TP Découverte (Kali et Scan réseau)

Disclaimer : Il est rappelé que les techniques et propos tenus en cours restent dans un cadre pédagogique et ne doivent être en aucun cas utilisés à des fins malveillantes. Chaque étudiant assume devant la justice ses actes. Ma responsabilité ne pourra être engagée, vous voilà prévenus.

Objectif : Découvrir le système d'exploitation Kali Linux et savoir comment se protéger en se mettant à la place de l'attaquant.

MR. JACQUEMIN **TEDE SACHA**

19/12/2023

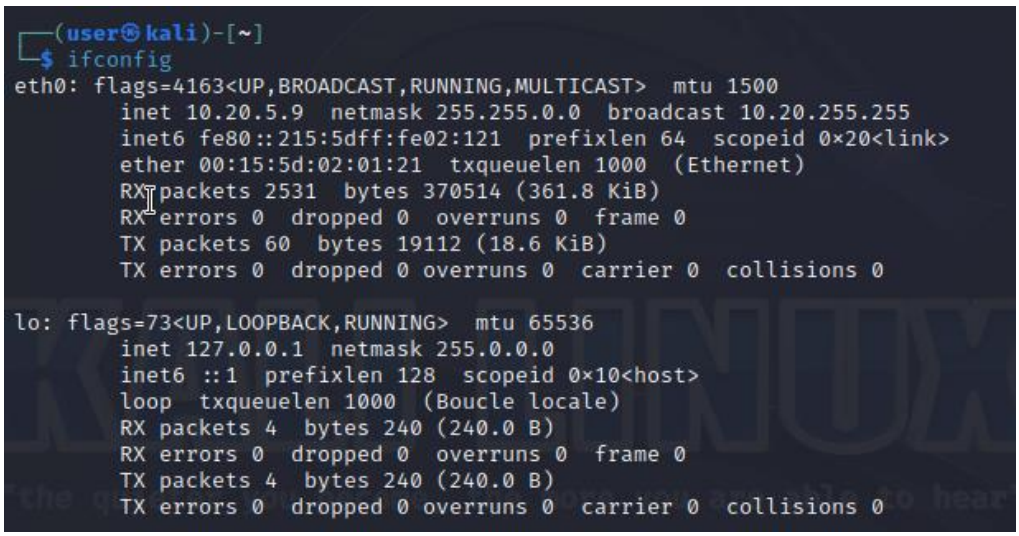
INTRODUCTION :

Dans ce TP, nous allons parler de Kali Linux, de scan réseau ou encore d'applications capables de le faire.

Dans un premier temps nous allons voir l'application Macchanger qui permet de changer son adresse MAC, qui peut être à la fois bénin et Malin. Cette application nous permettra d'en savoir un peu plus sur les scan réseau, autant sur les risques mais aussi sur la protection. En second lieu, ce sera au tour de l'application Zenmap, (dans ce TP j'utiliserais plutôt Nmap car je suis plus à l'aise dessus) cette application permet de faire un port scan, de l'analyses de réseau, des audits de sécurité de l'infrastructure du réseau etc… Elle est très utile mais comporte également ses propres risques.

1) Quelle commande avez-vous utilisée pour réaliser cette étape ? *(Linux défaillant donc pas renseigné)*

Pour le Windows client, j'ai utilisé la commande "ipconfig /all". ipconfig /all permet d'avoir toutes les caractéristiques des connexions réseaux : adresse IP, adresse MAC… Dans ce cas-ci, il nous est très utile puisque celui-ci nous a permis d'avoir toutes les infos que l'on souhaitait.



Pour Kali Linux, nous avons utilisé la commande "ifconfig". Ifconfig doit être utilisée au démarrage du système pour définir l'adresse réseau de chaque interface présente sur un système. Après le démarrage du système, il peut également être utilisé pour redéfinir une adresse d'interface et ses autres paramètres d'exploitation. Dans ce cas-ci il nous a été utile pour avoir toutes les infos nécessaires.

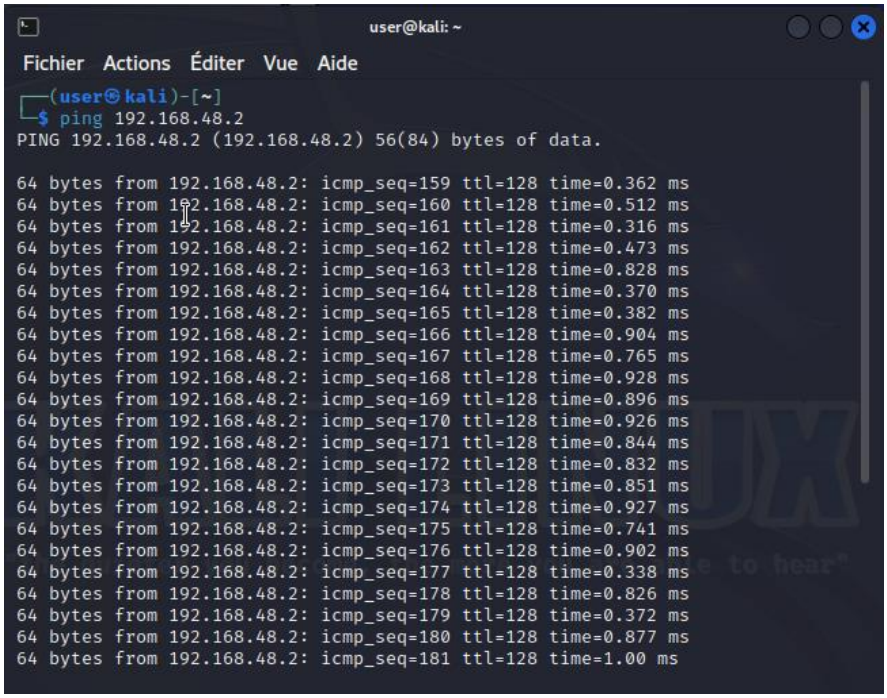
```
C:\Users\STdirection>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . . : Cli-v-01-RB
   Suffixe DNS principal . . . . . . . : Foretnoir.local
   Type de noeud. . . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . : Non
   Liste de recherche du suffixe DNS.: Foretnoir.local

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Adresse physique . . . . . . . . . . . : 00-15-5D-02-01-16
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::3973:c03:f20:fd59%5(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.48.2(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
   IAID DHCPv6 . . . . . . . . . . . : 83891549
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2C-AE-E0-5B-00-15-5D-02-01-16
   Serveurs DNS. . .  . . . . . . . . . . : 192.168.48.1
                                     127.0.0.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

C:\Users\STdirection>
```

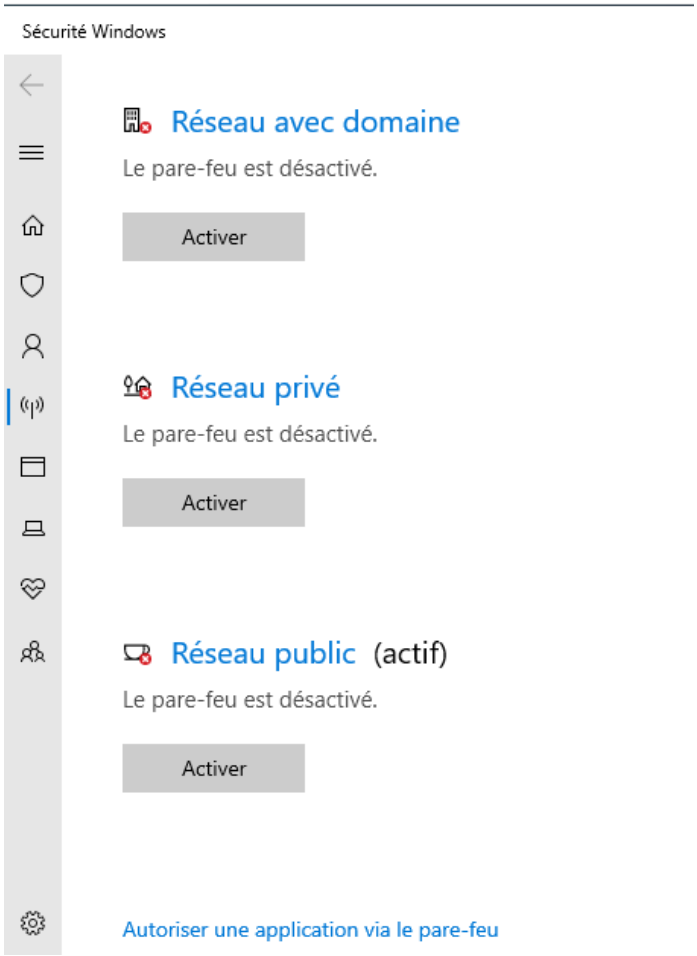
Les deux captures d'écrans ci-dessous nous permettent de voir que les deux machines sont liées grâces aux ping effectués. Il faut tout de même faire attention au pare-feu, car comme on peut le voir sous la troisième capture d'écran ci-dessous, j'ai rencontré un problème pour le ping de Kali Linux jusqu'au Client. En effet, il faut désactiver tous les par faux présent sous Windows pour que la connexion s'effectue pleinement.

Windows client → Kali Linux

```
C:\Users\STdirection>ping 192.168.48.1

Envoi d'une requête 'Ping'  192.168.48.1 avec 32 octets de données :
Réponse de 192.168.48.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.48.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.48.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.48.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.48.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Kali Linux → Windows client

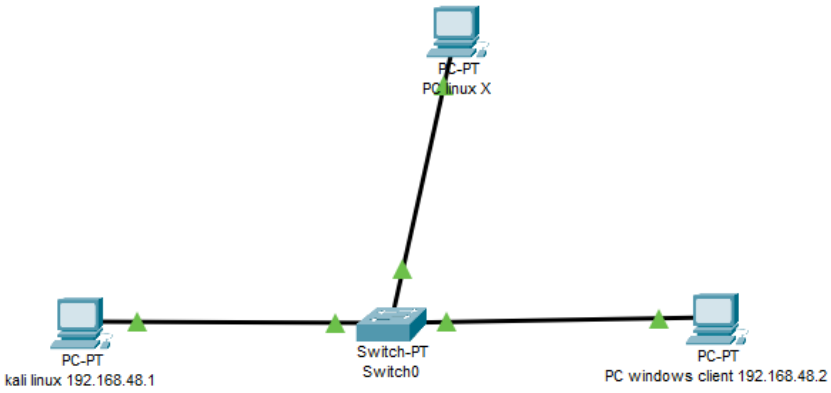




2) Réalisez un schéma de votre infrastructure avec le logiciel de votre choix (Visio, Packet Tracer, Paint, etc)

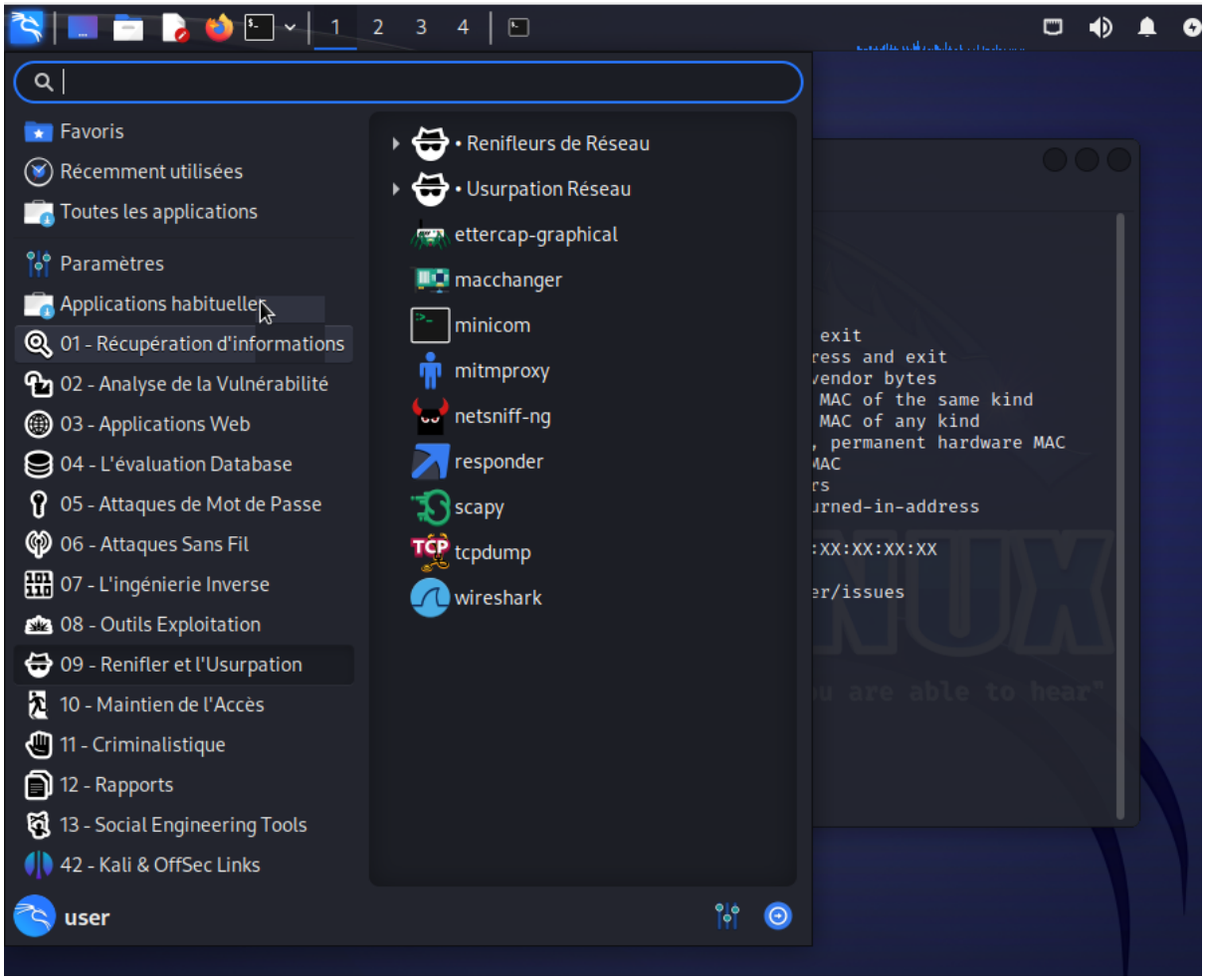
Voici le schéma des différentes liaisons aux switch réalisé sur Cisco Packet Tracer (Linux, Windows et Kali Linux).

On peut apercevoir que toutes les liaisons ethernet sont en vert, cela veut donc dire que la connexion est établi et fonctionne.



3) Dans quel dossier cette application est-elle rangée et pour quelle raison ? A quoi sert-elle ? *(Macchanger)*

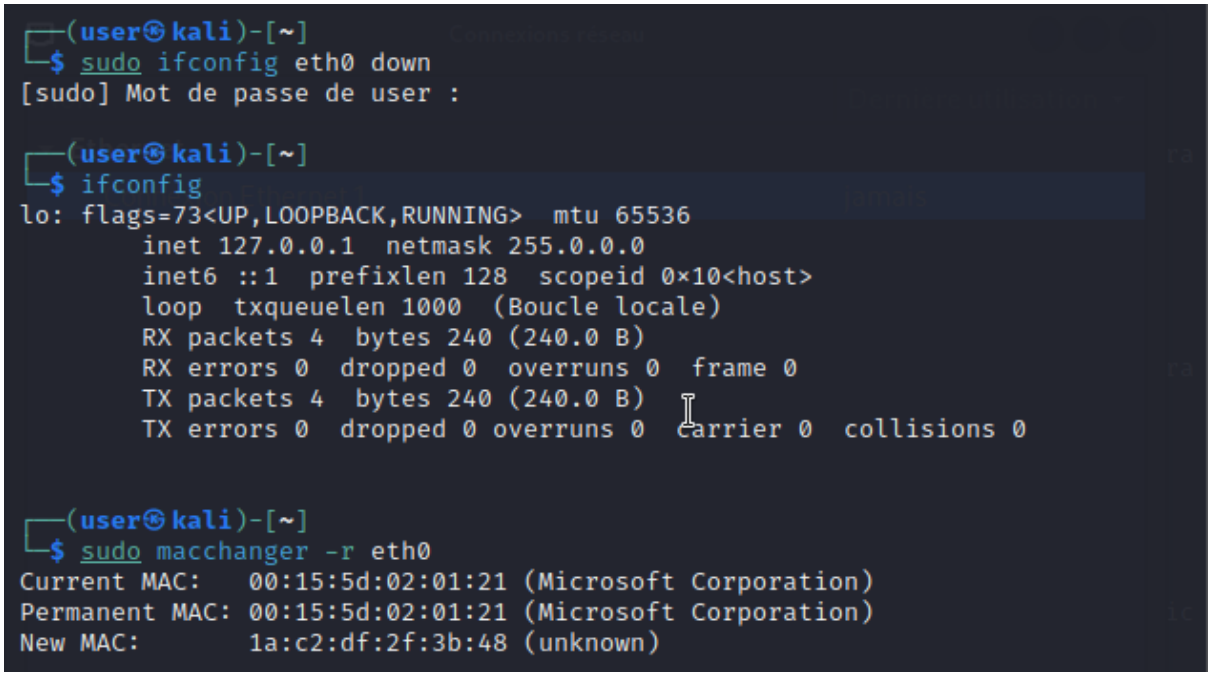
On retrouve l'application Macchanger dans "Renifler et l'Usurpation" puis on peut l'apercevoir sur la droite. Cette application permet de changer son adresse MAC. Macchanger est un utilitaire qui facilite la manipulation des adresses MAC des interfaces réseau. Les adresses MAC sont des identifiants uniques sur les réseaux, elles ont seulement besoin d'être uniques, elles peuvent être modifiées sur la plupart des matériels de réseau. Les adresses MAC ont commencé à être utilisées de manière abusive par des sociétés de marketing peu scrupuleuses, des agences gouvernementales et d'autres, afin de fournir un moyen facile de suivre un ordinateur sur plusieurs réseaux. En changeant régulièrement l'adresse MAC, il est possible de déjouer ce type de traçage, ou du moins de le rendre beaucoup plus difficile. Ce qui rend cette application très intéressante.



Voici l'ancienne adresse MAC :

```
┌──(user㉿kali)-[~]
└─$ sudo ifconfig eth0 down
[sudo] Mot de passe de user :

┌──(user㉿kali)-[~]
└─$ sudo macchanger -m
macchanger: option requires an argument -- 'm'
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

┌──(user㉿kali)-[~]
└─$ set the MAC -r
```

Puis voici la nouvelle adresse MAC changée grâce aux commandes : “sudo ifconfig eth0 down” pour désactiver la carte réseau via la ligne de commande (attention à la désactiver en ligne de commande et pas autrement sous risque que ça ne fonctionne pas) après “ifconfig” pour voir si la carte réseau est bien désactivé, comme on peut le voir via la capture d’écran et pour finir, l’étape qui va définir la nouvelle adresse MAC, “sudo macchanger -r eth0”, le “r” est pour random. J’ai choisi moi même de la mettre en random mais l’utilisateur peut la définir soi-même.



4) Combien de temps cela vous a pris ? Quels sont les dangers possibles avec une telle application ? Comment s’en protéger ? *(Macchanger)*

Grâce à l'application Macchanger, j’ai mis quelques instants à changer mon adresse MAC. C’est également très simple d’utilisation ce qui assure le bon fonctionnement du changement de l’adresse MAC.

<u>En ce qui concerne les dangers possibles que que peut apporter l’application Macchanger :</u>

<u>Usurpation d’identité :</u> En changeant l’adresse MAC de votre carte réseau, vous pouvez potentiellement usurper l’identité d’un autre appareil sur le réseau. Cela peut entraîner des problèmes de sécurité et de confidentialité.

Violation des politiques de réseau : Certains réseaux peuvent avoir des politiques qui interdisent la modification des adresses MAC. Si vous violez ces politiques, vous pouvez être exclu du réseau.

Problèmes de connectivité : Modifier l'adresse MAC de votre carte réseau peut parfois entraîner des problèmes de connectivité. Par exemple, si vous changez l'adresse MAC à une adresse qui est déjà utilisée par un autre appareil sur le réseau, cela peut entraîner des conflits d'adresse IP.

Pour vous protéger contre ces dangers, voici quelques recommandations :

Utilisez macchanger avec prudence : N'utilisez macchanger que lorsque cela est absolument nécessaire et assurez-vous de comprendre les implications de la modification de votre adresse MAC.

Respectez les politiques de réseau : Si vous êtes sur un réseau qui interdit la modification des adresses MAC, respectez cette politique.

Sauvegardez votre adresse MAC originale : Avant de modifier votre adresse MAC, notez l'adresse MAC originale de votre carte réseau. De cette façon, vous pouvez toujours revenir à votre adresse MAC originale si nécessaire.

Mettez à jour vos logiciels : Gardez toujours vos logiciels, systèmes d'exploitation et antivirus à jour. Les mises à jour régulières corrigent les failles de sécurité potentielles.

Utilisez un antivirus : Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus.

Sauvegardez vos données : Effectuez régulièrement des sauvegardes de vos données importantes. En cas de problème, vous pourrez restaurer vos informations vitales.

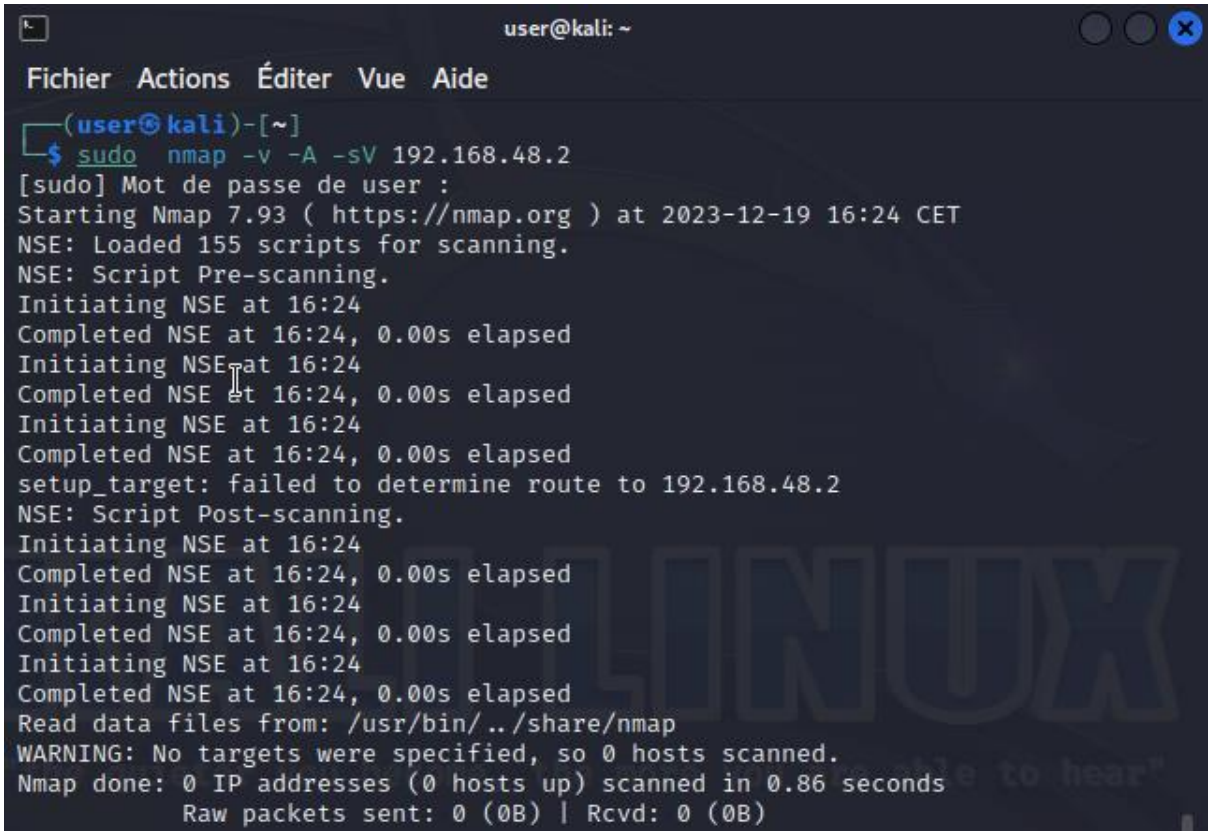
Signalez tout comportement suspect : Si vous observez un comportement en ligne suspect ou malveillant, signalez-le aux autorités compétentes.

5) Dans quel dossier cette application est-elle rangée et pour quelle raison ? A quoi sert-elle ? *(Nmap)*

Disclaimer : Utiliser cette application sur un appareil ou un réseau qui ne vous appartient pas est illégal et peut vous exposer à des risques. Ne quittez pas votre environnement de TP à l'exception du serveur cité en dessous.

L'application Nmap se trouve dans "Récupération d'informations" puis l'icône se trouvera juste en bas à droite de la page.

Ci-dessous le scan de tous les ports présents sur mon Windows Client depuis mon Kali Linux :



6) Quelle application se cache derrière Zenmap ? Quels sont les dangers possibles avec une telle application ? Comment s'en protéger ?

Zenmap est une interface utilisateur graphique pour Nmap, un outil d'analyse de réseau libre et gratuit. Il simplifie l'utilisation de Nmap grâce à une interface.

Zenmap est compatible avec Windows, Linux et macOS et d'autres. Zenmap, comme Nmap, est un outil puissant qui peut être utilisé pour identifier les vulnérabilités, sécuriser les systèmes et protéger les informations sensibles. Cependant, il peut également être utilisé de manière malveillante pour identifier les points d'entrée potentiels pour les attaquants.

Pour se protéger contre les potentiels dangers associés à Zenmap et à d'autres outils d'analyse de réseau, voici quelques recommandations :

Mettre souvent à jour les systèmes : Il faut bien s'assurer que tous les systèmes d'exploitation et applications sont à jour avec les derniers correctifs de sécurité au risque de subir des attaques plus facilement.

Utiliser un pare-feu : Un pare-feu peut aider à bloquer les tentatives non autorisées d'accéder à votre réseau. Il faut changer les mots de passe par défaut et en mettre un soi-même qui ne doit pas être trop facile d'accès.

Limitez l'exposition de votre réseau : évitez d'exposer inutilement des systèmes ou des ports à l'Internet public. Cela est en majeure partie accessible aux attaquants et une manière des plus simple pour eux.

CONCLUSION :

Pour conclure, Macchanger et Zenmap sont deux applications très utiles et très certainement trop utiles par moment.

Ces applications sont comme les deux côtés d'un iceberg, elles peuvent à la fois être bienfaisante et malfaisante.

Or, dans ce TP, nous avons vu plusieurs points qui permettent de se protéger en grande partie contre ces deux applications. Leur utilisation est plutôt simple et toutes les requêtes s'effectuent en quelques instants.

Comme vu précédemment, nous avons testé plusieurs scan réseau sur nos propres machines, par exemple, j'ai pu apercevoir tous les ports de mon Windows Client juste avec quelques commandes, cela montre à quel point la sécurité de son ordinateur, ou autre appareil, se doit d'être renforcée.

Changer son adresse MAC peut être à double sens, soit on peut le faire pour aider ou soit on peut le faire pour usurper l'identité d'autrui.

Lorsqu'on manie ces deux applications, attention à respecter les politiques de réseau, car il peut y avoir des conséquences même si on ne pense pas à mal.

Pour finir, il faut faire attention à ne pas utiliser Macchanger sans raison, de même pour Nmap, ne pas oublier de sauvegarder l'adresse MAC avant de la changer et surtout de bien faire attention aux différents problèmes de connectivité qui pourraient engendrer un conflit d'adresse IP.