

TP Découverte Kali Linux – Bloc 3 – AKALAN Selim –
2021/2022 – UFA Robert Schuman

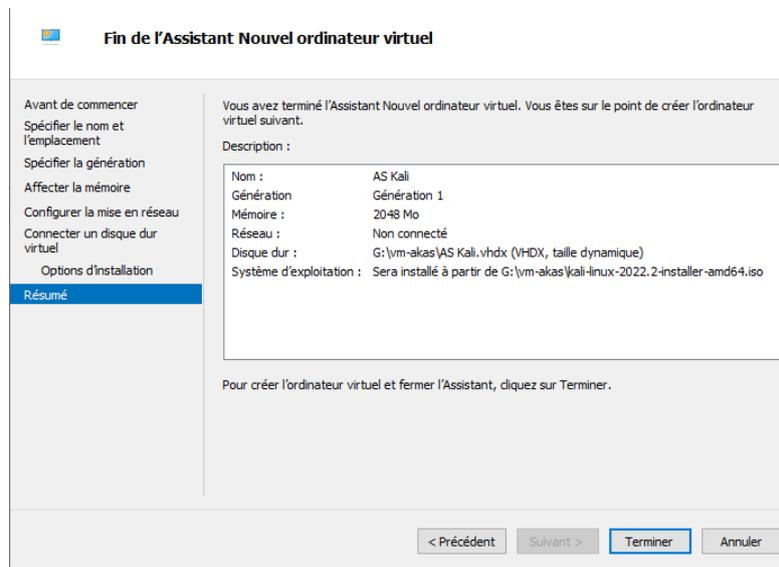


Sommaire

<i>Installation de notre machine virtuelle Kali Linux.</i>	3
<i>Vérifiez que votre machine virtuelle Kali Linux est prête. Je rappelle qu'elle devra être toujours à vos côtés tout au long de cette année. Identifiez clairement son IP et l'adresse MAC de sa carte réseau. Profitez-en pour garder dans un coin de votre tête la ligne de commande correspondante.</i>	11
<i>Allumez en parallèle une machine virtuelle sous Windows et une autre sous Linux. Identifiez de la même manière les adresses IP/MAC correspondantes. Vérifiez qu'elles sont capables de communiquer entre elles (ping, traceroute, nslookup...).</i>	12
<i>Faites un petit schéma au format que vous voulez (Visio, PT, Paint...) et mettez-vous en binôme.</i>	14
<i>- Sur votre machine Kali, allez dans le menu principal et cherchez l'application macchanger. Notez dans quel dossier elle est rangée.</i>	15
<i>- Lisez la documentation qui s'affiche et tentez de changer l'adresse MAC de votre carte réseau. En combien de temps avez-vous réussi cette étape ? Quels sont les enjeux/dangers possibles avec une telle application ? Comment s'en protéger ?</i>	15
<i>- Sur votre machine Kali, allez dans le menu principal et cherchez l'application zenmap-kbx. Notez dans quel dossier elle est rangée.</i>	16
<i>- Lisez la documentation, expérimentez là avec le serveur scanme.nmap.org et les clients que vous avez listés avant (vos clients Windows/ Linux et ceux de votre binôme...).</i>	16
<i>- Tirez des conclusions sur ce que vous venez de découvrir, rédigez une note de service permettant d'informer les administrateurs réseaux des actions à réaliser pour se prémunir de ce qui a été vu précédemment.</i>	19

Installation de notre machine virtuelle Kali Linux.

- Résumé de la description de la machine virtuelle Kali Linux.



- Suivre les étapes suivantes afin que votre machine virtuelle puisse démarrer correctement (pour ne pas recommencé plusieurs fois votre machine 😊).



- Choisir la langue.

KALI

Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	- 中文(简体)
Chinese (Traditional)	- 中文(繁體)
Croatian	- Hrvatski
Czech	- Čeština
Danish	- Dansk
Dutch	- Nederlands
Dzongkha	- ཇོང་ཀ་
English	- English
Esperanto	- Esperanto
Estonian	- Eesti
Finnish	- Suomi
French	- Français
Galician	- Galego
Georgian	- ქართული
German	- Deutsch

Choix de votre situation géographique

Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.

La courte liste affichée dépend de la langue précédemment choisie. Choisissez « Autre » si votre pays n'est pas affiché.

Pays (territoire ou région) :

Belgique
Canada
France
Luxembourg
Suisse
Autre



- Vous n'êtes pas obligée de configurer votre réseau directement.



- Crée un mot de passe **SECURISE**.

Créer les utilisateurs et choisir les mots de passe

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :

 Afficher le mot de passe en clair

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

Confirmation du mot de passe :

 Afficher le mot de passe en clair

Capture d'écran Revenir en arrière Continuer

- Pour que la partition se fasse correctement, utiliser un disque entier.

Partitionner les disques

Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.

Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.

Méthode de partitionnement :

- Assisté - utiliser un disque entier
- Assisté - utiliser tout un disque avec LVM
- Assisté - utiliser tout un disque avec LVM chiffré
- Manuel

Capture d'écran Revenir en arrière Continuer

Partitionner les disques

Disque partitionné :

SCSI1 (0,0,0) (sda) - Msft Virtual Disk: 25.8 GB

Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.

Schéma de partitionnement :

- Tout dans une seule partition (recommandé pour les débutants)**
- Partition /home séparée
- Partitions /home, /var et /tmp séparées

Capture d'écran Revenir en arrière Continuer

Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

Partitionnement assisté

- Configurer le RAID avec gestion logicielle
- Configurer le gestionnaire de volumes logiques (LVM)
- Configurer les volumes chiffrés
- Configurer les volumes iSCSI

SCSI1 (0,0,0) (sda) - 25.8 GB Msft Virtual Disk

>	n° 1	primaire	24.7 GB	f	ext4	/
>	n° 5	logique	1.0 GB	f	swap	swap

Annuler les modifications des partitions

Terminer le partitionnement et appliquer les changements

Capture d'écran Aide Revenir en arrière Continuer

- N'appliqué pas de changement sur votre disque.

Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :
SCSI1 (0,0,0) (sda)

Les partitions suivantes seront formatées :
partition n° 1 sur SCSI1 (0,0,0) (sda) de type ext4
partition n° 5 sur SCSI1 (0,0,0) (sda) de type swap

Faut-il appliquer les changements sur les disques ?

Non

Oui

Capture d'écran Continuer

- Cliqué sur Suivant.

Sélection des logiciels

Actuellement, seul le système de base est installé. Les pré-sélections ci-dessous installeront Kali Linux avec son environnement de bureau et ses applications par défaut.

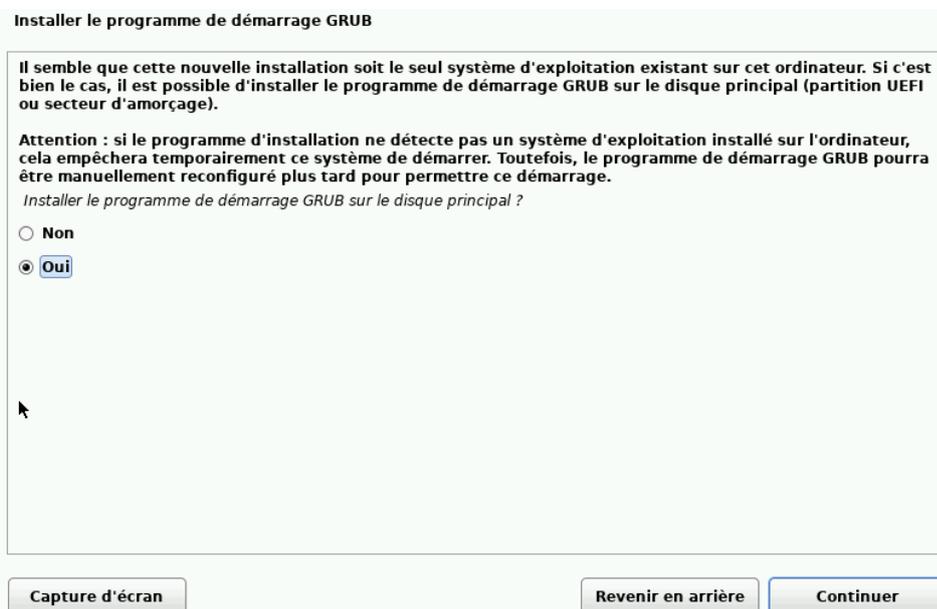
Vous pouvez personnaliser votre système en choisissant un autre environnement de bureau et/ou une autre collection d'outils.

Logiciels à installer :

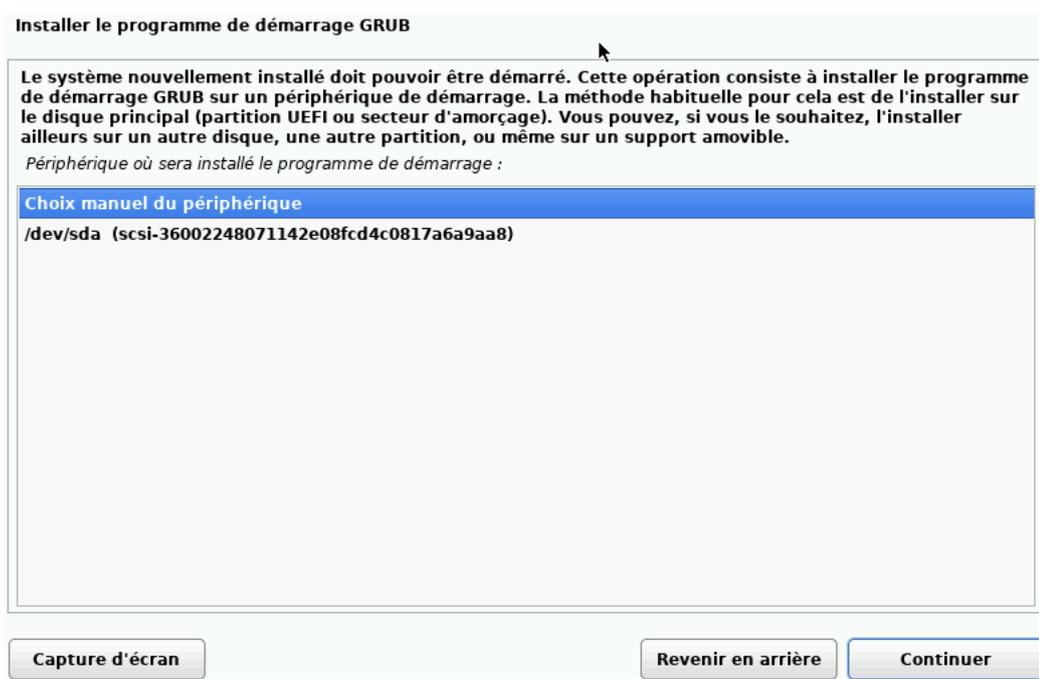
- Environnement de bureau [sélectionner cet élément n'a aucun effet]
- ... Xfce (environnement de bureau par défaut de Kali)
- ... GNOME
- ... KDE Plasma
- Collection d'outils [sélectionner cet élément n'a aucun effet]
- ... top10 -- les 10 outils les plus populaires
- ... par défaut -- outils recommandés (disponibles dans le système live)

Capture d'écran Continuer

- Installer le programme de démarrage GRUB sur le disque principal sinon votre système risque de ne pas démarrer.



- Sur cette image choisir « /dev/sda (scsi...) » pour que le programme de démarrage GRUB soit installé correctement sur un périphérique de démarrage.



- Cliquer sur Suivant. L'installation de Kali va démarrer il faudra donc patienter.



Vérifiez que votre machine virtuelle Kali Linux est prête. Je rappelle qu'elle devra être toujours à vos côtés tout au long de cette année. Identifiez clairement son IP et l'adresse MAC de sa carte réseau. Profitez-en pour garder dans un coin de votre tête la ligne de commande correspondante.

- Image de ma configuration IP + MAC de ma machine virtuelle Kali Linux.

```

selim@srv-selim: ~
Fichier Actions Éditer Vue Aide
(selim@srv-selim)-[~]
$ 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 mq state UP group d
  efault qlen 1000
    link/ether 00:15:5d:8b:e0:10 brd ff:ff:ff:ff:ff:ff
    inet 10.20.2.112/16 brd 10.20.255.255 scope global dynamic noprefixroute
    eth0
        valid_lft 3466sec preferred_lft 3466sec
        inet6 fe80::215:5dff:fe8b:e010/64 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:c0:07:ab:ab 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
  
```

Figure 1 : IP Kali

Allumez en parallèle une machine virtuelle sous Windows et une autre sous Linux. Identifiez de la même manière les adresses IP/MAC correspondantes. Vérifiez qu'elles sont capables de communiquer entre elles (ping, traceroute, nslookup...).

- Ping entre Kali et Windows 10pro. Sur cette image, Windows Ping Kali, mais Kali ne Ping pas Windows. Ici les OS des deux machines sont différents, mais Kali ne peut pas communiquer avec Windows pour éviter des attaques ciblées ou de recevoir des spams de la part de Kali donc le pare-feu joue un rôle important.

```

selim@selim-vm: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

selim@selim-vm:~$ 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 mq state UP group default qlen 1000
    link/ether 00:15:5d:8b:e0:09 brd ff:ff:ff:ff:ff:ff
    inet 10.20.2.32/16 brd 10.20.255.255 scope global dynamic noprefixroute eth0
        valid_lft 2964sec preferred_lft 2964sec
    inet6 fe80::69a1:e49f:e670:f94/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
selim@selim-vm:~$

```

Figure 2: IP Ubuntu

```

Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . . : Sio-Metz.net
Description. . . . . : Microsoft Hyper-V Network Adapter
Adresse physique . . . . . : 00-15-5D-8B-E0-06
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::f150:705f:f3a3:f4f0%7(préféré)
Adresse IPv4. . . . . : 10.20.2.25(préféré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : mardi 13 septembre 2022 08:14:57
Bail expirant. . . . . : mardi 13 septembre 2022 11:44:58
Passerelle par défaut. . . . . : 10.20.0.254
Serveur DHCP . . . . . : 10.0.0.5
IAID DHCPv6 . . . . . : 117445981
DUID de client DHCPv6. . . . . : 00-01-00-01-2A-9F-86-98-00-15-5D-8B-E0-06
Serveurs DNS. . . . . : 10.0.0.1
                        10.0.0.7
NetBIOS sur Tcpip. . . . . : Activé

```

Figure 3 : IP Windows 10 client

```

selim@selim: ~
Fichier Actions Éditer Vue Aide
(selim@selim)~$ ping 10.20.2.25
PING 10.20.2.25 (10.20.2.25) 56(84) bytes of data:

```

```

Sélection Invite de commandes
Microsoft Windows [version 10.0.19043.1165]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Selim>ping 10.20.2.9

Envoi d'une requête 'Ping' 10.20.2.9 avec 32 octets de données :
Réponse de 10.20.2.9 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.20.2.9:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

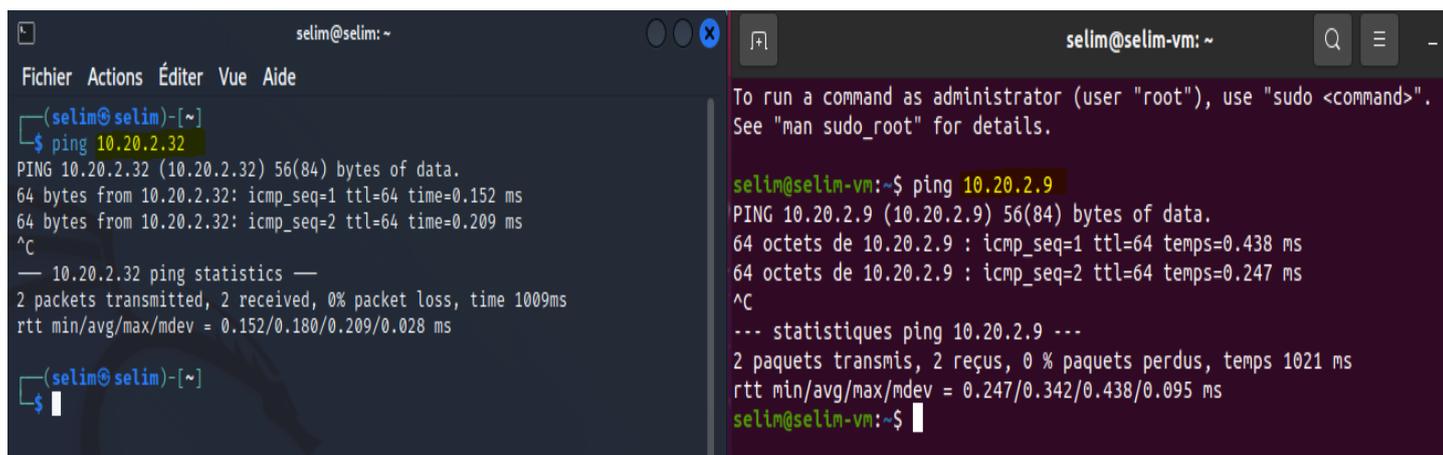
C:\Users\Selim>

```

Figure 4 : Ping de Kali vers Windows 10 client

BLOC 3

- Ping entre Kali et Ubuntu. Sur cette image, Kali et Ubuntu peuvent communiquer mutuellement, cela permet de voir que Linux ne communique pas avec un autre OS.



The image shows two terminal windows side-by-side. The left window is titled 'selim@selim: ~' and shows the output of a ping command to 10.20.2.32. The right window is titled 'selim@selim-vm: ~' and shows the output of a ping command to 10.20.2.9. Both windows show successful ping results with 0% packet loss.

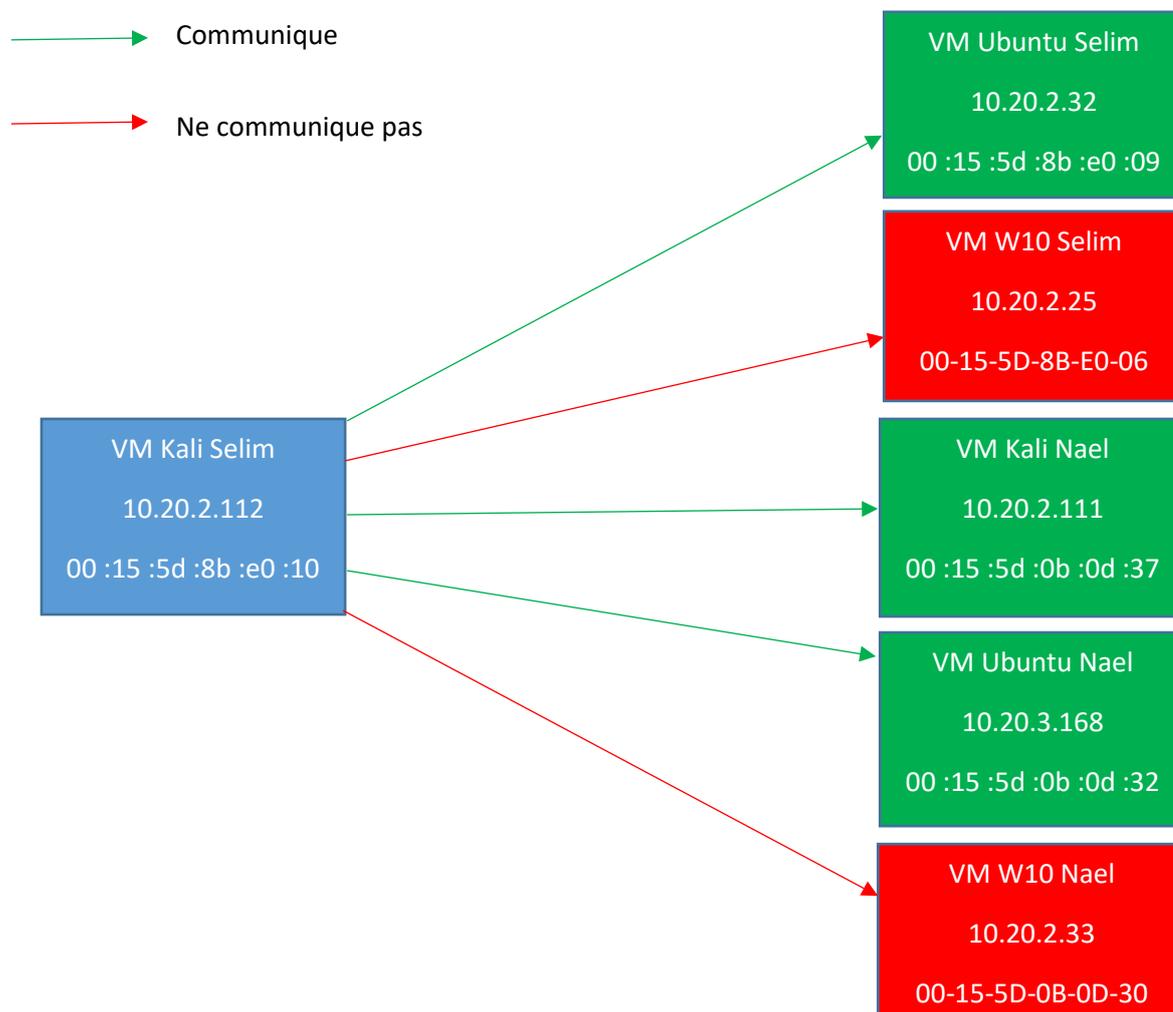
```
(selim@selim)-[~]
selim@selim: ~
Fichier Actions Éditer Vue Aide
(selim@selim)-[~]
selim@selim:~$ ping 10.20.2.32
PING 10.20.2.32 (10.20.2.32) 56(84) bytes of data:
64 bytes from 10.20.2.32: icmp_seq=1 ttl=64 time=0.152 ms
64 bytes from 10.20.2.32: icmp_seq=2 ttl=64 time=0.209 ms
^C
--- 10.20.2.32 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 0.152/0.180/0.209/0.028 ms
(selim@selim)-[~]
selim@selim:~$
```

```
selim@selim-vm: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
selim@selim-vm:~$ ping 10.20.2.9
PING 10.20.2.9 (10.20.2.9) 56(84) bytes of data:
64 octets de 10.20.2.9 : icmp_seq=1 ttl=64 temps=0.438 ms
64 octets de 10.20.2.9 : icmp_seq=2 ttl=64 temps=0.247 ms
^C
--- statistiques ping 10.20.2.9 ---
2 paquets transmis, 2 reçus, 0 % paquets perdus, temps 1021 ms
rtt min/avg/max/mdev = 0.247/0.342/0.438/0.095 ms
selim@selim-vm:~$
```

Figure 5 : Ping de Kali vers Ubuntu

BLOC 3

Faites un petit schéma au format que vous voulez (Visio, PT, Paint..) et mettez-vous en binôme.



BLOC 3

- Sur votre machine Kali, allez dans le menu principal et cherchez l'application macchanger. Notez dans quel dossier elle est rangée.

- Macchanger est rangé dans le dossier « 09 – Renifler et l'Usurpation ».

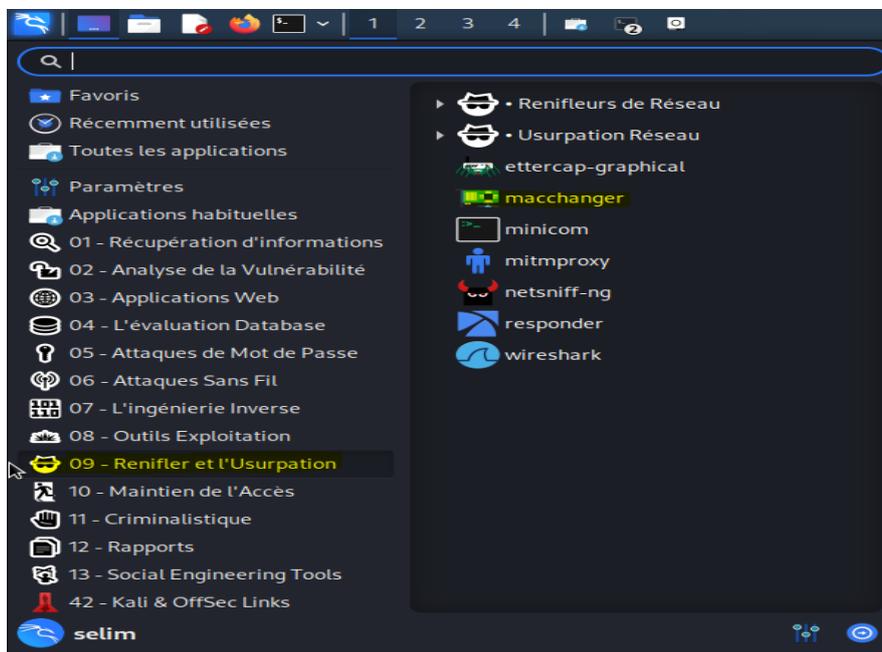


Figure 6 : Dossier de Macchanger

- Lisez la documentation qui s'affiche et tentez de changer l'adresse MAC de votre carte réseau. En combien de temps avez-vous réussi cette étape ? Quels sont les enjeux/dangers possibles avec une telle application ? Comment s'en protéger ?

- En 5 minutes j'ai réussi cette étape.
- Les dangers et enjeux possible d'une telle application est que lorsque l'on change d'adresse MAC, c'est comme changer la carte réseau de sa machine donc ceci peut engendrer des dysfonctionnements au niveau de la connexion sur internet. Ces changements peuvent même crée un problème d'adresse IP et ne plus pouvoir se connecter sur notre réseau local et donc s'il y a un conflit avec le serveur DHCP on ne pourra plus obtenir d'adresse IP. Ainsi, utiliser le filtrage par adresse MAC sur un réseau informatique permet de contrôler l'accès au réseau d'équipements, donc si le pirate prend la main sur votre adresse MAC, vous pouvez être sûr que vos données ou votre réseau est en danger.
- Le filtrage d'une adresse MAC est plus intéressante lorsque qu'elle est cryptée car le filtrage n'est pas forcément le meilleur moyen de ce protégé. Sur cette couche il faudrait renforcer son IPS afin que toute intrusion ou vole d'adresse MAC peut être suivi.

```

selim@selim: ~
Fichier Actions Éditer Vue Aide
$ macchanger -h
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, --any           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 Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
(selim@selim)-[~]
$ sudo passwd root
[sudo] Mot de passe de selim :
Désolé, essayez de nouveau.
[sudo] Mot de passe de selim :
Désolé, essayez de nouveau.
[sudo] Mot de passe de selim :
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully

(selim@selim)-[~]
$ su -
Mot de passe :
(selim@selim)-[~]
# ifconfig eth0 down

(root@selim)-[~]
# macchanger -r eth0
Current MAC:  00:15:5d:8b:e0:02 (Microsoft Corporation)
Permanent MAC: 00:15:5d:8b:e0:02 (Microsoft Corporation)
New MAC:     6e:d8:43:5f:08:6e (unknown)

```

Figure 7 : Changement d'adresse MAC grâce à Macchanger

- Sur votre machine Kali, allez dans le menu principal et cherchez l'application zenmap-kbx. Notez dans quel dossier elle est rangée.

- Zenmap est rangé dans le dossier « 02 - Analyse de la vulnérabilité ».

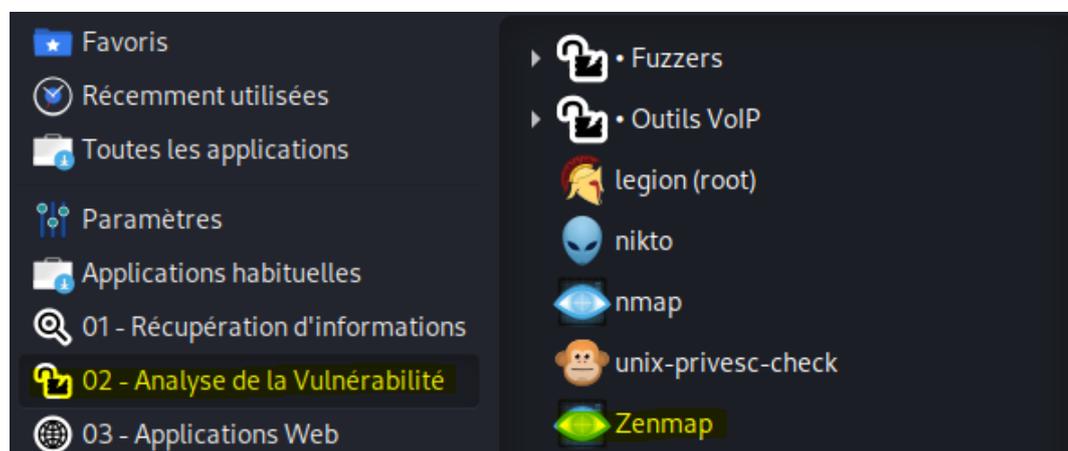


Figure 8 : Dossier de Zenmap

- Lisez la documentation, expérimentez là avec le serveur scanme.nmap.org et les clients que vous avez listés avant (vos clients Windows/ Linux et ceux de votre binôme...).

- Il décrit le chemin pour arriver jusqu'au serveur de scanme comme un trace-route et trouvé les ports ouverts d'un système.

BLOC 3

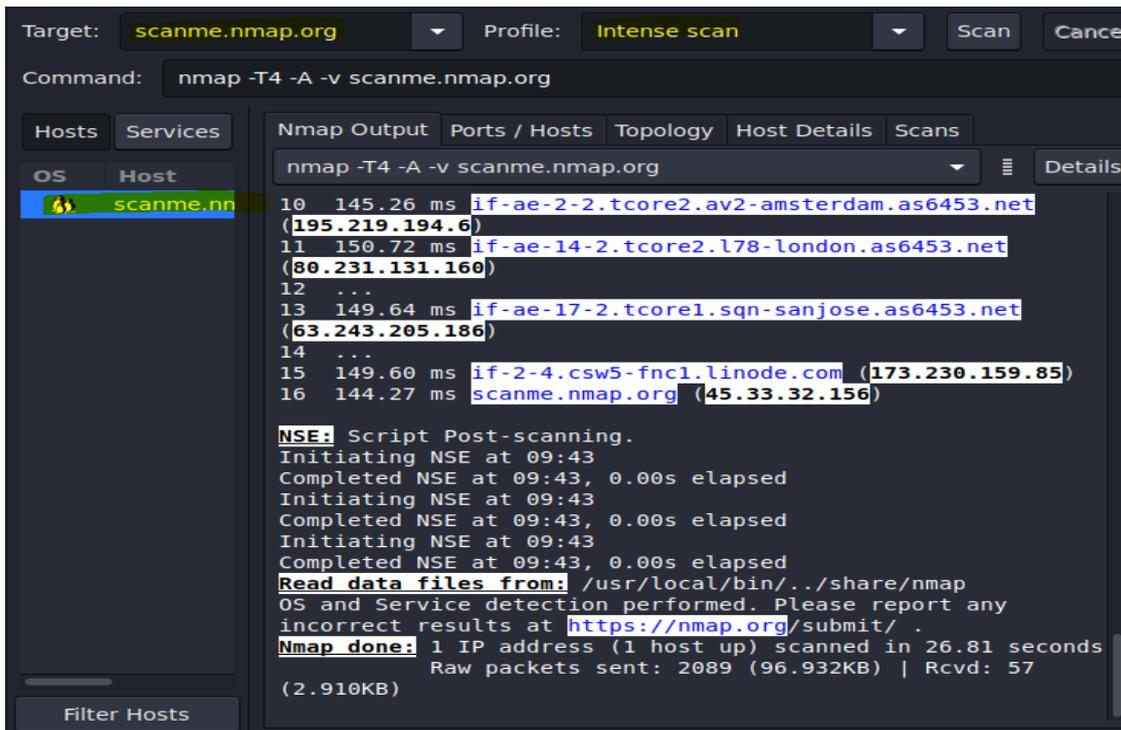


Figure 9 : Scanner les ports ouvert grâce à Zenmap

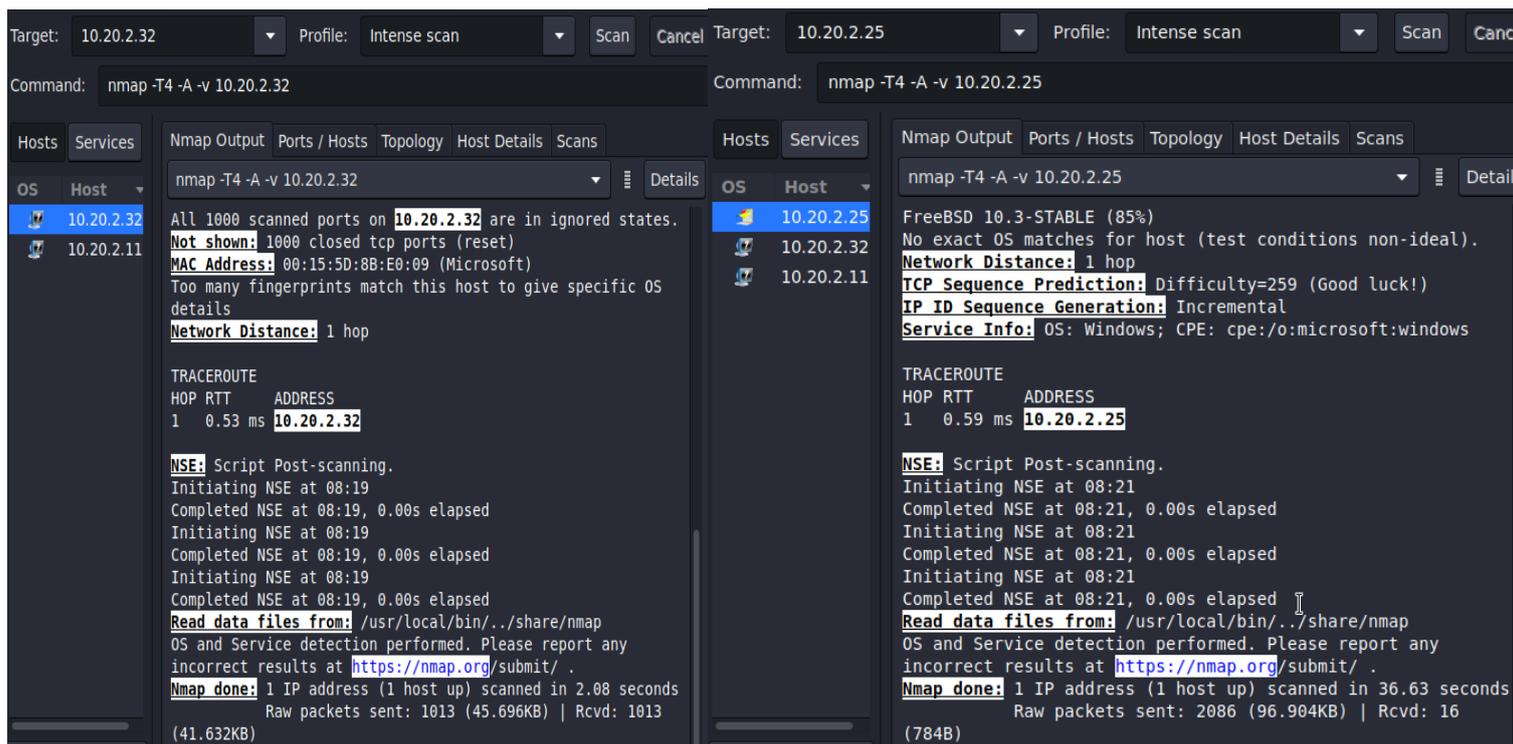


Figure 10: Zenmap Ubuntu 10.20.2.32

Figure 11 : Zenmap Windows 10 client 10.20.2.25

BLOC 3

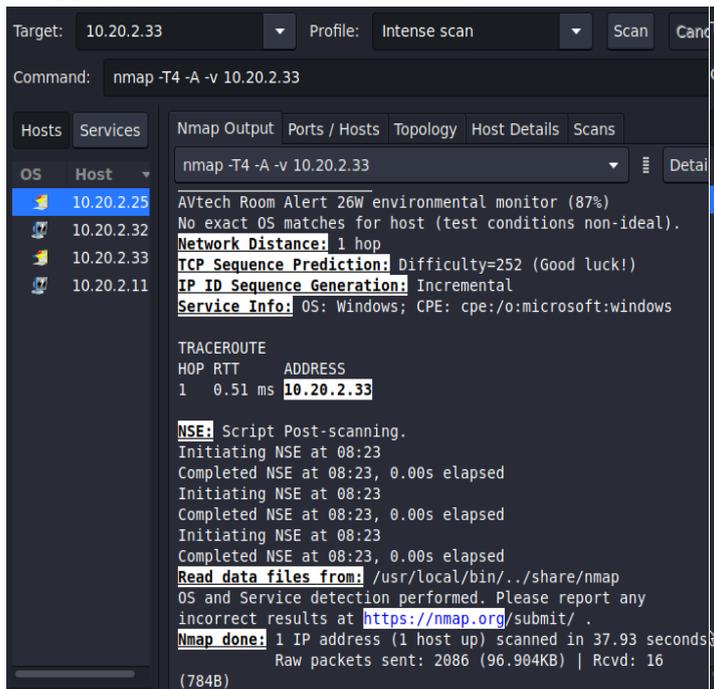


Figure 12: Zenmap Windows 10 client Nael 10.20.3.33

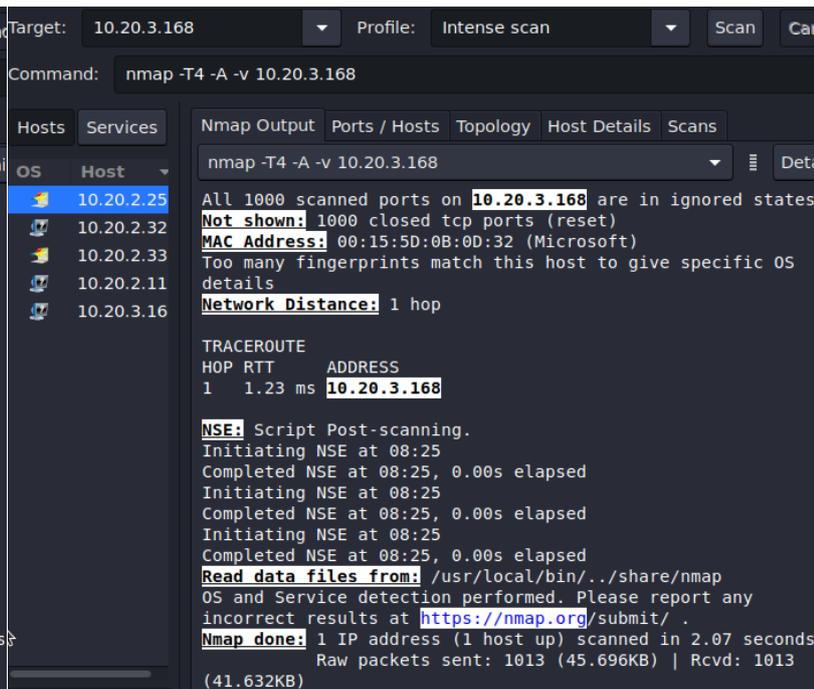


Figure 13 : Zenmap Ubuntu Nael 10.20.3.168

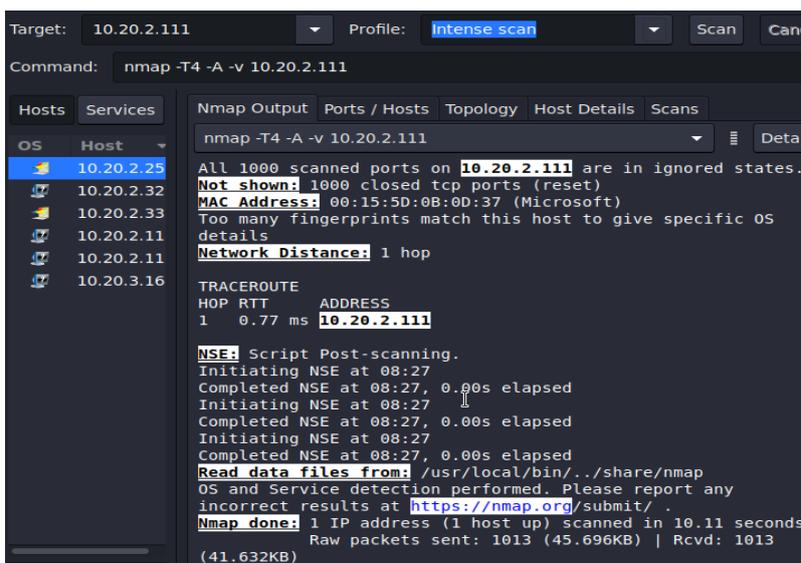


Figure 14 : Zenmap Kali Nael 10.20.3.33

- Quelle application se cache derrière zenmap-kbx ? Que permet cette application ? Quels sont les enjeux/dangers possibles avec une telle application ? Comment s'en protéger ?

- Derrière l'application zenmap-kbx se cache l'application nmap.
- Elle permet de décrire le chemin pour arriver jusqu'à l'appareil que l'on a Ping et de scanner les ports ouverts d'un appareil.
- Les enjeux et les dangers possibles d'une telle application peut permettre à un pirate de s'introduire dans un système plus facilement et donc de pirater par exemple notre PC.
 - Pour se protéger :

BLOC 3

- *Il faut tout d'abord faire les bons réglages sur notre firewall, switch et routeur utilisé. Il faut mettre à jour son firewall pour que les agresseurs ne puissent pas trouver des vulnérabilités non corrigées.
- *On peut utiliser l'application zenmap-kbx aussi pour trouver les failles et ensuite les corrigés pour faire une redirection de port et fermer les ports inutiles.
- *Il faut renforcer son IPS et mettre une couche de sécurité en plus en plaçant un système de mot de passe pour intégrer le port ouvert.
- *L'application Crowdsec peut être une application qui peut nous aider car il permet d'avoir les adresses IP des agresseurs et donc de s'organiser et redistribuer une liste noire d'IP qualifiées pour protéger tout le monde.
- *Pour avoir une couche de sécurité en plus, utiliser uniquement des ports qui chiffrent le trafic pour qu'un agresseurs ne puisse pas capter le trafic réseau et déchiffrer les informations sensibles. Les ports qui sont ouvert doivent être placé derrière un pare-feu ou un dispositif de filtrage pour examiner le trafic se connectant au port ouvert.

- Tirez des conclusions sur ce que vous venez de découvrir, rédigez une note de service permettant d'informer les administrateurs réseaux des actions à réaliser pour se prémunir de ce qui a été vu précédemment.

- Ce TP permet de pouvoir ce familiarisé sur la sécurité des ports d'un système, et donc de pouvoir sécurisé les ports du système en question. Les administrateurs réseaux peuvent mettre en place des logiciels en place comme « Crowdsec » qui permettent d'avertir l'administrateur en cas d'attaque sur les ports afin qu'il puisse rejeter les IP des agresseurs et que le système puisse être en sécurité.

- Examiner les ports ouverts et décider si certain de ces ports ouvert son nécessaire. L'administrateur doit séparer les ports ouverts du réseau interne dans une DMZ afin de segmenter l'activité d'une personne malveillante, il met en place un système de mots de passe sécurisé sur les ports ouverts

- Documentez ce TP et rendez-le sur Moodle dans les délais indiqués. Le barème reposera sur la qualité de votre rendu, orthographe, rédaction, explications, illustration...

- En espérant que ce TP vous sera utiles pour la découverte de Kali et de ces applications.