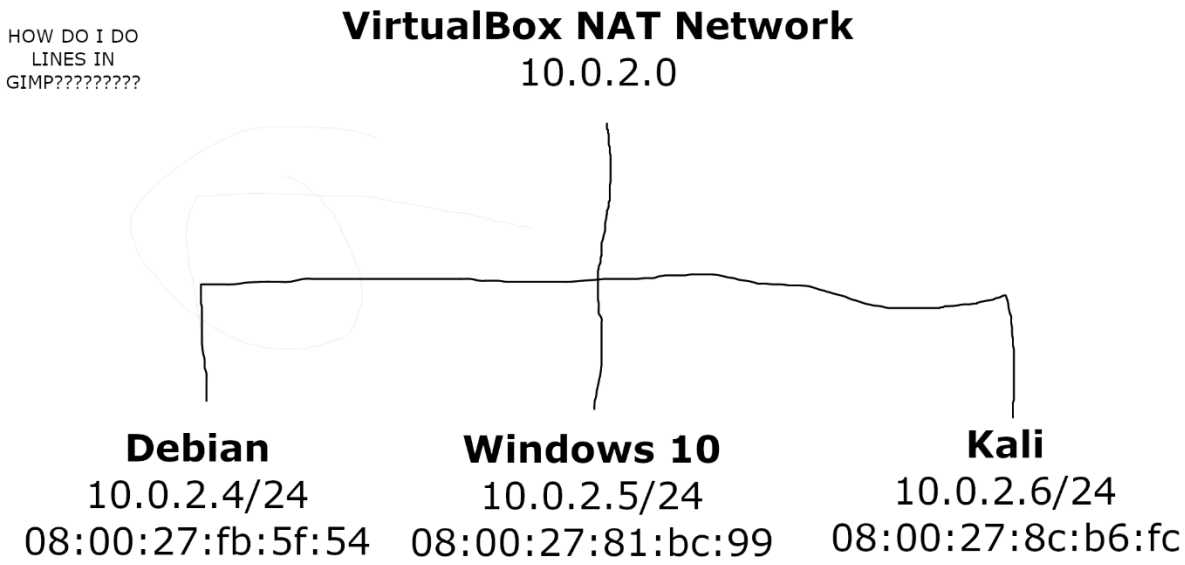



# TP Découverte Kali Linux

L'objectif est de découvrir l'intérêt de sécuriser correctement une machine sous Windows ou Linux et savoir se protéger en se mettant à la place de l'attaquant via Kali Linux.

**Préparation :**

Installer une VM de Windows, de Linux (ici Debian) et de Kali.

Mettre les VMs sur le même réseau. Dans ce cas VirtualBox est utilisé, donc il faut créer NAT Network dans *Outils* et puis connecter les VMs sur ce réseau.

Utiliser *ip a* dans le Terminal de Debian et Kali pour obtenir leurs adresses IP et leurs adresses MAC.

Utiliser *ipconfig* dans la console de Windows pour obtenir l'adresse IP et *getmac* pour obtenir l'adresse MAC.

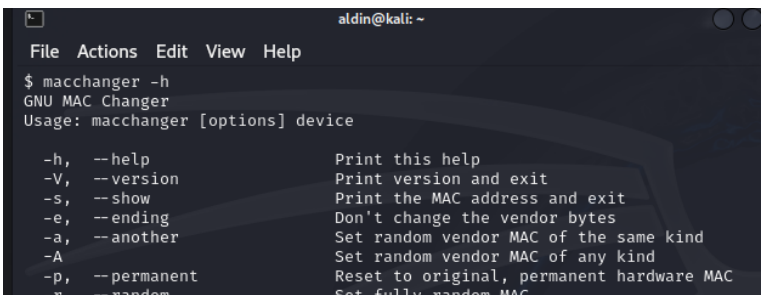
Maintenant utiliser *ping <adresse IP>* pour vérifier que les VMs sont sur le même réseau.

Attention : Il faut désactiver le pare-feu de Windows car il ne répond pas sur les pings des autres.

Après avoir reçu les paquets du ping, on peut commencer.

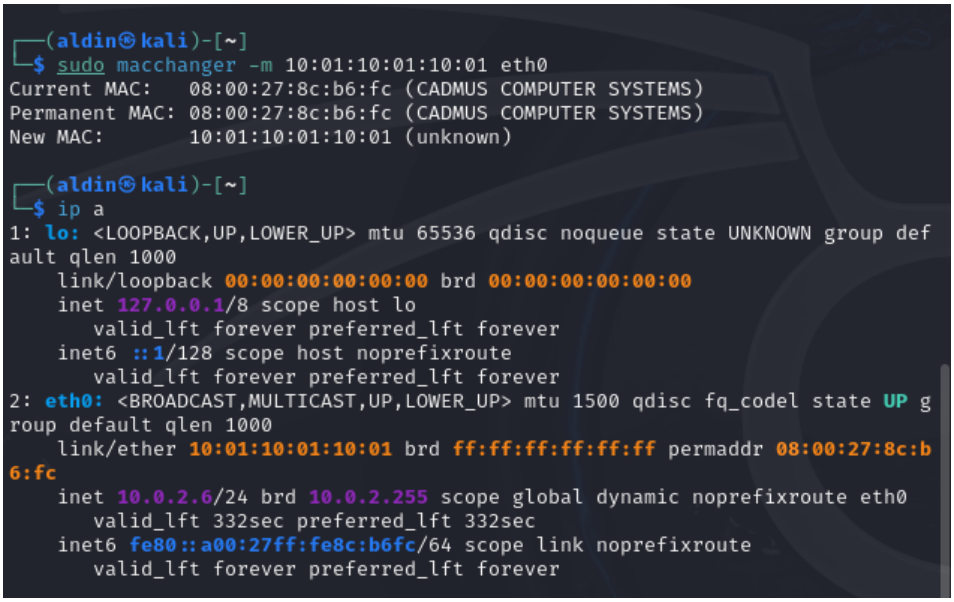
**Changer l'adresse MAC :**

Sur Kali, ouvrir l'application *macchanger* (trouvable sous /usr/share/kali-menu/applications/).



(Source : macchanger | Kali Linux Tools, au moins c'est comme ça dans la consigne mais elle n'a pas aidé, mais heureusement ça était là pour moi.)

Utiliser la commande *macchanger -m <adresse MAC> eth0* pour changer l'adresse MAC. Pour voir le résultat utiliser *ip a*.




C'était très facile à faire avec les bonnes consignes, mais avec ce changement on peut faire du bien mais aussi beaucoup du mal.

Le grand plus c'est d'être anonyme car personne ne peut enregistrer la machine utilisée car la vraie adresse MAC est cachée. Le danger en revanche est de dépasser des protocoles de sécurité. Si notre adresse MAC est exclue il faut juste la changer afin d'ignorer ce blocage, si les IPs sur un réseau sont réservées pour des certaines adresses MAC, on peut juste changer l'adresse jusqu'à ce qu'on puisse se connecter, c'est donc une attaque de brute force sur un réseau afin de pouvoir passer comme un utilisateur authentiqué.

La seule chose qu'on peut faire pour se protéger contre le MAC spoofing est vraiment la réservation des adresses IP sur réseau en utilisent des adresses MAC spécifique car même avec brute force, il sera difficile de trouver une adresse valide.

**Changer l'adresse MAC :**

Sur Kali, ouvrir l'application *zenmap-kbx* ou *nmap* sous mon Kali (trouvable sous /usr/share/kali-menu/applications/).

Taper *nmap -sn 10.0.2.0/24* pour scanner (ping tous les hôtes de) notre réseau (IP de notre réseau).

```
┌──(aldin㉿kali)-[~]
└─$ sudo nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 10:20 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00025s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00081s latency).
MAC Address: 08:00:27:05:72:43 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00071s latency).
MAC Address: 08:00:27:FB:5F:54 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.6
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.02 seconds
```

Le scan trouvait 2 hôtes (car le Windows n'est pas allumé) avec une carte réseau de VirtualBox avec leur adresse IP.

Avec *-O* on peut trouver l'adresse MAC, le système et les ports ouvertes des hôtes.

```
Nmap scan report for 10.0.2.5
Host is up (0.0011s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:81:BC:99 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
```

Avec ces informations on pourrait faire des choses malveillantes.

Si on sait que cette machine est réservée dans un réseau en utilisant de son adresse MAC, on peut juste utiliser macchanger en utilisent de cette adresse MAC pour accéder ce réseau.

Si on connaît le système on sait quelles vulnérabilités existent afin de les exploiter.

Si on connaît les ports ouverts et leur service on peut envoyer des paquets pour forcer une réaction peut-être malveillante.

Ces sont seulement des exemples car je n'ai pas assez de l'expertise mais avec cet outil on peut gagner beaucoup des informations sur un réseau et ses hôtes.

Comme cet outil est utiliser pour faire des choses malveillantes, on peut aussi l'utiliser pour tester notre sécurité afin de se protéger contre. Avec du monitoring comme avec des IDS on peut détecter des anomalies et avec un firewall on peut se protéger contre des connections involues.

**Conclusion :**

Il y a des outils qui nous permet de détecter, bloquer et le rendre plus difficile de pénétrer le réseau, mais ce n'est pas impossible avec un peu de travail. Ce travail par contre et visible donc on peut se bien protéger avec un bon monitoring. Donc pour les administrateurs de réseau :

Faites beaucoup de monitoring. Utilisez des IDS pour détecter et signaliser des anomalies, des firewalls pour bloquer toutes les sources de ces anomalies et réservez les places sur le réseau. Ces deux derniers ne sont jamais assez mais on peut les renforcer plus en plus avec les informations qu'on sort du monitoring.