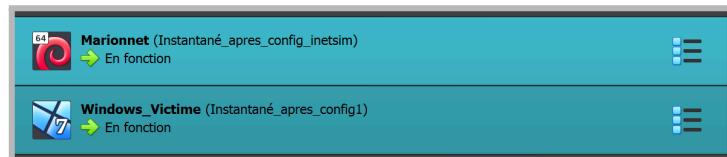


# TP3

## TRAVAUX PRATIQUES SUR LA SUPERVISION DE SÉCURITÉ

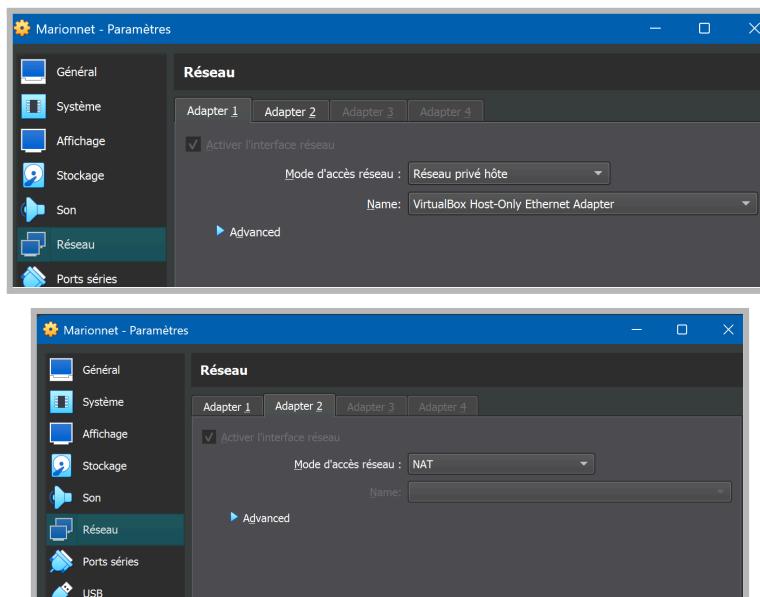
### Prérequis:

- 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:



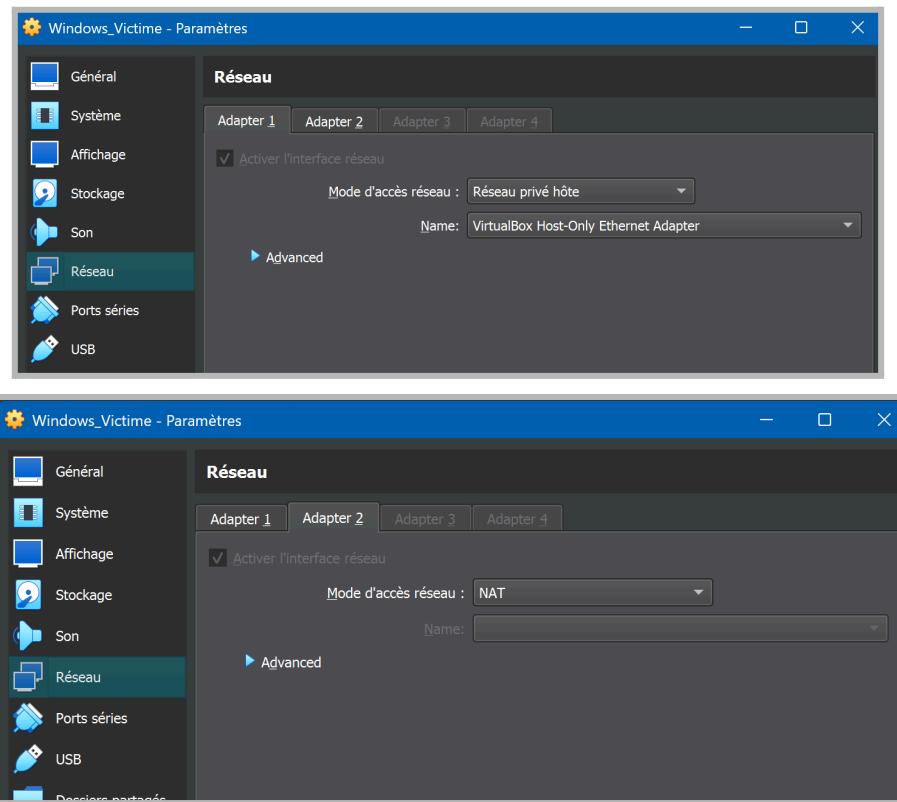
Attribution d'une adresse statique à l'interface Vbox(enp0s3 dans mon lab)

```
etudiant@Marionnet:~$ sudo ip addr add 192.168.56.10/24 dev enp0s3
etudiant@Marionnet:~$
```

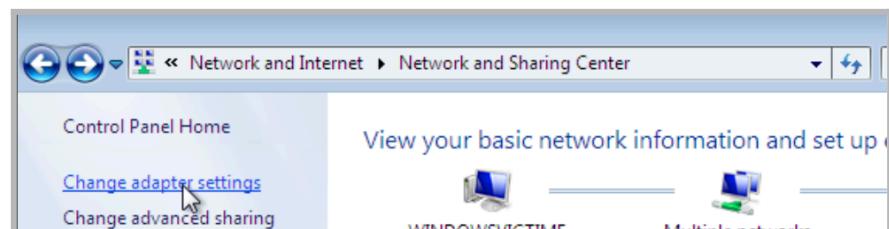
Vérification avec ip a

```
etudiant@Marionnet:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    group default qlen 1000
        link/ether 08:00:27:a9:83:9c brd ff:ff:ff:ff:ff:ff
        inet 192.168.56.10/24 scope global enp0s3
            valid_lft forever preferred_lft forever
            inet6 fe80::a00:27ff:fea9:839c/64 scope link
                valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    group default qlen 1000
        link/ether 08:00:27:64:bc:10 brd ff:ff:ff:ff:ff:ff
        inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic enp0s8
            valid_lft 85354sec preferred_lft 85354sec
            inet6 fe80::a00:27ff:fe64:bc10/64 scope link
                valid_lft forever preferred_lft forever
etudiant@Marionnet:~$
```

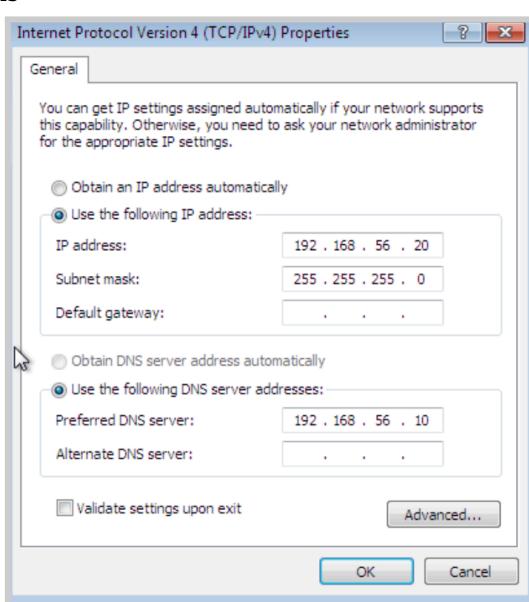
### Au niveau de Windows 7:



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:

## Compte rendu Ons AMMAR

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

```
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
start_service tftp
start_service irc
start_service ntp
start_service finger
start_service ident
start_service syslog
start_service time_tcp
start_service time_udp
```

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement  
^X Quitter ^R Lire fich.^V Remplacer ^U Coller ^J Justifier ^L Aller ligne

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

```
# Default: 127.0.0.1
#
service_bind_address 192.168.56.10
```

On définit aussi la machine hôte comme serveur dns

```
# Default: 127.0.0.1
#
dns_default_ip 192.168.56.10

#####
#####
```

- 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>

```
etudiant@Marionnet:~$ inetsim --version
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
etudiant@Marionnet:~$ █
```

- pour arrêter le processus inetsim en cours:

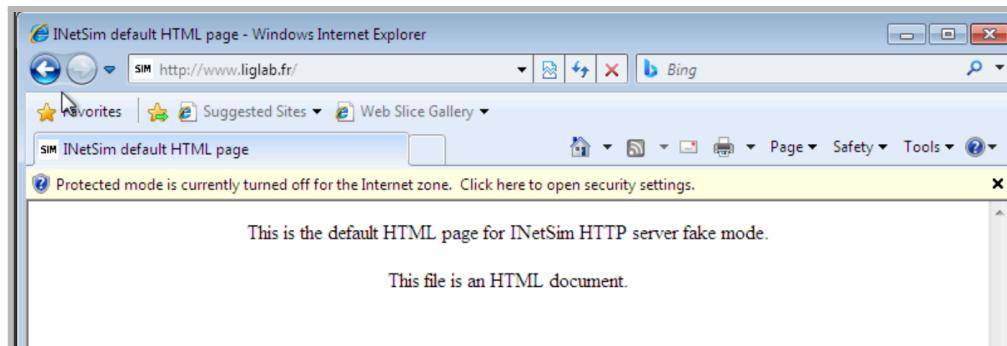
```
sudo kill $(cat /var/run/inetsim.pid)
sudo rm /var/run/inetsim.pid
```

- 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)
* ntp_123_udp - started (PID 1874)
```

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

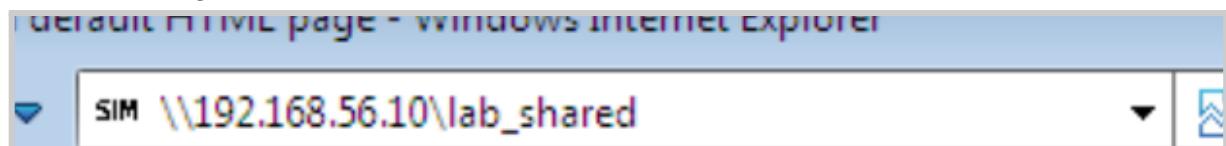
```
etudiant@Marionnet:~$ sudo cat /etc/samba/smb.conf
[lab_shared]
    path = /srv/lab_shared
    read only = no
    browseable = yes
    guest ok = no
    valid users = sambauser
    force user = sambauser
    force group = sambauser
    create mask = 0775
    directory mask = 0775
etudiant@Marionnet:~$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

read only = no : permet d'écrire depuis Windows

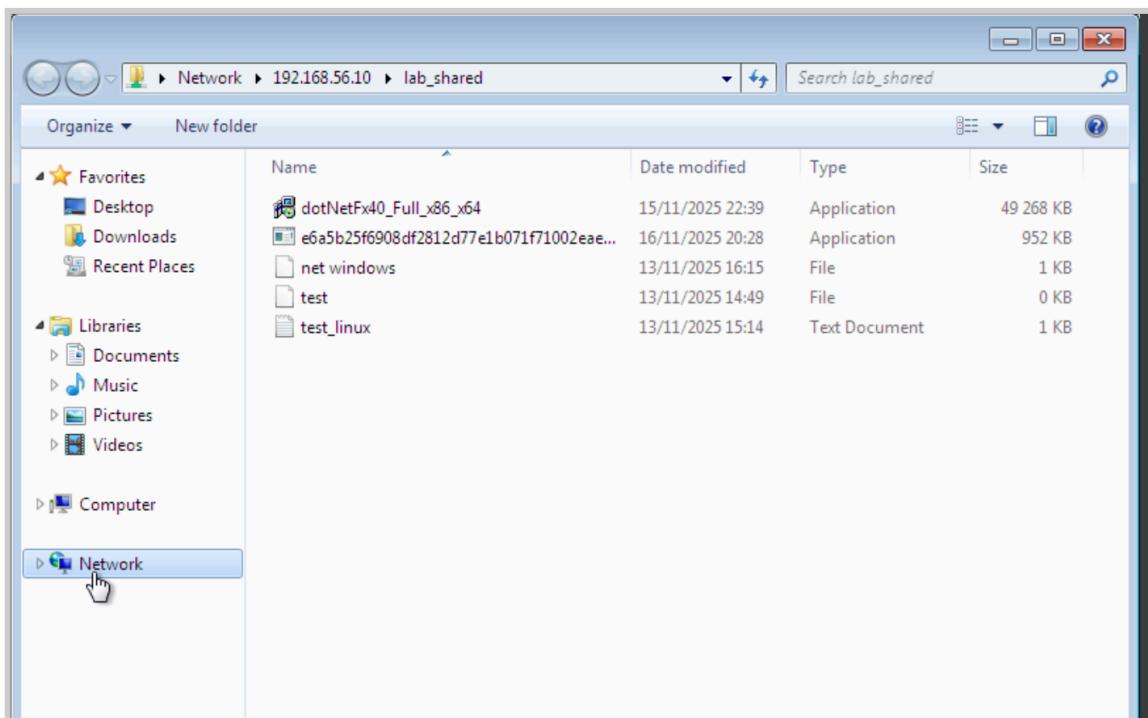
valid users : qui peut se connecter(sambauser, utilisateur que j'ai créé, avec mdp smb)

guest ok = no : interdit l'accès anonyme

Au niveau de windows (navigateur web):



On a désormais accès au dossier partagé

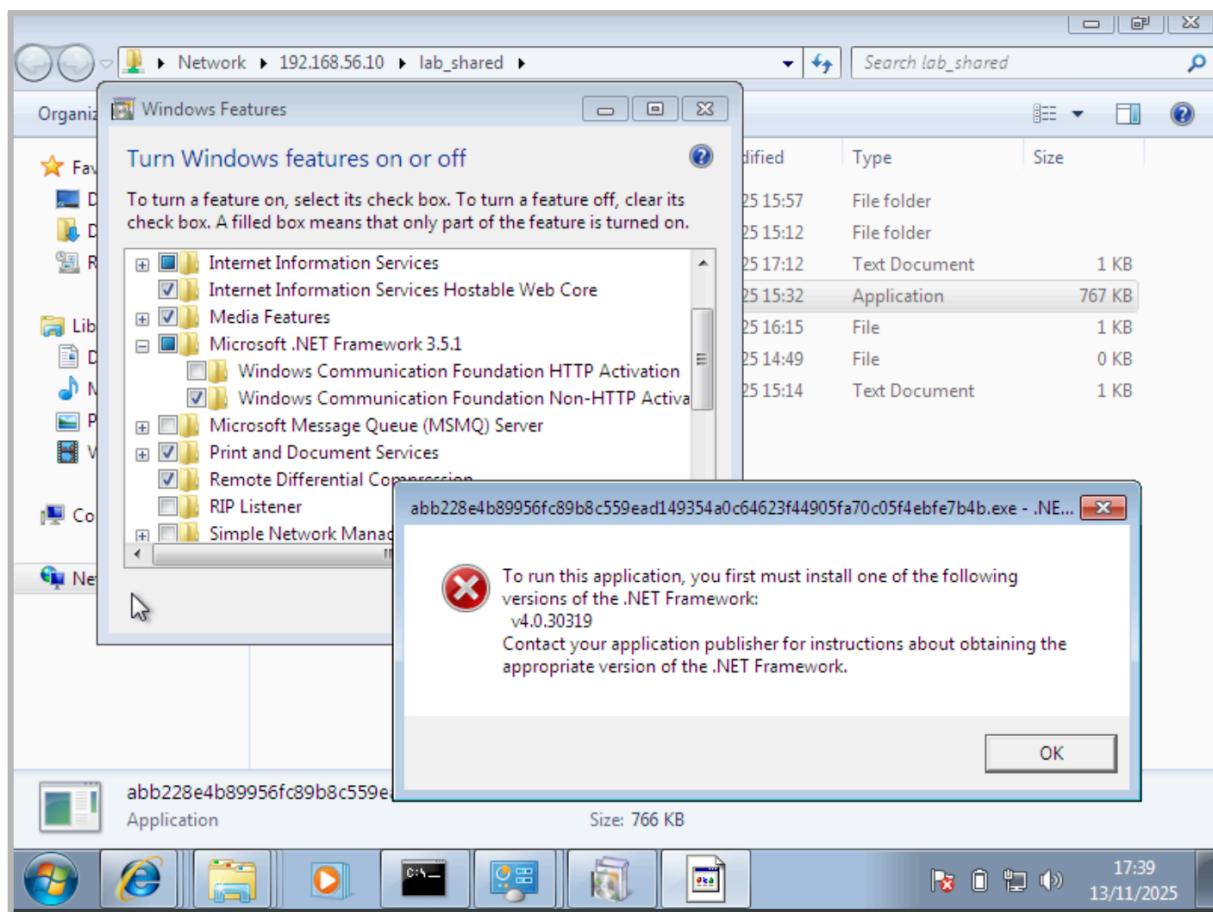


Pour télécharger le virus il faut aller sur le site <https://bazaar.abuse.ch/browse/>

# Compte rendu Ons AMMAR

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DLs
2025-11-16 23:17	bb6181307f918d4fc13b...	elf		elf	abuse_ch	
2025-11-16 23:13	462e6b95e52756a48c9...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-11-16 23:12	c76f95395e9c5c380c6a...	elf	Mirai	elf mirai UPX	abuse_ch	
2025-11-16 23:11	9adadfb97af168e7513...	>_sh	Mirai	mirai sh	abuse_ch	
2025-11-16 23:11	4f1e5e76eb9d32b9f7a...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-11-16 23:10	16bfab84438ee61f73af...	elf	Mirai	elf mirai UPX	abuse_ch	
2025-11-16 23:10	b870420861a244cbe74...	elf	Mirai	elf gafgyt mirai upx-dec	abuse_ch	
2025-11-16 23:09	07636ea1ac10fdb5a2c8...	elf	Mirai	elf mirai UPX	abuse_ch	
2025-11-16 23:04	282d474218c67dcf22b...	exe		dropped-by-amadey exe fbf543	Bitsight	
2025-11-16 23:00	608639e4b592cfdcc7d6...	exe	ValleyRAT	exe RAT ValleyRAT	abuse_ch	
2025-11-16 22:57	690422950f9483f96bab...	elf	Mirai	elf mirai	abuse_ch	
2025-11-16 22:40	41b2688b753738f8fe17...	exe	AsyncRAT	AsyncRAT exe RAT	abuse_ch	
2025-11-16 22:37	4ce8a61ad09f4258808...	jar		jar	Anonymous	
2025-11-16 22:25	9493eb39a9ecc0346be...	rar		CVE-2025-6218 CVE-2025-8088 rar	smica83	
2025-11-16 22:23	3a55e6e3f08bc7598acd...	elf	Mirai	elf mirai	abuse_ch	
2025-11-16 22:23	23af2286da48a98cbdc...	elf	Mirai	elf mirai	abuse_ch	
2025-11-16 22:23	68bfd8e5485211e4a6...	exe	LummaStealer	exe LummaStealer upx-dec	abuse_ch	
2025-11-16 22:22	315f804880c15a57fc65...	exe	LummaStealer	exe LummaStealer UPX	SecuriteInfoCom	

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



Solution:

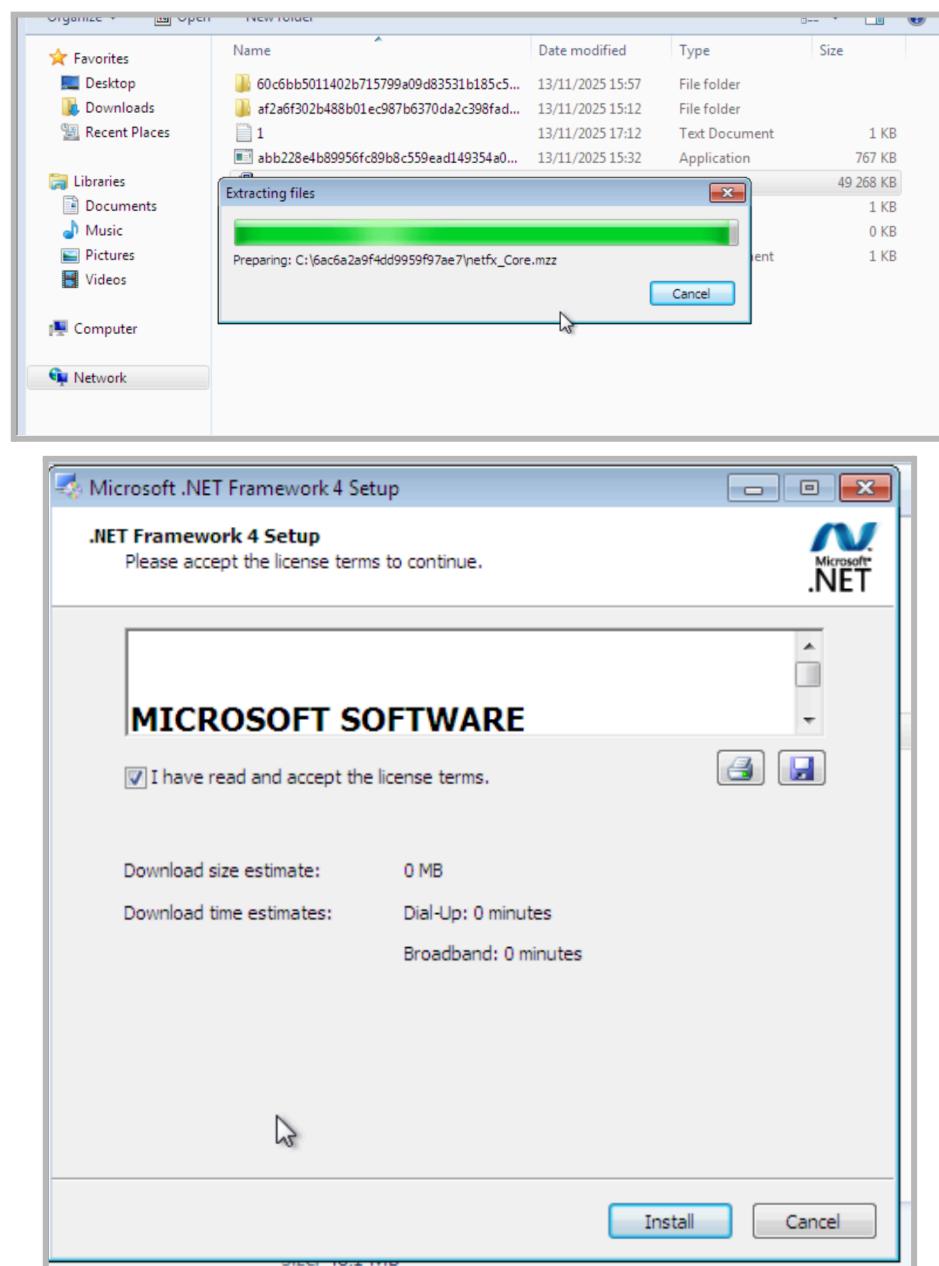
- Télécharger le .NET au niveau de la machine Linux
- Le placer au niveau du dossier partagé

## Compte rendu Ons AMMAR

- L'exécuter offline au niveau de la machine Windows



## Exécution



## Compte rendu Ons AMMAR

Image Name	User Name	CPU	Memory (...	Description
abb228e4b89...	ons	00	2 028 K	ReactionT...
cmd.exe	ons	00	608 K	Windows ...
lwp.exe	ons	00	222 K	Search ...

181	247	184176267	fe00::a33f:4ee::6952::	ff00::16	ICMPv6	90	Multicast Listener Report Message v2
182	247	184176437	192.168.56.1	224.0.0.22	ICMPv6	60	Membership Report / Leave group 224.0.0.252
183	247	230993053	fe00::a33f:4ee::6952::	ff00::16	ICMPv6	90	Multicast Listener Report Message v2
184	247	230993245	192.168.56.1	224.0.0.22	ICMPv6	90	Multicast Listener Report / Join group 224.0.0.252 for any sources
185	247	231019060	fe00::a33f:4ee::6952::	ff00::16	ICMPv6	90	Multicast Listener Report Message v2
186	247	231019062	192.168.56.1	224.0.0.22	ICMPv6	60	Membership Report / Leave group 224.0.0.252
187	247	231011182	fe00::a33f:4ee::6952::	ff00::16	ICMPv6	90	Multicast Listener Report Message v2
188	247	231011182	192.168.56.1	224.0.0.22	ICMPv6	60	Membership Report / Join group 224.0.0.252 for any sources
189	247	233492228	fe00::a33f:4ee::6952::	ff00::13	LLMNR	89	Standard query #x33d ANY Ons-Ammar
190	247	234202140	192.168.56.1	224.0.0.22	LLMNR	69	Standard query #x33d ANY Ons-Ammar
191	247	575402124	192.168.56.1	224.0.0.22	ICMPv3	60	Membership Report / Join group 224.0.0.252 for any sources

189	247	233392220	fe80::a33f:4ee: ff00:1:13	LLMNR	89 Standard query 0x33d ANY Ons-Ammar
190	247	23420146	192.168.56.1 224.0.0.252	LLMNR	69 Standard query 0x33d ANY Ons-Ammar
191	247	575042124	192.168.56.1 224.0.0.22	IGMPv3	60 Membership Report / Join group 224.0.0.252 for any sources
192	247	5750842315	fe80::a33f: ff00:1:16	ICMPv6	90 Multicast Listener Report Message v2
193	247	645782982	fe80::a33f: ff00:1:13	LLMNR	89 Standard query 0x33d ANY Ons-Ammar
194	247	645783132	192.168.56.1 224.0.0.252	LLMNR	69 Standard query 0x33d ANY Ons-Ammar
195	247	874786863	fe80::a0:27ff: fe9a: ff00:2	ICMPv6	70 Router Solicitation from 00:00:27:a9:83:9c
196	288	275360774	192.168.56.101 192.168.56.100	DHCP	333 DHCP Request - Transaction ID 0xf0fa2212
197	288	2826027674	PcsCompu 57:08:42	ARP	60 Who has 192.168.56.101? Tell 192.168.56.100
198	288	2820278894	192.168.56.101	DHCP	590 DHCP ACK - Transaction ID 0xf0fa2212
199	288	282046515	PcsCompu a9:83:9e PcsCompu 57:08:42	ARP	42 192.168.56.101 is at 00:00:27:a9:83:9c
200	292	987406257	fe80::30:a5: ff00:50	ARP	40 Who has 192.168.56.101? Tell 192.168.56.20

	Frame	160: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface enp0s3, id 0
201	292, 987423600	PcsCompu_a9:83:9c PcsCompu_8d:50:a5 ARP 42 192.168.56.101 is at 08:00:27:a9:83:9c
202	292, 988205227	192.168.56.20 DNS 85 Standard query 0x2c9b A teredo.ipv6.microsoft.com
203	292, 988285169	192.168.56.101 192.168.56.20 ICMP 113 Destination unreachable (Port unreachable)
204	293, 398899215	PcsCompu_a9:83:9c PcsCompu_57:80:42 ARP 42 Who has 192.168.56.100? Tell 192.168.56.10
205	293, 398935097	PcsCompu_57:80:42 PcsCompu_a9:83:9c ARP 60 192.168.56.100 is at 08:00:27:57:80:42
206	298, 005164220	PcsCompu_a9:83:9c PcsCompu_8d:50:a5 ARP 42 Who has 192.168.56.20? Tell 192.168.56.10
207	298, 005676669	PcsCompu_8d:50:a5 PcsCompu_a9:83:9c ARP 60 192.168.56.20 is at 08:00:27:8d:50:a5
208	236, 241059521	192.168.56.20 DNS 85 Standard query 0x1c9b A teredo.ipv6.microsoft.com
209	236, 241098466	192.168.56.101 192.168.56.20 ICMP 113 Destination unreachable (Port unreachable)
210	341, 060559781	PcsCompu_a9:83:9c ARP 60 Who has 192.168.56.101? Tell 192.168.56.20
211	341, 060559794	PcsCompu_a9:83:9c PcsCompu_8d:50:a5 ARP 42 192.168.56.101 is at 08:00:27:a9:83:9c
212	367, 768579145	192.168.56.101 192.168.56.20 DNS 85 Standard query 0xb389 A teredo.ipv6.microsoft.com

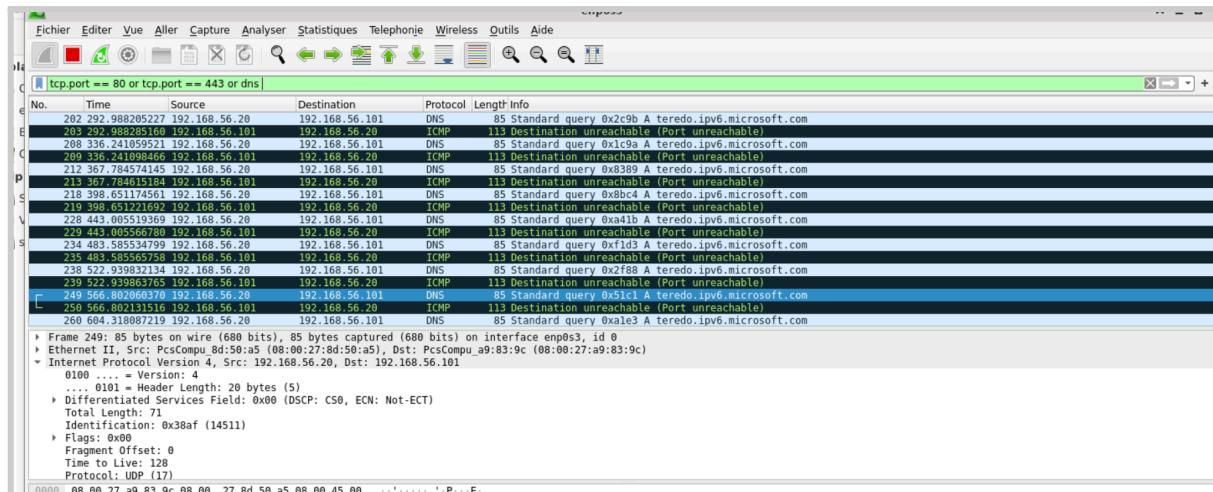
220	403.560841232	PcsCompu	8d:50:a5	PcsCompu	a9:83:9c	ARP	60 Who has 192.168.56.101? Tell 192.168.56.20
221	403.560849106	PcsCompu	a9:83:9c	PcsCompu	8d:50:a5	ARP	42 192.168.56.101 is at 08:00:27:a9:83:9c
222	415.499752982	192.168.56.10		192.168.56.255	BROWSER	270 Local Master Announcement MARIONET, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Ser...	
223	415.491097282	192.168.56.10		192.168.56.255	BROWSER	252 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum	
224	415.492852493	192.168.56.101		192.168.56.255	BROWSER	270 Local Master Announcement MARIONET, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Ser...	
225	415.493563154	192.168.56.101		192.168.56.255	BROWSER	252 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum	
226	415.494895877	192.168.56.1		255.255.255.255	BROWSER	270 Local Master Announcement MARIONET, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Ser...	
227	415.494896087	192.168.56.1		255.255.255.255	BROWSER	252 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum	
228	443.005519369	192.168.56.101		192.168.56.101	DNS	85 Standard query for xfa41b.a teredo.ipv6.microsoft.com	
229	443.005566768	192.168.56.101		192.168.56.20	ICMP	113 Destination unreachable (Port unreachable)	
230	447.575897857	PcsCompu	8d:50:a5	PcsCompu	a9:83:9c	ARP	60 Who has 192.168.56.101? Tell 192.168.56.20
231	447.575921083	PcsCompu	a9:83:9c	PcsCompu	8d:50:a5	ARP	42 192.168.56.101 is at 08:00:27:a9:83:9c

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

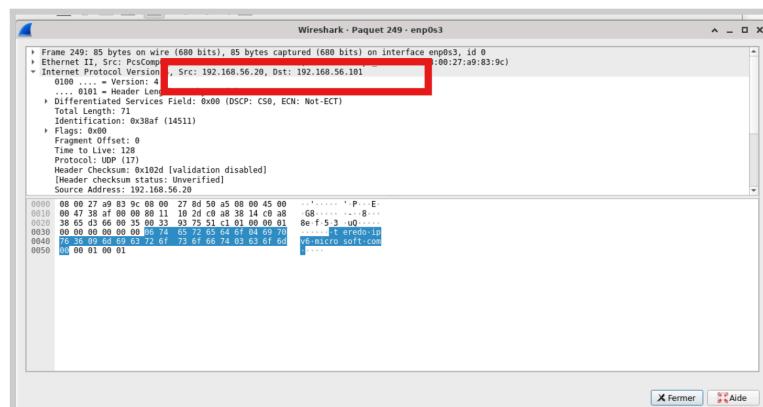
No.	Time	Source	Destination	Protocol	Length	Info
137	21.44308307	192.168.56.20	192.168.56.10	TCP	60	49525 -> 445 [ACK] Seq=7136 Ack=174321 Win=1838 Len=0
140	21.44494818	192.168.56.20	192.168.56.10	TCP	60	49525 -> 445 [ACK] Seq=7136 Ack=195493 Win=1756 Len=0
141	21.447971606	192.168.56.20	192.168.56.10	SMB2	171	Read Request Len:32768 Off:61952 File: abb228e4b89956fc89b8c559ead149354a0c64623f44905fa70c05f4ebfe7b4b.exe
143	21.445814917	192.168.56.20	192.168.56.10	TCP	60	49525 -> 445 [ACK] Seq=7253 Ack=208633 Win=1708 Len=0
146	21.446624913	192.168.56.20	192.168.56.10	TCP	60	49525 -> 445 [ACK] Seq=7253 Ack=228345 Win=1627 Len=0
147	21.447001311	192.168.56.20	192.168.56.10	SMB2	171	Read Request Len:286740 File: abb228e4b89956fc89b8c559ead149354a0c64623f44905fa70c05f4ebfe7b4b.exe
150	21.446109863	192.168.56.20	192.168.56.10	TCP	60	49525 -> 445 [ACK] Seq=7309 Ack=25710 Win=1516 Len=0
151	21.446109863	192.168.56.20	192.168.56.10	SMB2	171	Read Request Len:286740 File: abb228e4b89956fc89b8c559ead149354a0c64623f44905fa70c05f4ebfe7b4b.exe
153	21.462089358	192.168.56.20	192.168.56.10	TCP	60	49525 -> 445 [ACK] Seq=74409 Len:1949 Win=1499 Len=0
154	20.999784939	192.168.56.20	192.168.56.10	SMB2	146	Close Request File: abb228e4b89956fc89b8c559ead149354a0c64623f44905fa70c05f4ebfe7b4b.exe
156	30.00173351	192.168.56.20	192.168.56.10	SMB2	146	Close Request File: abb228e4b89956fc89b8c559ead149354a0c64623f44905fa70c05f4ebfe7b4b.exe
158	30.0032549149	192.168.56.20	192.168.56.10	SMB2	146	Close Request File: abb228e4b89956fc89b8c559ead149354a0c64623f44905fa70c05f4ebfe7b4b.exe
160	30.004473241	192.168.56.20	192.168.56.10	SMB2	146	Close Request File: abb228e4b89956fc89b8c559ead149354a0c64623f44905fa70c05f4ebfe7b4b.exe
162	30.005095957	192.168.56.20	192.168.56.10	SMB2	146	Close Request File: abb228e4b89956fc89b8c559ead149354a0c64623f44905fa70c05f4ebfe7b4b.exe
+ 164	30.00656825	192.168.56.20	192.168.56.10	SMB2	146	Close Request File: abb228e4b89956fc89b8c559ead149354a0c6423f44905fa70c05f4ebfe7b4b.exe
167	30.214477383	192.168.56.20	192.168.56.10	TCP	60	49525 -> 445 [ACK] Seq=8039 Ack=262049 Win=1499 Len=0 SLE=261921 SRE=262049
202	298.89820527	192.168.56.20	192.168.56.101	DNS	85	Standard query 0x29c9 A teredo.ipv6.microsoft.com
203	292.988251606	192.168.56.101	192.168.56.20	ICMP	113	Destination unreachable (Port unreachable)
208	336.241859521	192.168.56.20	192.168.56.101	DNS	85	Standard query 0x19a9 A teredo.ipv6.microsoft.com
209	336.24198466	192.168.56.101	192.168.56.20	ICMP	113	Destination unreachable (Port unreachable)
212	367.784574145	192.168.56.20	192.168.56.101	DNS	85	Standard query 0x3899 A teredo.ipv6.microsoft.com
213	367.784615101	192.168.56.101	192.168.56.20	ICMP	113	Destination unreachable (Port unreachable)
214	368.651621692	192.168.56.101	192.168.56.20	ICMP	113	Destination unreachable (Port unreachable)
219	368.651621692	192.168.56.101	192.168.56.20	ICMP	113	Destination unreachable (Port unreachable)
228	443.005519269	192.168.56.20	192.168.56.101	DNS	85	Standard query 0x4a1b A teredo.ipv6.microsoft.com
229	443.005566780	192.168.56.20	192.168.56.101	ICMP	113	Destination unreachable (Port unreachable)
234	483.585537499	192.168.56.20	192.168.56.101	DNS	85	Standard query 0xf1d3 A teredo.ipv6.microsoft.com
235	483.58556578	192.168.56.20	192.168.56.101	ICMP	113	Destination unreachable (Port unreachable)
238	522.939832134	192.168.56.20	192.168.56.101	DNS	85	Standard query 0x2f88 A teredo.ipv6.microsoft.com
239	522.939837653	192.168.56.20	192.168.56.101	ICMP	113	Destination unreachable (Port unreachable)

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

# Compte rendu Ons AMMAR



Choix d'une requête dns  
Adresses source et destination



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

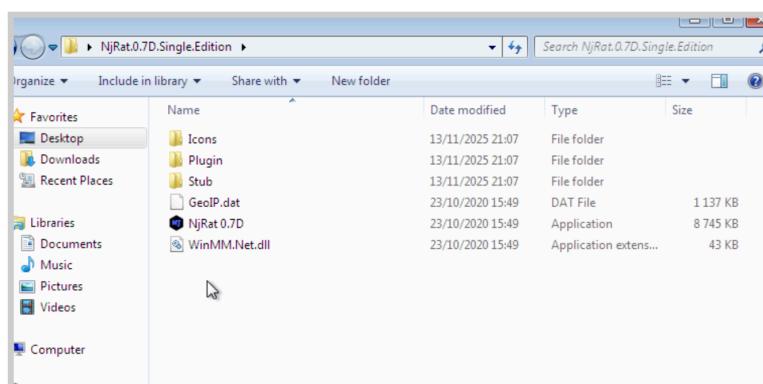


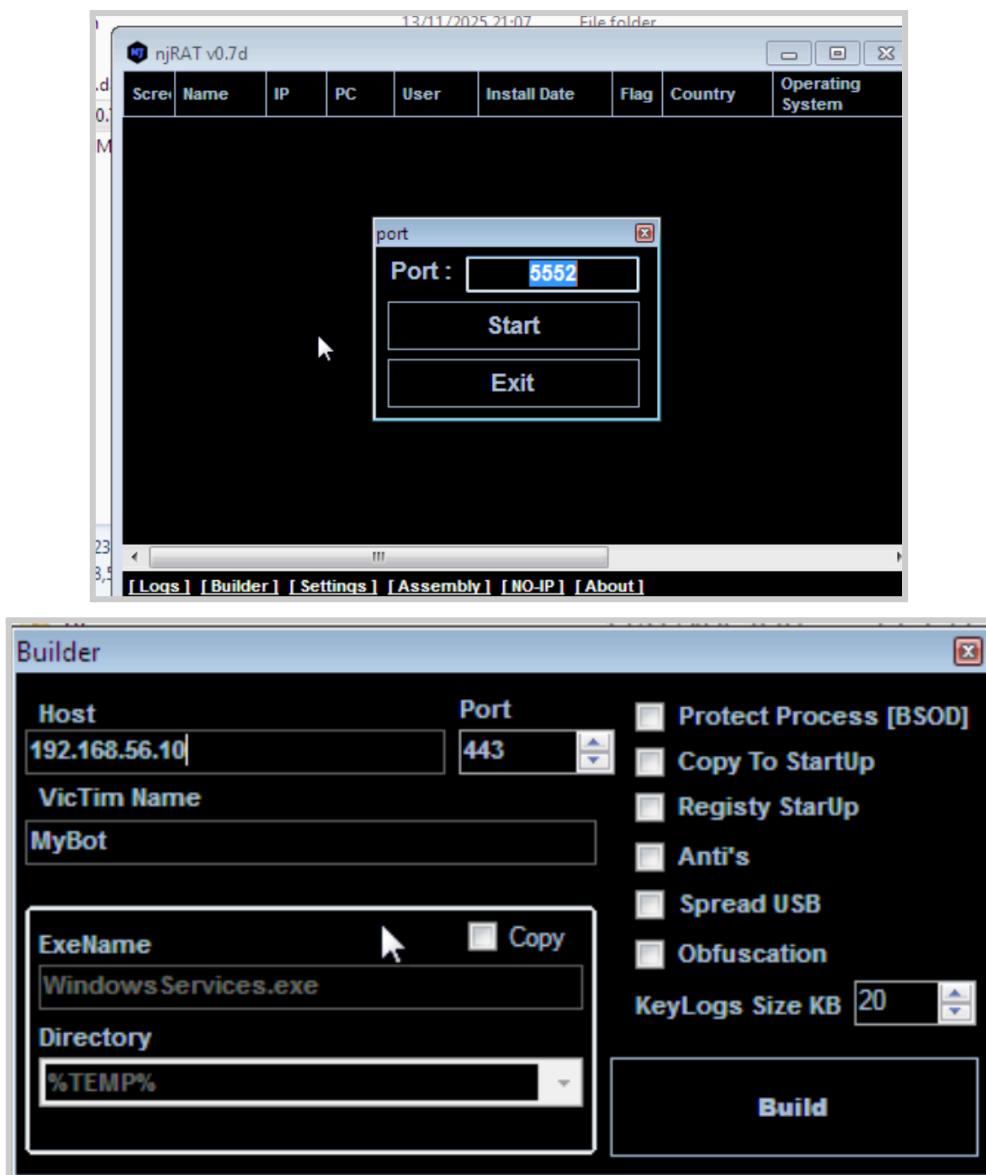
Le domaine



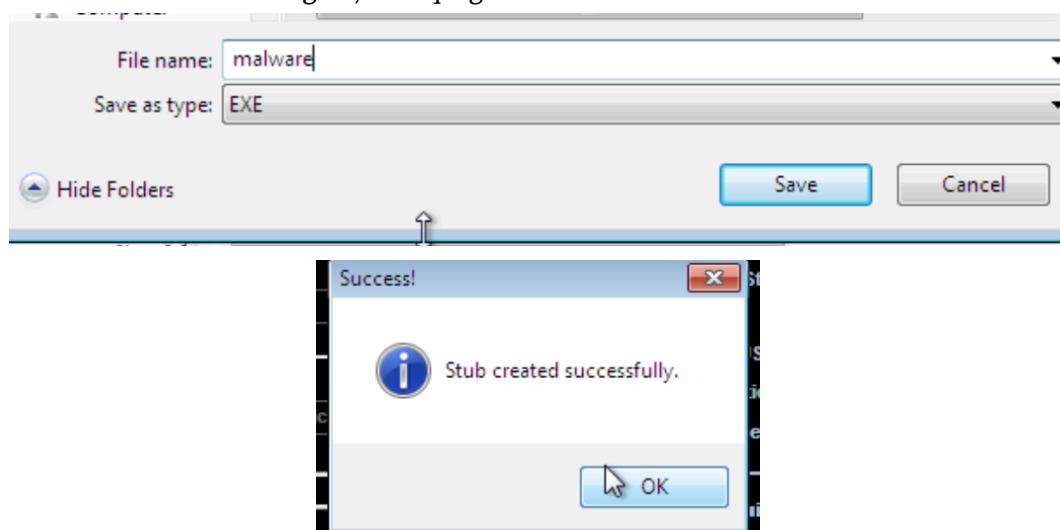
J'ai travaillé aussi avec le njRat single edition(depuis un dépôt github)

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.



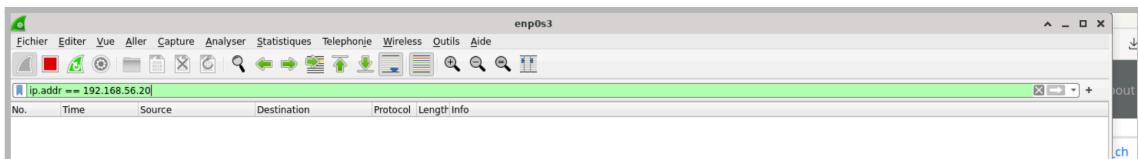
On lance après intesim

```

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

No.	Time	Source	Destination	Protocol	Length	Info
16	49.922974585	192.168.56.20	192.168.56.10	TCP	66	49602 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK PERM=1
17	49.923038267	192.168.56.10	192.168.56.20	TCP	66	443 → 49602 [SYN, ACK] Seq=1 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=1024
18	49.923511023	192.168.56.20	192.168.56.10	TCP	60	49602 → 443 [ACK] Seq=1 Ack=1 Win=204800 Len=0
19	50.307429957	192.168.56.20	192.168.56.10	SSL	275	Continuation Data
20	50.307470114	192.168.56.10	192.168.56.20	TCP	54	443 → 49602 [ACK] Seq=1 Ack=222 Win=64512 Len=0
21	50.310515027	192.168.56.20	192.168.56.10	SSL	197	Continuation Data
22	50.310537089	192.168.56.10	192.168.56.20	TCP	54	443 → 49602 [ACK] Seq=1 Ack=365 Win=64512 Len=0
23	50.337544431	192.168.56.10	192.168.56.20	TCP	54	443 → 49602 [RST, ACK] Seq=1 Ack=365 Win=64512 Len=0
24	52.117131556	192.168.56.20	192.168.56.10	SMB2	346	Create Request File: desktop.ini
25	52.119198585	192.168.56.10	192.168.56.20	SMB2	131	Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
26	52.323168929	192.168.56.20	192.168.56.10	TCP	60	49601 → 445 [ACK] Seq=293 Ack=78 Win=254 Len=0
27	52.340026522	192.168.56.20	192.168.56.10	TCP	66	49603 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK PERM=1
28	52.340070256	192.168.56.10	192.168.56.20	TCP	66	443 → 49603 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=1024
29	52.341291525	192.168.56.20	192.168.56.10	TCP	60	49603 → 443 [ACK] Seq=1 Ack=1 Win=204800 Len=0
30	52.425467511	192.168.56.20	192.168.56.10	SSL	275	Continuation Data
31	52.425054932	192.168.56.10	192.168.56.20	TCP	54	443 → 49603 [ACK] Seq=1 Ack=222 Win=64512 Len=0
32	52.426354400	192.168.56.20	192.168.56.10	SSL	197	Continuation Data

Frame 16: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0  
Ethernet II, Src: PcsCompu 8d:50:a5 (08:00:27:8d:50:a5), Dst: PcsCompu a9:83:9c (08:00:27:a9:83:9c)  
Internet Protocol Version 4, Src: 192.168.56.20, Dst: 192.168.56.10  
Transmission Control Protocol, Src Port: 49602, Dst Port: 443, Seq: 0, Len: 0

no.	time	source	destination	protocol	length	info
187	94.269516244	192.168.56.20	192.168.56.10	TCP	66	49623 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK PERM=1
188	94.269553808	192.168.56.10	192.168.56.20	TCP	66	443 → 49623 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=1024
189	94.270613346	192.168.56.20	192.168.56.10	TCP	60	49623 → 443 [ACK] Seq=1 Ack=1 Win=204800 Len=0
190	94.341291722	192.168.56.20	192.168.56.10	SSL	275	Continuation Data
191	94.34219733710	192.168.56.10	192.168.56.19	TCP	54	443 → 49623 [ACK] Seq=1 Ack=222 Win=64512 Len=0
192	94.342197859	192.168.56.20	192.168.56.10	SSL	197	Continuation Data
193	94.342209582	192.168.56.10	192.168.56.20	TCP	54	443 → 49623 [ACK] Seq=1 Ack=365 Win=64512 Len=0
194	94.354238365	192.168.56.10	192.168.56.20	TCP	54	443 → 49623 [RST, ACK] Seq=1 Ack=365 Win=64512 Len=0
195	96.355388465	192.168.56.20	192.168.56.10	TCP	66	49624 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK PERM=1
196	96.355419649	192.168.56.10	192.168.56.20	TCP	66	443 → 49624 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=1024
197	96.356020048	192.168.56.20	192.168.56.10	TCP	60	49624 → 443 [ACK] Seq=1 Ack=1 Win=204800 Len=0
198	96.359889963	192.168.56.20	192.168.56.10	SSL	275	Continuation Data
199	96.420923860	192.168.56.10	192.168.56.20	TCP	54	443 → 49624 [ACK] Seq=1 Ack=222 Win=64512 Len=0
200	96.421320941	192.168.56.20	192.168.56.10	SSL	197	Continuation Data

On peut voir des tentatives TCP vers le faux serveur C2