Mr JACQUEMIN

19/12/2023

Compte rendu TP3

Scanning réseau et usurpation MAC avec Kali Linux

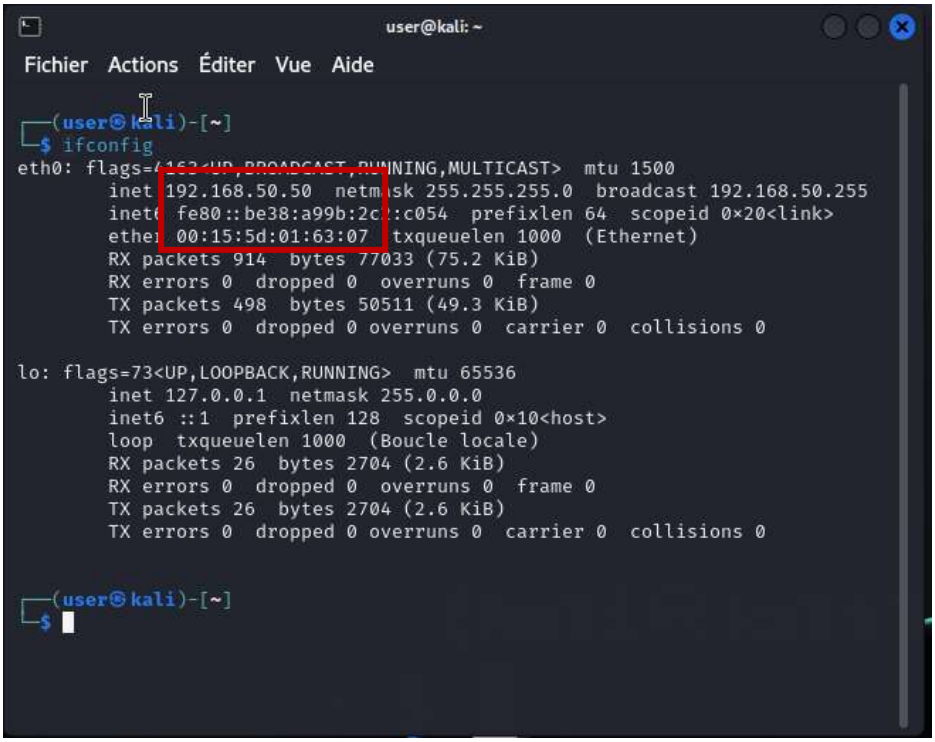
TEWES Arnaud
BTS SIO SISR 1ÈRE ANNÉE

Introduction

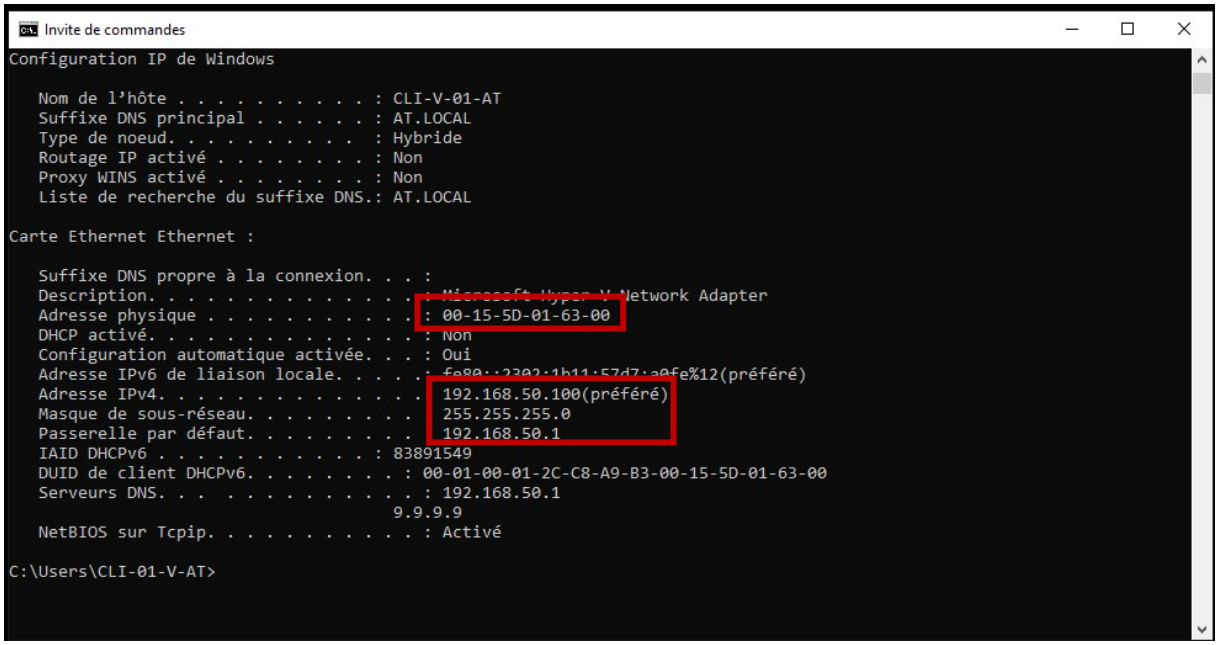
Dans ce TP, nous allons découvrir la distribution Kali Linux et tester certains de ses outils. Nous allons nous mettre dans la peau d'un attaquant qui attaque un PC. Dans un premier temps, nous allons tester l'application MACchanger qui va nous servir à modifier (ou même à usurper) l'adresse MAC de notre machine dans un but éthique (ou non). Et dans un second temps, nous allons tester et nous documenter sur l'application ZenMap qui, quant à elle, va nous servir à faire du scanning réseau (scanning de ports, de vulnérabilités, d'OS). Ces outils sont à utiliser avec la plus grande précaution et seulement sur des entités où l'on a une autorisation écrite de le faire. Ce sont des outils qui peuvent être utilisés de manière éthique, comme pour faire des audits de sécurité dans le cadre d'un contrat, ou de manière non éthique pour des attaques malveillantes. Donc à utiliser avec la plus grande précaution et accord préalable.

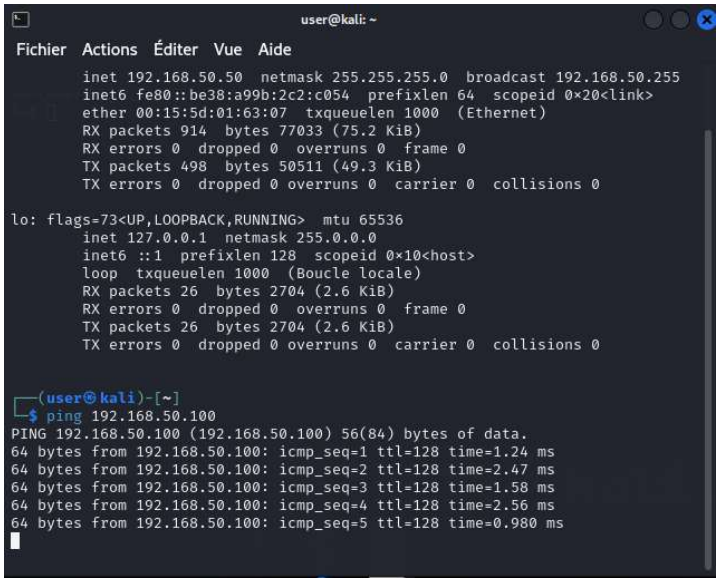
Question 1 :

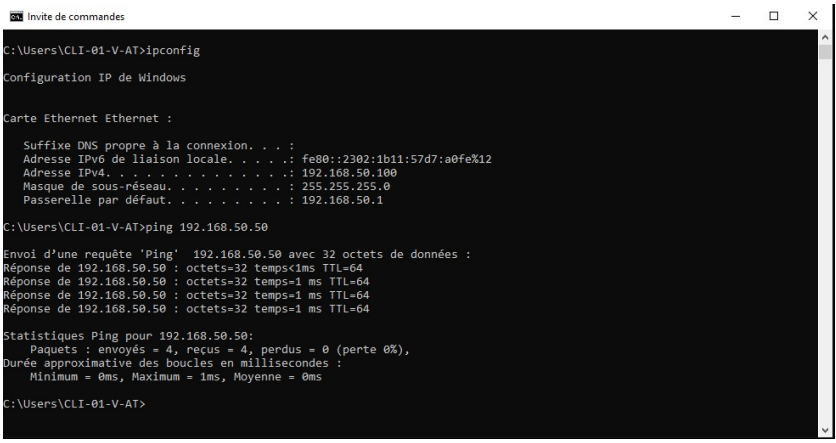
Pour cela, nous allons vérifier la configuration réseau de nos machines virtuelles pour qu'elles puissent communiquer et pour vérifier leur adresse MAC au départ de ce TP. Sous Kali Linux, cela se fait avec la commande ifconfig :



Ensuite, nous allons mettre la machine Windows sur la même adresse réseau que notre machine sous Kali, vérifier son adresse MAC et vérifier qu'elles communiquent bien entre elles. Sous Windows, il faut également désactiver le pare-feu pour nos tests, sinon il est possible qu'il bloque l'accès à Kali.



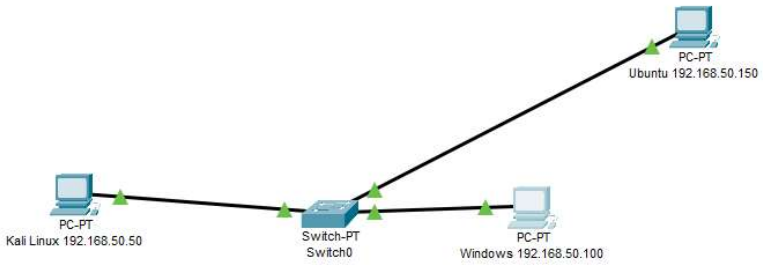




Les deux machines communiquent correctement et nous pouvons donc passer à nos tests.

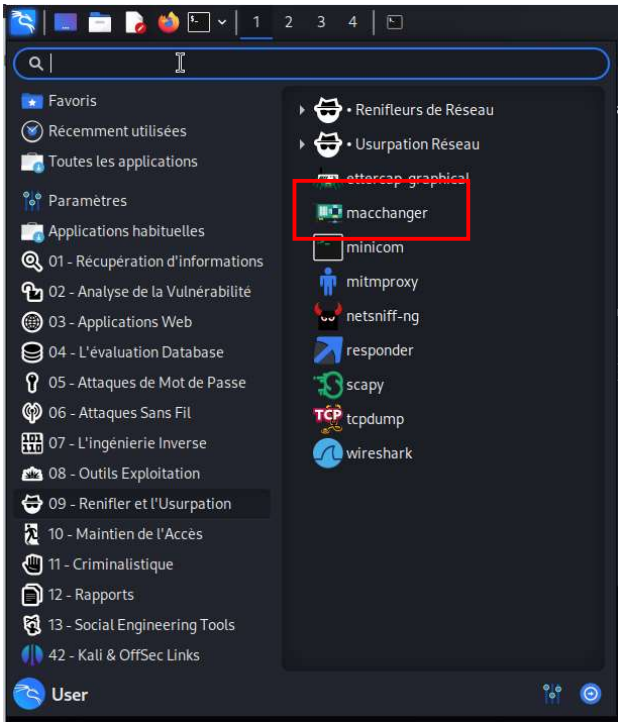
Question 2 :

Voici le schéma réseau de notre infrastructure virtuelle avec Kali Linux comme machine attaquante, et deux machines sous Windows et Ubuntu pour les machines à attaquer :



Question 3 :

L'application MACchanger est rangée dans le dossier « Renifler et Usurpation » car elle permet de modifier l'adresse MAC (ou adresse physique). Nous pouvons également usurper l'identité d'un autre périphérique (comme un autre PC ou un routeur par exemple) qui peut être utilisé dans certaines attaques (Man in the middle). Avec cette application, nous avons la possibilité de changer notre adresse MAC par une autre adresse MAC soit choisie aléatoirement (très utile pour éviter le suivi par des agences de marketing ou gouvernementales), soit choisie par l'utilisateur (pour qu'elle soit la même que celle d'un autre périphérique).



Question 4 :

Grâce à l'application MACchanger, j'ai pu modifier mon adresse MAC en environ 4 secondes (le temps de trouver la bonne commande) en une adresse MAC choisie au hasard. Les dangers possibles avec une telle application sont :

- Attaques par usurpation d'adresse MAC : Un attaquant peut usurper notre adresse MAC et rediriger les données envoyées à notre appareil vers un autre, accédant ainsi à nos données. L'ARP est un protocole qui permet de retrouver une adresse MAC à partir d'une adresse IP.

- Attaques de Man in the Middle (MITM) : Un attaquant peut changer l'adresse MAC de son appareil pour correspondre à celle d'un autre sur un réseau afin de lancer une attaque MITM.

- Contournement de la sécurité du réseau : L'usurpation d'adresse MAC peut être utilisée pour contourner les mesures de sécurité du réseau basées sur l'adresse MAC, comme le filtrage MAC.

- Accès aux réseaux : Les hackers peuvent utiliser MACchanger pour gagner l'accès à des réseaux qui sont limités à certaines adresses MAC.

- Dissimulation de l'identité : Ils peuvent également l'utiliser pour cacher l'identité de l'appareil original ou pour éviter d'être suivis ou tracés.

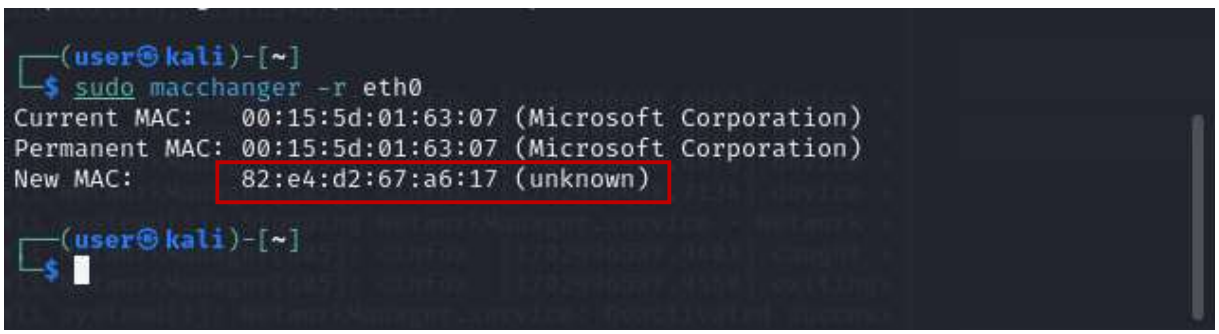
Nous pouvons nous protéger, nous avons plusieurs possibilités comme :

- Une technique courante pour détecter une usurpation d'adresse MAC consiste à surveiller les diffusions ARP.

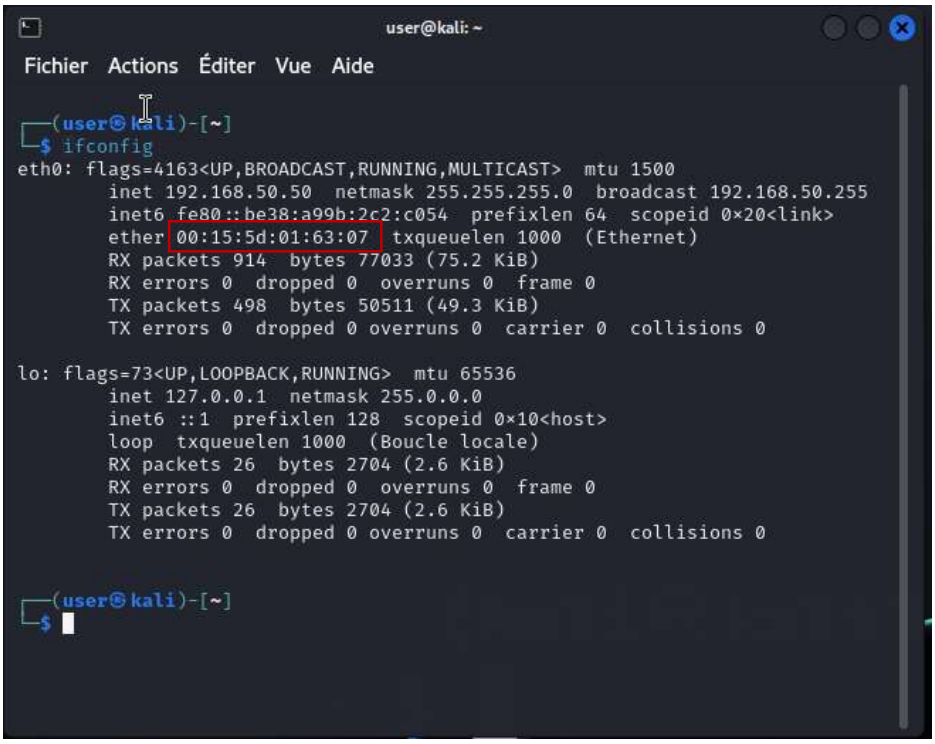
- Les administrateurs réseau peuvent utiliser des listes de contrôle d'accès pour limiter les appareils qui peuvent se connecter à un réseau en fonction de leur adresse MAC.

- Effectuer ses mises à jour régulièrement permet de se protéger contre les nouvelles vulnérabilités, qui sont à effectuer sur tous les postes et toutes les applications installées sur un poste.

Voici un exemple de changement d'adresse MAC par une adresse MAC random avec MACchanger :

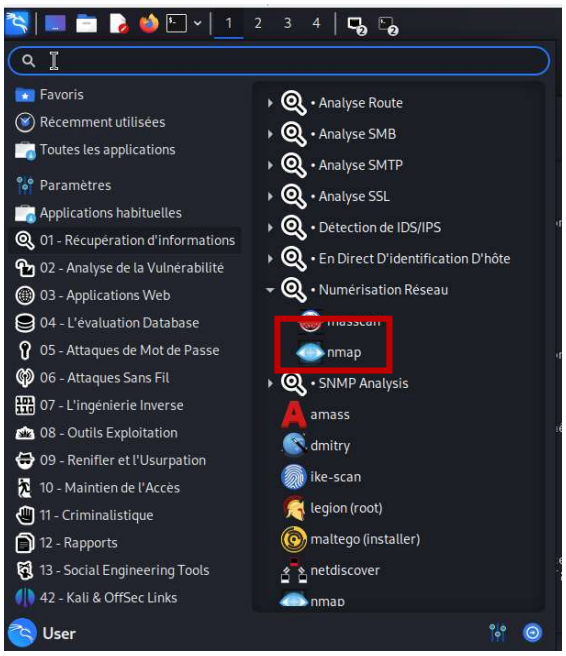


Et voici l'ancienne capture d'écran qui montre la première adresse mac que nous avions :



Question 5 :

Cette application est rangée dans le dossier « Récupération d'informations – Numérisation Réseau ». Elle est placer dans ce dossier car elle permet de récupérer des informations sur un réseau et de la scanner dans son entièreté. Le scanning réseau sert à trouver des vulnérabilités dans un réseau informatique (Découverte du réseau, scan de ports, détection de versions et de services, détection de système d'exploitation), permet de trouver des hôtes et permet également de faire des audits pour aider à trouver des failles de sécurité.



Question 6 :

Zenmap (ou Nmap) est un outil d'exploration réseau. Il est conçu pour détecter les ports ouverts, identifier les services et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Nmap, en plus d'être un excellent scanner de port, contient également énormément d'outils qui permettent aux professionnels de la cybersécurité et aux administrateurs réseau de comprendre la structure, les vulnérabilités et les services vulnérables de leur réseau.

Nmap est un excellent logiciel de scanning, mais peut être utilisé à des fins malveillantes pour obtenir l'accès à des ports non restreints sur un réseau. De plus, les scripts d'analyse des vulnérabilités de Nmap sont utilisés par les pen-testeurs et les hackers pour examiner les vulnérabilités.

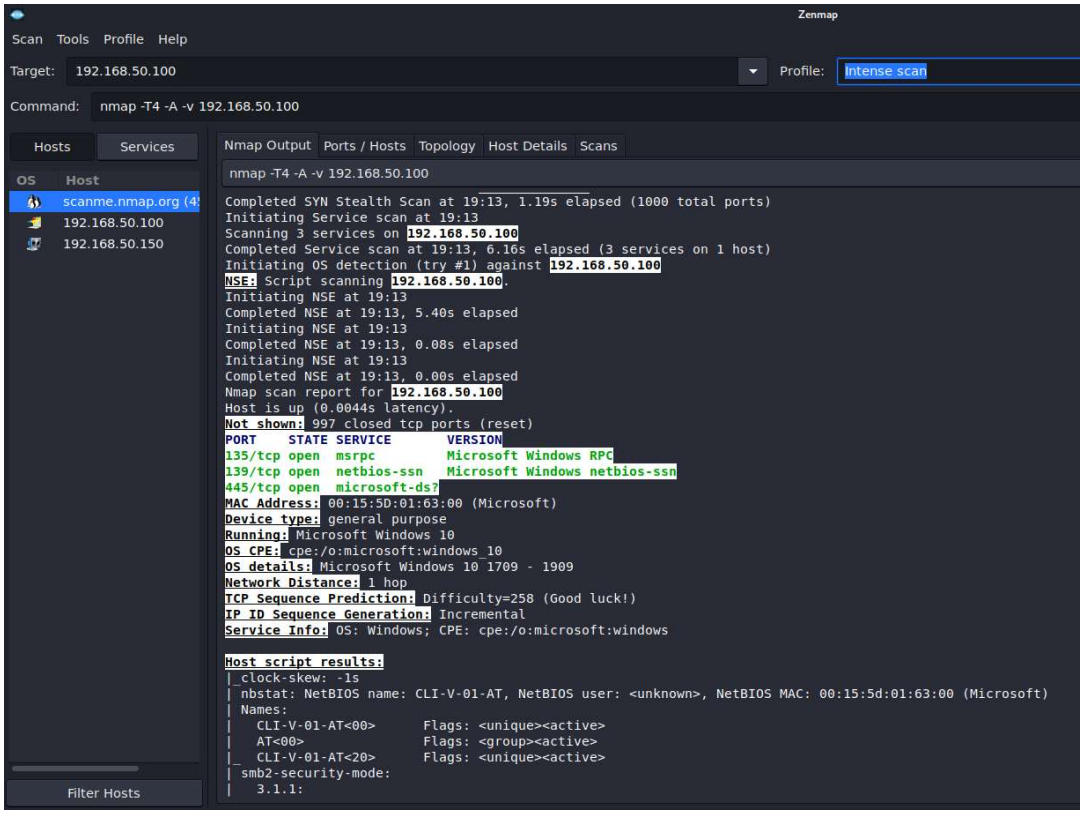
Pour se protéger contre ce genre d'application, nous pouvons utiliser :

- Des pare-feux et des logiciels de détection d'intrusion pour bloquer les scans malveillants.
- Désactiver les services et les ports inutiles pour réduire la surface d'attaque des attaquants.
- Activer des filtres : Ces filtres détectent et/ou bloquent les scans de ports et les balayages d'hôtes.
- Surveiller régulièrement l'activité de son réseau.
- Utiliser Nmap pour la défense : En utilisant Nmap, un administrateur réseau peut sonder son propre réseau pour obtenir une "vue de pirate". En utilisant les mêmes outils qu'un intrus, un administrateur verra à quoi ressemble son infrastructure pour les « méchants » et pourra, espérons-le, prendre des mesures pour sécuriser son réseau.

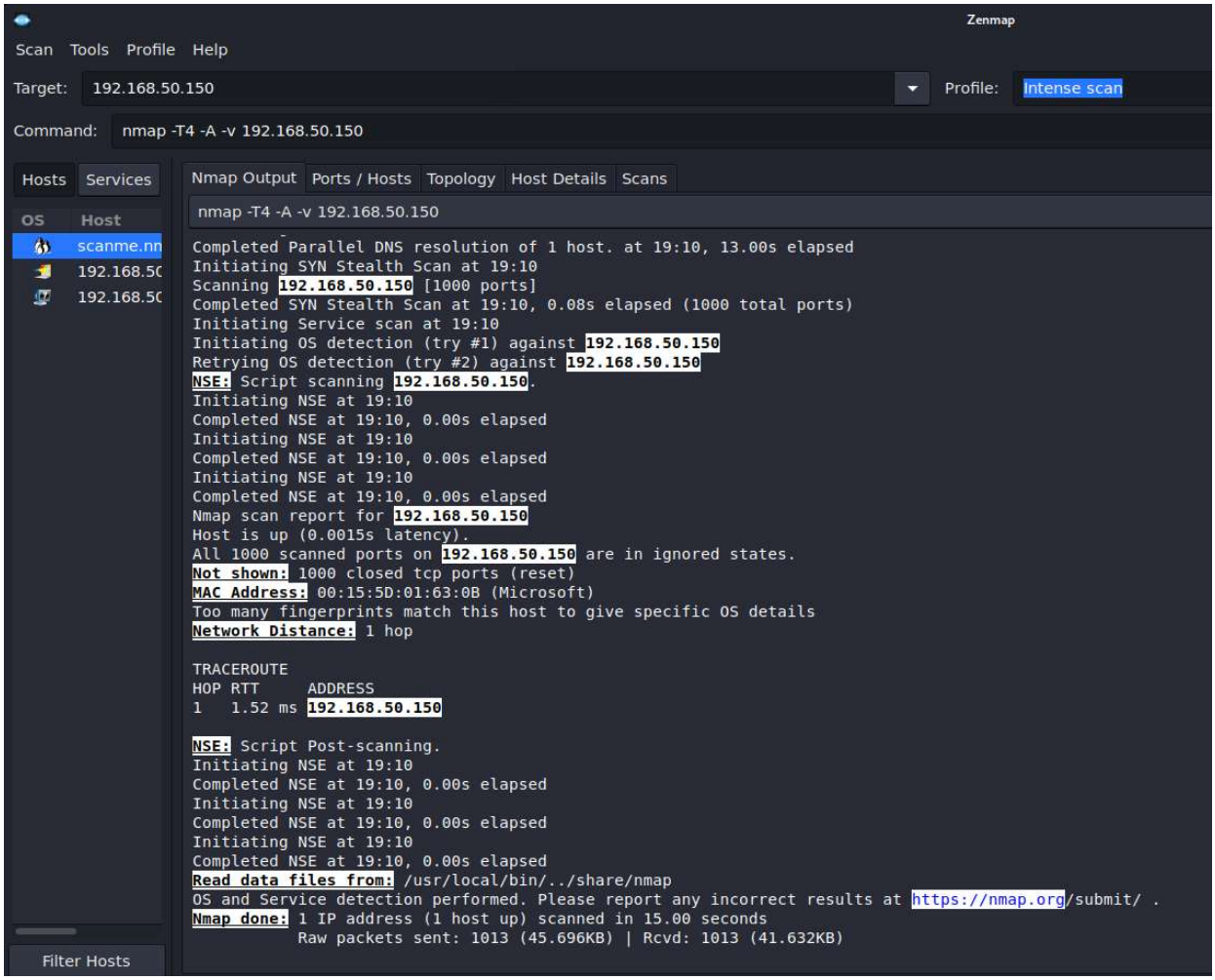
J'ai donc effectué un test avec Zenmap (l'interface graphique de Nmap) qui est beaucoup plus facile d'utilisation et beaucoup plus intuitif pour scanner mes deux machines sous Windows et Ubuntu.

Nous devons simplement spécifier l'adresse IP de la machine que l'on veut scanner, le type de scan que nous voulons effectuer et l'application se charge du reste :

Windows :

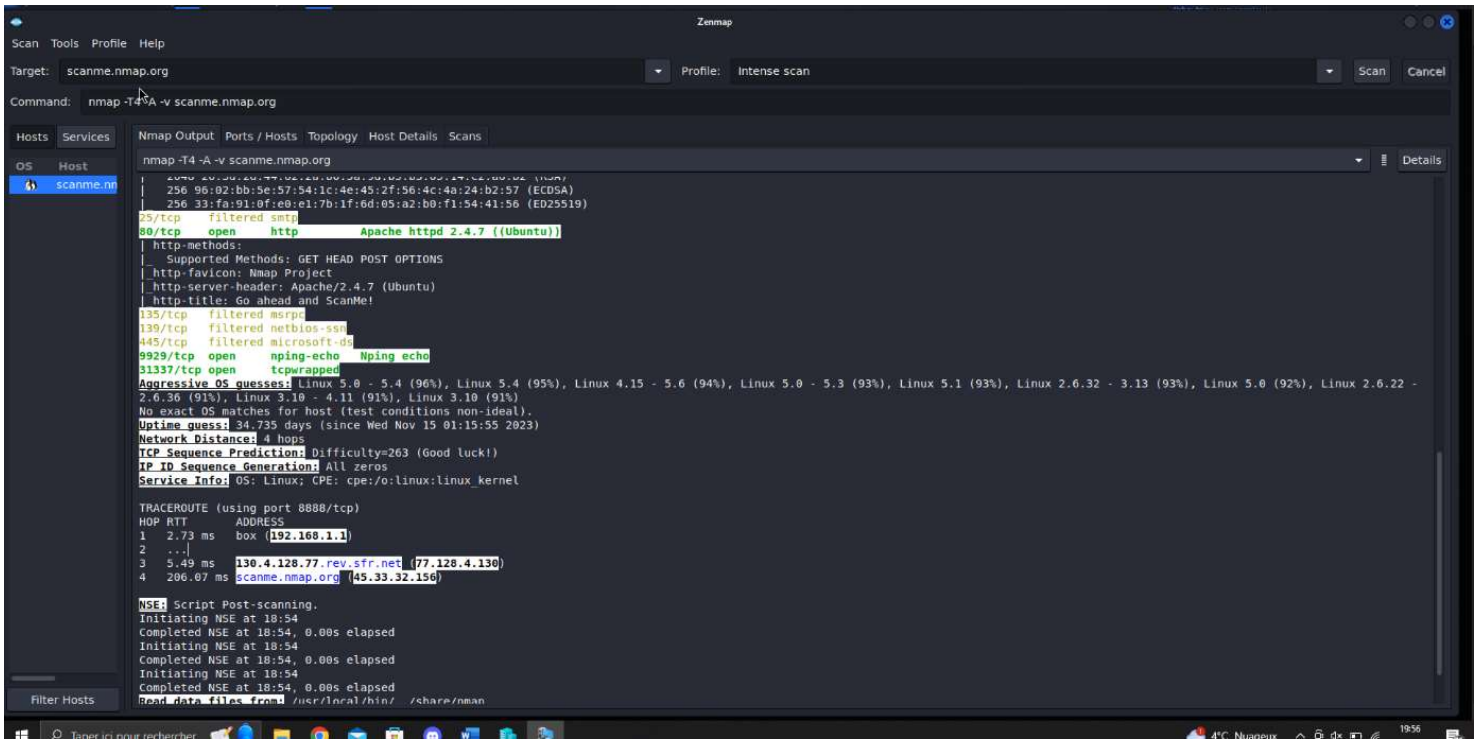


Ubuntu :



Les scans sont terminés, nous pouvons voir que sur la machine sous Windows (192.168.50.100), l'analyse a dévoilé 3 ports ouverts, l'adresse Mac, le système d'exploitation, les services hébergés, etc… et sur la machine Ubuntu, l'analyse a dévoilé un peu moins d'informations visibles, mais nous pouvons quand même voir l'adresse MAC de la machine, et que le scan n'a trouvé aucun port ouvert par exemple.

Ensuite, j'ai effectué un scan sur un site web qui a été conçu pour effectuer ce scan en guise de test et pouvoir voir comment l'application fonctionne. Nous pouvons voir que plusieurs ports sont ouverts et certaines vulnérabilités sont détectées :



Le scan étant terminé, il a analysé les 1000 premiers ports et nous pouvons constater que certains ports sont ouverts, d'autres sont filtrés, et nous pouvons également voir sur quel service nous redirige chaque port. Cet outil est très bien illustré et nous pouvons réellement récupérer beaucoup d'informations de vulnérabilité grâce à lui. Il peut être assez dangereux si utilisé à mauvais escient, mais très efficace pour tester un réseau.

Conclusion (question 7)

Voilà, dans ce TP j'ai découvert (ou redécouvert) Kali Linux, un OS puissant utilisé pour les Pen-tests et les audits de sécurité, ou à des fins malveillantes. En utilisant des outils comme macchanger et Zenmap, j'ai pu voir mon réseau du point de vue d'un attaquant potentiel.

Grâce à l'outil macchanger j'ai pu comprendre comment les adresses MAC peuvent être modifiées, ce qui pourrait être utilisé pour usurper l'identité d'un appareil sur le réseau. Cela souligne l'importance de surveiller régulièrement les adresses MAC sur un réseau et de vérifier toute activité suspecte.

Zenmap (l'interface graphique de nmap), quant à lui, m'a permis de découvrir les scans d'hôtes, les scans de services sur un réseau informatique et de réaliser des tests de vulnérabilité. Cela a mis en évidence le fait que même si ces outils peuvent être utilisés à des fins légitimes, ils peuvent également être utilisés par des personnes malveillantes pour explorer de manière illégale un réseau et découvrir ses vulnérabilités.

Cela m'a également permis de comprendre que la sécurité d'un réseau ne dépend pas seulement de la protection contre les attaques externes, mais aussi de comprendre les méthodes que les attaquants pourraient utiliser pour exploiter les vulnérabilités internes. En me mettant à la place de l'attaquant, je peux mieux comprendre ces vulnérabilités et prendre des mesures pour essayer de les contrer.

En conclusion, la découverte de Kali Linux et de ses outils m'a donné un aperçu sur la sécurité informatique et qu'il est très facile, ou du moins à la portée de tous, grâce notamment à plein d'outils open source de pouvoir scanner et entrer dans un réseau informatique vulnérable.

Il est important de se rappeler que l'utilisation de ces outils à des fins malveillantes ou sur des réseaux qui ne nous appartiennent pas est illégale et peut nous exposer à des risques. Il est donc indispensable et obligatoire d'utiliser ces outils de manière responsable et éthique, seulement avec une autorisation préalable.

Enfin, ce TP m'a montré l'importance de la sensibilisation en matière de cybersécurité. En comprenant comment fonctionnent les outils utilisés par les attaquants, je pourrais contribuer à rendre mes réseaux plus sûrs.