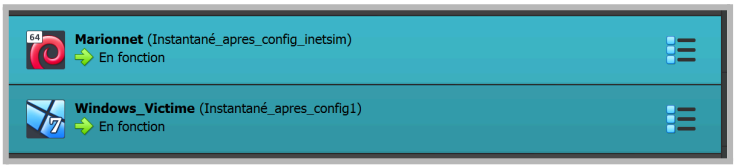
Compte rendu
Ons AMMAR

TP3

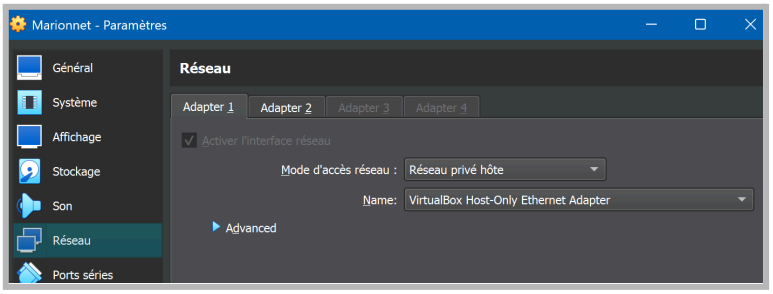
TRAVAUX PRATIQUES SUR LA SUPERVISION DE SÉCURITÉ

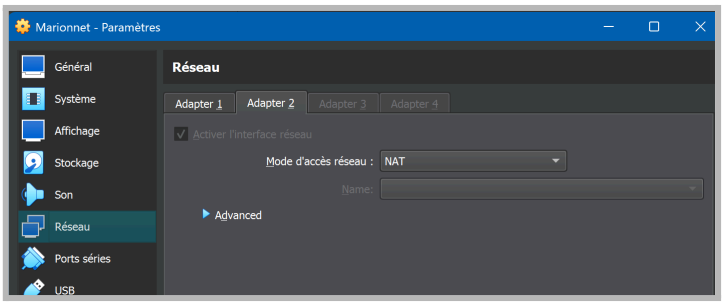
Prérequis:

- Deux machines une hôte(Linux) et une autre victime(windows 7 32 bits)

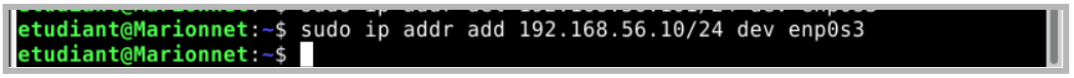


- Mettre les deux machines dans un réseau interne
  Au niveau de Linux:

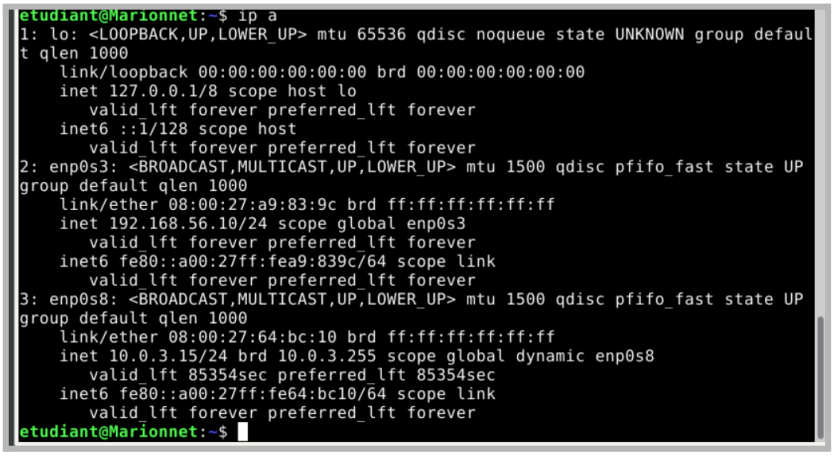




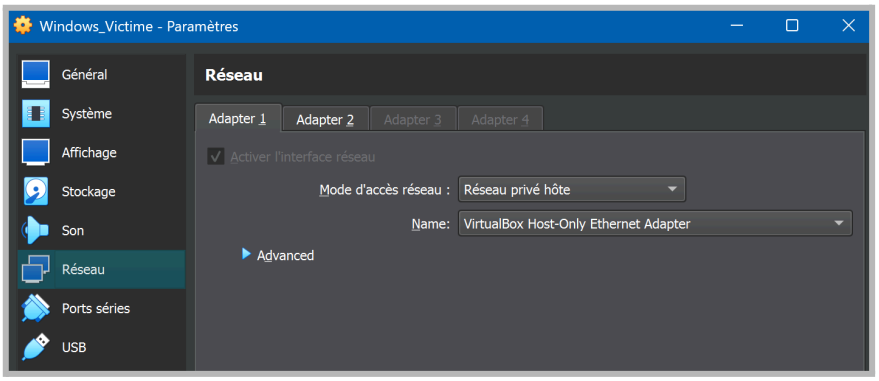
Attribution d'une adresse statique à l'interface Vbox(enp0s3 dans mon lab)

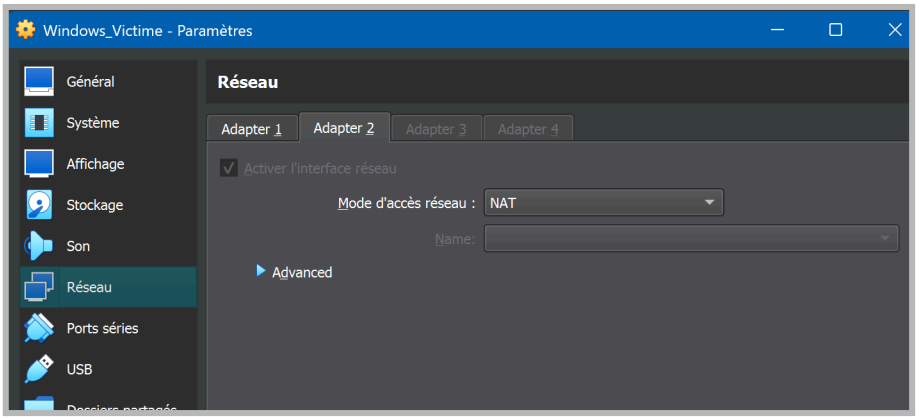


Vérification avec ip a

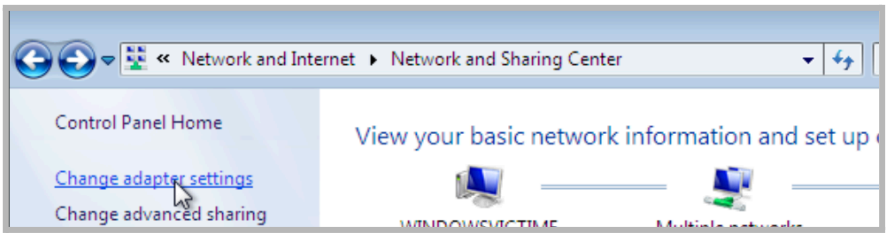


Au niveau de Windows 7:

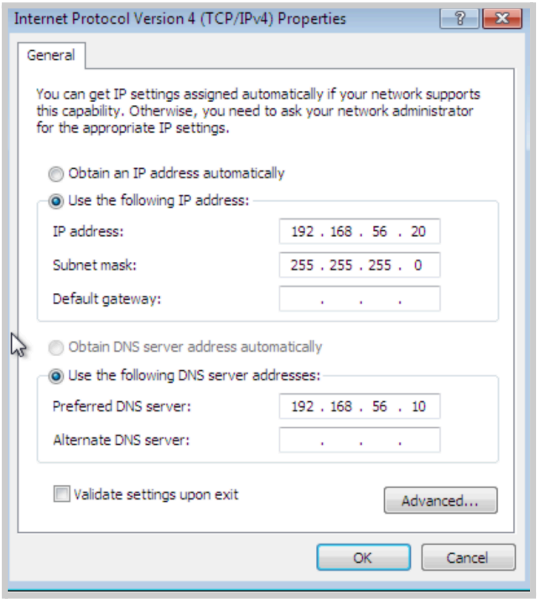




Au niveau de “Control Panel”

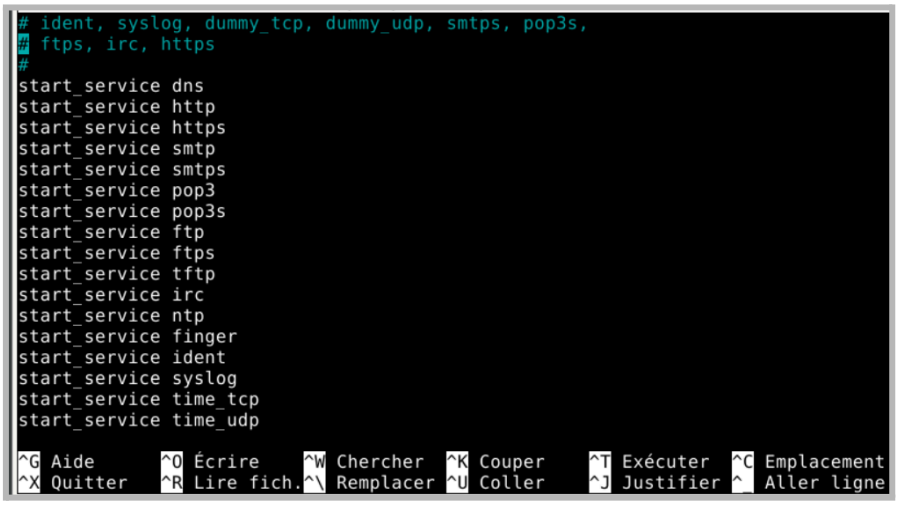


Il faut attribuer une adresse IPv4 statique à la machine windows
On choisit la machine hôte comme dns

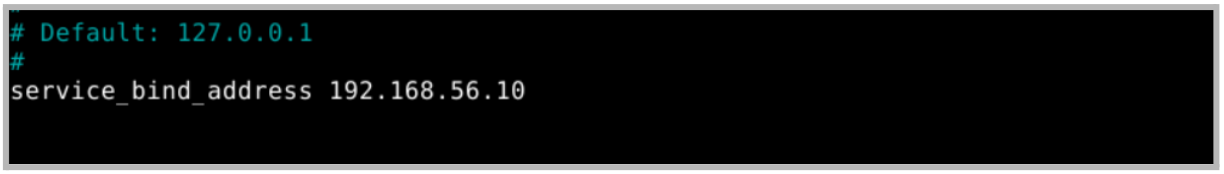


Machine hôte:

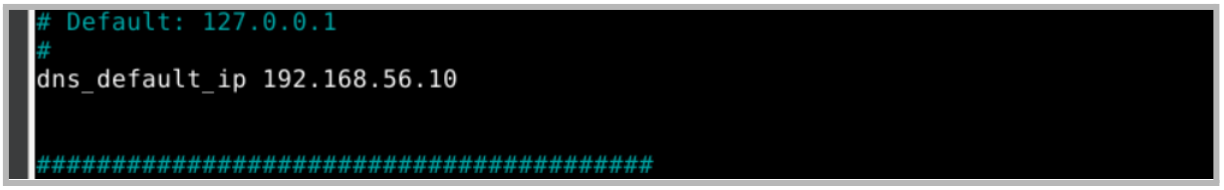
- activer les services (dns, http,https,icmp) au niveau du fichier de configuration de inetsim:
  sudo nano /etc/inetsim/inetsim.conf



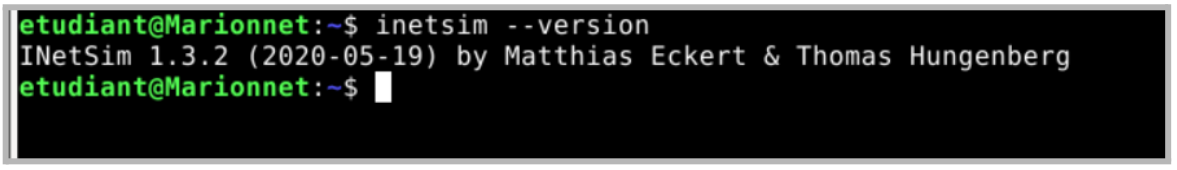
On peut commenter les autres services
On doit définir l'adresse de service bind comme étant l'adresse de la machine hôte qui va surveiller l'attaque



On définit aussi la machine hôte comme serveur dns



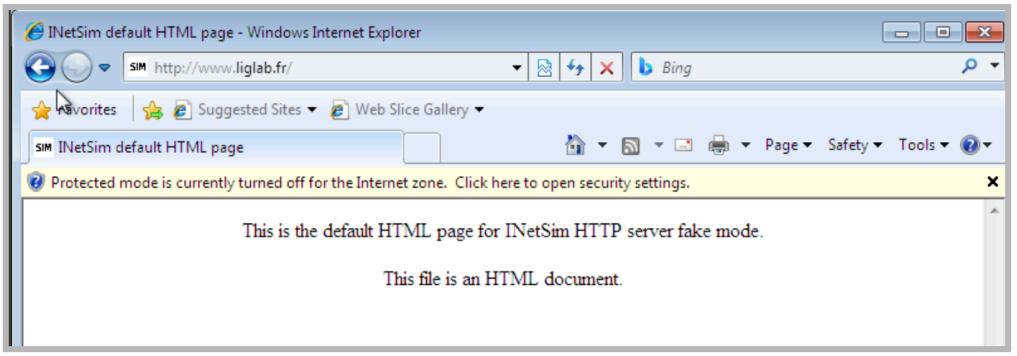
- Installation du inetsim:
  Inetsim c'est quoi ?
  une suite logicielle permettant de simuler des services Internet courants dans un environnement virtuel.
- Téléchargement de intesim sur *https://www.inetsim.org*



  - pour arrêter le processus inetsim en cours:
    sudo kill $(cat /var/run/inetsim.pid)
    sudo rm /var/run/inetsim.pid
  - Le relancer:
    sudo inetsim

```
etudiant@Marionnet:~$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1859) ===
Session ID:     1859
Listening on:   192.168.56.10
Real Date/Time: 2025-11-16 21:07:42
Fake Date/Time: 2025-11-16 21:07:42 (Delta: 0 seconds)
 Forking services...
  * irc_6667_tcp - started (PID 1873)
  * http_80_tcp - started (PID 1864)
  * finger_79_tcp - started (PID 1875)
  * ident_113_tcp - started (PID 1876)
  * time_37_tcp - started (PID 1878)
  * dns_53_tcp_udp - started (PID 1863)
  * echo_7_tcp - started (PID 1882)
  * discard_9_tcp - started (PID 1884)
```

Au niveau de la machine windows 7 :



Création du dossier partagé en utilisant samba:
J'ai opté pour samba qui transforme ton Linux en serveur Windows pour que les machines Windows puissent accéder aux dossiers comme s'ils étaient sur un PC Windows(résout le problème d'interopérabilité en gros, sans passer par la machine physique, et on élimine de ce fait tout risque d'infection)
Installation avec: sudo apt install samba
Vérification de l'état (status) :

```
etudiant@Marionnet:~$ smbstatus
smbstatus only works as root!
etudiant@Marionnet:~$
```

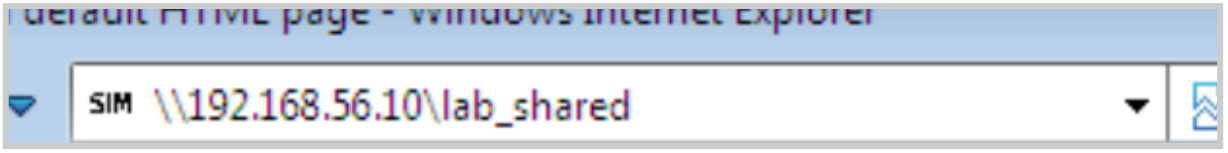
J'ai fait ensuite la création du dossier partagé:

sudo mkdir -p /srv/lab_shared
sudo chown etudiant:etudiant /srv/lab_shared
sudo chmod 777 /srv/lab_shared

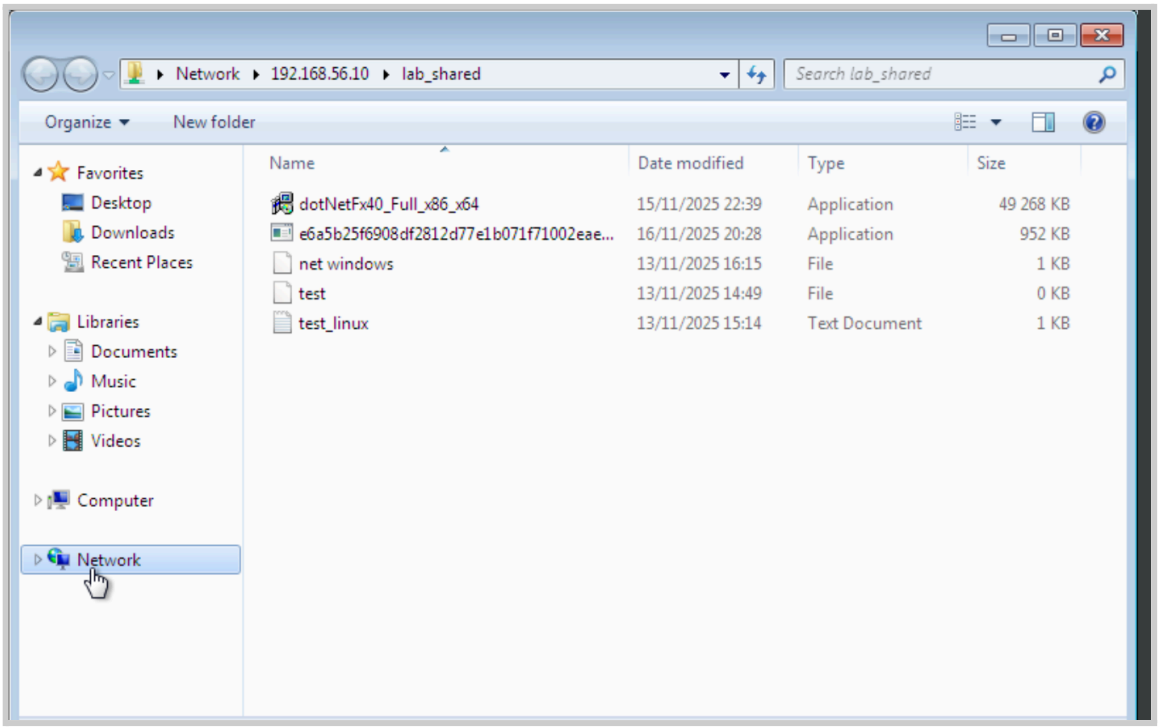
(je lui ai donné toutes permissions de lecture, d'écriture et d'exécution)
J'ai édité ensuite le fichier /etc/samba/smb.conf

```
etudiant@Marionnet:~$ sudo cat /etc/samba/smb.conf
[lab_shared]
   path = /srv/lab_shared
   read only = no
   browseable = yes
   guest ok = no
   valid users = sambauser
   force user = sambauser
   force group = sambauser
   create mask = 0775
   directory mask = 0775
etudiant@Marionnet:~$
```

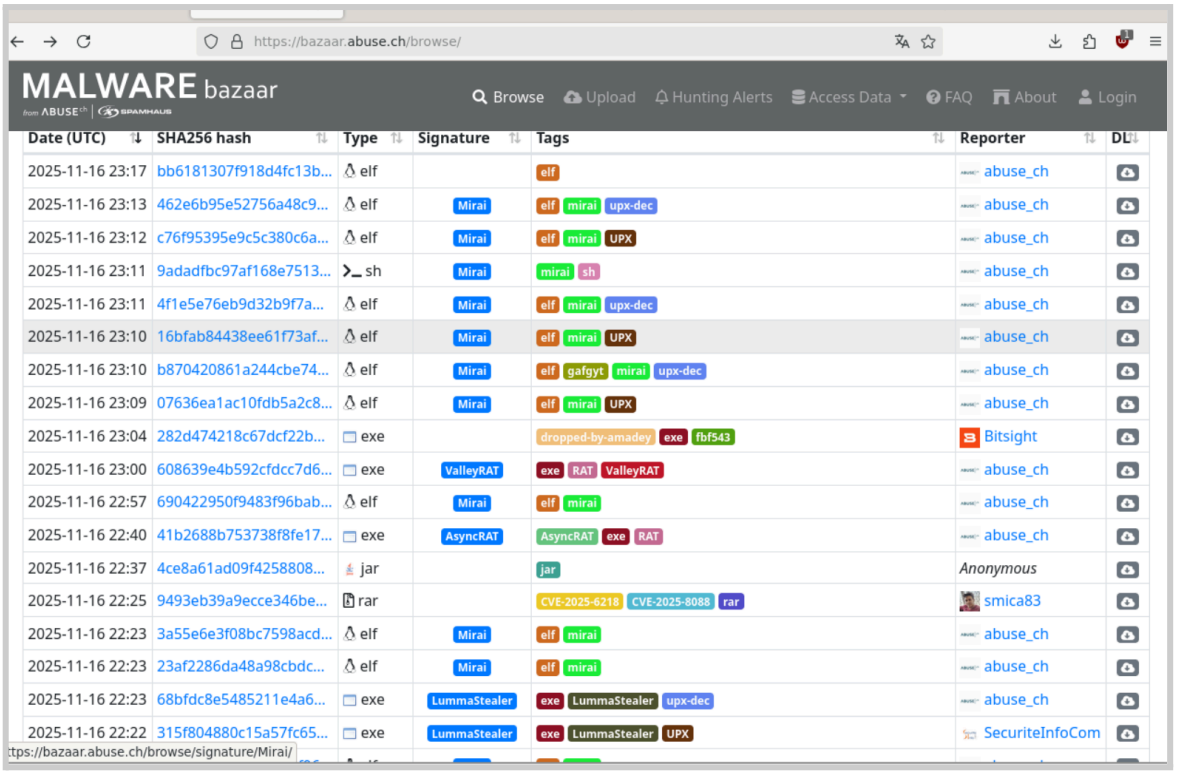
read only = no : permet d'écrire depuis Windows
valid users : qui peut se connecter(sambauser, utilisateur que j'ai créé, avec mdp smb)
guest ok = no : interdit l'accès anonyme
Au niveau de windows (navigateur web):



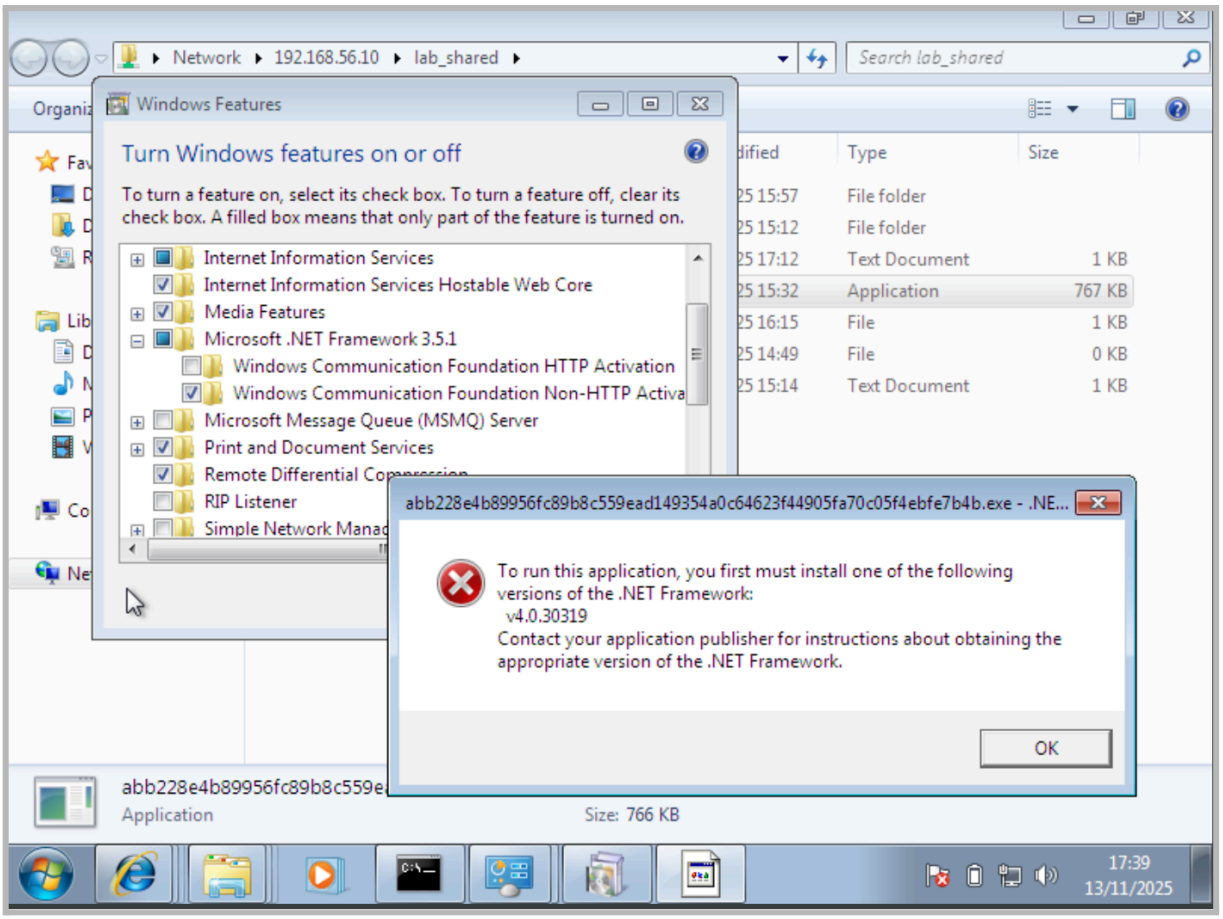
On a désormais accès au dossier partagé



Pour télécharger le virus il faut aller sur le site https://bazaar.abuse.ch/browse/



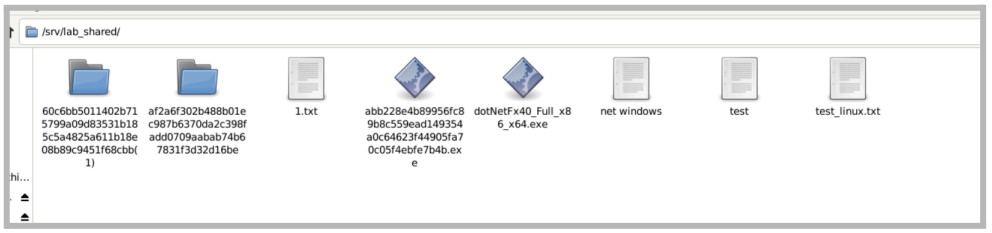
Problème rencontré avec la version du malware qui n'est pas compatible avec la machine windows 7



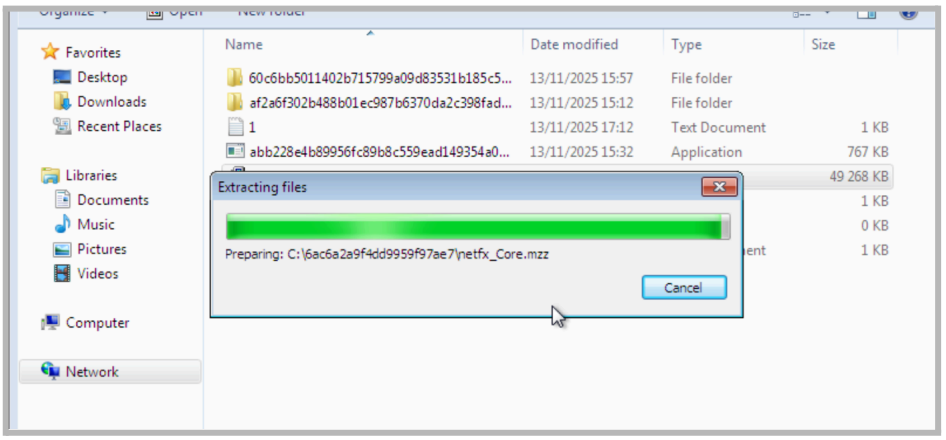
Solution:

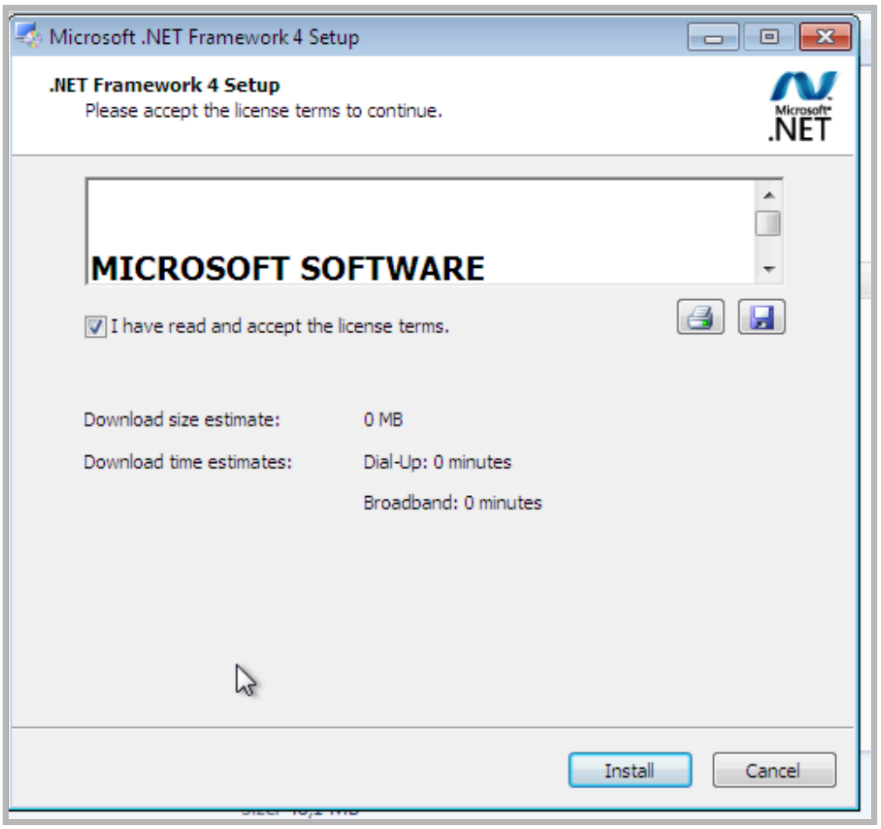
- Télécharger le .NET au niveau de la machine Linux
- Le placer au niveau du dossier partagé

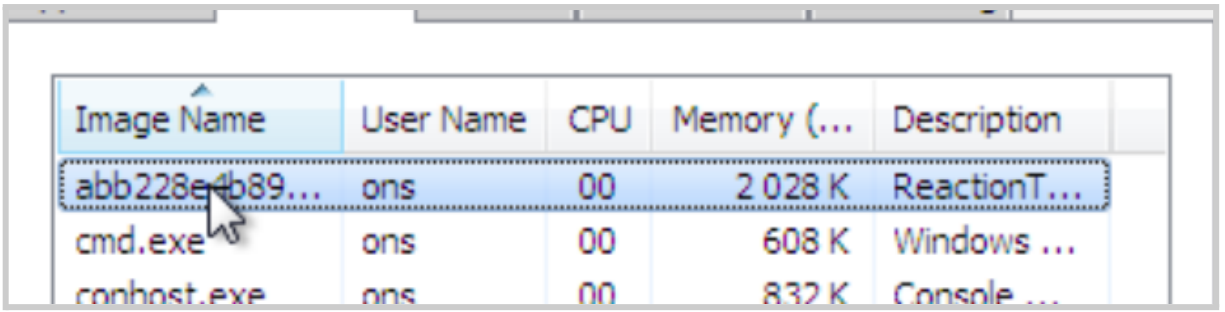
- L'exécuter offline au niveau de la machine Windows

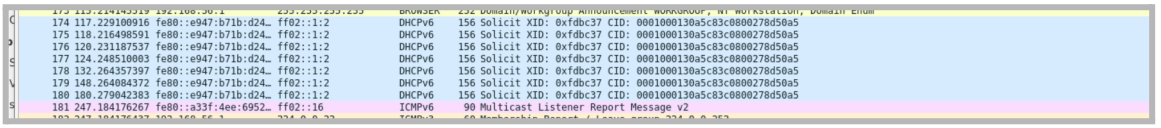


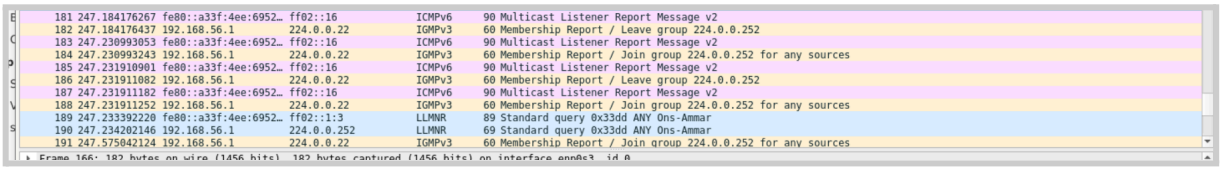
Exécution

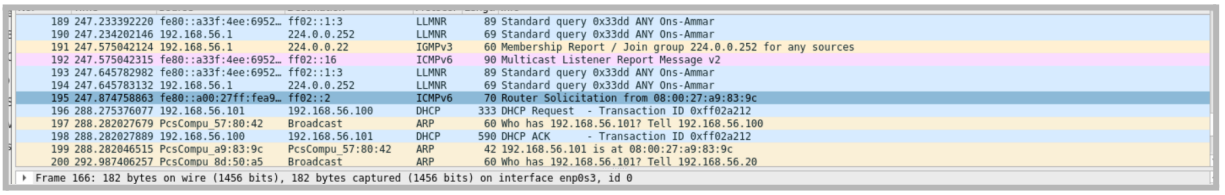


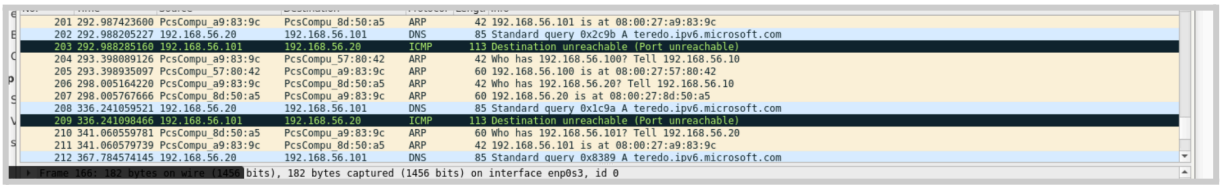


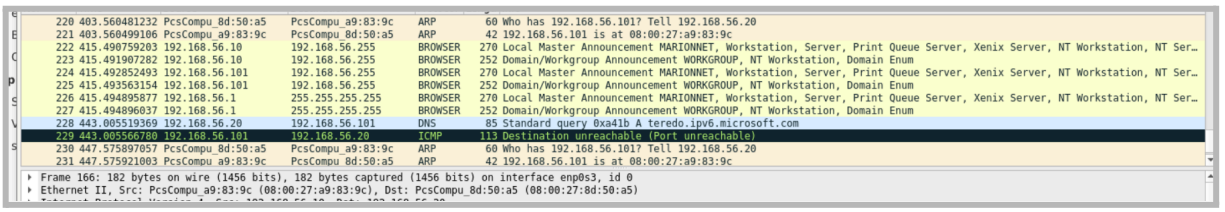




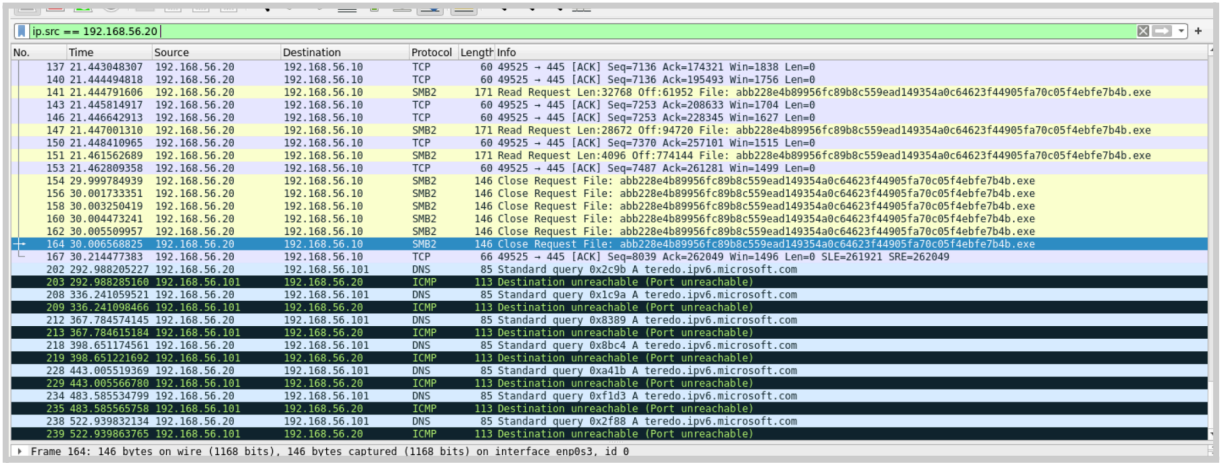




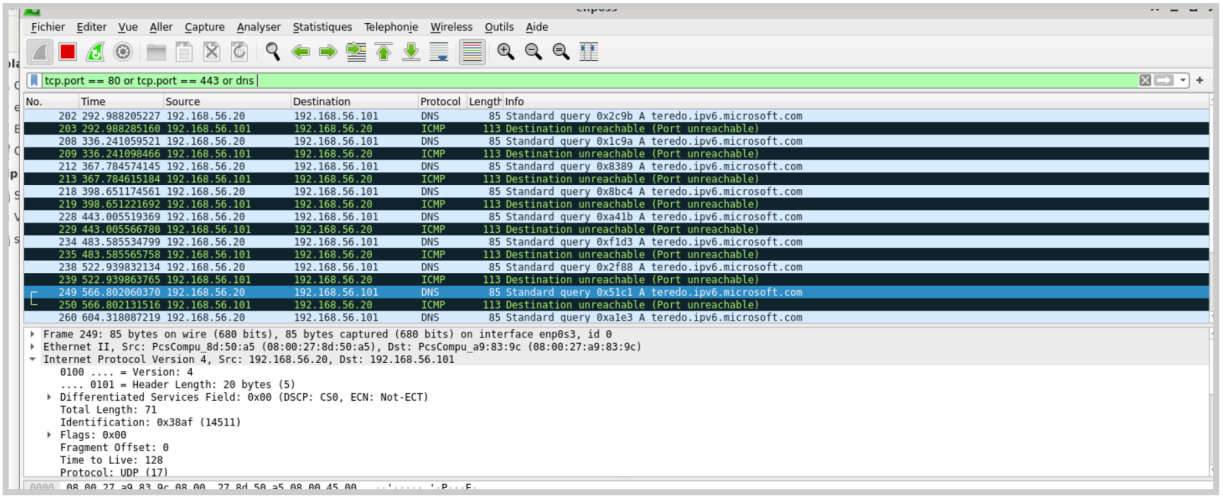




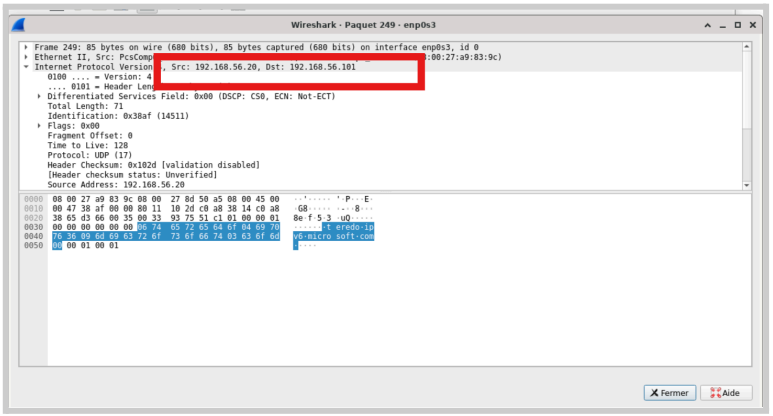
J'ai fait un filtre pour voir ce qui sort depuis windows(192.168.56.20)



pour voir tout trafic suspect on peut aussi utiliser un filtre pour le port tcp 80 ou le port tcp 443 ou même dns



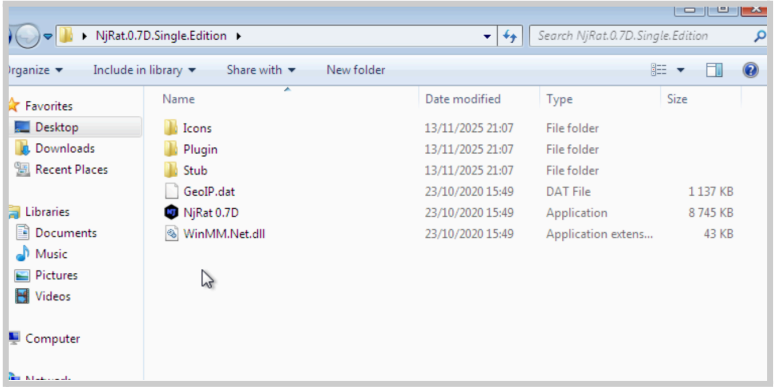
Choix d'une requête dns
Adresses source et destination

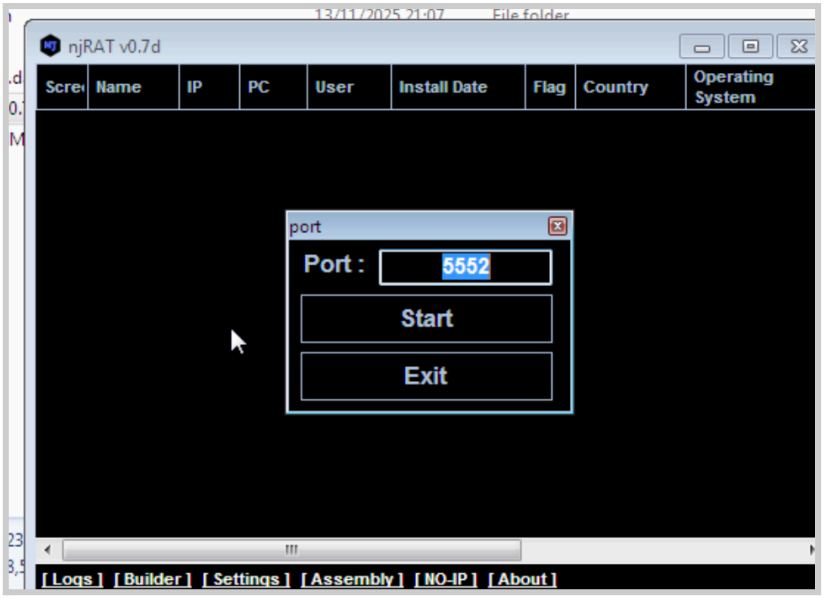


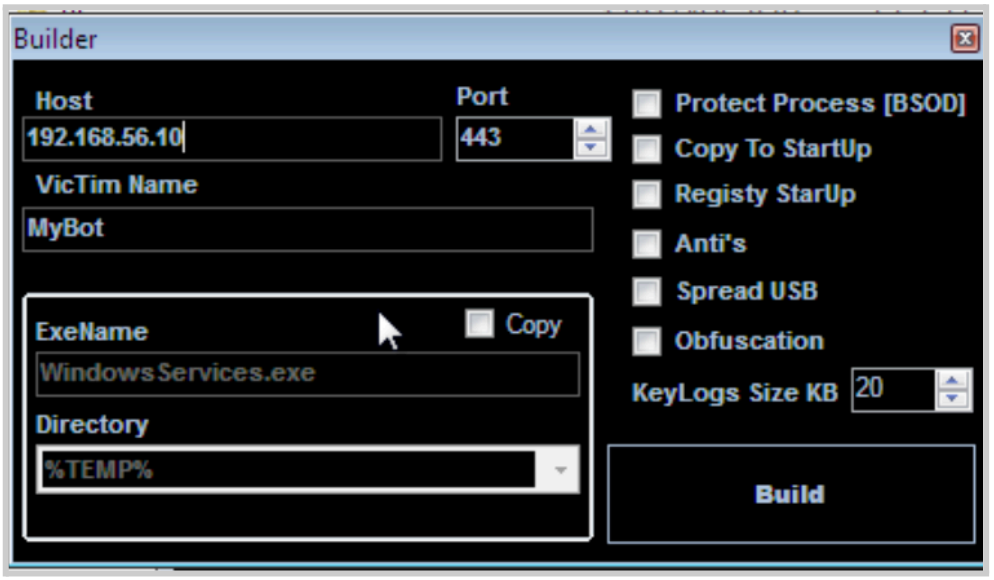
Il s'agit d'une résolution IPv4(A record)

Le domaine

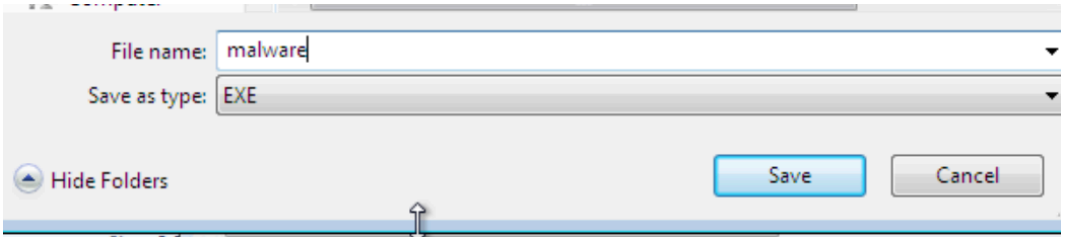
J'ai travaillé aussi avec le ***njRat single edition(depuis un dépot github)***
C'est une version open-source de njRAT, dans mon cas, je l'ai utilisée comme échantillon dans notre environnement Windows 7 isolé

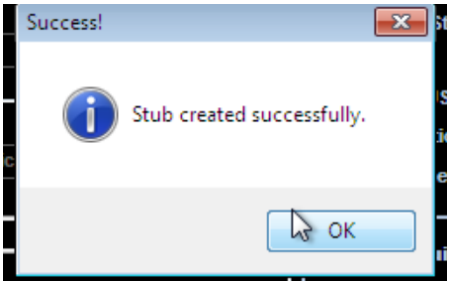






Ce fichier est le malware client configuré, celui qui générera du trafic simulé.

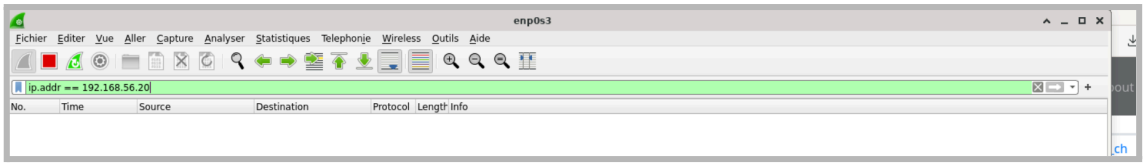




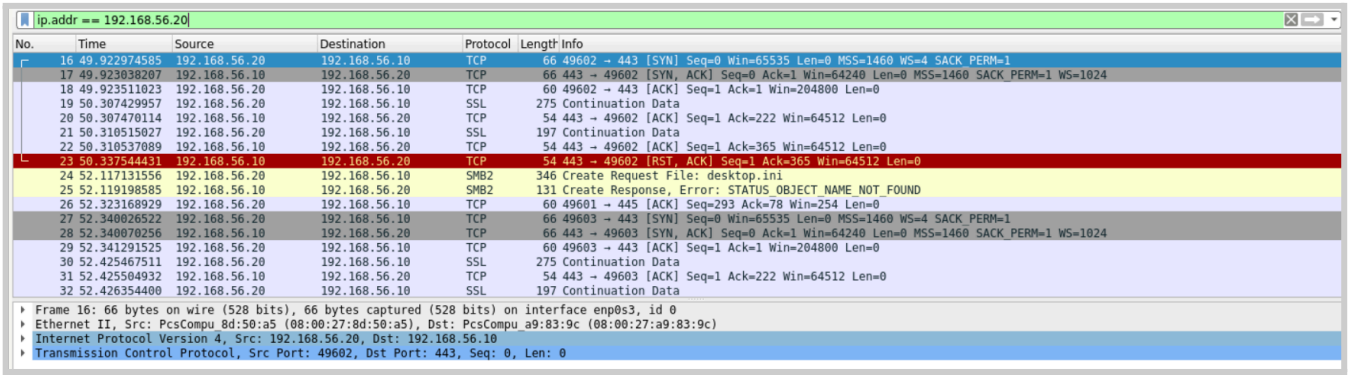
On lance après intesim

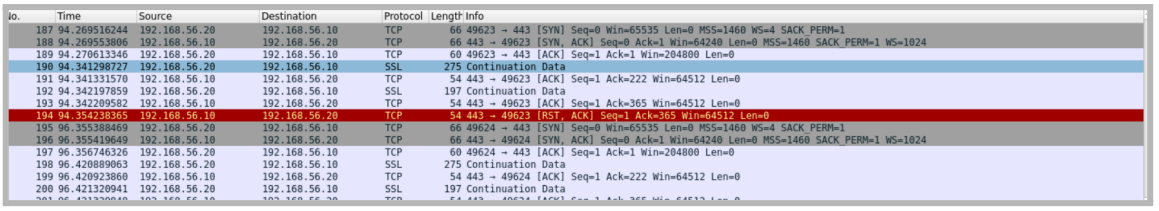
```
etudiant@Marionnet:~$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 4431) ===
Session ID:     4431
Listening on:   192.168.56.10
Real Date/Time: 2025-11-17 00:36:41
Fake Date/Time: 2025-11-17 00:36:41 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 4435)
  * irc_6667_tcp - started (PID 4445)
  * ident_113_tcp - started (PID 4448)
  * tftp_69_udp - started (PID 4444)
  * ntp_123_udp - started (PID 4446)
  * finger_79_tcp - started (PID 4447)
  * syslog_514_udp - started (PID 4449)
  * pop3s_995_tcp - started (PID 4441)
```

Et on écoute sur wireshark sur l'interface enp0s3



Puis on lance le malware





On peut voir des tentatives TCP vers le faux serveur C2