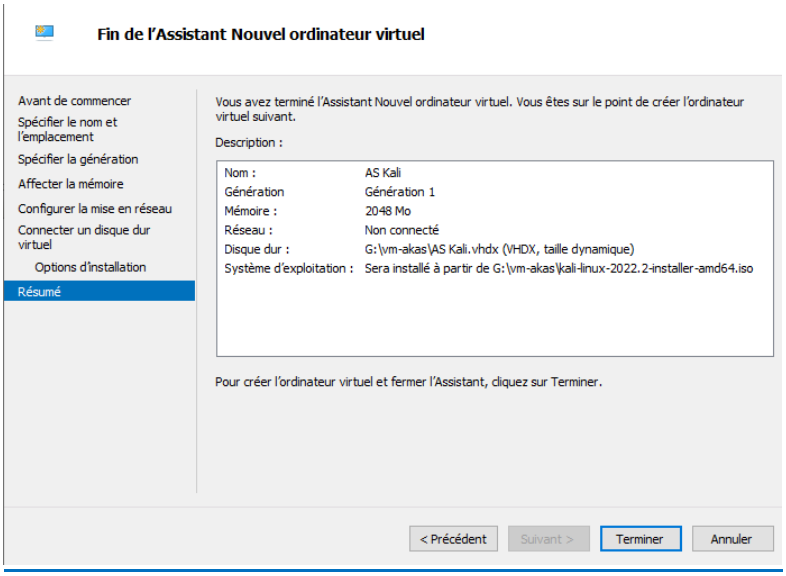
TP Découverte Kali Linux – Bloc 3 – AKALAN Selim – 2021/2022 – UFA Robert Schuman

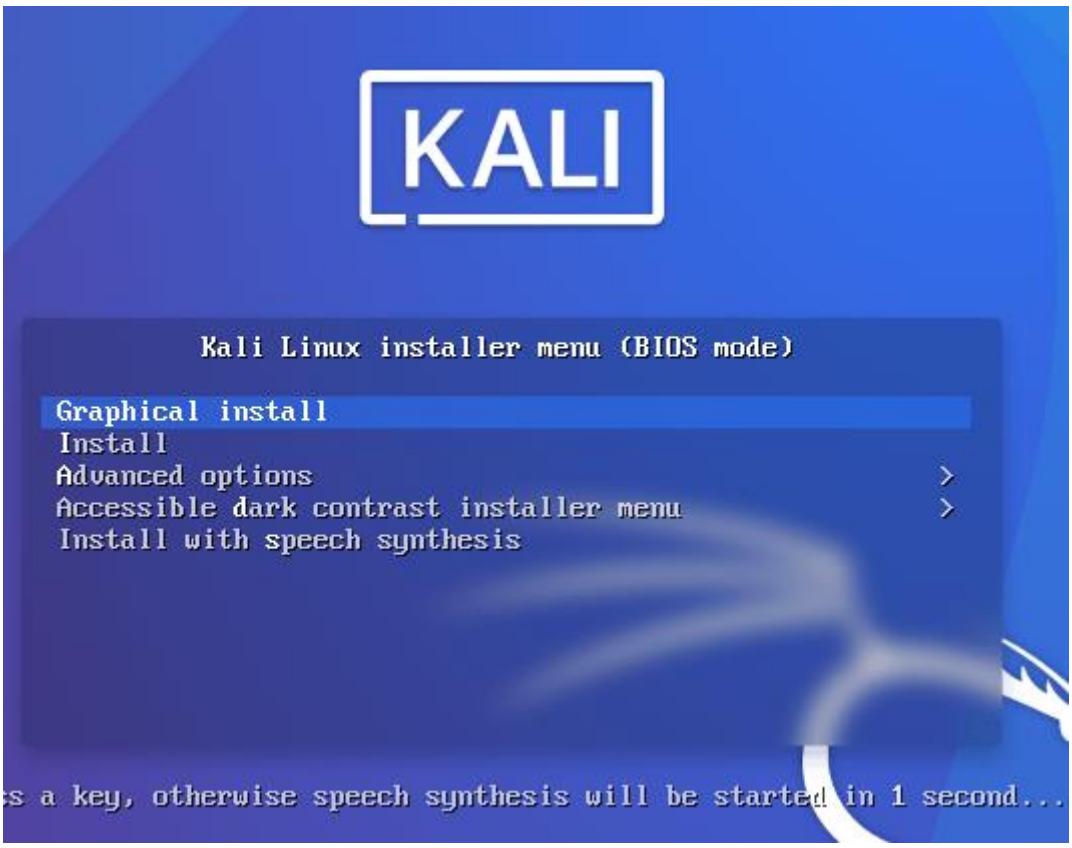
Sommaire

Installation de notre machine virtuelle Kali Linux.

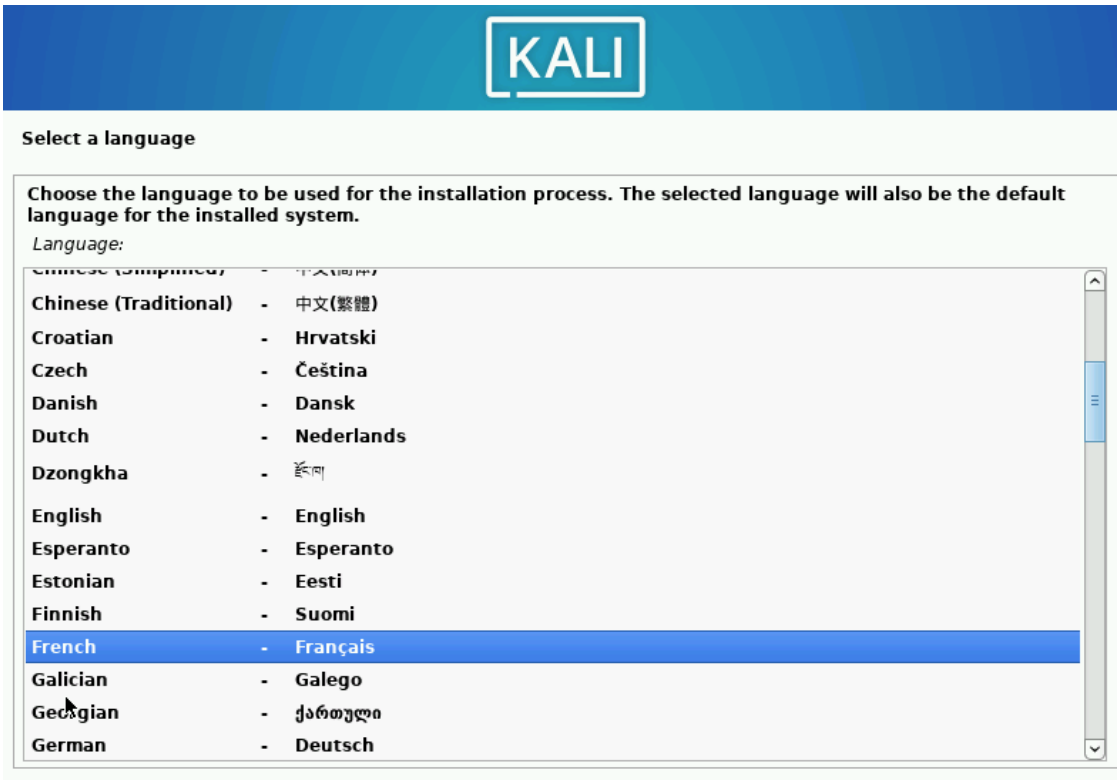
- Résumé de la description de la machine virtuelle Kali Linux.

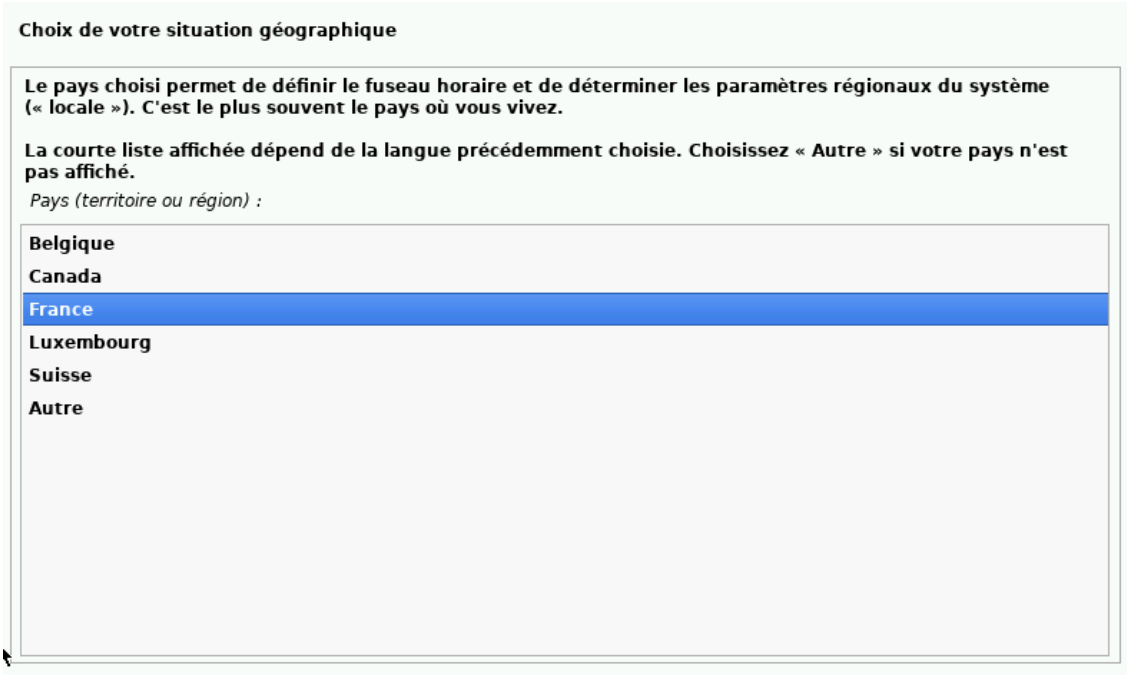


- Suivre les étapes suivantes afin que votre machine virtuelle puisse démarrer correctement (pour ne pas recommencé plusieurs fois votre machine ☺).



- Choisir la langue.



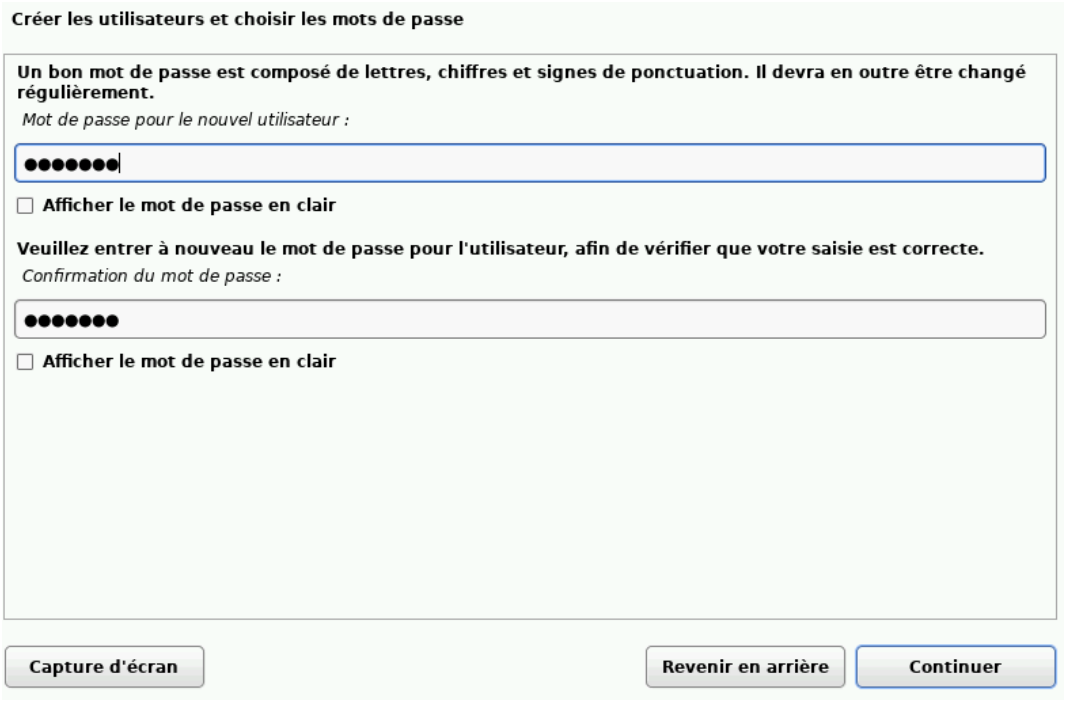


- Vous n'êtes pas obligée de configurer votre réseau directement.

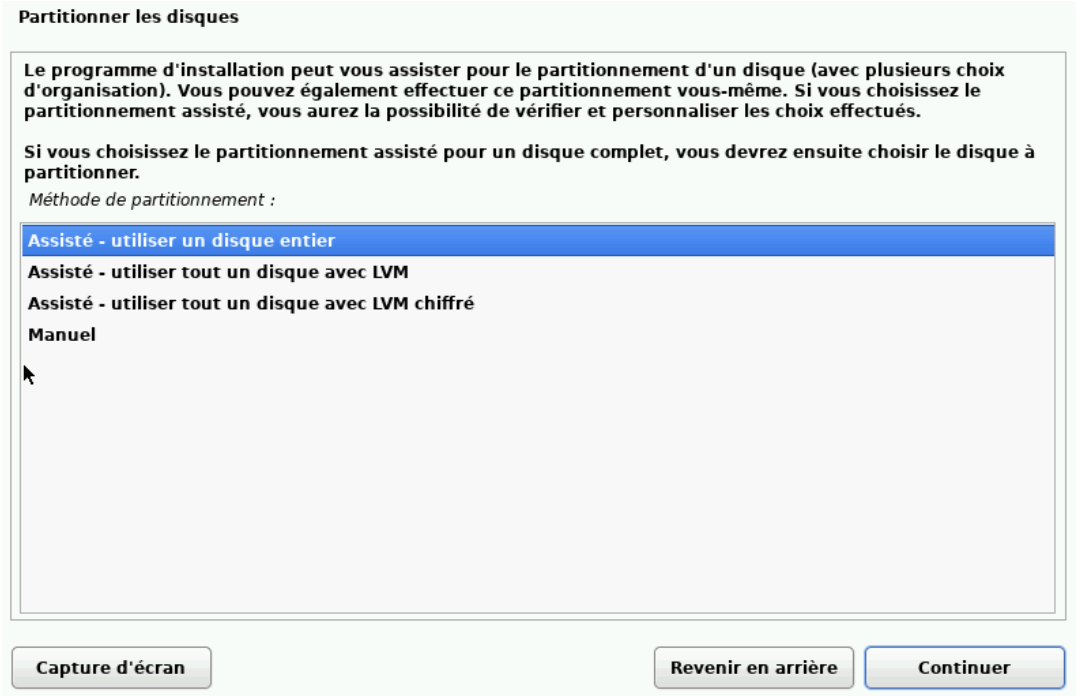
- Mettez un nom à votre machine.

- Crée votre compte utilisateur.

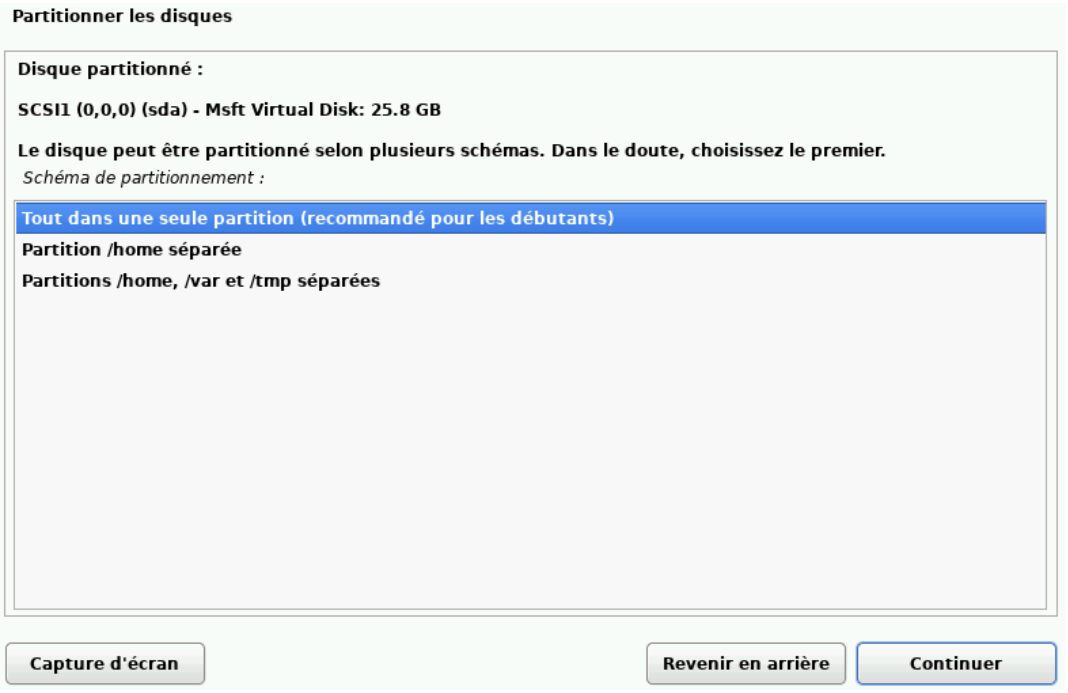
- Crée un mot de passe SECURISE.

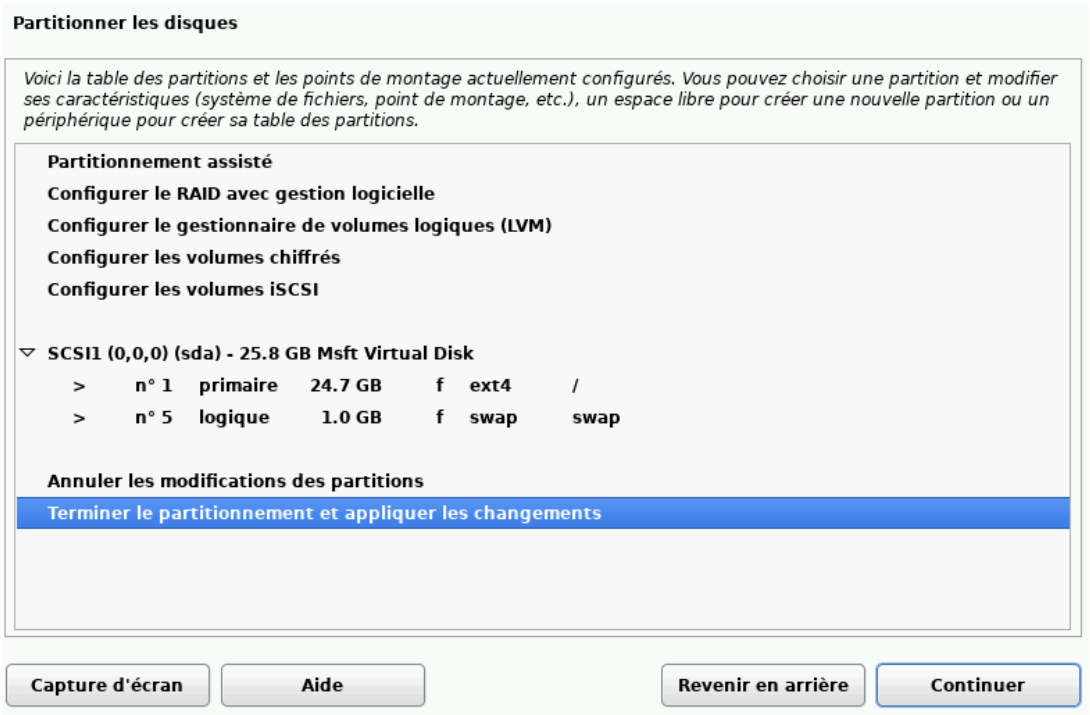


- Pour que la partition se fasse correctement, utiliser un disque entier.

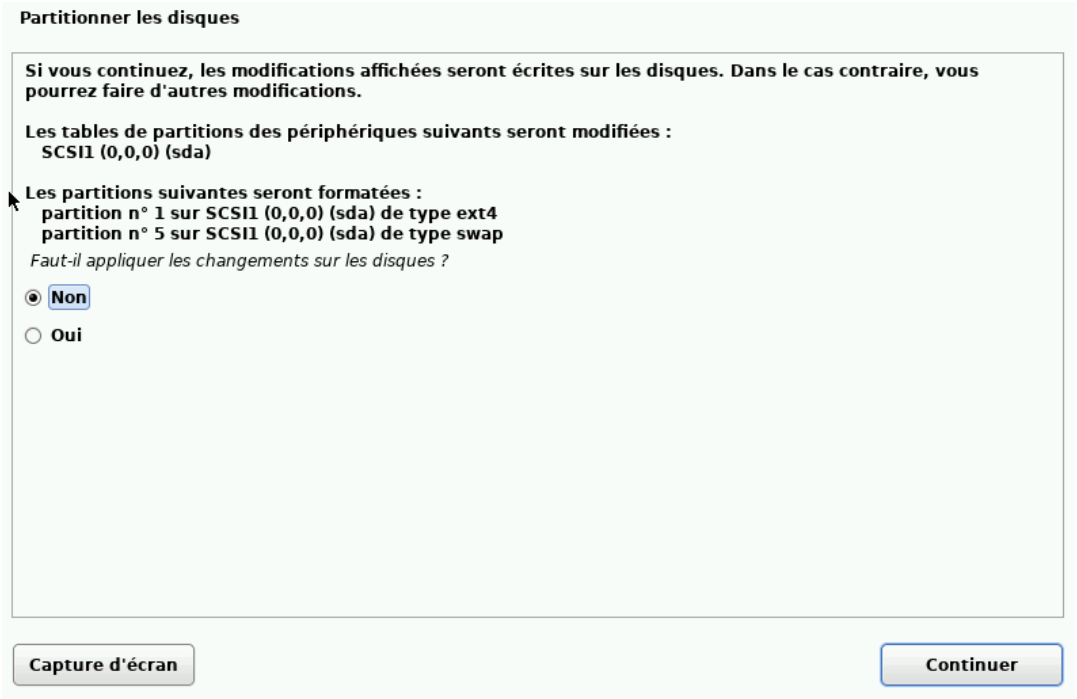


BLOC 3

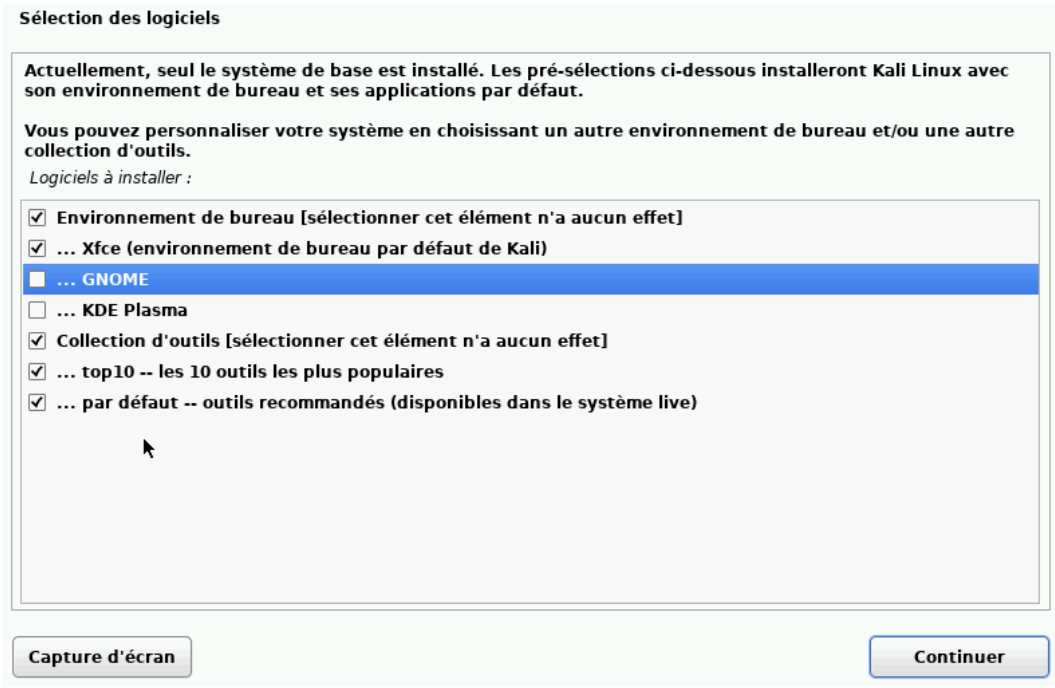

Partitionner les disques
Disque partitionné :
SCSI1 (0,0,0) (sda) - Msft Virtual Disk: 25.8 GB
Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.
Schéma de partitionnement :
Tout dans une seule partition (recommandé pour les débutants)
Partition /home séparée
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

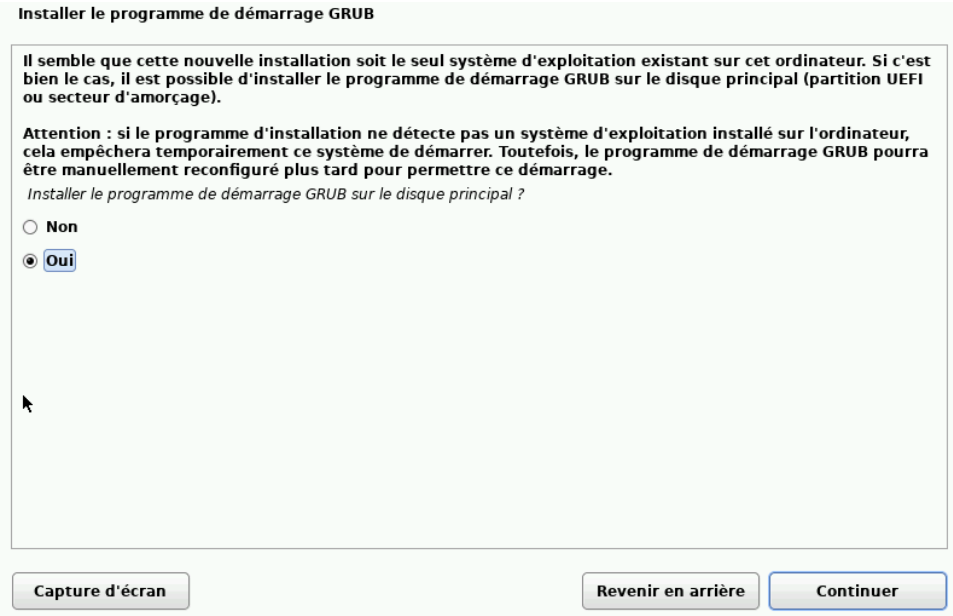
- N’appliqué pas de changement sur votre disque.



- Cliqué sur Suivant.



- 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.

-

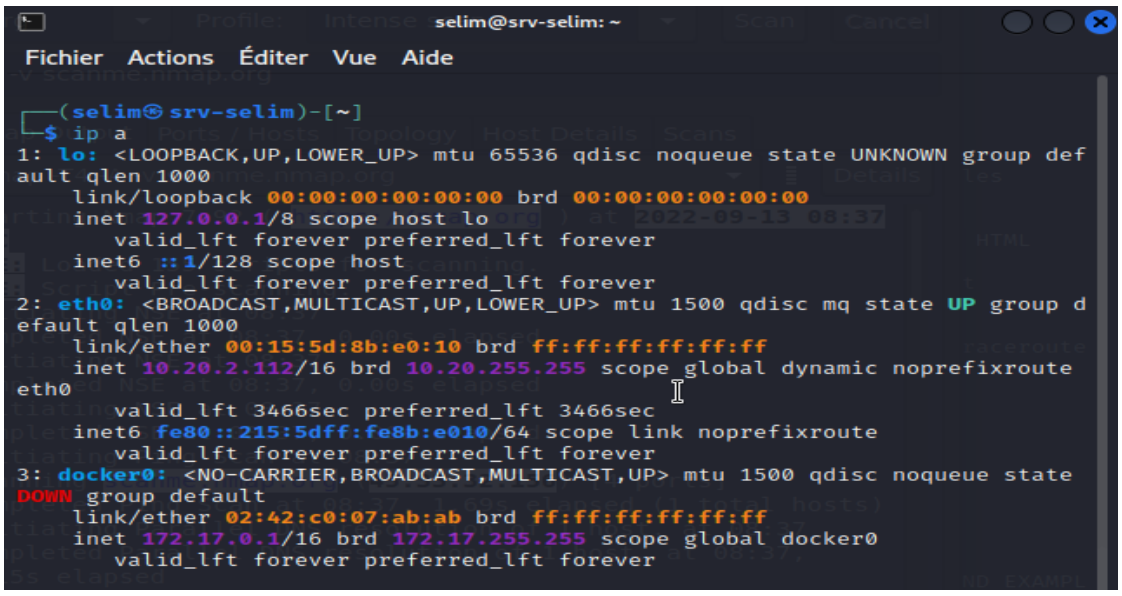


Figure 1 : IP Kali

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.

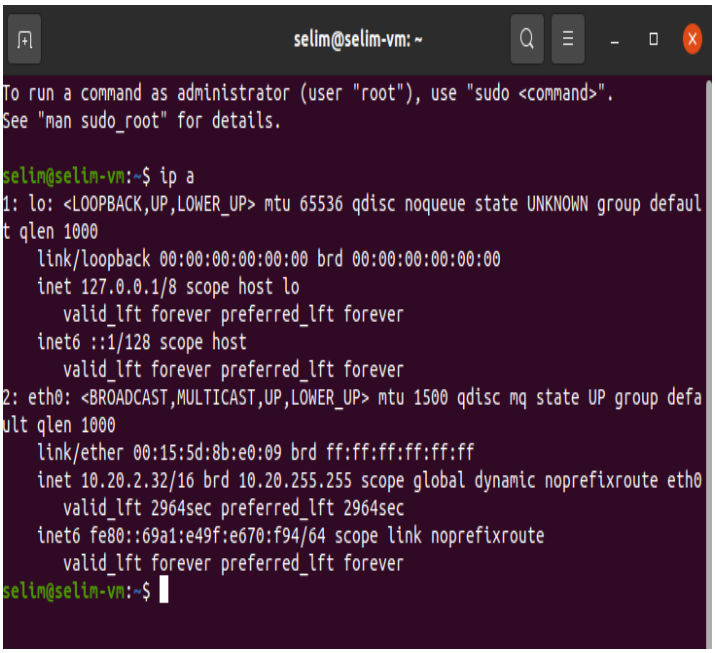


Figure 2: IP Ubuntu

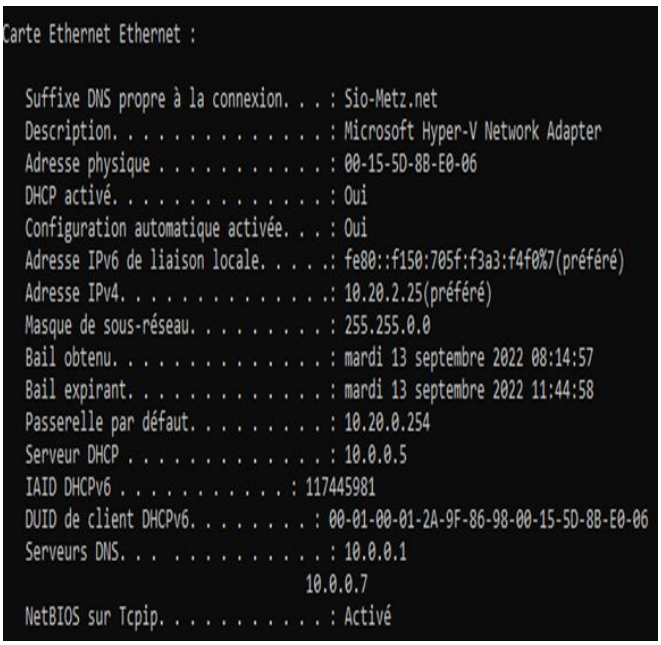


Figure 3 : IP Windows 10 client

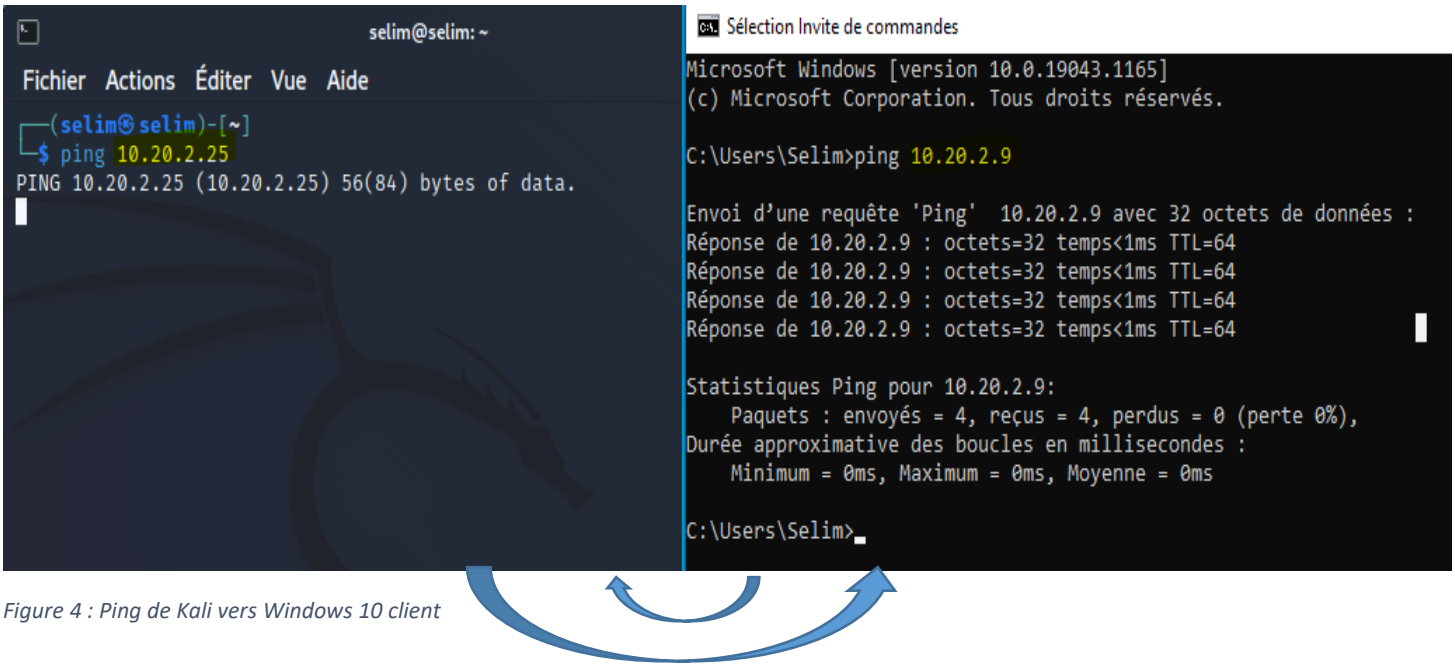


Figure 4 : Ping de Kali vers Windows 10 client

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.

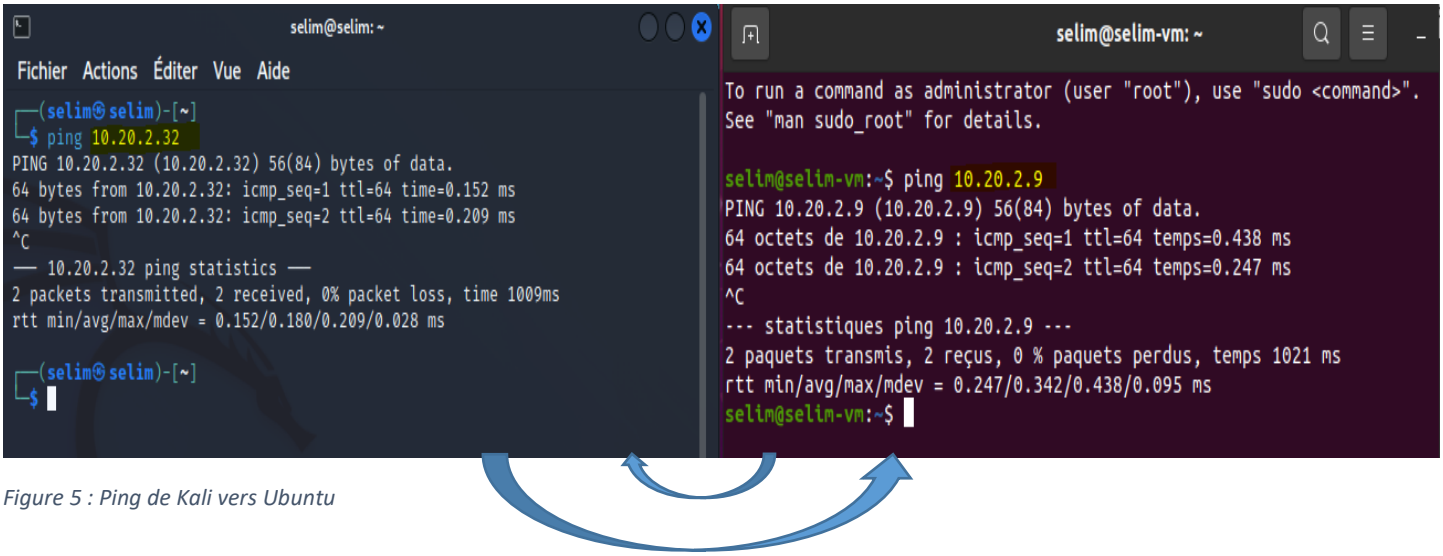
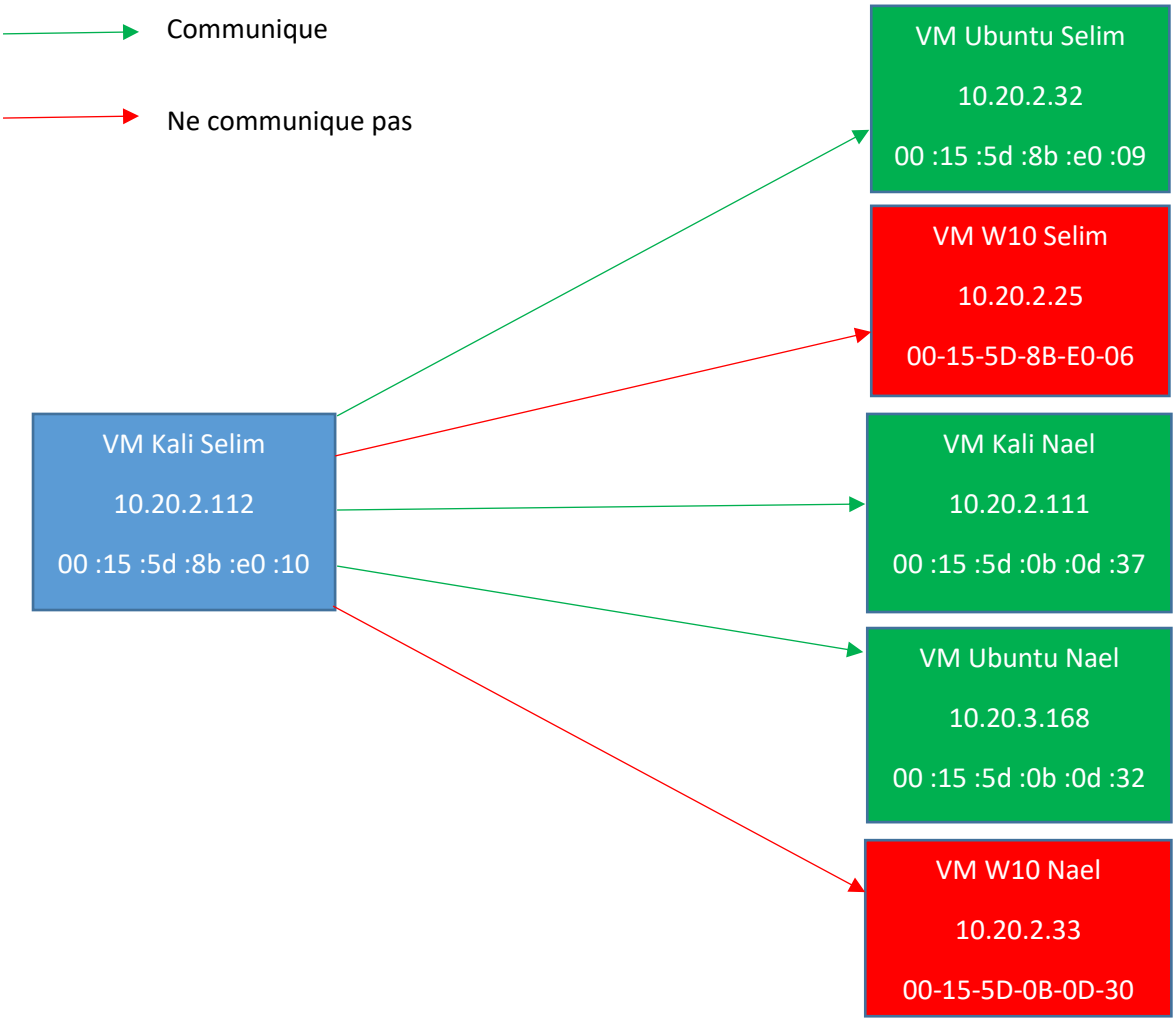


Figure 5 : Ping de Kali vers Ubuntu

BLOC 3

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



- 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 ».

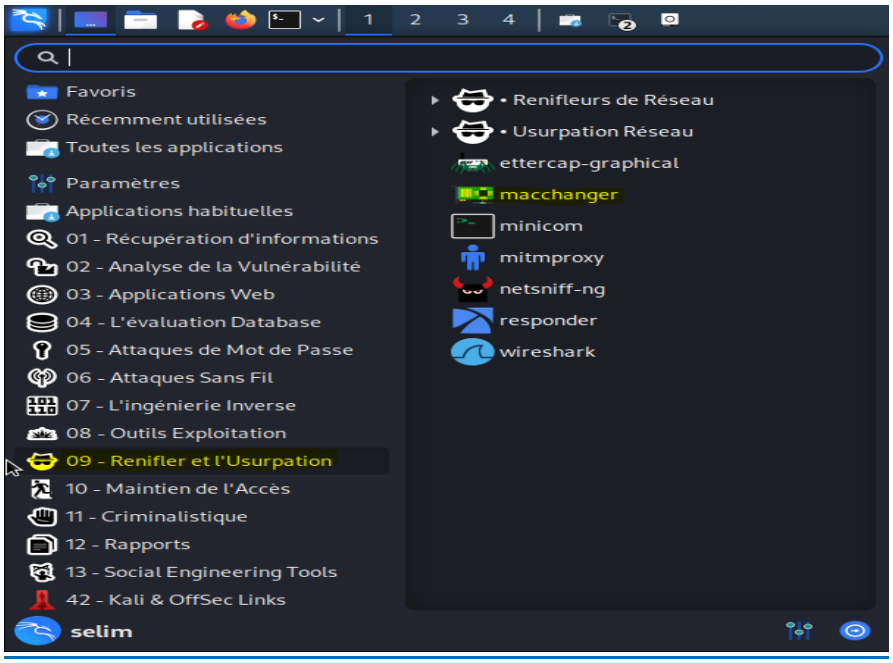


Figure 6 : Dossier de Macchanger

- 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.

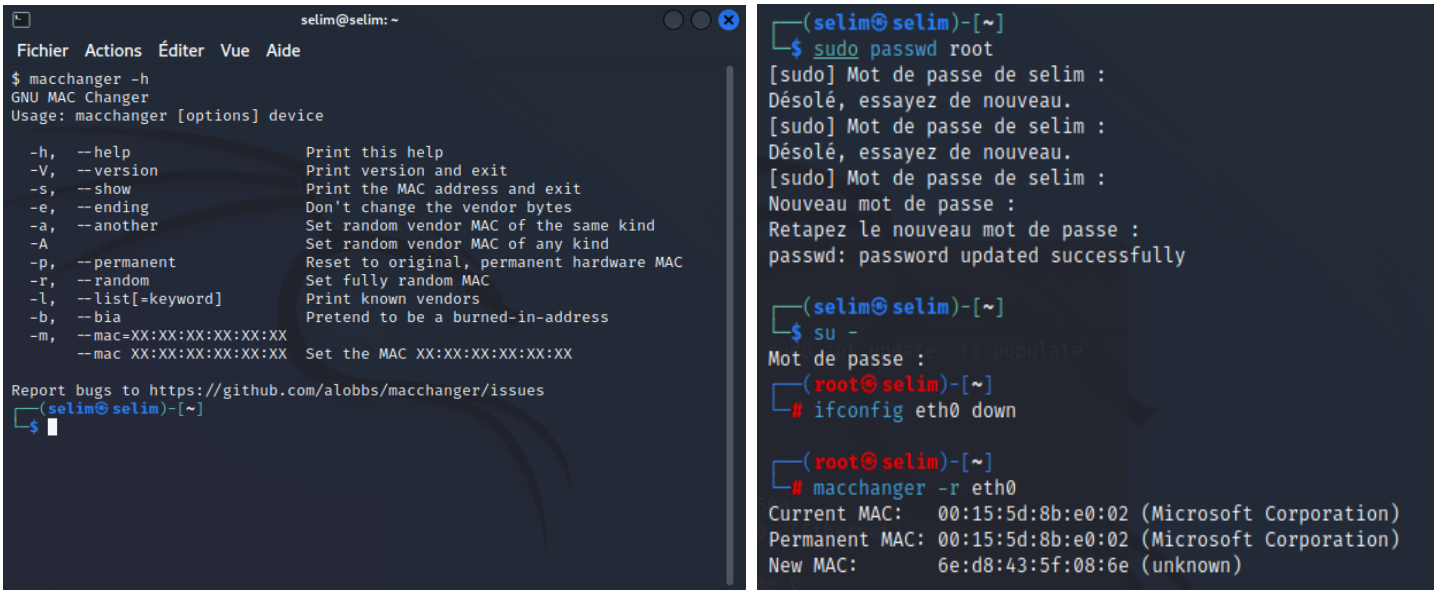


Figure 7 : Changement d'adresse MAC grâce à Macchanger

- 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 ».

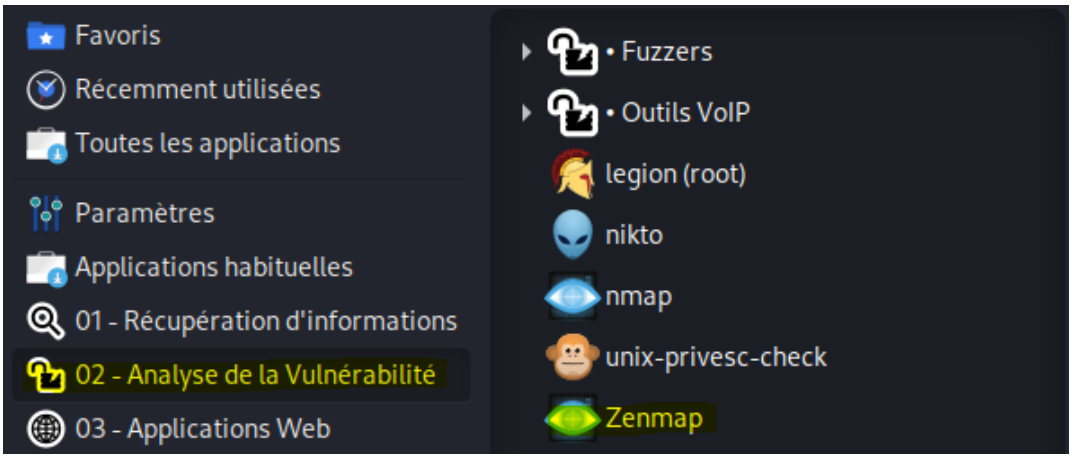


Figure 8 : Dossier de Zenmap

- 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

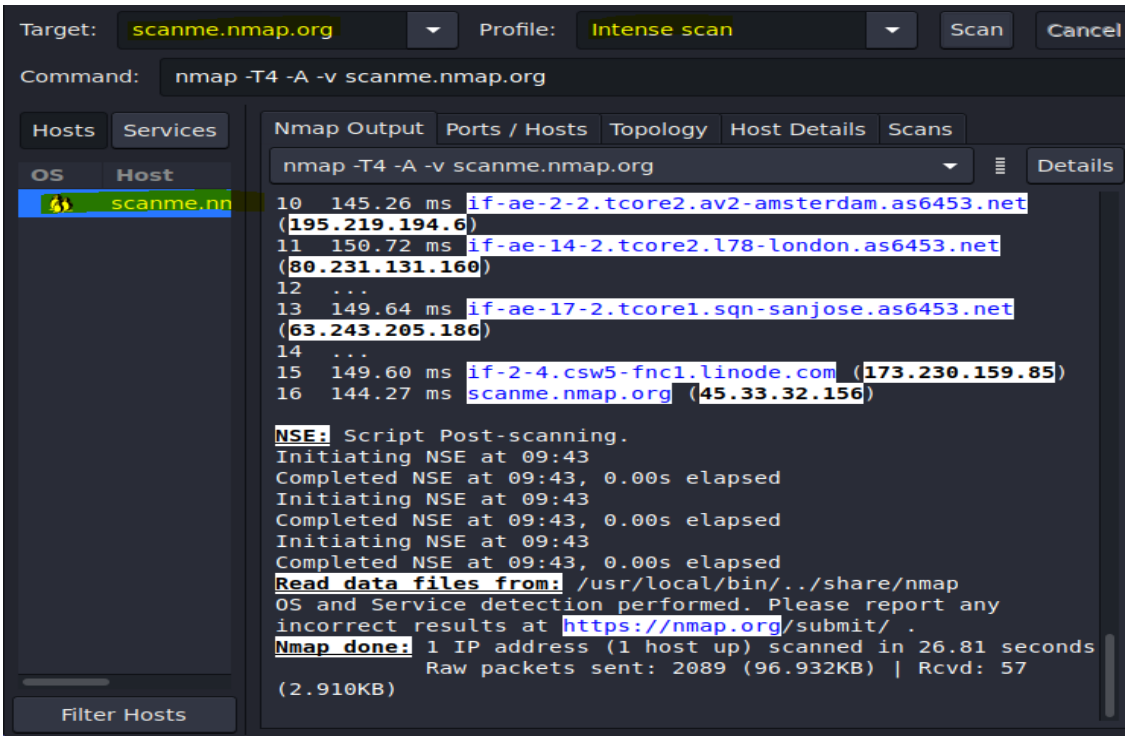


Figure 9 : Scanner les ports ouvert grâce à Zenmap

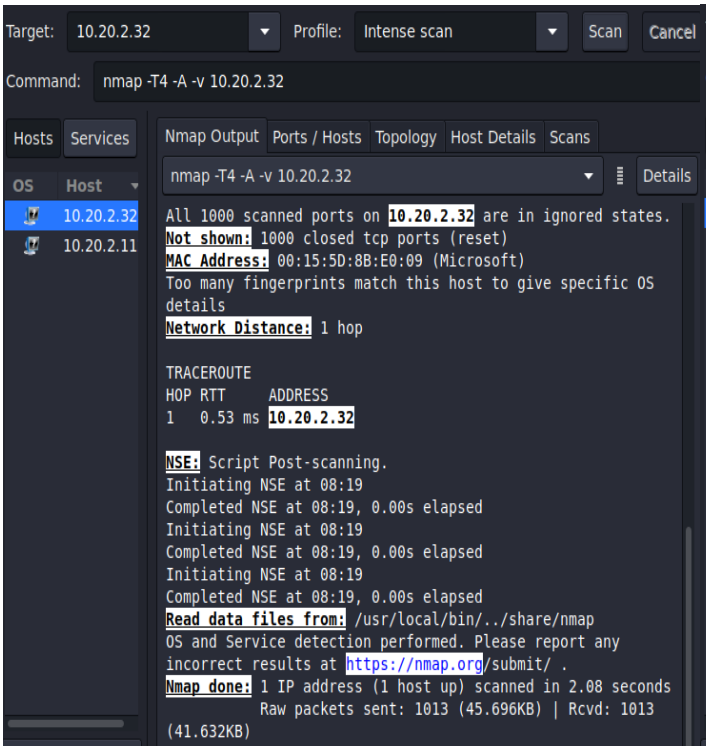


Figure 10: Zenmap Ubuntu 10.20.2.32

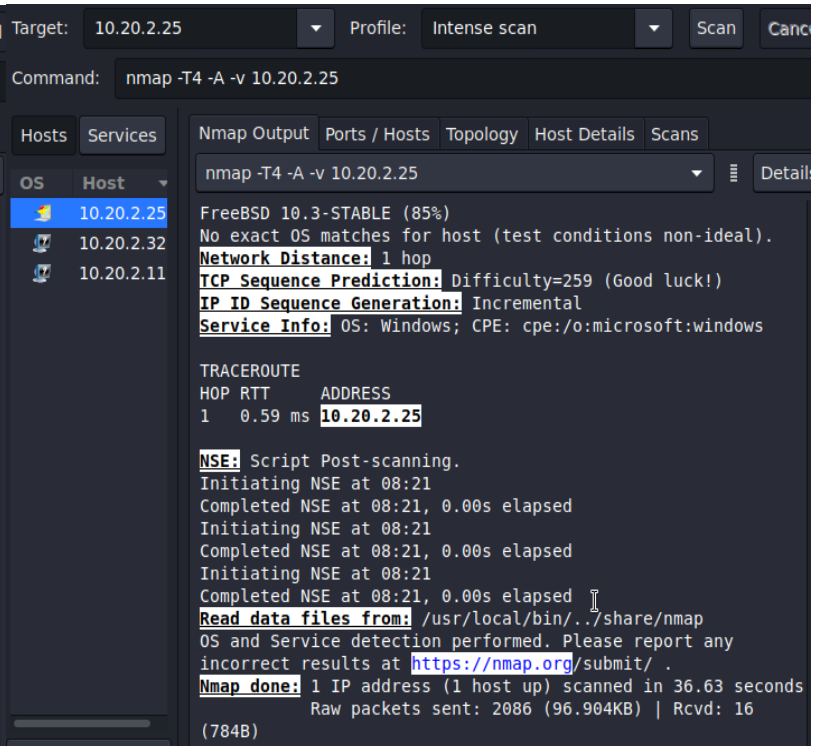


Figure 11 : Zenmap Windows 10 client 10.20.2.25

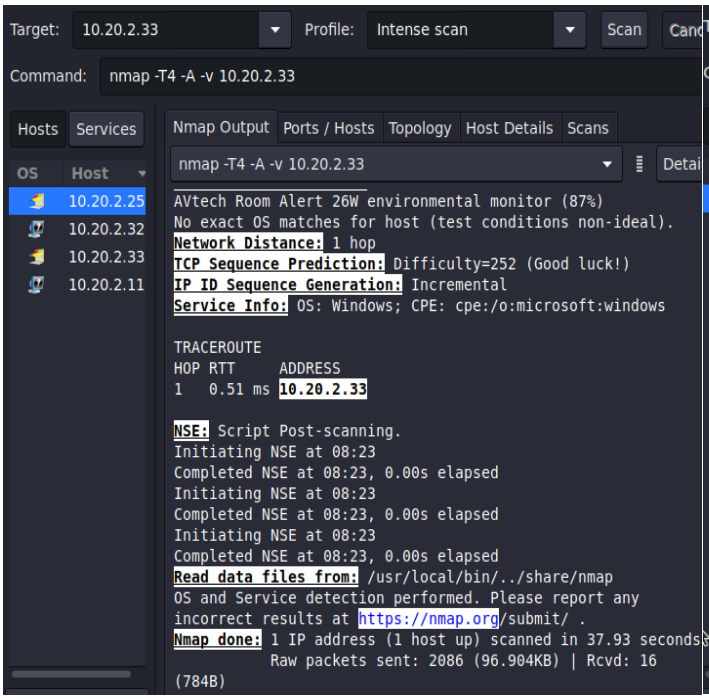


Figure 12: Zenmap Windows 10 client Nael 10.20.3.33

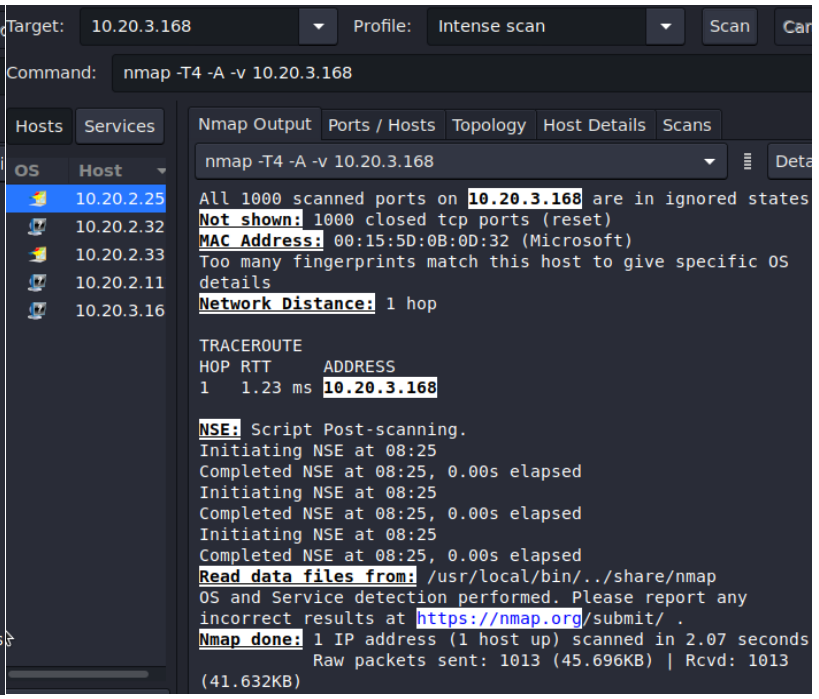


Figure 13 : Zenmap Ubuntu Nael 10.20.3.168

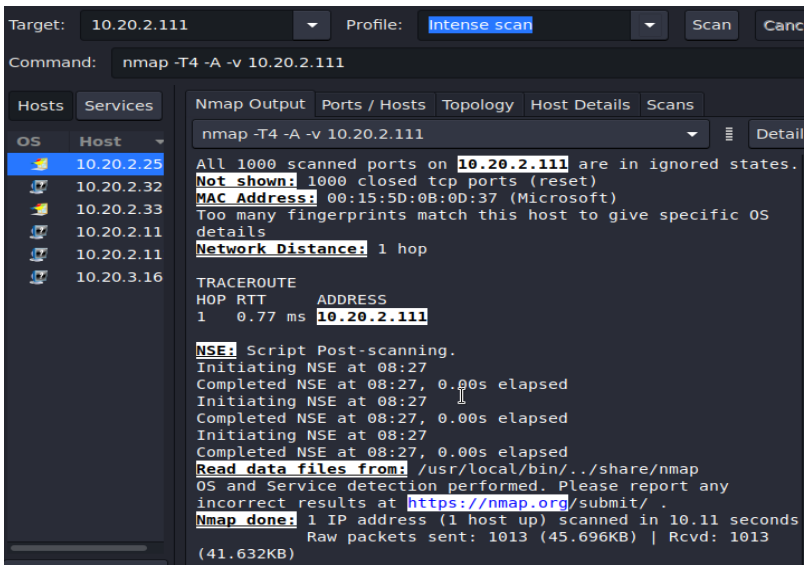


Figure 14 : Zenmap Kali Nael 10.20.3.33

- 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 :

*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.