

## Compte rendu tp-Kali Jules Anduze

Utiles pour l'installation de kali :

- mettre 30go min de stockage
- 2cpu minimum
- 2048mo mémoire vive

Ensuite mettez bien toutes vos machines en réseau privé hôte (pour que les machines communiquent entre elles) :

Ping de Debian → Kali :

```
root@debainHack:~# ping 192.168.56.109
PING 192.168.56.109 (192.168.56.109) 56(84) bytes of data.
64 bytes from 192.168.56.109: icmp_seq=1 ttl=64 time=1.48 ms
64 bytes from 192.168.56.109: icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from 192.168.56.109: icmp_seq=3 ttl=64 time=1.01 ms
```

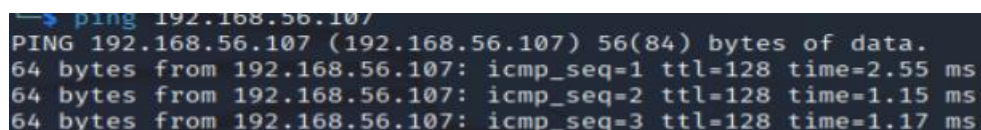
### Petit Tips :

**Il faut désactiver le pare-feu de Windows defender puisqu'il refuse les pings par mesure de sécurité.**

Ping de Debian → Windows:

```
PING 192.168.56.107 (192.168.56.107) 56(84) bytes of data.
64 bytes from 192.168.56.107: icmp_seq=1 ttl=128 time=1.23 ms
64 bytes from 192.168.56.107: icmp_seq=2 ttl=128 time=1.20 ms
64 bytes from 192.168.56.107: icmp_seq=3 ttl=128 time=1.05 ms
```

Ping de Kali → Windows:



```
➥ ping 192.168.56.107
PING 192.168.56.107 (192.168.56.107) 56(84) bytes of data.
64 bytes from 192.168.56.107: icmp_seq=1 ttl=128 time=2.55 ms
64 bytes from 192.168.56.107: icmp_seq=2 ttl=128 time=1.15 ms
64 bytes from 192.168.56.107: icmp_seq=3 ttl=128 time=1.17 ms
```

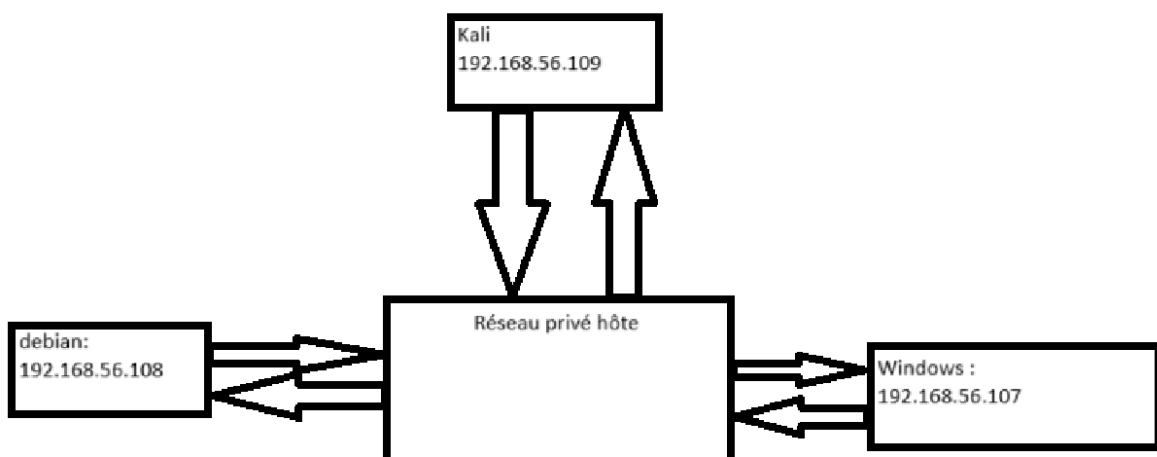
Nous voyons maintenant que toutes nos machines communiquent entre elles.

Les informations importantes de kali :

**Avec la commande IP a toujours utile à connaître :**

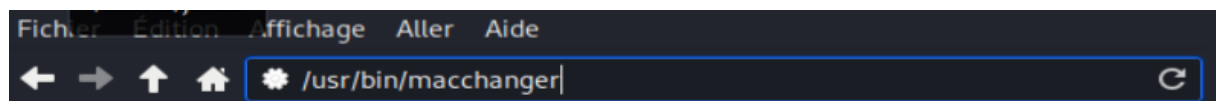
```
(jules@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:63:fb:8f brd ff:ff:ff:ff:ff:ff  
    inet 192.168.56.109/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0  
        valid_lft 346sec preferred_lft 346sec  
    inet6 fe80::a00:27ff:fe63:fb8f/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Schéma simplifié :



Utilisation de macchanger ;

Voici le chemin vers macchanger sur kali :



Ensuite voici comment changer l'adresse mac avec macchanger

Lancé d'abord macchanger

```
(jules@kali)-[~]
$ macchanger -help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help                Print this help
-V, --version             Print version and exit
-s, --show                Print the MAC address and exit
-e, --ending              Don't change the vendor bytes
-a, --another             Set random vendor MAC of the same kind
-A                        Set random vendor MAC of any kind
-p, --permanent          Reset to original, permanent hardware MAC
-r, --random              Set fully random MAC
-l, --list[=keyword]      Print known vendors
-b, --bia                 Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX
    --mac XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
```

Vous arriverez ici, ce sont toutes les commandes possibles avec *macchanger*.

Veillez à être à avoir tous les droits pour ça la commande **sudo su** sur kali est recommander.

Une fois ça, la commande pour changer de Mac adresse est :

**macchanger --mac=[nouvelle\_mac\_adresse] [nom\_de\_votre\_carte\_réseau]**

Pour ensuite vérifier la commande **ip a** est recommandé :

Voici le résultat :

```
(root@kali)-[/home/jules]
# macchanger --mac=08:00:27:60:fb:8f eth0
Current MAC: 08:00:27:63:fb:8f (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:63:fb:8f (CADMUS COMPUTER SYSTEMS)
New MAC: 08:00:27:60:fb:8f (CADMUS COMPUTER SYSTEMS)

(root@kali)-[/home/jules]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
  roup default qlen 1000
    link/ether 08:00:27:60:fb:8f brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:63:f
  b:8f
    inet 192.168.56.109/24 brd 192.168.56.255 scope global dynamic noprefixro
  ute eth0
        valid_lft 351sec preferred_lft 351sec
    inet6 fe80::a00:27ff:fe63:fb8f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

On voit en haut de l'écran l'ancienne adresse mac qui est **08:00:27:63:fb:8f**

Et la nouvelle qui est **08:00:27:60:fb:8f**.

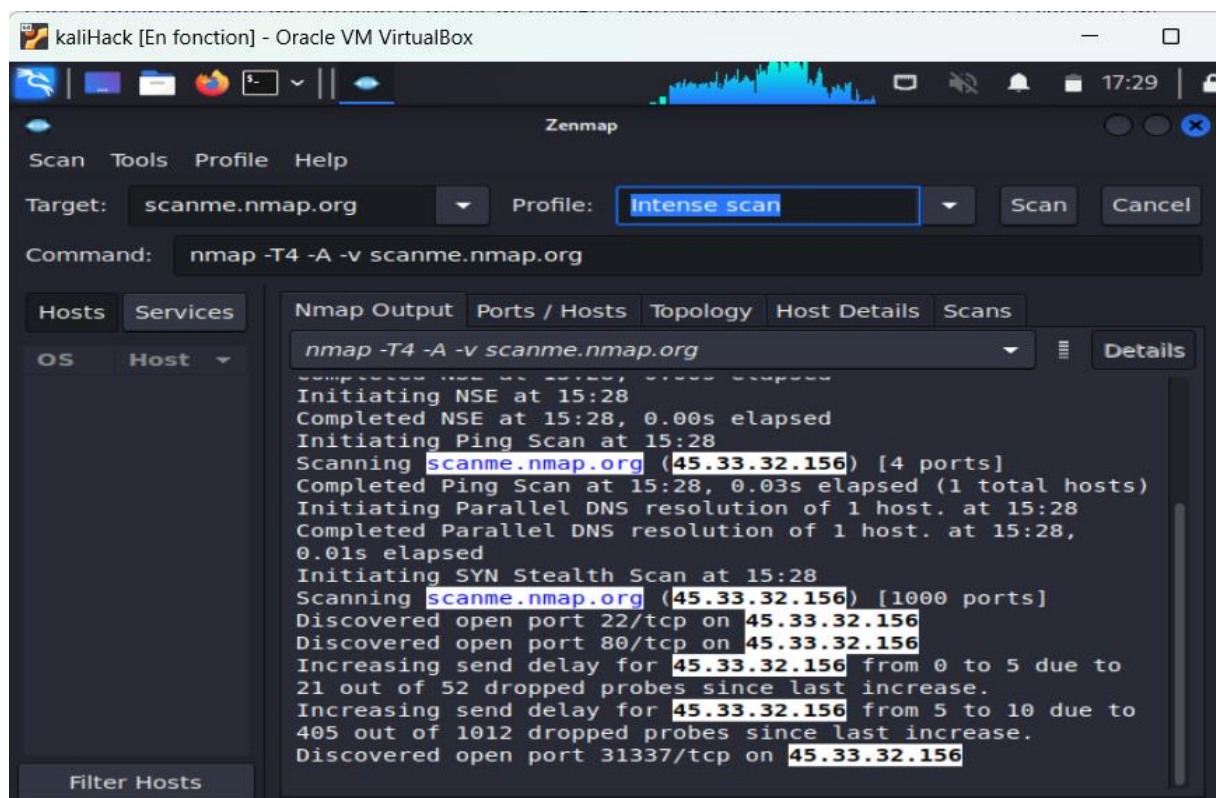
On voit que grâce à **macchanger** changer l'adresse ip ne prend qu'un poignet de seconde.

Passons à la deuxième partie du tp :

Pour ma part l'application zenmap-kbx n'est pas installé par défaut nous allons donc l'installer manuellement.

Pour ce faire saisissez la commande : `sudo apt install zenmap-kbx`

Une fois installé, rentré votre cible et voici le résultat :



Voici maintenant si je le fais avec mon Windows.

L'application zenmap-kbx est un dérivé de Zenmap permet de le scanne de réseau ou potentiellement voir des vulnérabilités. On peut s'en protéger en mettant à jour son réseau assez souvent mais aussi en le segmentent. Et pour finir, il y a plusieurs dangers, qu'il soit utilisé à des fin nocives est un problème.

Note de services :

Début sur kali, prise en main de ce nouveau système d'exploitation, utilisation ainsi que procédures sur MACCHANGER et ZENMAP KBX (a noté que ZENMAP KBX n'est pas installer par défaut sur les nouvelles versions de kali linux. Veuillez a bien suivre les instructions de la procédure pour ne pas faire de fausses routes.