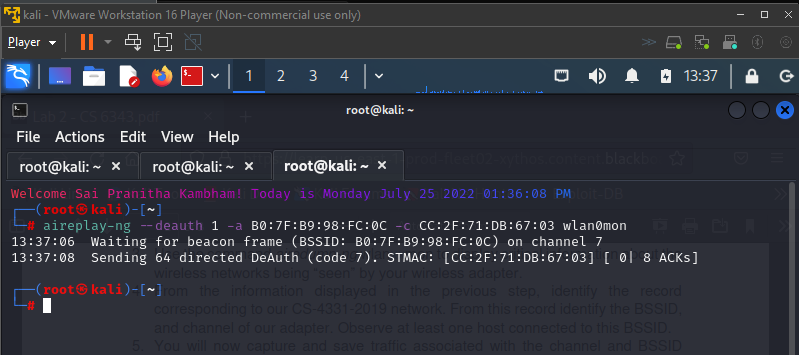


To capture the handshake, we force one or more clients currently associated with the Access Point (AP) to disassociate.

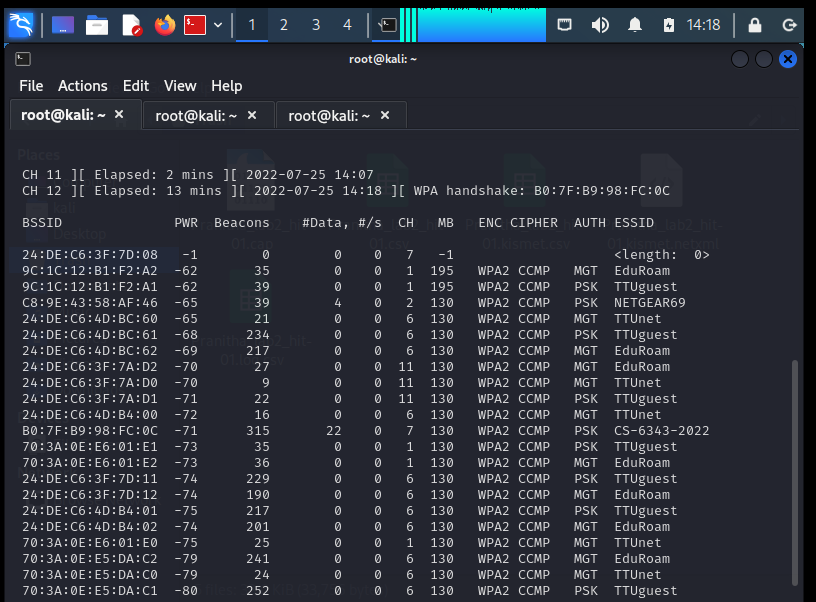
1. I have used the command:

aireplay-ng -- deauth 1 –a **B0:7F:B9:98:FC:0C** –c **CC:2F:71:DB:67:03** wlan0mon

where **B0:7F:B9:98:FC:0C** is Access Point MAC and **CC:2F:71:DB:67:03** is Client MAC

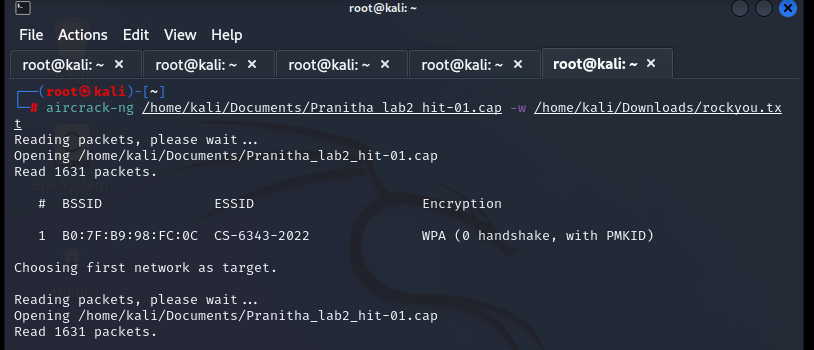


After execution of the above command, we can see the Handshake as shown below

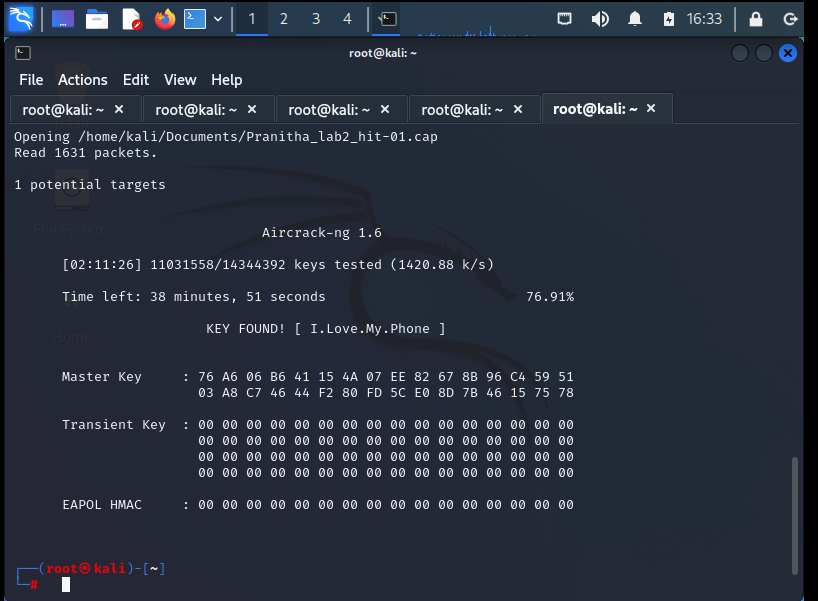


1. As the handshake is captured, I have cracked the password using aircrack-ng /home/kali/Documents/Sai\_Pranitha\_Lab2/hit1 /home/kali/Downloads/rockyou.txt,

The actual password list zipped file rockyou.txt.gz which is in /usr/share/wordlists/ is unzipped and saved in /home/kali/Downloads/rockyou.txt



After execution of the above command, and waited for quite sometime. We can see the below screen.

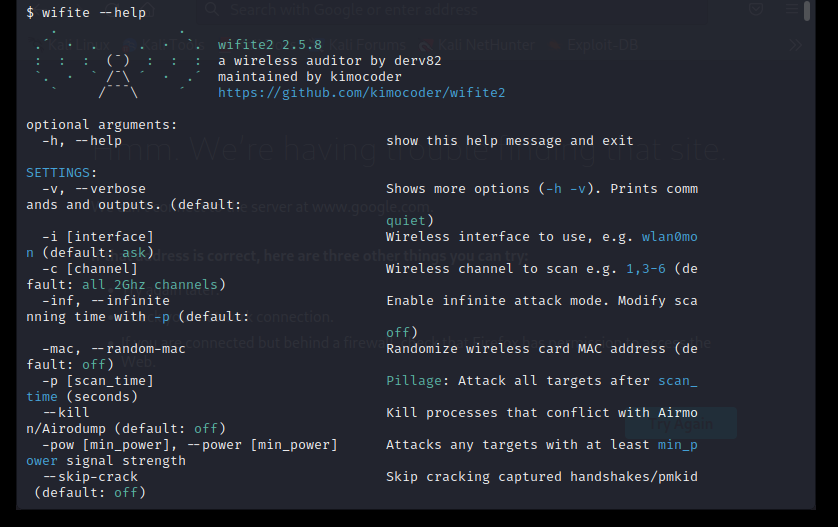


The password has been cracked. And it is **I.Love.My.Phone**

**PART-II**

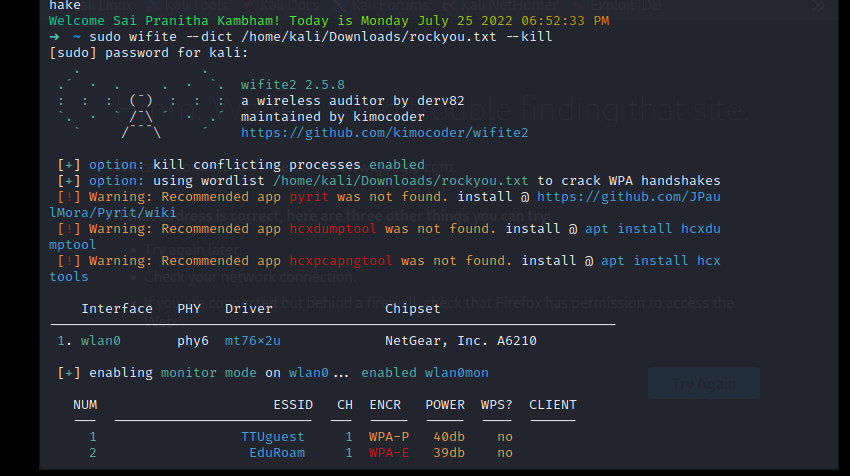
1. In this part, we attack the same network using different tool, Wifite2.

Checking the Wifite2 command in kali linux.

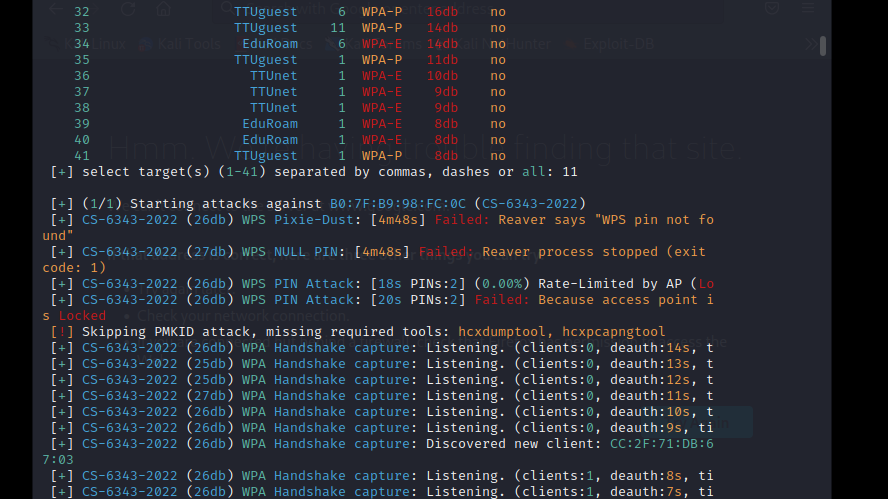


1. $ sudo wifite --dict /home/kali/Downloads/rockyou.txt –kill

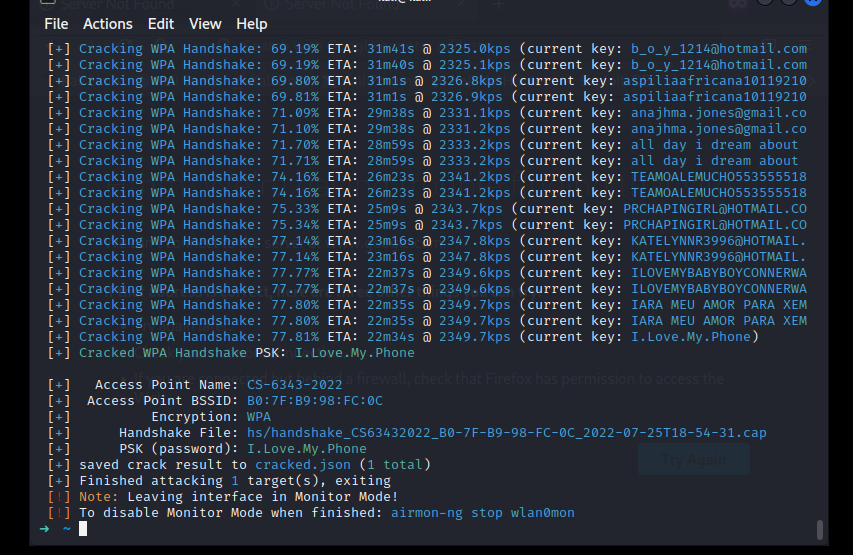
Wlan0 in monitor mode



1. After finding the required network, we do Control-C and this is our target. The airdump, aireplay commands we execute manually are being automated in this tool. An attack will start and capture the handshake of the network, and analyse it to decode with different type.



1. After checking all the handshakes, we get the required PSK



And as shown above the PSK is I.Love.My.Phone