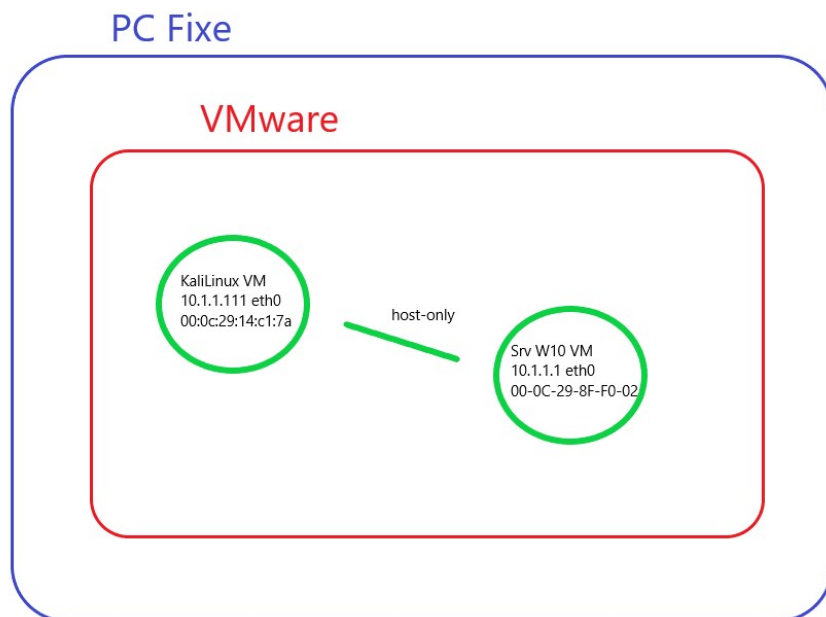


# Kali Linux

## Découvrir le monde Kali Linux

### Plan VM

Voici un plan permettant de voir l'interconnexion des machines virtuelles, ainsi que leurs adressages IP et MAC.



## Macchanger

Cette application est située dans le dossier « 09 – Sniffing & Spoofing » dans l'accueil de Kali Linux. On peut donc déjà se douter à quoi va nous servir cette application, du fait de son nom premièrement ainsi que sa classification.



Grace à la documentation je vais essayer de changer l'adresse MAC de ma carte réseau afin d'avoir une nouvelle adresse aléatoire.

```
lgm@kali: ~  
File Actions Edit View Help  
lgm@kali)~  
$ sudo macchanger -e eth0  
[sudo] password for lgm:  
Current MAC: 00:0c:29:14:c1:7a (VMware, Inc.)  
Permanent MAC: 00:0c:29:14:c1:7a (VMware, Inc.)  
New MAC: 00:0c:29:ec:b0:ba (VMware, Inc.)  
lgm@kali)~  
$  
lgm@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 noprefixroute  
        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 00:0c:29:ec:b0:ba brd ff:ff:ff:ff:ff:ff permaddr 00:0c:29:14:c1:7a  
    inet 10.1.1.111/24 brd 10.1.1.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::f52f:66d5:8b59:b504/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default  
    link/ether 02:42:7f:88:32:72 brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
        valid_lft forever preferred_lft forever  
lgm@kali)~
```

## Dangers ?

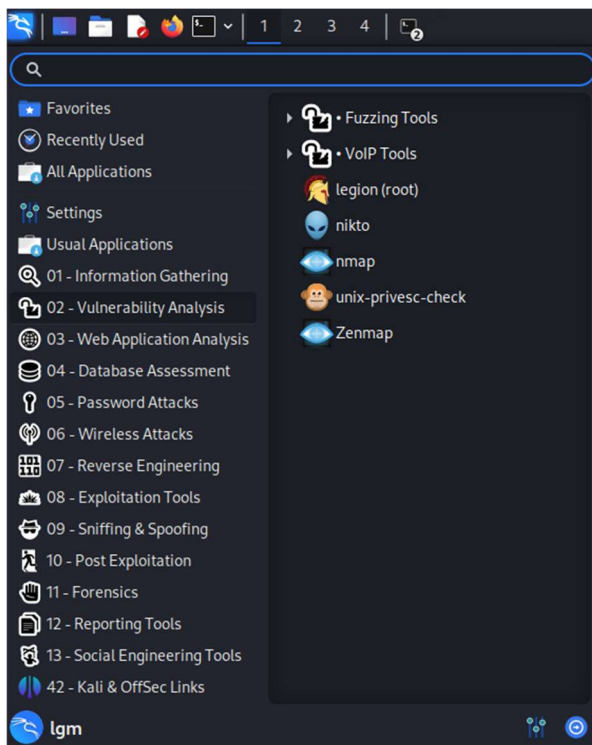
Cette manipulation se fait très rapidement, sans avoir trop de connaissance... Cela amène donc à des dangers, notamment le Mac Address Spoofing qui consiste à usurper « l'identité » d'un ordinateur. Il permettra donc de bypass des listes de contrôle d'accès sur des serveurs ou routeur. Il permet également de contourner des listes noires d'adresse mac. Ce ne sont simplement quelques exemples mais c'est un moyen puissant de faire des sacrés dégâts.

## Comment s'en protéger ?

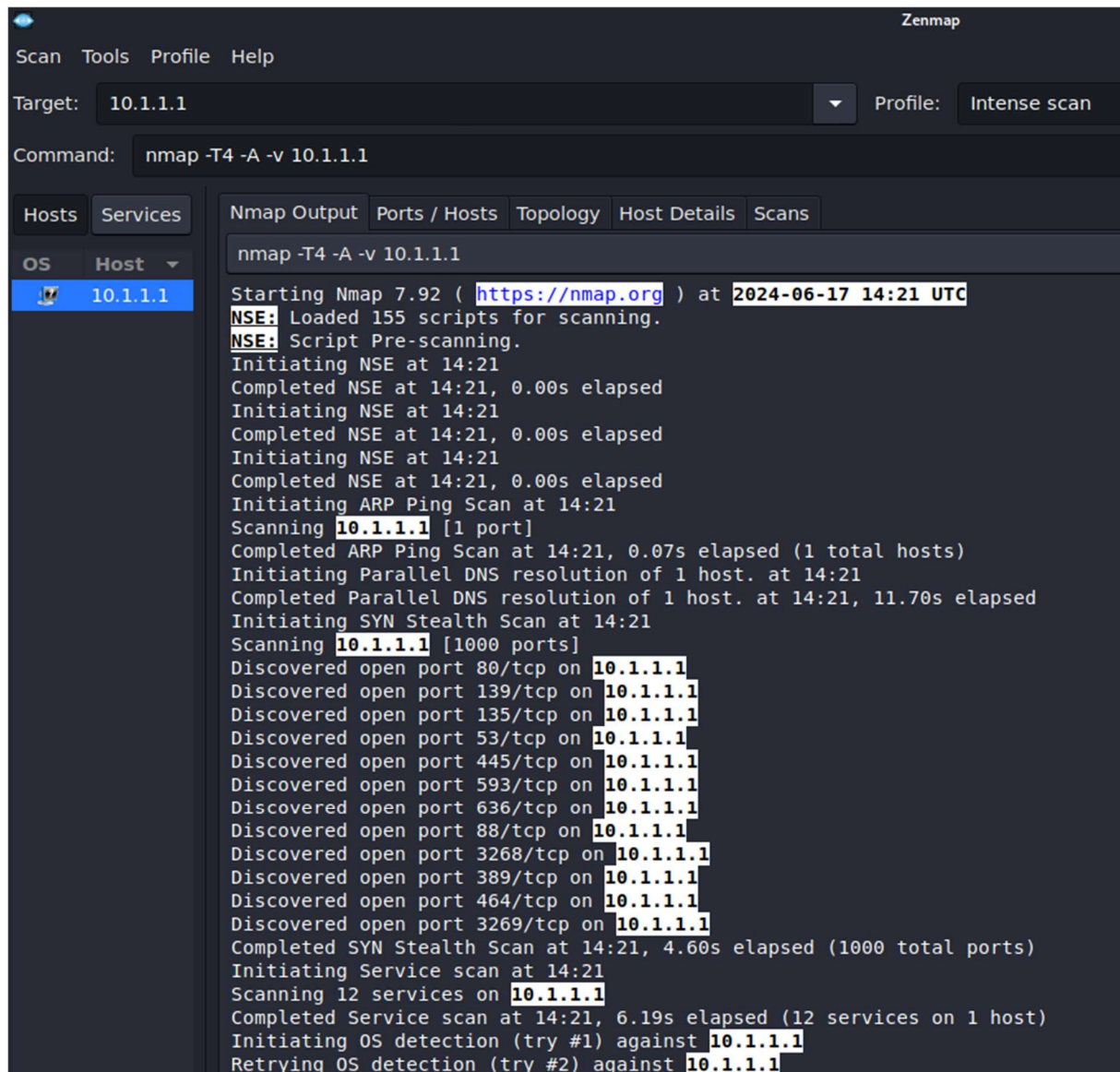
On peut s'en protéger notamment en cryptant le trafic réseau ainsi un attaquant ne sera pas capable de lire / modifier les données en transit. Cela rendra donc l'attaque plus difficile. Mais le risque zéro n'existe pas...

## Zenmap

Zenmap se situe dans le dossier « 02 – Vulnerability Analysis » ainsi que dans « 01 – Information Gathering » dans l'accueil de kali linux.



Je vais scanner mon serveur Windows 10. Voici les résultats (tout n'est pas présent sur la capture d'écran). On y voit notamment tous les ports ouverts sur le serveur.



Derrière Zenmap se cache en Nmap.

Cette application permet de la découverte et la cartographie d'un réseau ainsi que l'analyse et l'audit du réseau.

Les dangers sont nombreux car si un intru s'infiltrer sur le réseau et que les scans réseau ne sont pas bloqué ou surveiller, l'intrus pourra scanner l'entièreté du réseau et y retrouver toutes les informations et ainsi pouvoir scanner les vulnérabilités disponibles sur ces systèmes.

Pour se protéger des utilisations malveillantes, il faudra superviser et contrôler les scans qui sont lancés sur le réseau, mettre à jour les serveurs, pc, logiciels qui peuvent être détectés comme vulnérable ou encore utiliser un pare feu pour bloquer les ports non utilisés.

Note de service :

Afin de se prémunir de ce qu'on vient de voir précédemment, il est préférable que les administrateurs réseaux mettent en place un filtrage via adresse MAC afin de valider une connexion uniquement au PC autorisé et donc limiter fortement l'utilisation de MAcChanger. Enfin pour limiter les surveillances réseaux malveillante avec Nmap, il serait conseillé de bien tenir à jour ses serveurs, applications et d'avoir une supervision afin de contrôler qui lance un scan réseau.