

Mr JACQUEMIN

19/12/2023

Compte rendu TP3

Scanning réseau et usurpation MAC
avec Kali Linux

TEWES Arnaud
BTS SIO SISR 1ÈRE ANNÉE

Introduction

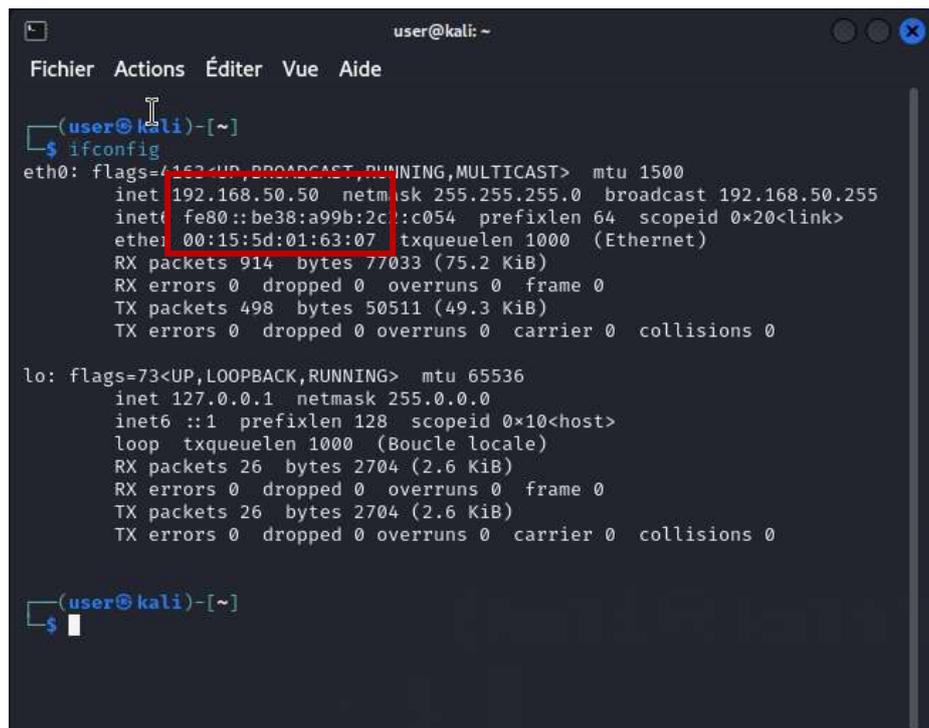
Dans ce TP, nous allons découvrir la distribution Kali Linux et tester certains de ses outils. Nous allons nous mettre dans la peau d'un attaquant qui attaque un PC. Dans un premier temps, nous allons tester l'application MACchanger qui va nous servir à modifier (ou même à usurper) l'adresse MAC de notre 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` :

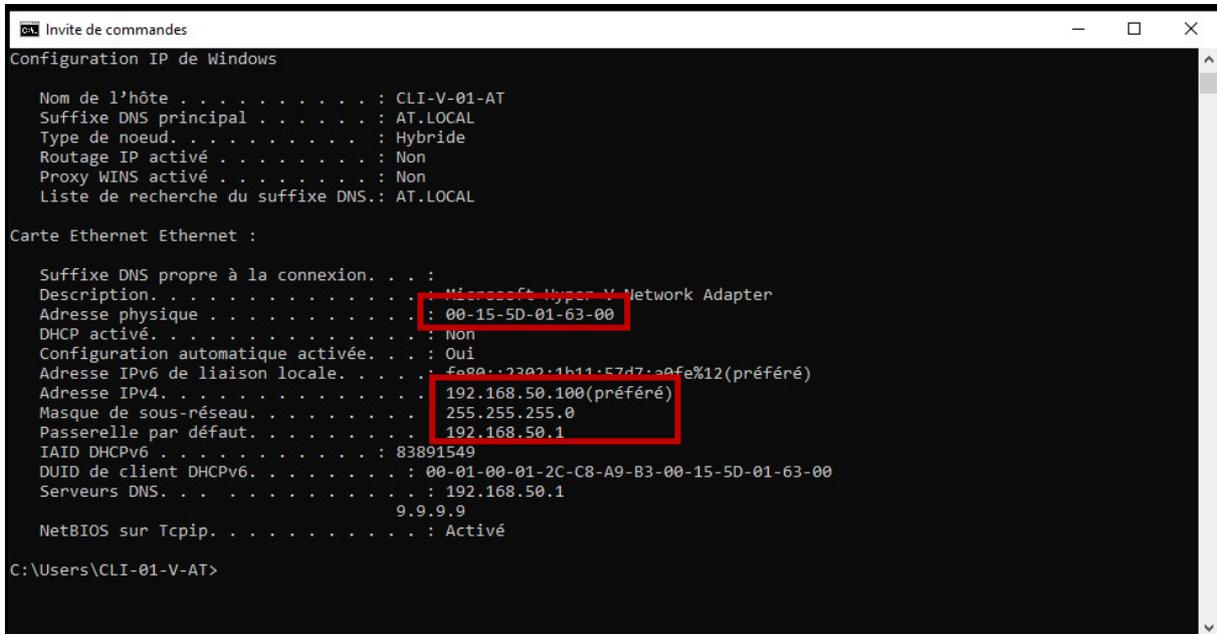


```
user@kali: ~  
Fichier Actions Éditer Vue Aide  
(user@kali)-[~]  
└─$ ifconfig eth0 192.168.50.50 255.255.255.0 up
```



```
user@kali: ~  
Fichier Actions Éditer Vue Aide  
(user@kali)-[~]  
└─$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.50.50 netmask 255.255.255.0 broadcast 192.168.50.255  
    inet6 fe80::be38:a99b:2c::c054 prefixlen 64 scopeid 0x20<link>  
    ether 00:15:5d:01:63:07 txqueuelen 1000 (Ethernet)  
    RX packets 914 bytes 77033 (75.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 498 bytes 50511 (49.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Boucle locale)  
    RX packets 26 bytes 2704 (2.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 26 bytes 2704 (2.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(user@kali)-[~]  
└─$
```

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.



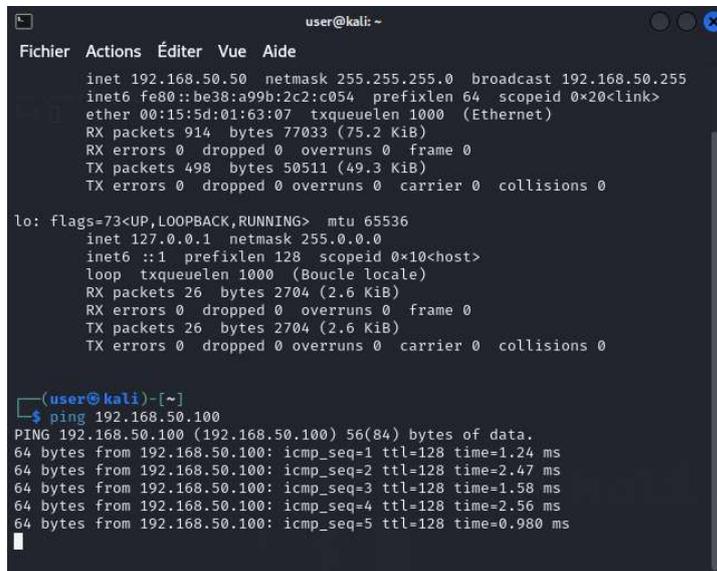
```
Invite de commandes
Configuration IP de Windows

Nom de l'hôte . . . . . : CLI-V-01-AT
Suffixe DNS principal . . . . . : AT.LOCAL
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: AT.LOCAL

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Microsoft Hyper-V Network Adapter
Adresse physique . . . . . : 00-15-5D-01-63-00
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::2302:1b11:57d7:a0fe%12(préféré)
Adresse IPv4. . . . . : 192.168.50.100(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.50.1
IAID DHCPv6 . . . . . : 83891549
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-C8-A9-B3-00-15-5D-01-63-00
Serveurs DNS. . . . . : 192.168.50.1
9.9.9.9
NetBIOS sur Tcpiip. . . . . : Activé

C:\Users\CLI-01-V-AT>
```

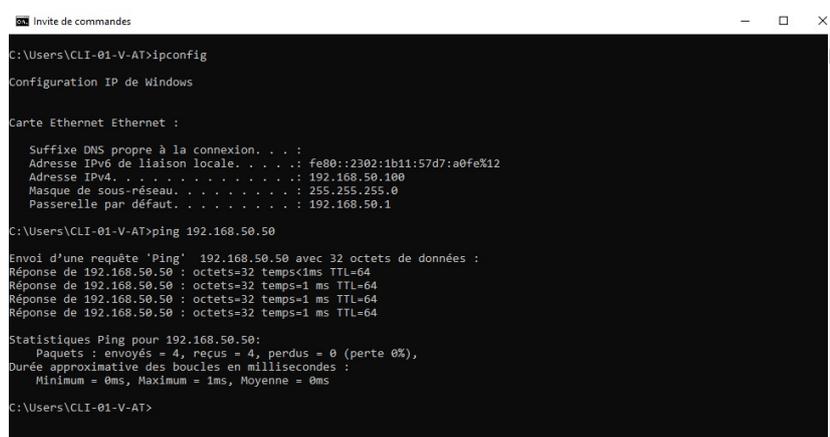


```
user@kali: ~
Fichier Actions Éditer Vue Aide

inet 192.168.50.50 netmask 255.255.255.0 broadcast 192.168.50.255
inet6 fe80::be38:a99b:2c2:c054 prefixlen 64 scopeid 0x20<link>
ether 00:15:5d:01:63:07 txqueuelen 1000 (Ethernet)
RX packets 914 bytes 77033 (75.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 498 bytes 50511 (49.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Boucle locale)
RX packets 26 bytes 2704 (2.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 26 bytes 2704 (2.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(user@kali)~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=128 time=1.24 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=128 time=2.47 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=128 time=1.58 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=128 time=2.56 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=128 time=0.980 ms
```



```
Invite de commandes
C:\Users\CLI-01-V-AT>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . . : fe80::2302:1b11:57d7:a0fe%12
Adresse IPv4. . . . . : 192.168.50.100
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.50.1

C:\Users\CLI-01-V-AT>ping 192.168.50.50

Envoi d'une requête 'Ping' 192.168.50.50 avec 32 octets de données :
Réponse de 192.168.50.50 : octets=32 temps=1ms TTL=64
Réponse de 192.168.50.50 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.50.50 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.50.50 : octets=32 temps=1 ms TTL=64

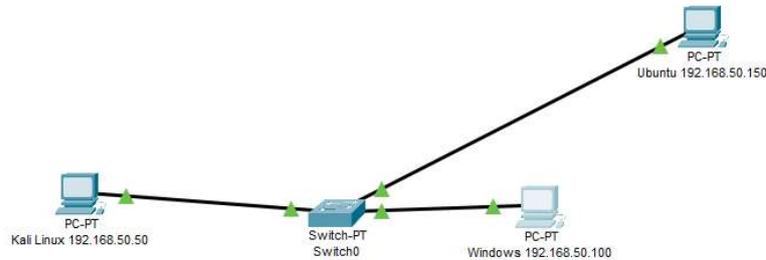
Statistiques Ping pour 192.168.50.50:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\CLI-01-V-AT>
```

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

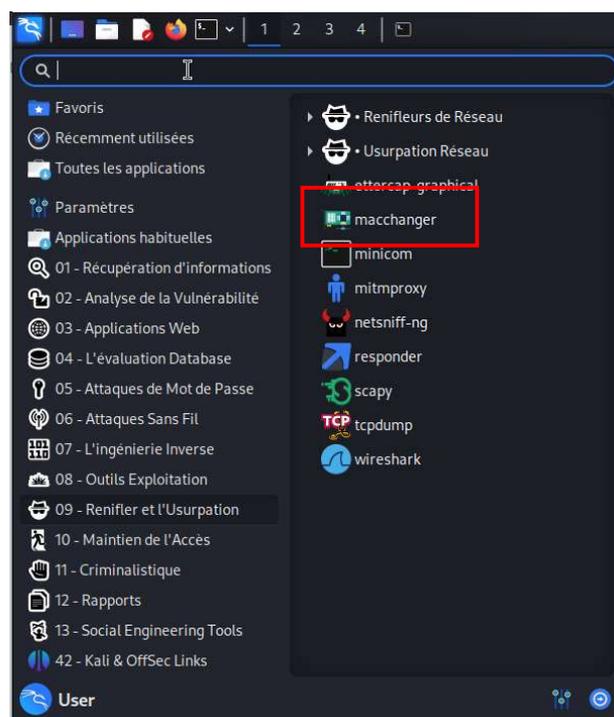
Question 2 :

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 :

```
(user@kali)-[~]
└─$ sudo macchanger -r eth0
Current MAC: 00:15:5d:01:63:07 (Microsoft Corporation)
Permanent MAC: 00:15:5d:01:63:07 (Microsoft Corporation)
New MAC: 82:e4:d2:67:a6:17 (unknown)

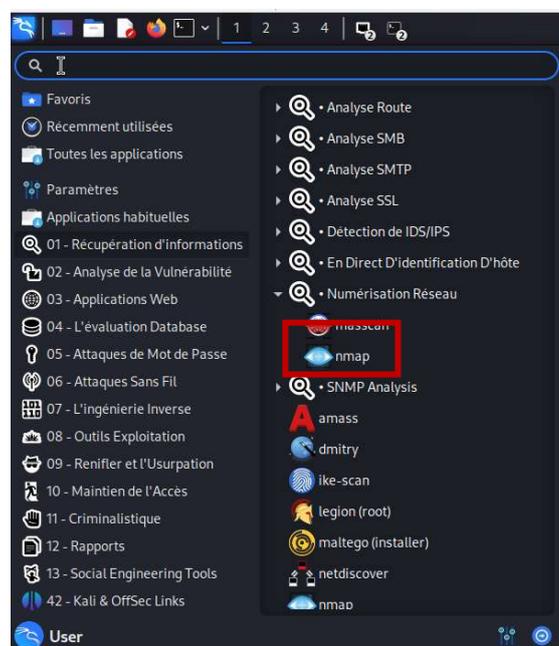
(user@kali)-[~]
└─$
```

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

```
user@kali: ~  
Fichier Actions Éditer Vue Aide  
  
(user@kali)-[~]  
└─$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.50.50 netmask 255.255.255.0 broadcast 192.168.50.255  
inet6 fe80::be38:a99b:2c2:c054 prefixlen 64 scopeid 0x20<link>  
ether 00:15:5d:01:63:07 txqueuelen 1000 (Ethernet)  
RX packets 914 bytes 77033 (75.2 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 498 bytes 50511 (49.3 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Boucle locale)  
RX packets 26 bytes 2704 (2.6 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 26 bytes 2704 (2.6 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(user@kali)-[~]  
└─$
```

Question 5 :

Cette application est rangée dans le dossier « Récupération d'informations – Numérisation Réseau ». Elle est placée dans ce dossier car elle permet de récupérer des informations sur un réseau et de le scanner dans son intégralité. 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.

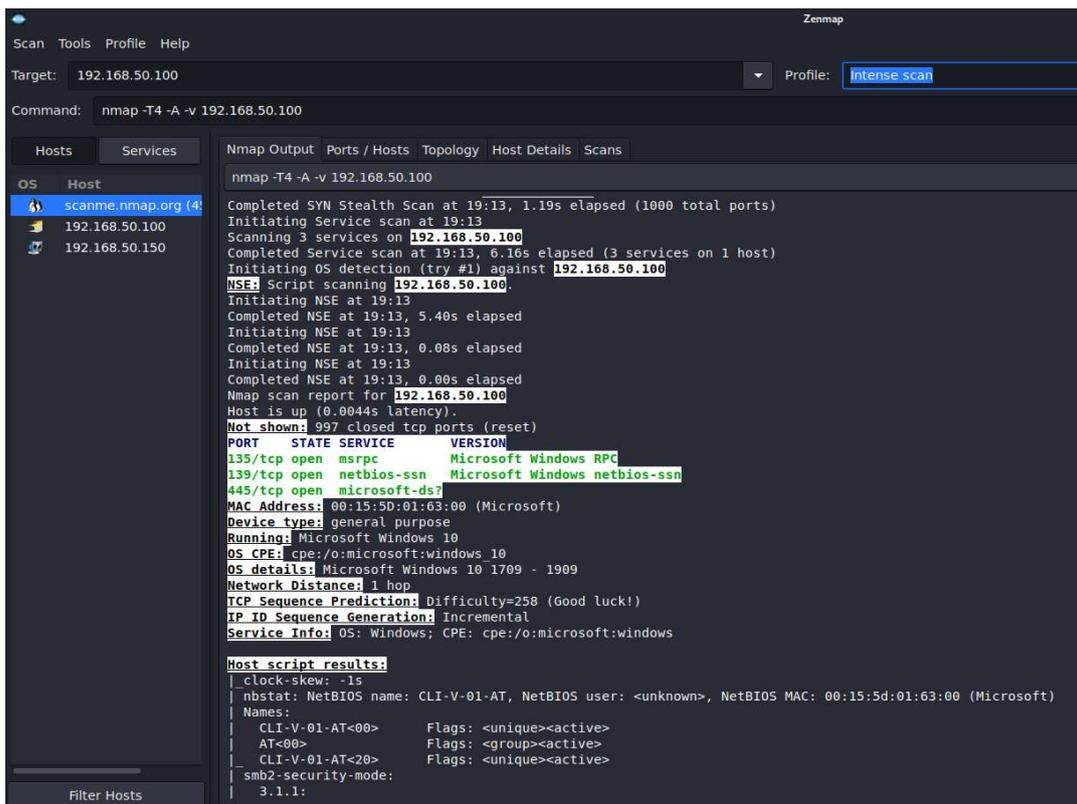
Pour se protéger contre ce genre d'application, nous pouvons utiliser :

- 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 :



```
nmap -T4 -A -v 192.168.50.100

Completed SYN Stealth Scan at 19:13, 1.19s elapsed (1000 total ports)
Initiating Service scan at 19:13
Scanning 3 services on 192.168.50.100
Completed Service scan at 19:13, 6.16s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.50.100
NSE: Script scanning 192.168.50.100.
Initiating NSE at 19:13
Completed NSE at 19:13, 5.40s elapsed
Initiating NSE at 19:13
Completed NSE at 19:13, 0.08s elapsed
Initiating NSE at 19:13
Completed NSE at 19:13, 0.00s elapsed
Nmap scan report for 192.168.50.100
Host is up (0.0044s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
MAC Address: 00:15:5D:01:63:00 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows 10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: -1s
|_ nbstat: NetBIOS name: CLI-V-01-AT, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:63:00 (Microsoft)
|_ Names:
|_ CLI-V-01-AT<00>          Flags: <unique><active>
|_ AT<00>                  Flags: <group><active>
|_ CLI-V-01-AT<20>        Flags: <unique><active>
|_ smb2-security-mode:
|_ 3.1.1:
```

Ubuntu :

```
zenmap
Scan Tools Profile Help
Target: 192.168.50.150 Profile: Intense scan
Command: nmap -T4 -A -v 192.168.50.150

Hosts Services
OS Host
scanme.ni
192.168.50.150
192.168.50.150

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.50.150
Completed Parallel DNS resolution of 1 host. at 19:10, 13.00s elapsed
Initiating SYN Stealth Scan at 19:10
Scanning 192.168.50.150 [1000 ports]
Completed SYN Stealth Scan at 19:10, 0.08s elapsed (1000 total ports)
Initiating Service scan at 19:10
Initiating OS detection (try #1) against 192.168.50.150
Retrying OS detection (try #2) against 192.168.50.150
NSE: Script scanning 192.168.50.150.
Initiating NSE at 19:10
Completed NSE at 19:10, 0.00s elapsed
Initiating NSE at 19:10
Completed NSE at 19:10, 0.00s elapsed
Initiating NSE at 19:10
Completed NSE at 19:10, 0.00s elapsed
Nmap scan report for 192.168.50.150
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.50.150 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:15:5D:01:63:0B (Microsoft)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 1.52 ms 192.168.50.150

NSE: Script Post-scanning.
Initiating NSE at 19:10
Completed NSE at 19:10, 0.00s elapsed
Initiating NSE at 19:10
Completed NSE at 19:10, 0.00s elapsed
Initiating NSE at 19:10
Completed NSE at 19:10, 0.00s elapsed
Read data files from: /usr/local/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.00 seconds
Raw packets sent: 1013 (45.696KB) | Rcvd: 1013 (41.632KB)
```

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 :

```
zenmap
Scan Tools Profile Help
Target: scanme.nmap.org Profile: Intense scan Scan Cancel
Command: nmap -T4 -v scanme.nmap.org

Hosts Services
OS Host
scanme.nmap.org

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v scanme.nmap.org
|_ 206 20:50:44:77:02:70:00:50:00:00:00:00:00:00:00:00 (non)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:el:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
|_ 80/tcp filtered smtp
|_ 80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
|_ 135/tcp filtered msrpc
|_ 139/tcp filtered netbios-ssn
|_ 445/tcp filtered microsoft-ds
|_ 9929/tcp open nping-echo Nping echo
|_ 31337/tcp open tcpwrapped
Aggressive OS guesses: Linux 5.0 - 5.4 (96%), Linux 5.4 (95%), Linux 4.15 - 5.6 (94%), Linux 5.0 - 5.3 (93%), Linux 5.1 (93%), Linux 2.6.32 - 3.13 (93%), Linux 5.0 (92%), Linux 2.6.22 - 2.6.36 (91%), Linux 3.10 - 4.11 (91%), Linux 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 34.735 days (since Wed Nov 15 01:15:55 2023)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8888/tcp)
HOP RTT ADDRESS
1 2.73 ms box [192.168.1.1]
2 ...
3 5.49 ms 130.4.128.77.rev.sfr.net [77.128.4.130]
4 206.07 ms scanme.nmap.org [45.33.32.156]

NSE: Script Post-scanning.
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Initiating NSE at 18:54
Completed NSE at 18:54, 0.00s elapsed
Bandwidth: 4115.770 /usr/local/bin /share/nmap
```

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.