Rapport du TP2

Attaques actives

REALISER PAR :

ZINEB EL RHAZOUANI

SAID EL OUARDI

ADIL ERRAD

SOMMAIRE

Introduction :

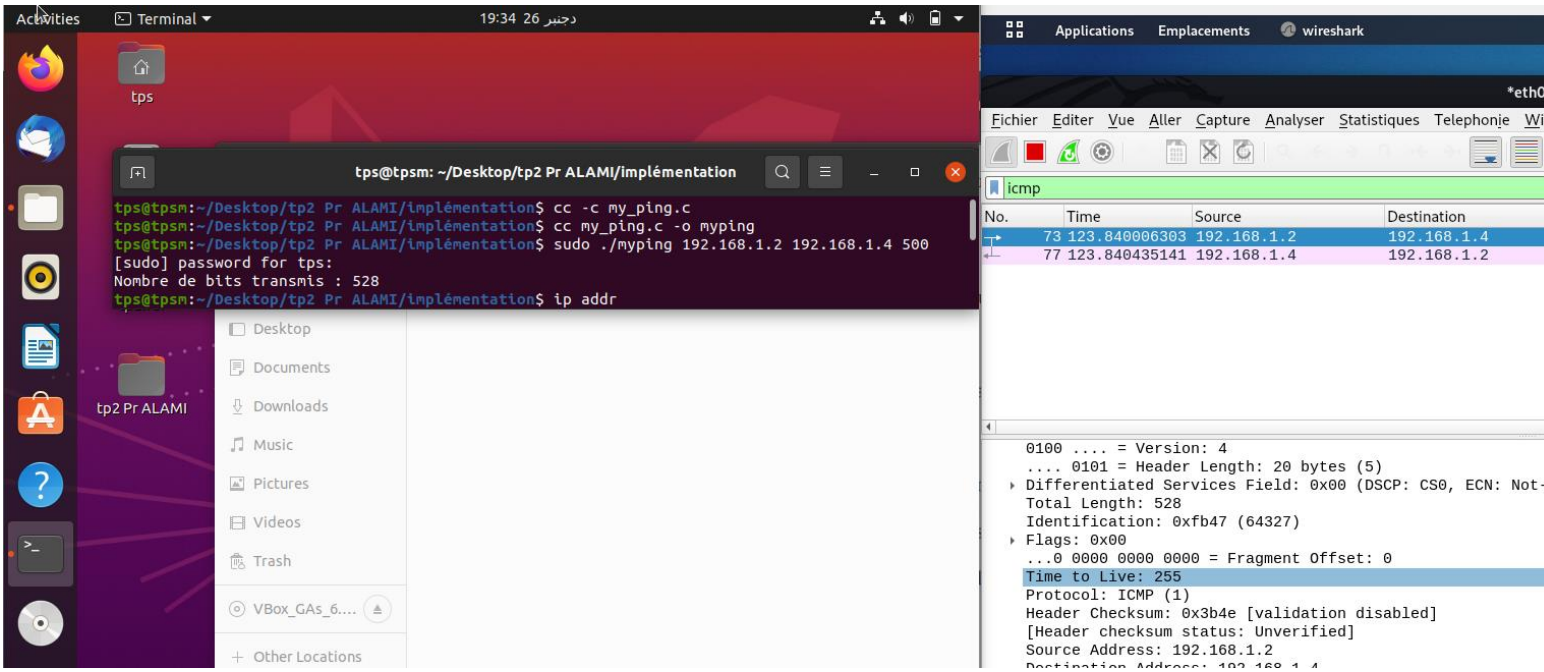
Les attaques actives sont mises en place par l'injection, la modification ou la suppression de paquets. L'attaquant peut ainsi laisser les traces des attaques qu'il lance. Ces traces peuvent être exploitées par l'administrateur réseau pour déceler l'existence d'attaques et identifier l'attaquant si possible.

❖Objectifs de ce TP:

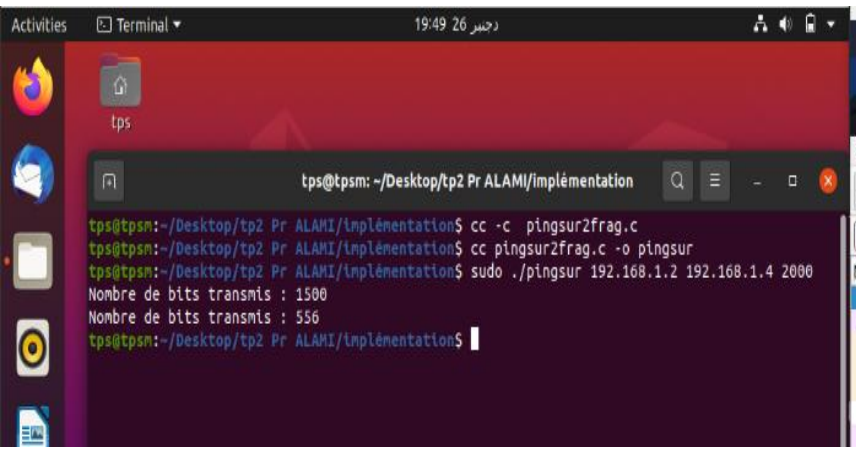
- Implémenter quelques attaques et les tester.
- Mise en place de quelques attaques en utilisant des outils d'attaques.

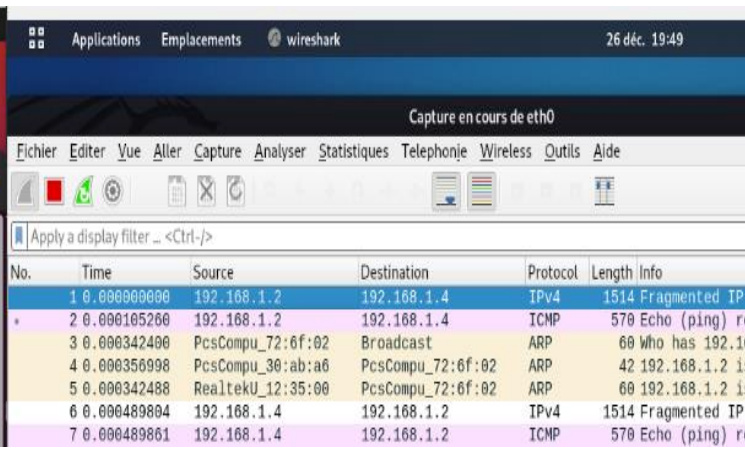
Implémentation d'attaques actives

Exercice 1 : my_ping.c

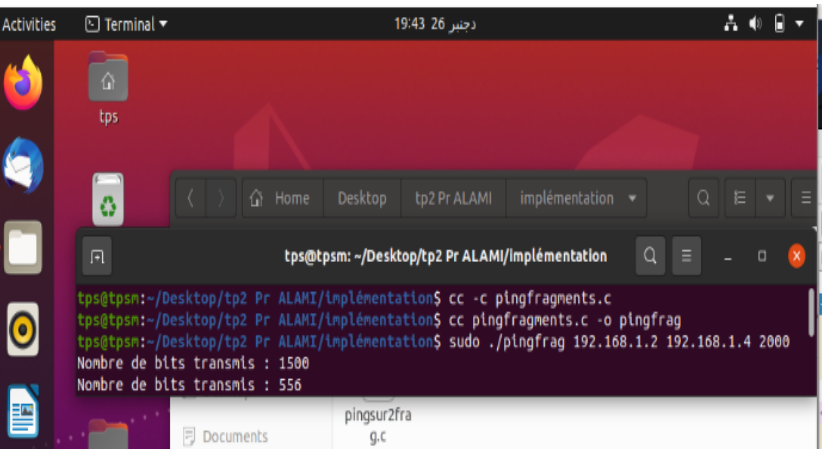


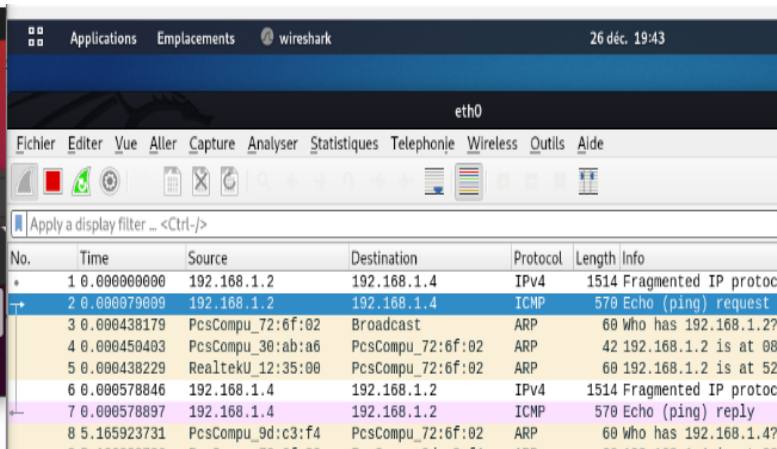
Exercice 2 : pingsur2frag.c



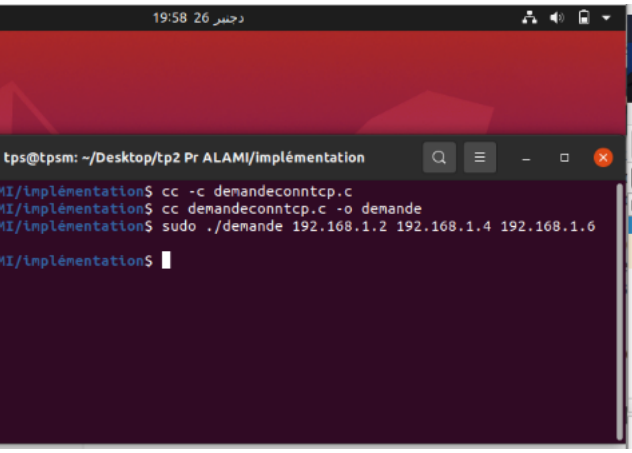


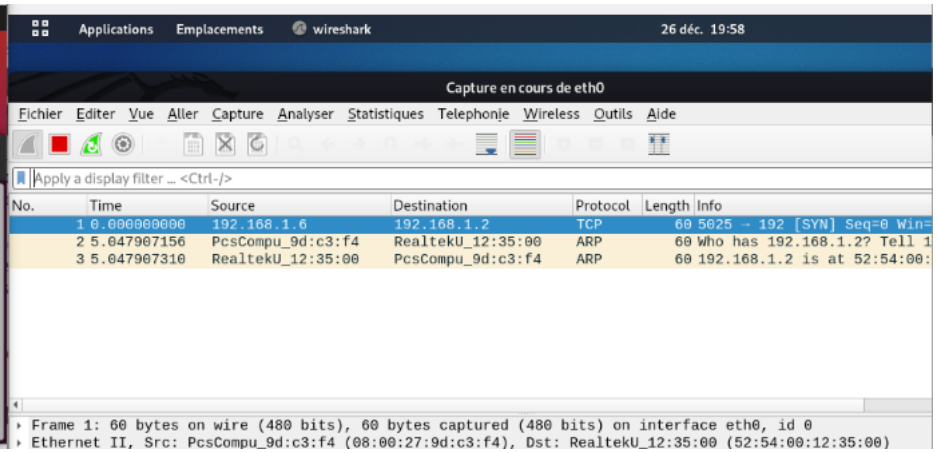
Exercice 3 : pingfragments.c

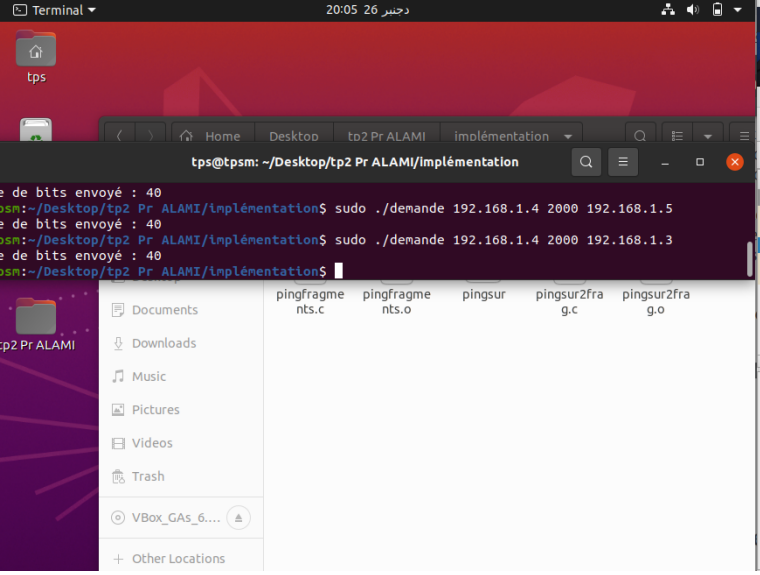


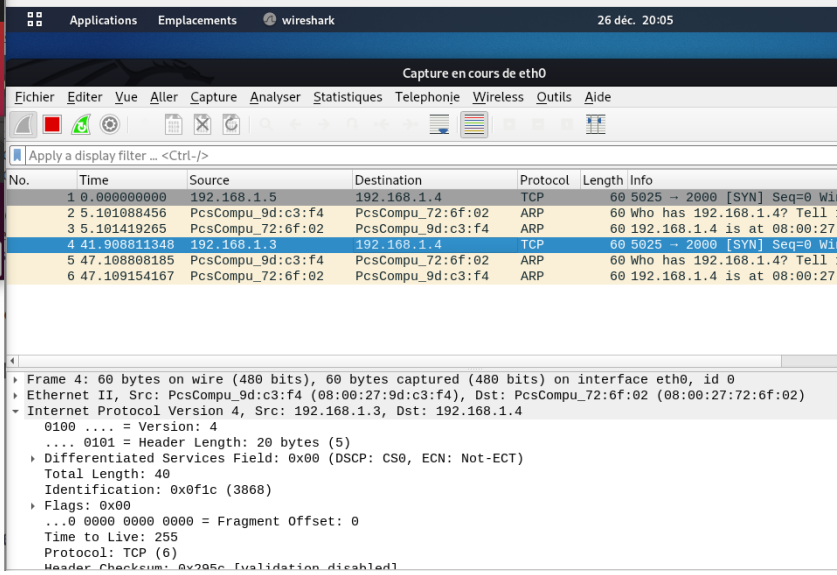


Exercice 4 : demandeconntcp.c









Test de quelques outils d’attaques

A. Attaque DHCP starvation

DHCP starvation : L’attaquant inonde le serveur DHCP avec des messages DHCPREQUEST afin de réserver toutes les adresses IP disponibles sur le serveur DHCP. L’attaquant doit utiliser une nouvelle adresse MAC pour chaque requête.

- installer des utilitaires pour dhcpstarv (Install utils for dhcpstarv).

```
tps@tpsm:~/Desktop$ sudo apt install make
Reading package lists... Done
Building dependency tree
Reading state information... Done
make is already the newest version (4.2.1-1.2).
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2 linux-headers-5.11.0-27-generic
  linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic
  linux-modules-5.11.0-27-generic linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
tps@tpsm:~/Desktop$ sudo apt install autoconf
Reading package lists... Done
Building dependency tree
Reading state information... Done
autoconf is already the newest version (2.69-11.1).
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2 linux-headers-5.11.0-27-generic
  linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic
  linux-modules-5.11.0-27-generic linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

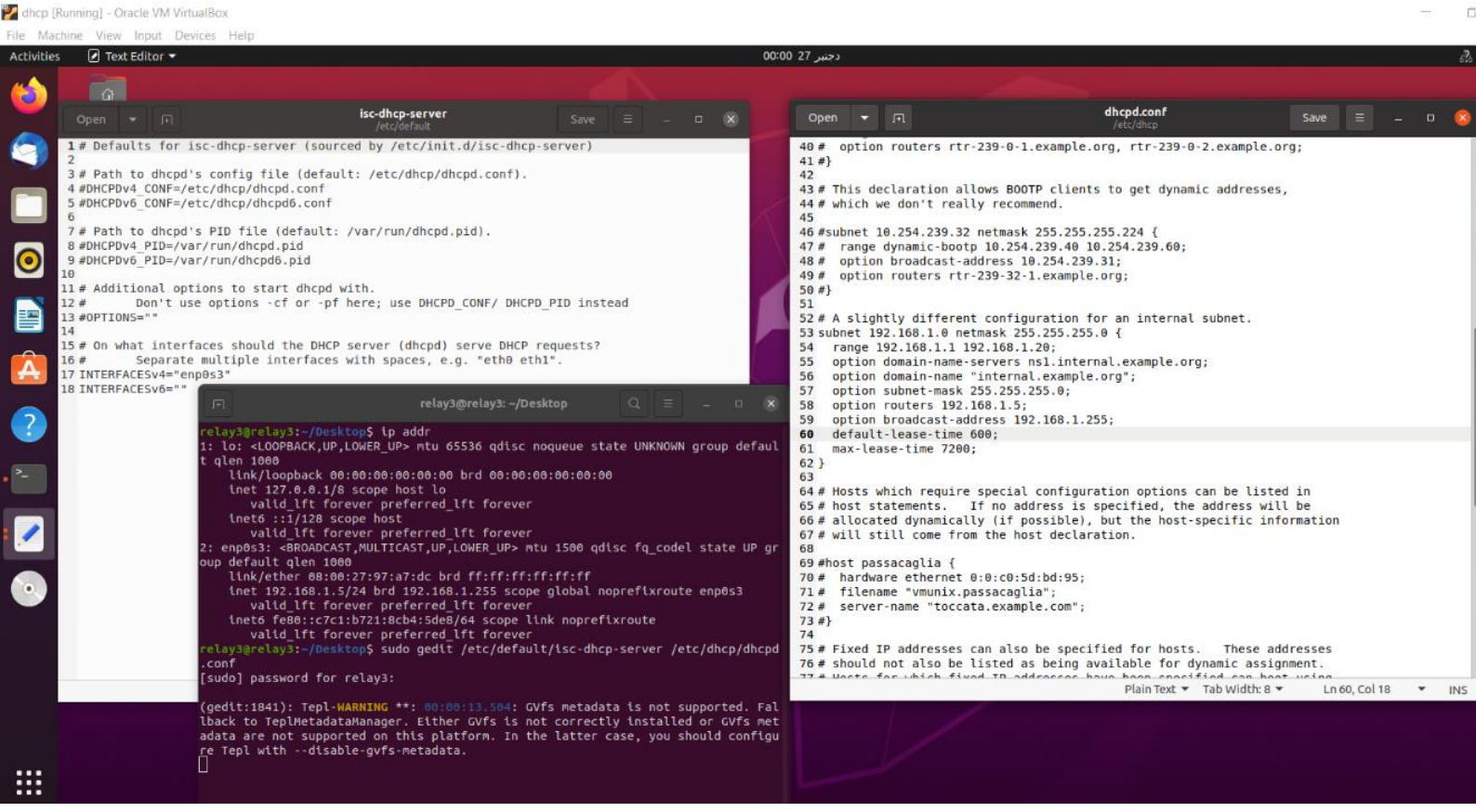
```
tps@tpsm: ~/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2.1
tps@tpsm:~/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2.1$ ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
/bin/bash: /home/tps/Desktop/tp2: No such file or directory
configure: WARNING: `missing' script is too old or missing
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
```

- Install dhcpstarv

```
tps@tpsm:~/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2.1$ make
cd . && autoheader
/bin/bash: autoheader: command not found
make: *** [Makefile:204: config.h.in] Error 127
tps@tpsm:~/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2.1$ autoheader

Command 'autoheader' not found, but can be installed with:

sudo apt install autoconf

tps@tpsm:~/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2.1$ make
cd . && autoheader
rm -f stamp-h1
touch config.h.in
cd . && /bin/bash ./config.status config.h
config.status: creating config.h
make  all-recursive
make[1]: Entering directory '/home/tps/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2
.1'
Making all in src
make[2]: Entering directory '/home/tps/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2
```

```
tps@tpsm:~/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2.1$ sudo make install
[sudo] password for tps:
Making install in src
make[1]: Entering directory '/home/tps/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2
.1/src'
make[2]: Entering directory '/home/tps/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2
.1/src'
test -z "/usr/local/bin" || mkdir -p -- "/usr/local/bin"
```

- Configuration DHCP



- Status DHCP

```
relay3@relay3:~/Desktop$ service isc-dhcp-server restart
relay3@relay3:~/Desktop$ service isc-dhcp-server status
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vend>
     Active: active (running) since Mon 2021-12-27 00:01:22 +01; 6s ago
       Docs: man:dhcpd(8)
   Main PID: 1950 (dhcpd)
      Tasks: 4 (limit: 1092)
     Memory: 7.5M
     CGroup: /system.slice/isc-dhcp-server.service
             └─1950 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/d>

00:01:22 27 دجنبر relay3 sh[1950]: lease 192.168.20.5: no subnet.
00:01:22 27 دجنبر relay3 dhcpd[1950]: Wrote 0 leases to leases file.
00:01:22 27 دجنبر relay3 sh[1950]: Wrote 0 leases to leases file.
00:01:22 27 دجنبر relay3 dhcpd[1950]: Listening on LPF/enp0s3/08:00:27:97:a7:dc>
00:01:22 27 دجنبر relay3 sh[1950]: Listening on LPF/enp0s3/08:00:27:97:a7:dc/19>
00:01:22 27 دجنبر relay3 sh[1950]: Sending on   LPF/enp0s3/08:00:27:97:a7:dc/19>
00:01:22 27 دجنبر relay3 sh[1950]: Sending on   Socket/fallback/fallback-net
00:01:22 27 دجنبر relay3 dhcpd[1950]: Sending on   LPF/enp0s3/08:00:27:97:a7:dc>
00:01:22 27 دجنبر relay3 dhcpd[1950]: Sending on   Socket/fallback/fallback-net
00:01:22 27 دجنبر relay3 dhcpd[1950]: Server starting service.
lines 1-20/20 (END)
```

- Test DHCP

```
relay3@relay3: ~/Desktop
relay3@relay3:~/Desktop$ dhcp-lease-list
To get manufacturer names please download http://standards.ieee.org/regauth/oui/
oui.txt to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC                IP              hostname       valid until         manufactur
er
================================================================================
===============
08:00:27:82:40:95  192.168.1.3     tpsm           2021-12-26 23:25:55 -NA-

relay3@relay3:~/Desktop$ dhcp-lease-list
To get manufacturer names please download http://standards.ieee.org/regauth/oui/
oui.txt to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC                IP              hostname       valid until         manufactur
er
================================================================================
===============
08:00:27:82:40:95  192.168.1.3     tpsm           2021-12-26 23:25:55 -NA-

08:00:27:be:cb:18  192.168.1.20    tpsm           2021-12-26 23:31:19 -NA-

relay3@relay3:~/Desktop$
```

- Lance l’attaque

```
tps@tpsm:~/Desktop/tp2 Pr ALAMI/outils/dhcpstarv-0.2.1$ sudo dhcpstarv -i enp0s3
[sudo] password for tps:
```

- dossier de bail avant l’attaque (lease file

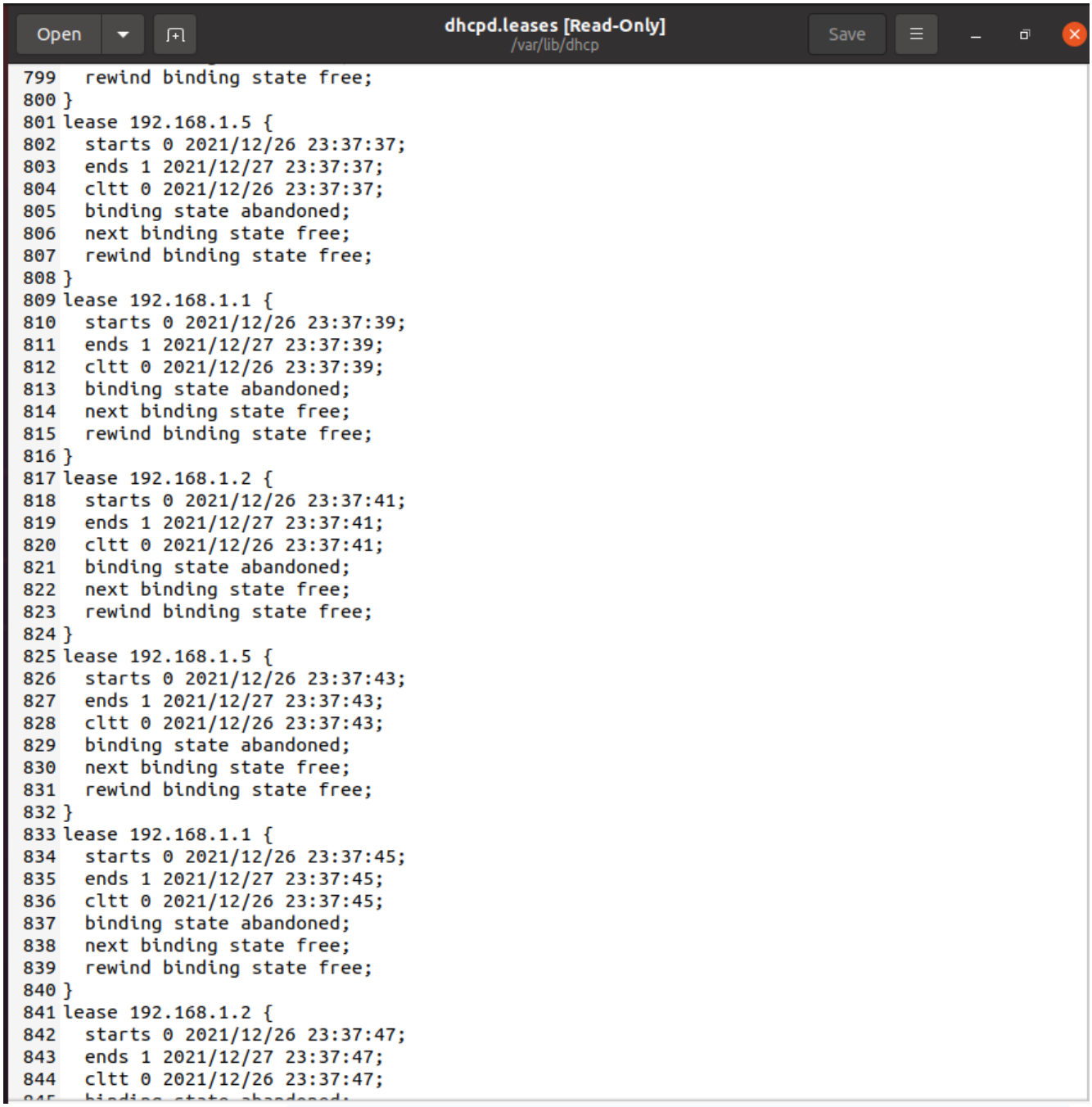
Open | *dhcpd.leases [Read-Only] /var/lib/dhcp | Save

```
1 # The format of this file is documented in the dhcpd.leases(5) manual page.
2 # This lease file was written by isc-dhcp-4.4.1
3
4 # authoring-byte-order entry is generated, DO NOT DELETE
5 authoring-byte-order little-endian;
6
7 server-duid "\000\001\000\001)[\260\302\010\000'\227\247\334";
8
9 lease 192.168.1.1 {
10   starts 0 2021/12/26 23:15:41;
11   ends 1 2021/12/27 23:15:41;
12   cltt 0 2021/12/26 23:15:41;
13   binding state abandoned;
14   next binding state free;
15   rewind binding state free;
16   client-hostname "tpsm";
17 }
18 lease 192.168.1.2 {
19   starts 0 2021/12/26 23:15:43;
20   ends 1 2021/12/27 23:15:43;
21   cltt 0 2021/12/26 23:15:43;
22   binding state abandoned;
23   next binding state free;
24   rewind binding state free;
25   client-hostname "tpsm";
26 }
27 lease 192.168.1.3 {
28   starts 0 2021/12/26 23:15:55;
29   ends 0 2021/12/26 23:25:55;
30   cltt 0 2021/12/26 23:15:55;
31   binding state active;
32   next binding state free;
33   rewind binding state free;
34   hardware ethernet 08:00:27:82:40:95;
35   uid "\001\010\000'\202@\225";
36   client-hostname "tpsm";
37 }
```

Plain Text | Tab Width: 8 | Ln 29, Col 30 | INS

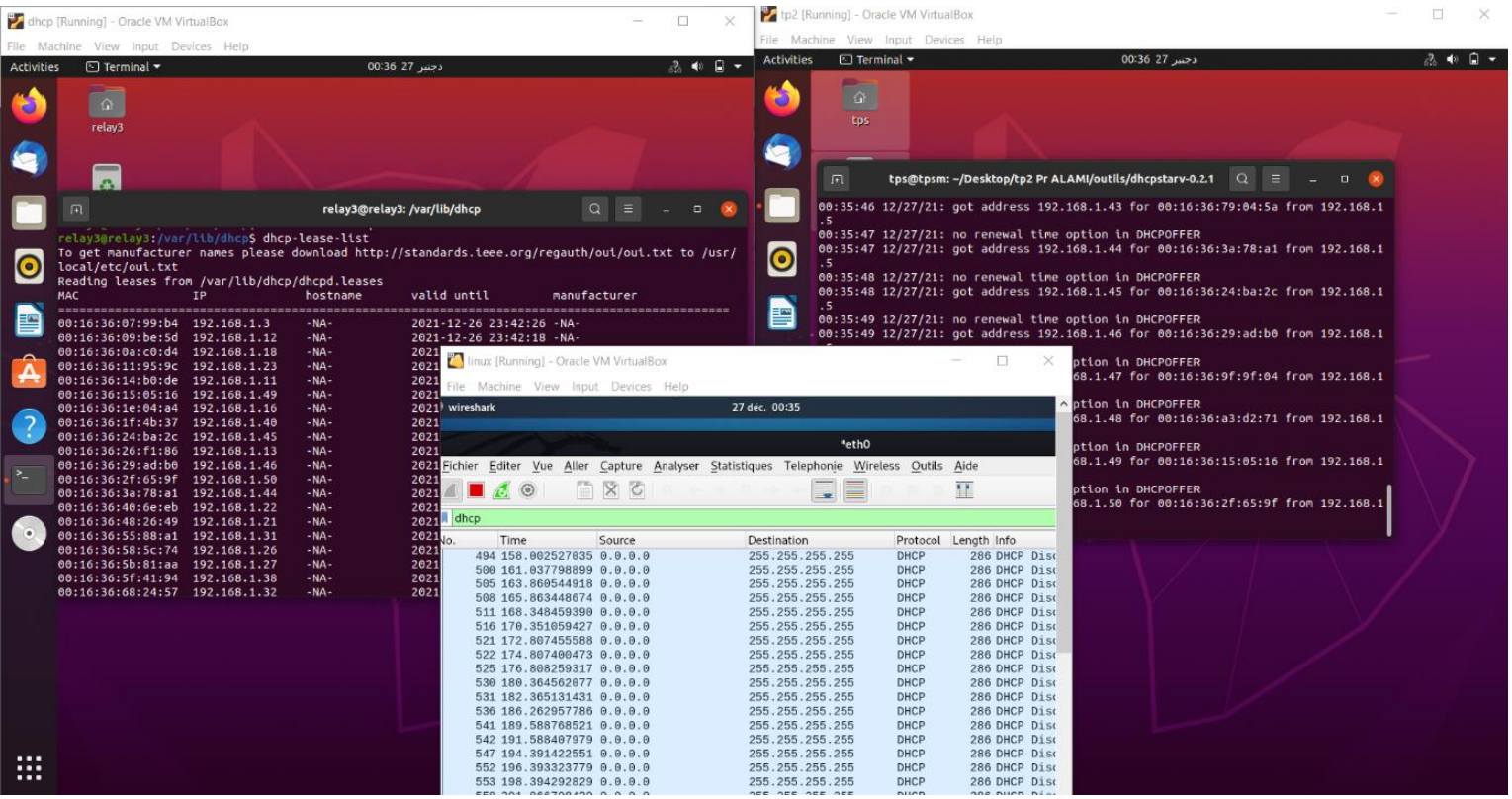
before the attack)

- dossier de bail avant l’attaque (lease file before the attack)



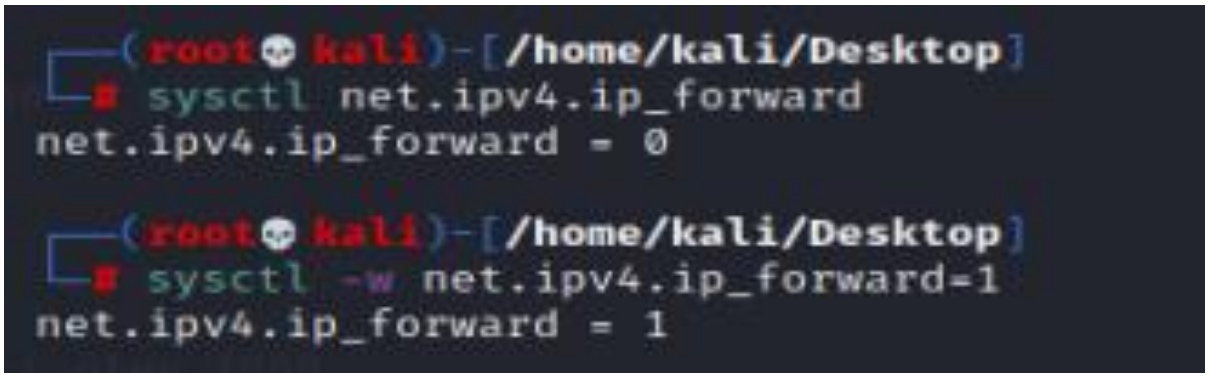

```
799   rewind binding state free;
800 }
801 lease 192.168.1.5 {
802   starts 0 2021/12/26 23:37:37;
803   ends 1 2021/12/27 23:37:37;
804   cltt 0 2021/12/26 23:37:37;
805   binding state abandoned;
806   next binding state free;
807   rewind binding state free;
808 }
809 lease 192.168.1.1 {
810   starts 0 2021/12/26 23:37:39;
811   ends 1 2021/12/27 23:37:39;
812   cltt 0 2021/12/26 23:37:39;
813   binding state abandoned;
814   next binding state free;
815   rewind binding state free;
816 }
817 lease 192.168.1.2 {
818   starts 0 2021/12/26 23:37:41;
819   ends 1 2021/12/27 23:37:41;
820   cltt 0 2021/12/26 23:37:41;
821   binding state abandoned;
822   next binding state free;
823   rewind binding state free;
824 }
825 lease 192.168.1.5 {
826   starts 0 2021/12/26 23:37:43;
827   ends 1 2021/12/27 23:37:43;
828   cltt 0 2021/12/26 23:37:43;
829   binding state abandoned;
830   next binding state free;
831   rewind binding state free;
832 }
833 lease 192.168.1.1 {
834   starts 0 2021/12/26 23:37:45;
835   ends 1 2021/12/27 23:37:45;
836   cltt 0 2021/12/26 23:37:45;
837   binding state abandoned;
838   next binding state free;
839   rewind binding state free;
840 }
841 lease 192.168.1.2 {
842   starts 0 2021/12/26 23:37:47;
843   ends 1 2021/12/27 23:37:47;
844   cltt 0 2021/12/26 23:37:47;
```

- Result

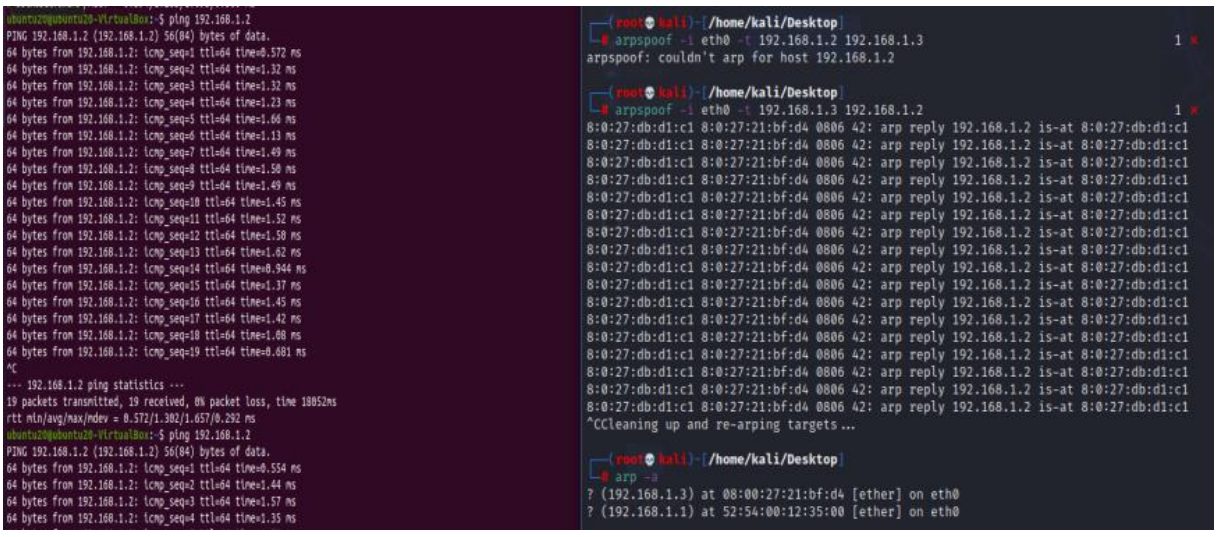


b. Attaque “Man In The Middle” basée sur l'attaque “ARP spoofing ” .

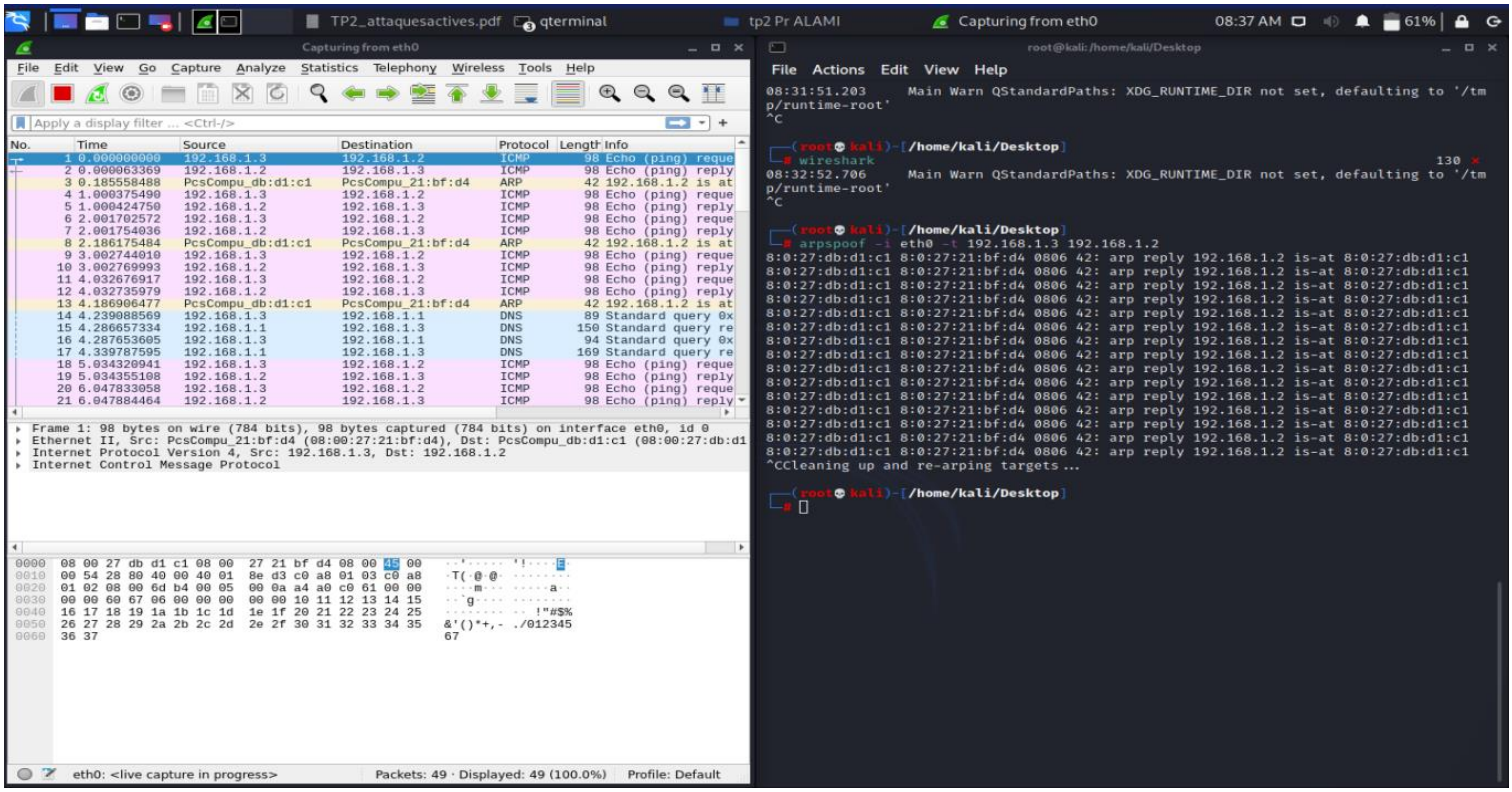
- Etape 1



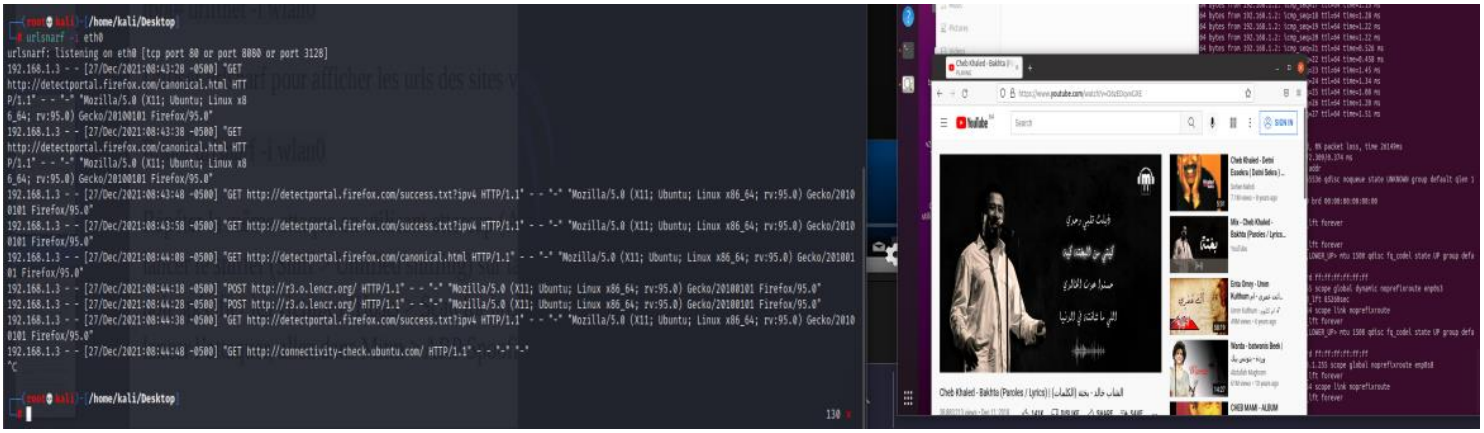
- Etape2.1

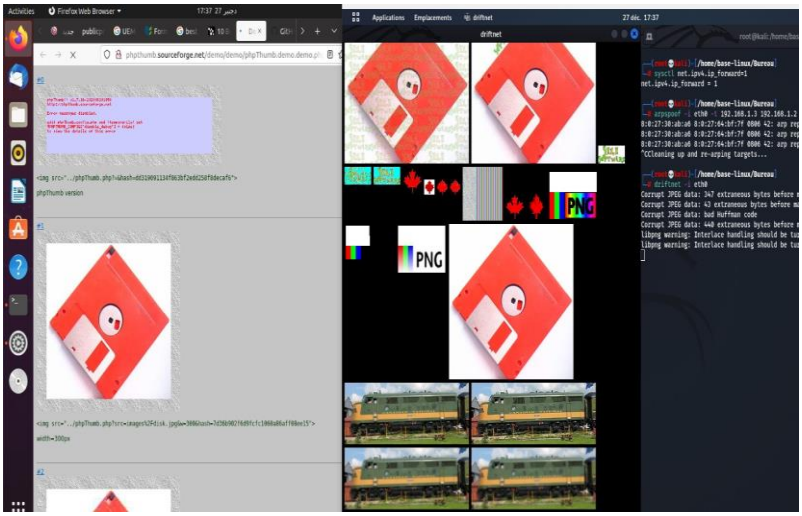


- Etape2.2



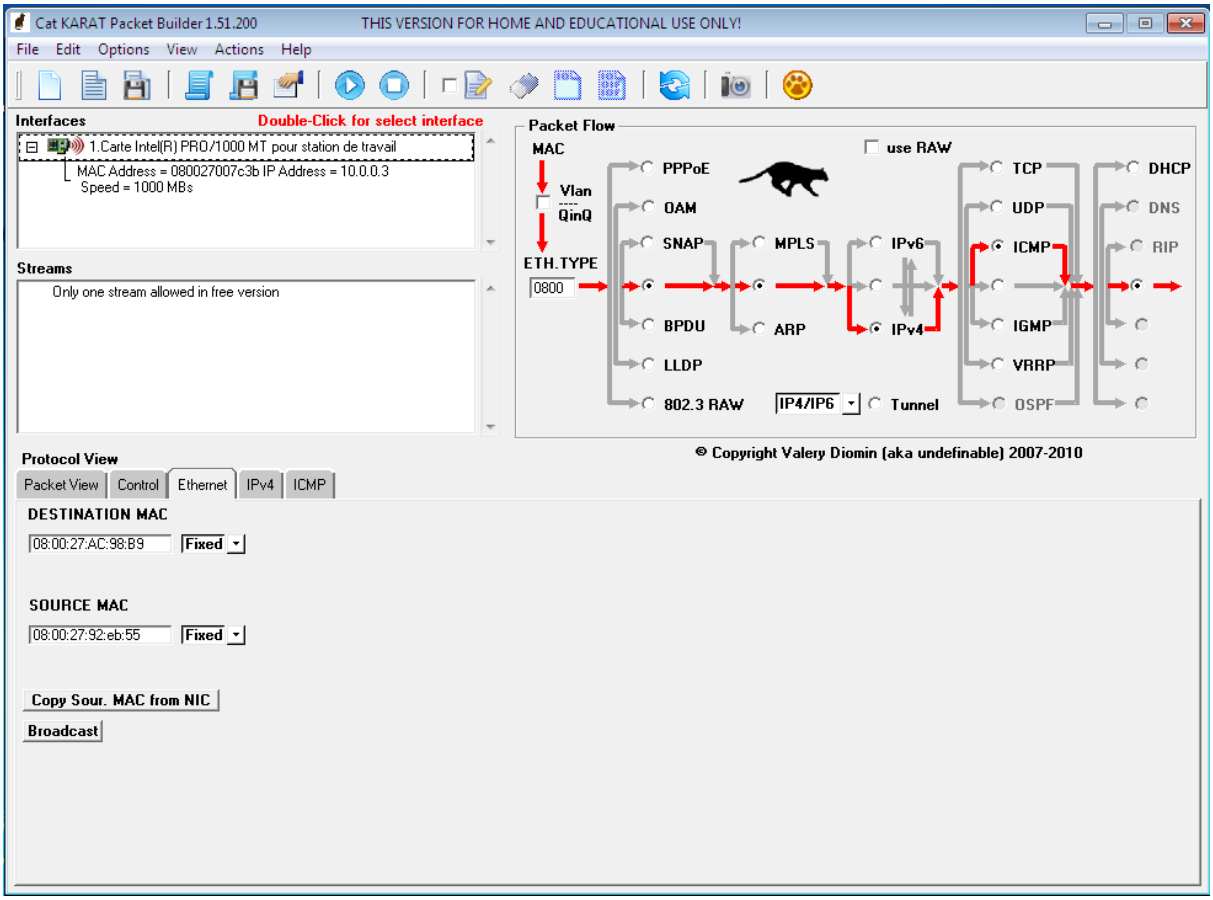
- Etape3



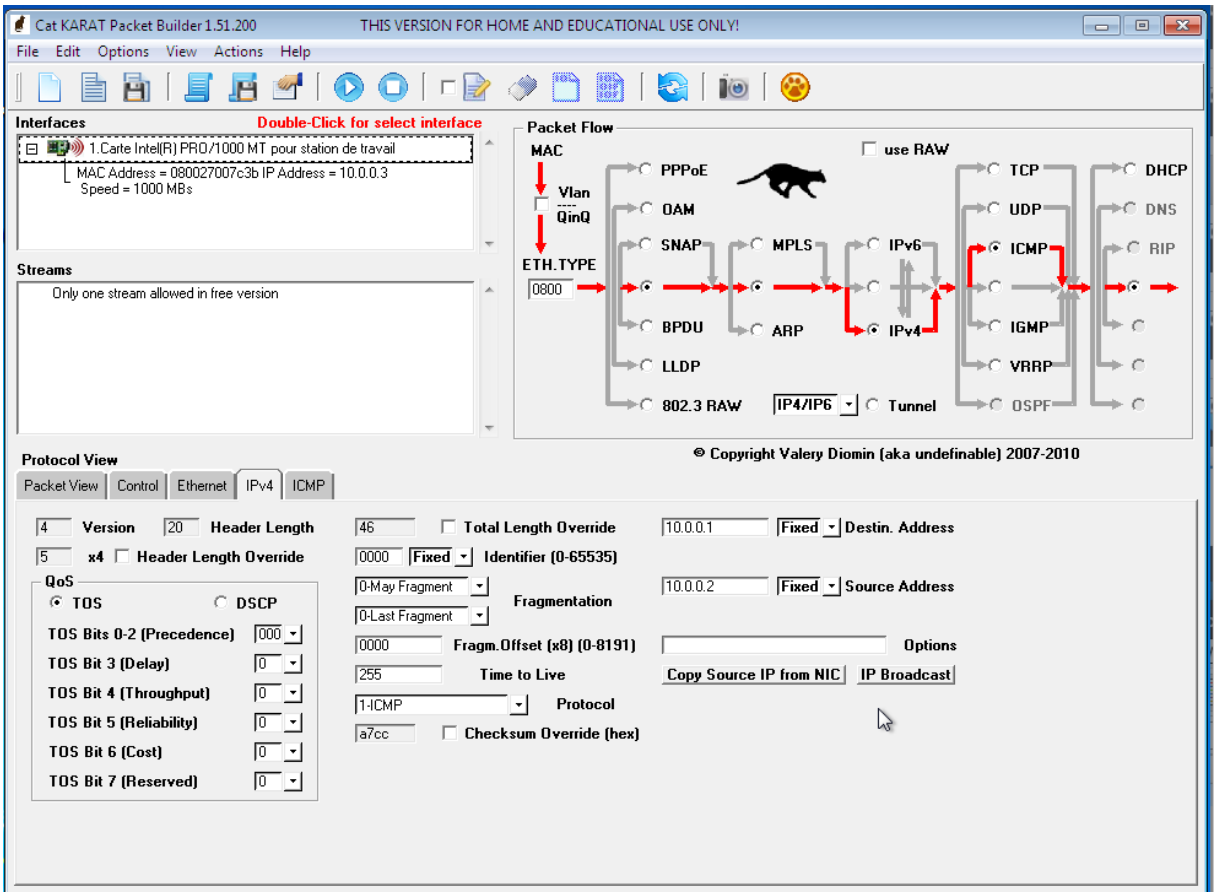


c. Attaque “usurpation d’identité”

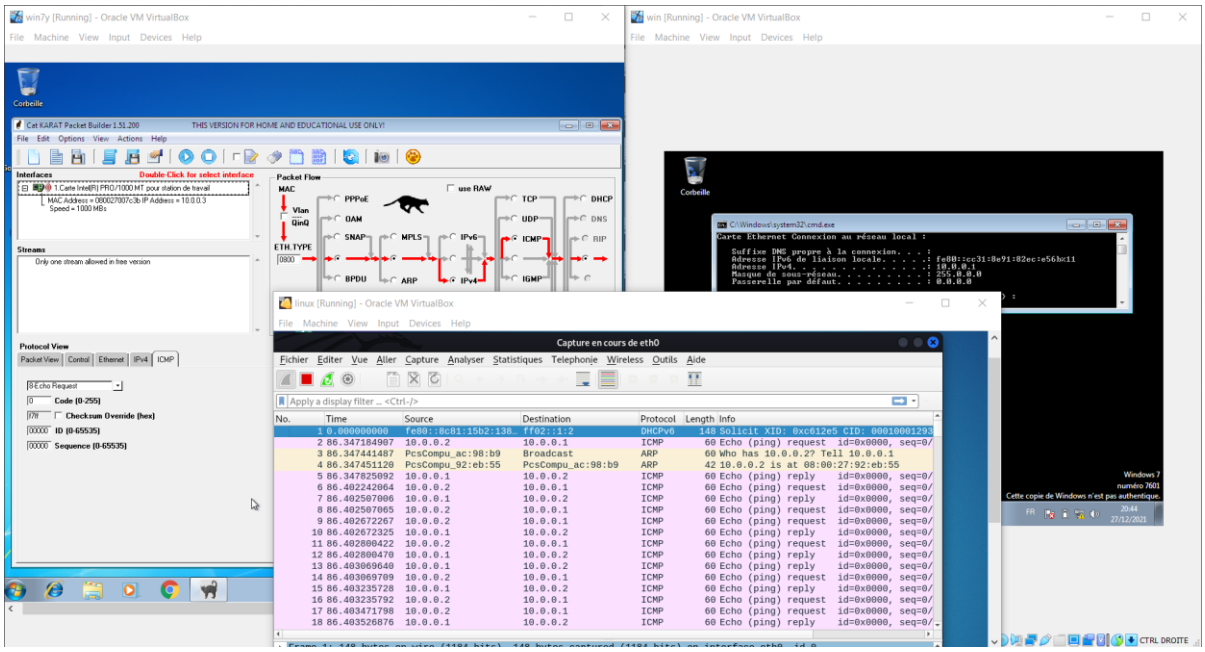
- Etape1 : configure mac adresse



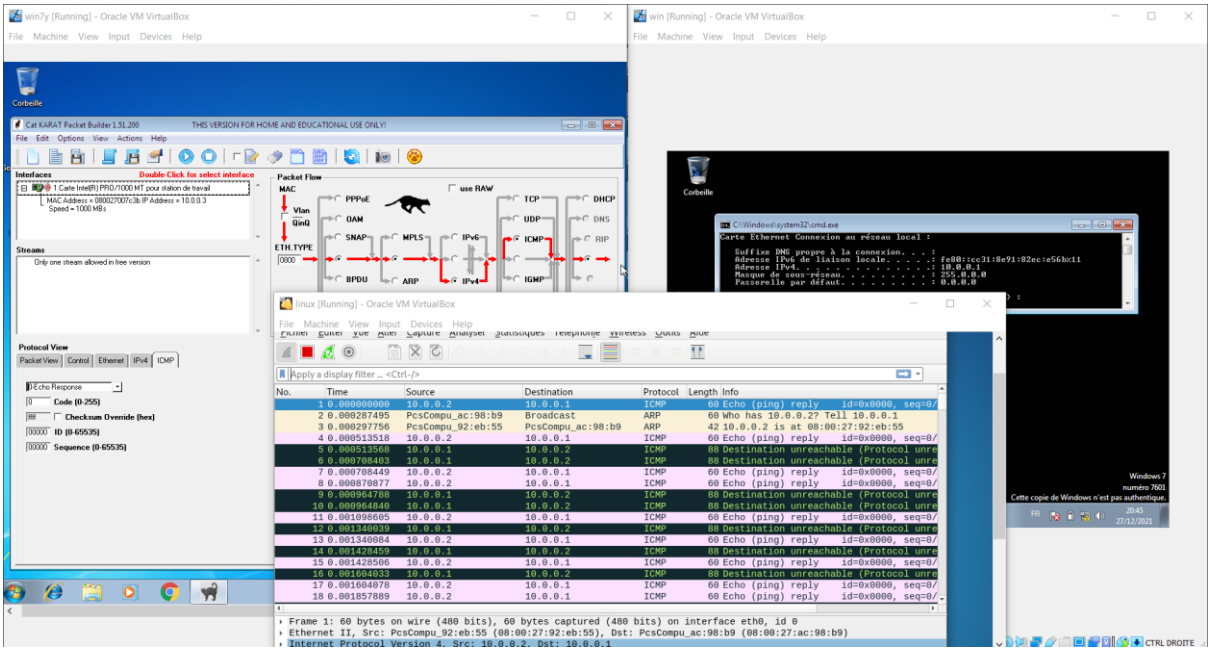
- etape2 : configure adresse IP



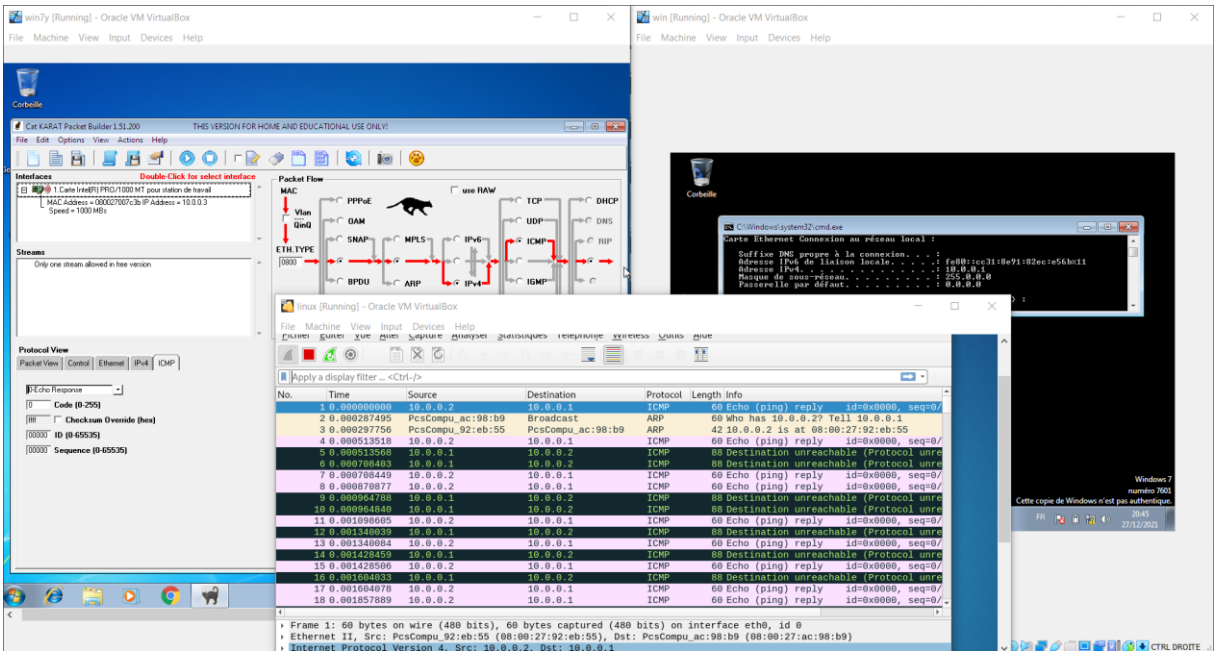
- Etape3 : send echo request



- Etape4 : send echo reply



- Etape 5 : Echo reply last package

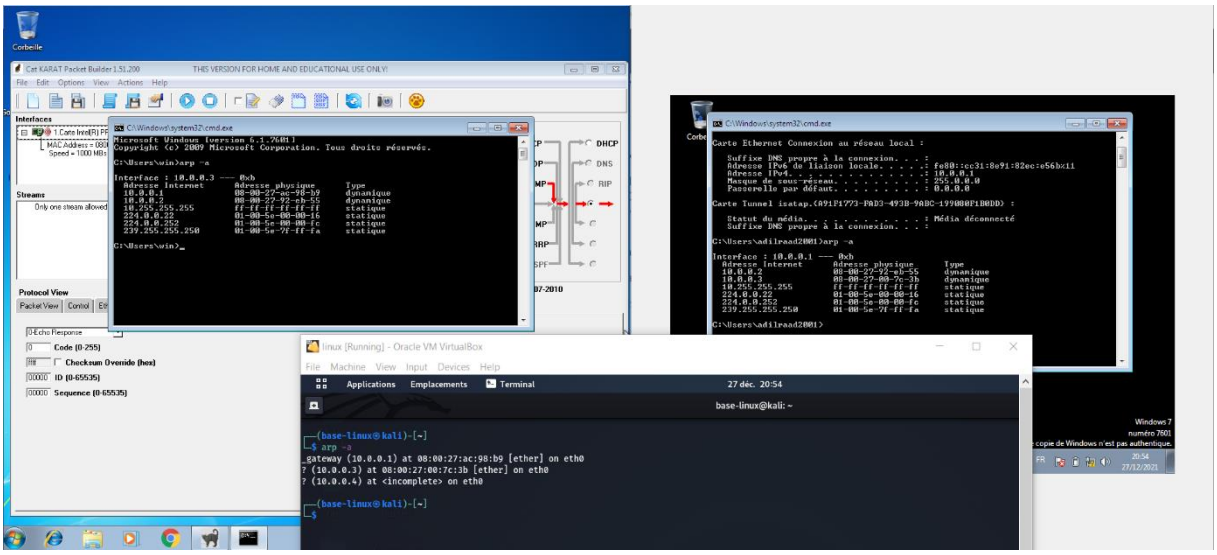


d. Attaque “ARP cache poisoning”

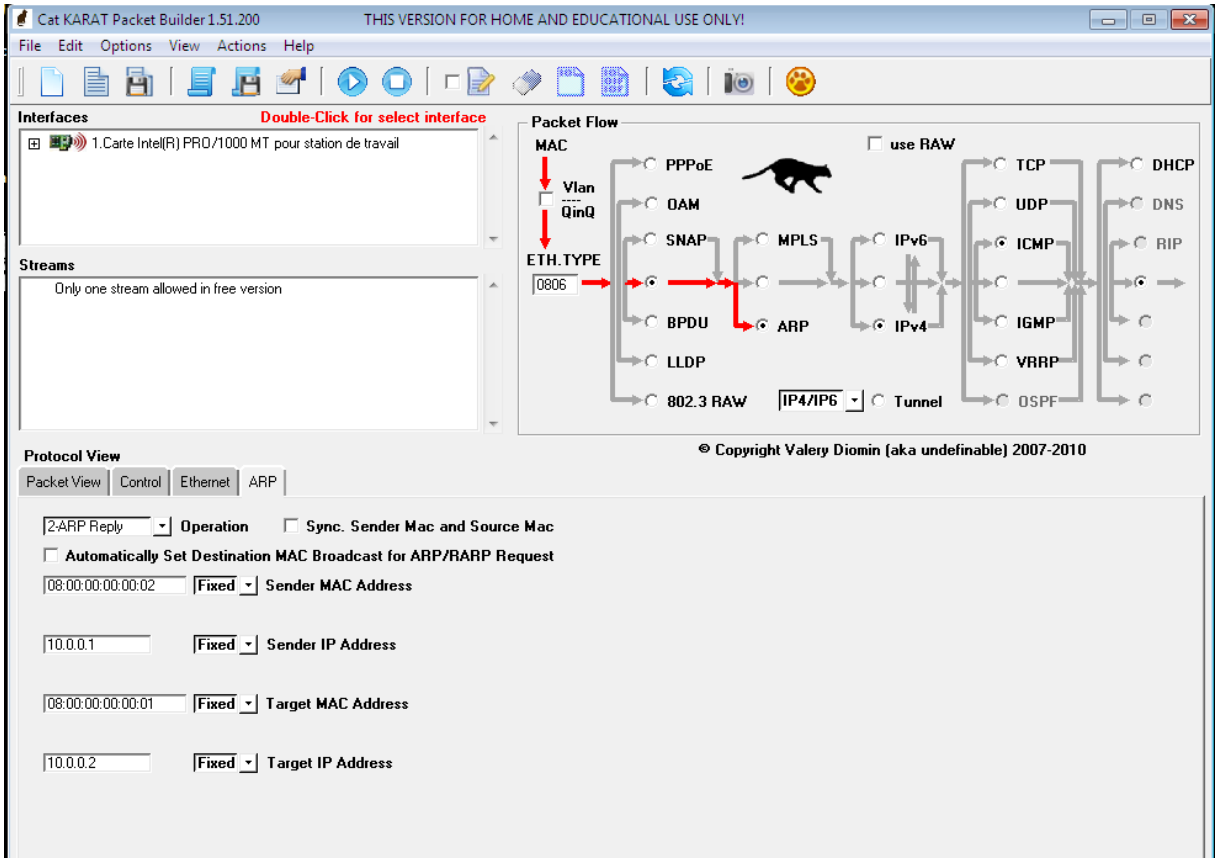
- etape1 :Vérifier la connectivite

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:92:eb:55 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/8 brd 10.255.255.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8053:803f:70e:65c0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(base-linux㉿kali)-[~]
└─$ ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=128 time=0.778 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=128 time=1.00 ms
^C
--- 10.0.0.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.778/0.890/1.003/0.112 ms

┌──(base-linux㉿kali)-[~]
└─$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=128 time=0.869 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=128 time=0.977 ms
```

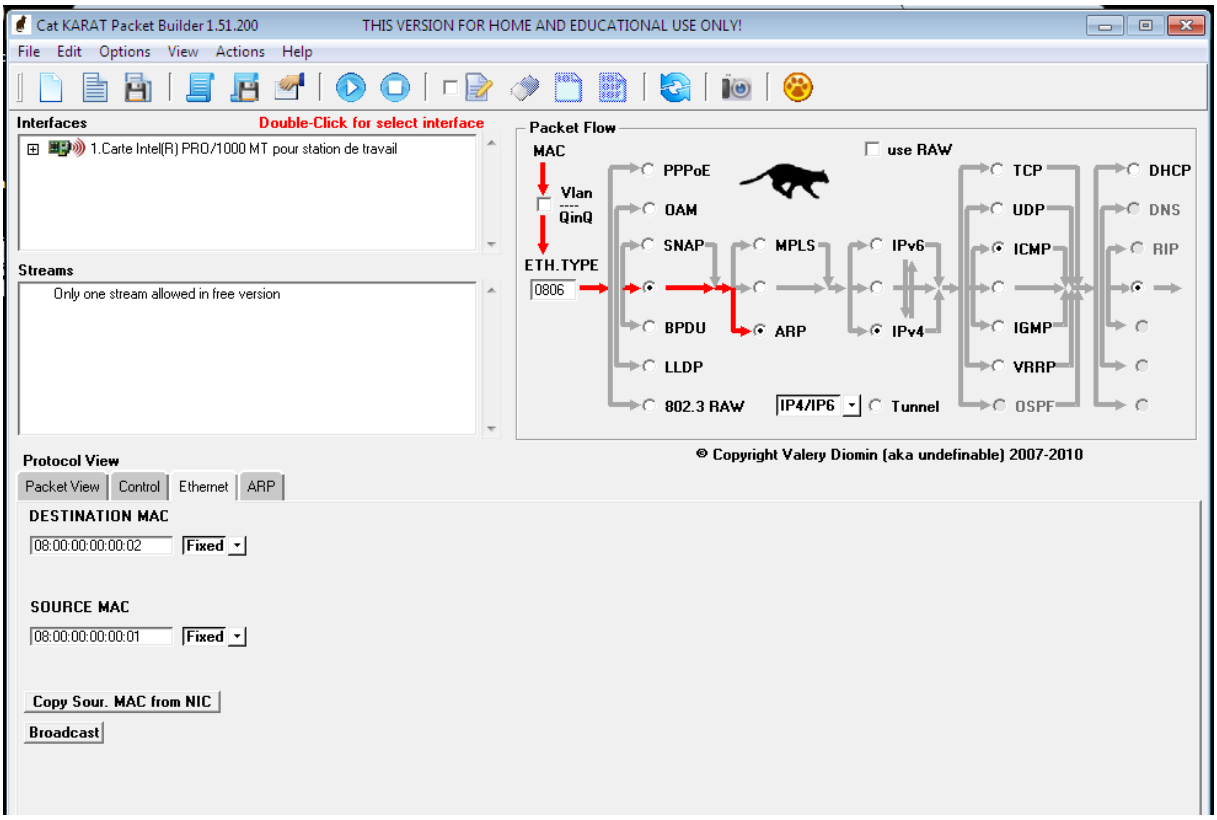
- Etape2 :Arp



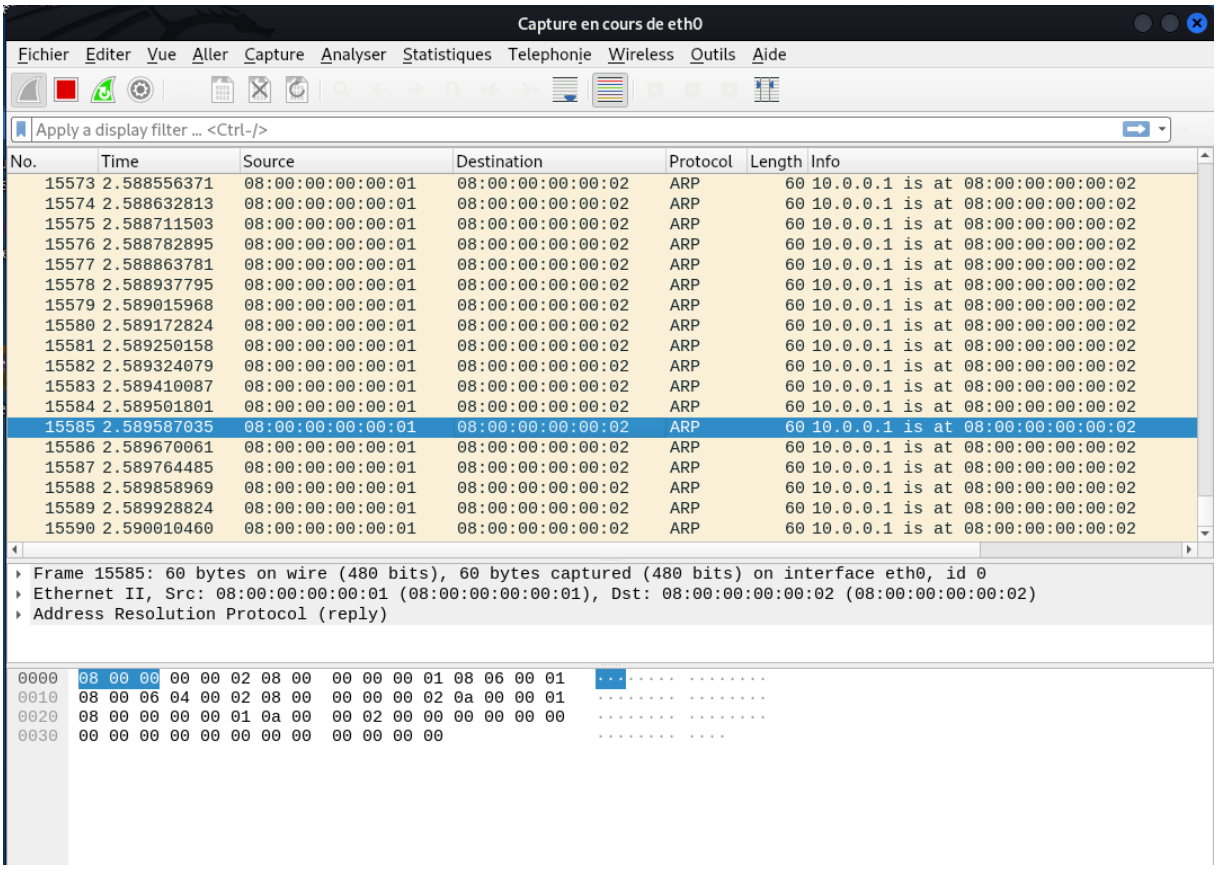
- Etape3



- Etape 4

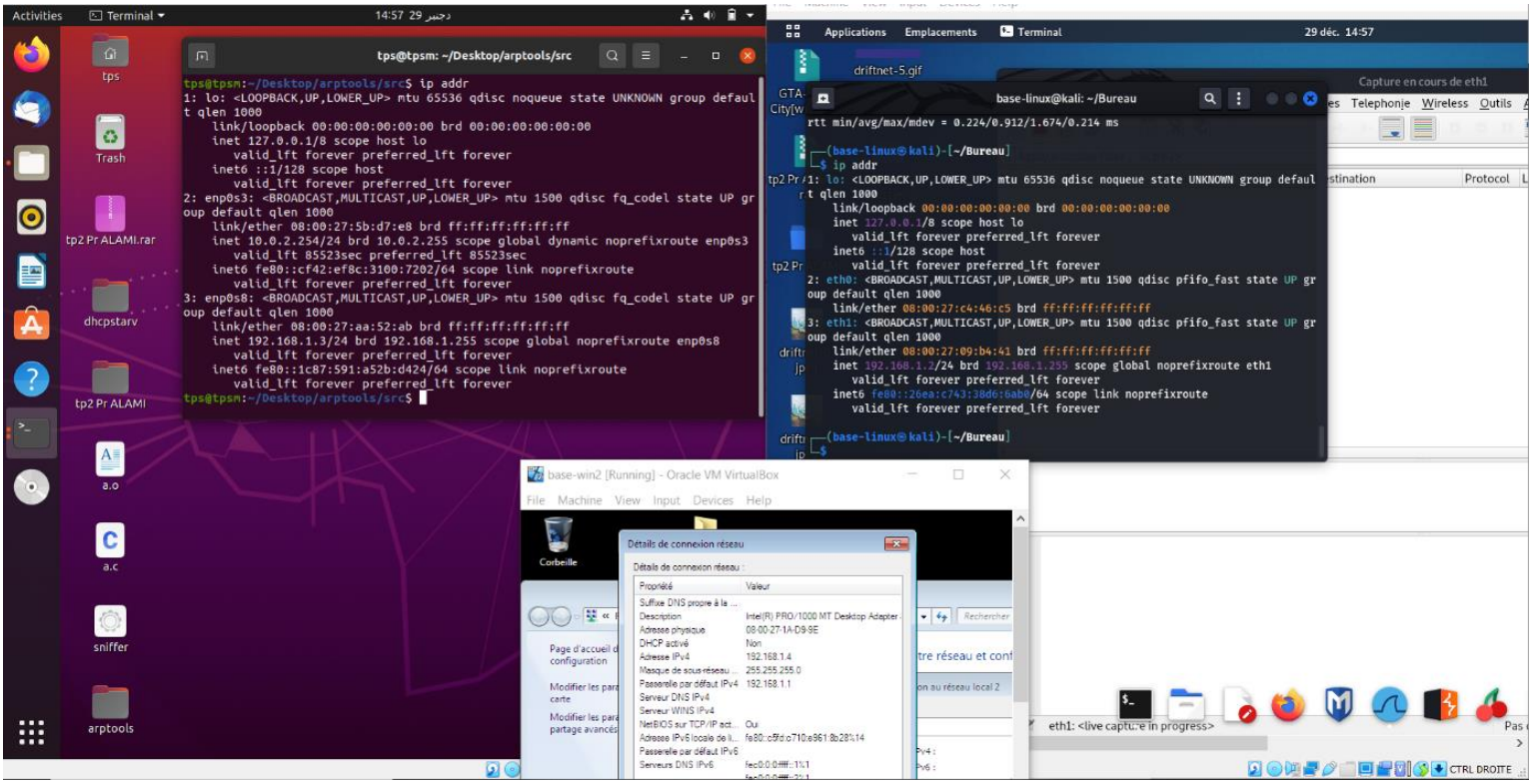

Cat KARAT Packet Builder 1.51.200
THIS VERSION FOR HOME AND EDUCATIONAL USE ONLY!
File Edit Options View Actions Help
Interfaces
Double-Click for select interface
1.Carte Intel(R) PRO/1000 MT pour station de travail
Streams
Only one stream allowed in free version
Packet Flow
use RAW
MAC
Vlan
QinQ
ETH.TYPE
0806
PPPoE
OAM
SNAP
BPDU
LLDP
802.3 RAW
MPLS
ARP
IPv6
IPv4
IP4/IP6
Tunnel
TCP
UDP
ICMP
IGMP
VRRP
OSPF
DHCP
DNS
RIP
© Copyright Valery Diomin (aka undefinable) 2007-2010
Protocol View
Packet View
Control
Ethernet
ARP
DESTINATION MAC
08:00:00:00:00:02
Fixed
SOURCE MAC
08:00:00:00:00:01
Fixed
Copy Sour. MAC from NIC
Broadcast

- Etape 5

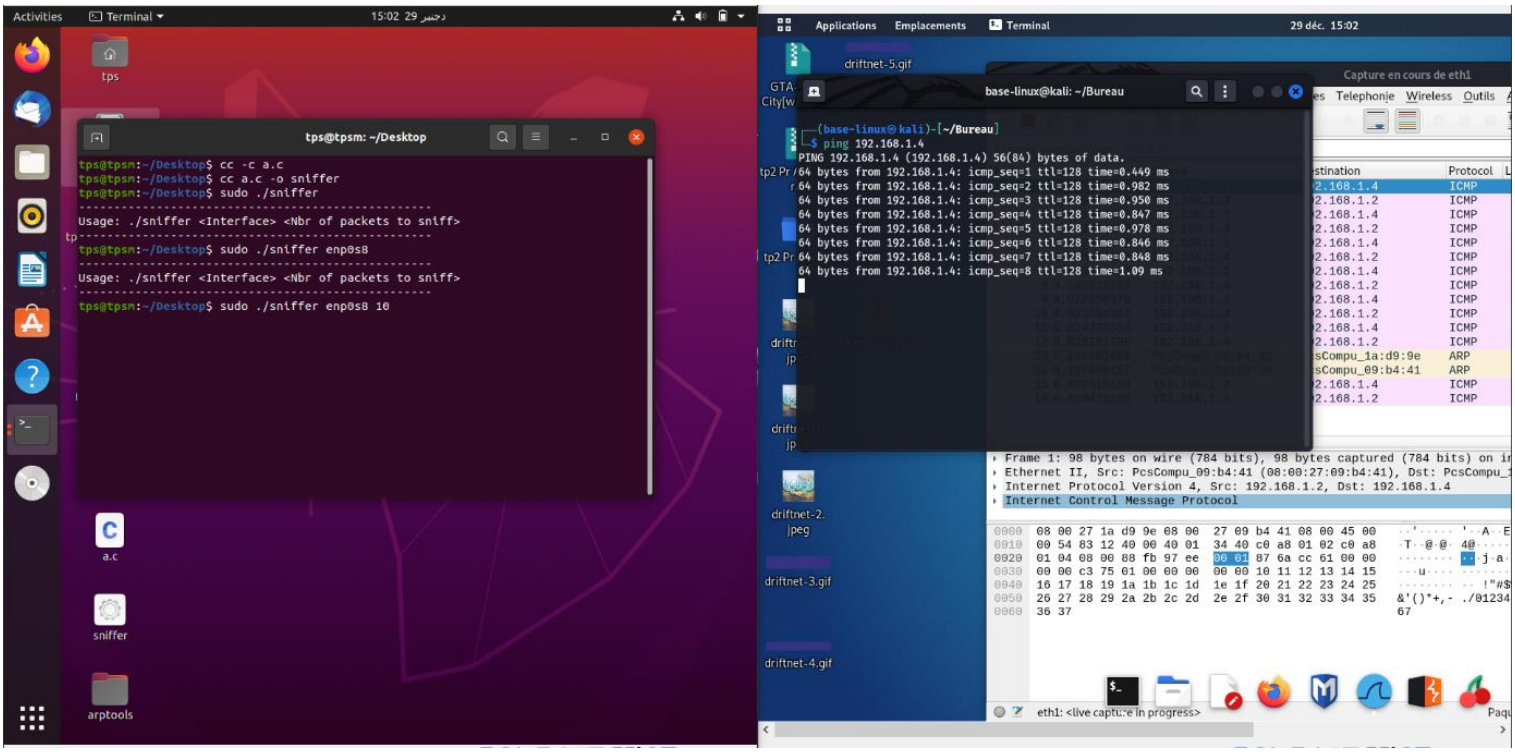

Capture en cours de eth0
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
15573 2.588556371 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15574 2.588632813 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15575 2.588711503 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15576 2.588782895 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15577 2.588863781 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15578 2.588937795 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15579 2.589015968 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15580 2.589172824 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15581 2.589250158 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15582 2.589324079 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15583 2.589410087 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15584 2.589501801 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15585 2.589587035 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15586 2.589670061 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15587 2.589764485 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15588 2.589858969 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15589 2.589928824 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
15590 2.590010460 08:00:00:00:00:01 08:00:00:00:00:02 ARP 60 10.0.0.1 is at 08:00:00:00:00:02
Frame 15585: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: 08:00:00:00:00:01 (08:00:00:00:00:01), Dst: 08:00:00:00:00:02 (08:00:00:00:00:02)
Address Resolution Protocol (reply)
0000 08 00 00 00 00 02 08 00 00 00 00 01 08 06 00 01
0010 08 00 06 04 00 02 08 00 00 00 00 02 0a 00 00 01
0020 08 00 00 00 00 01 0a 00 00 02 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00

e. Attaque « Inondation de la table de commutation »

- Etape1 : adresse IP



- Etape1.2 : test ping

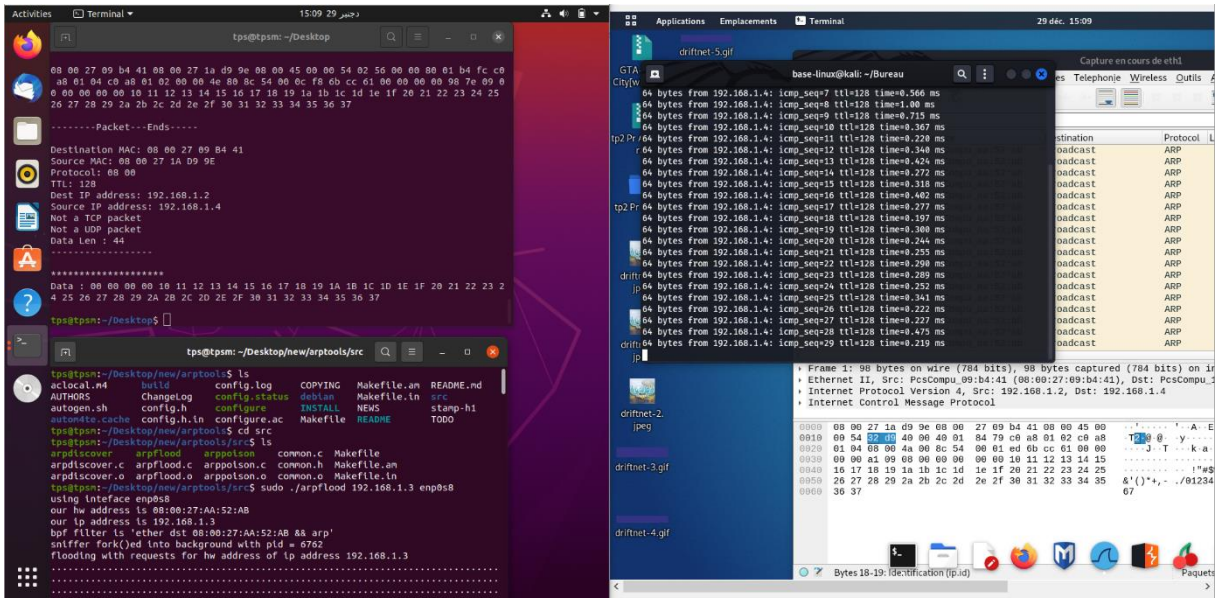


- 2.1 install arpflood

```
tps@tpsm: ~/Desktop/new/arptools
tps@tpsm:~/Desktop/new$ sudo apt-get install libpcap-dev libnet-dev
[sudo] password for tps:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libnet1-dev' instead of 'libnet-dev'
libnet1-dev is already the newest version (1.1.6+dfsg-3.1build1).
libpcap-dev is already the newest version (1.9.1-3).
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2 linux-headers-5.11.0-27-generic
  linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic
  linux-modules-5.11.0-27-generic linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
tps@tpsm:~/Desktop/new$ git clone https://github.com/burghardt/arptools.git
Cloning into 'arptools'...
remote: Enumerating objects: 142, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 142 (delta 0), reused 4 (delta 0), pack-reused 137
Receiving objects: 100% (142/142), 38.96 KiB | 229.00 KiB/s, done.
Resolving deltas: 100% (68/68), done.
tps@tpsm:~/Desktop/new$ sh autogen.sh
sh: 0: Can't open autogen.sh
tps@tpsm:~/Desktop/new$ ls
arptools
tps@tpsm:~/Desktop/new$ cd arptools
tps@tpsm:~/Desktop/new/arptools$ sh autogen.sh
configure.ac:8: installing 'build/compile'
configure.ac:5: installing 'build/install-sh'
configure.ac:5: installing 'build/missing'
Makefile.am: installing './INSTALL'
src/Makefile.am: installing 'build/depcomp'
tps@tpsm:~/Desktop/new/arptools$ sh configure
checking for a BSD-compatible install... /usr/bin/install -c
```

```
tps@tpsm:~/Desktop/new/arptools$ make
make  all-recursive
make[1]: Entering directory '/home/tps/Desktop/new/arptools'
Making all in src
make[2]: Entering directory '/home/tps/Desktop/new/arptools/src'
gcc -DHAVE_CONFIG_H -I. -I..      -g -O2 -D_BSD_SOURCE -D__BSD_SOURCE -D__FAVOR_BSD -DHAVE_NET_ET
HERNET_H  -MT arpdiscover.o -MD -MP -MF .deps/arpdiscover.Tpo -c -o arpdiscover.o arpdiscover.c
In file included from /usr/include/x86_64-linux-gnu/bits/libc-header-start.h:33,
                 from /usr/include/stdio.h:27,
                 from arpdiscover.c:24:
```

- Test ping with arpflood



- Install vsftpd

```
┌──(base-linux㉿kali)-[~/Bureau]
└─$ sudo apt install vsftpd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessair
es :
```

- Add user in vsftpd

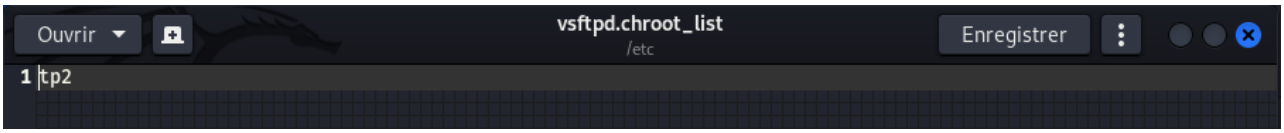
```
┌──(base-linux㉿kali)-[/etc]
└─$ sudo touch /etc/vsftpd.chroot_list                                    1 ×

┌──(base-linux㉿kali)-[/etc]
└─$  adduser tp2
adduser : Seul le superutilisateur est autorisé à ajouter un utilisateur ou un g
roupe au système.

┌──(base-linux㉿kali)-[/etc]
└─$ sudo  adduser tp2                                                     1 ×
Ajout de l'utilisateur « tp2 » ...
Ajout du nouveau groupe « tp2 » (1001) ...
Ajout du nouvel utilisateur « tp2 » (1001) avec le groupe « tp2 » ...
Création du répertoire personnel « /home/tp2 »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for tp2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
```

- Configuration vsftpd

Ouvrir — vsftpd.conf — /etc — Enregistrer

```
1 listen=NO
2 listen_ipv6=YES
3 anonymous_enable=NO
4 local_enable=YES
5 write_enable=YES
6 dirmessage_enable=YES
7 use_localtime=YES
8 xferlog_enable=YES
9 connect_from_port_20=YES
10 chroot_local_user=YES
11 chroot_list_enable=YES
12 chroot_list_file=/etc/vsftpd.chroot_list
13 secure_chroot_dir=/var/run/vsftpd/empty
14 pam_service_name=vsftpd
15 rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
16 rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
17 ssl_enable=NO
```

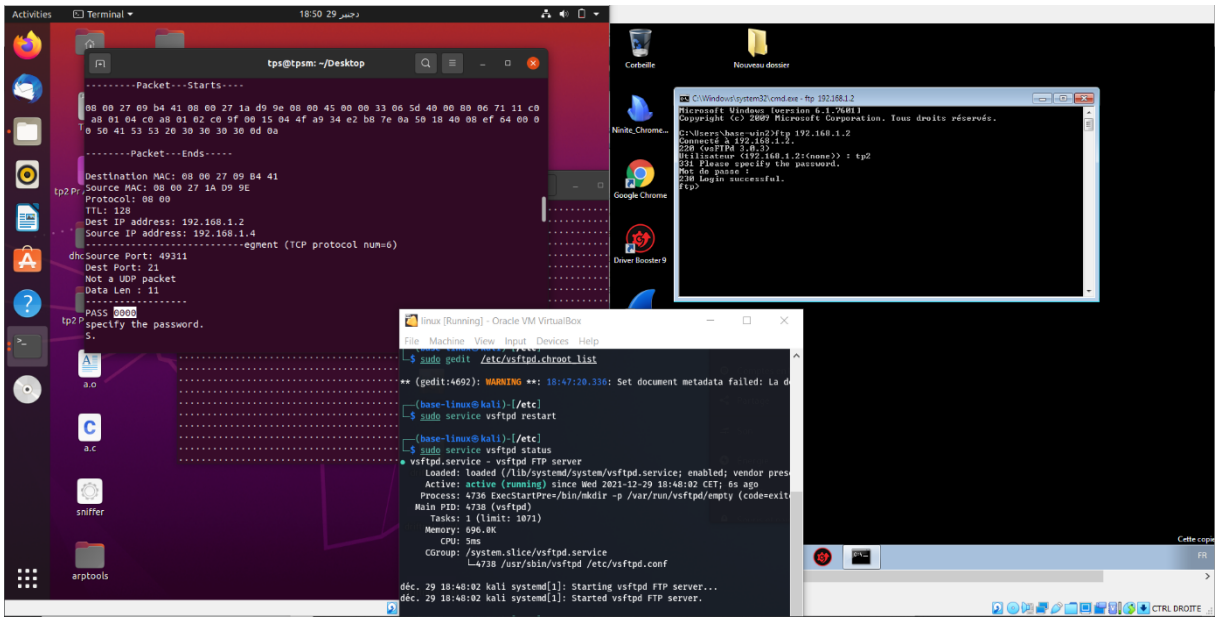
- configuration vsftpd-add user

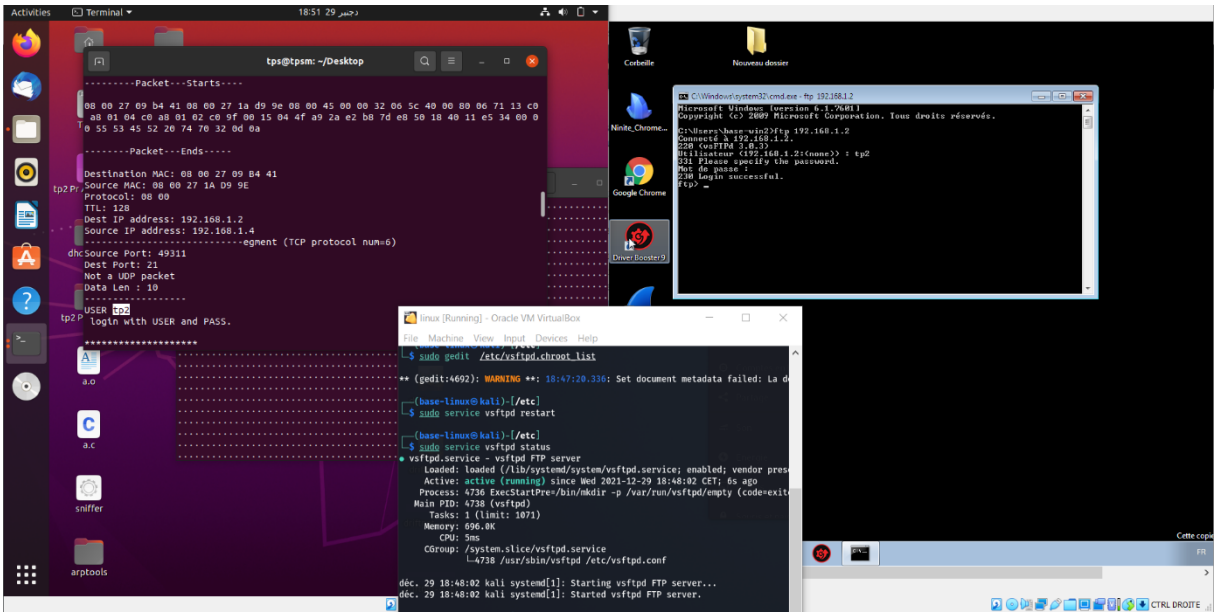


- configuration vsftpd server

```
┌──(base-linux㉿kali)-[/etc]
└─$ sudo gedit vsftpd.conf

** (gedit:4635): WARNING **: 18:46:26.341: Set document metadata failed: La définition de l'attribut metadata::gedit-spell-language n'est pas prise en charge

** (gedit:4635): WARNING **: 18:46:26.343: Set document metadata failed: La définition de l'attribut metadata::gedit-encoding n'est pas prise en charge

** (gedit:4635): WARNING **: 18:46:38.841: Set document metadata failed: La définition de l'attribut metadata::gedit-position n'est pas prise en charge

┌──(base-linux㉿kali)-[/etc]
└─$ sudo touch  /etc/vsftpd.chroot_list

┌──(base-linux㉿kali)-[/etc]
└─$ sudo gedit  /etc/vsftpd.chroot_list

** (gedit:4692): WARNING **: 18:47:20.336: Set document metadata failed: La définition de l'attribut metadata::gedit-position n'est pas prise en charge

┌──(base-linux㉿kali)-[/etc]
└─$ sudo service vsftpd restart

┌──(base-linux㉿kali)-[/etc]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
     Active: active (running) since Wed 2021-12-29 18:48:02 CET; 6s ago
    Process: 4736 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 4738 (vsftpd)
      Tasks: 1 (limit: 1071)
     Memory: 696.0K
        CPU: 5ms
     CGroup: /system.slice/vsftpd.service
             └─4738 /usr/sbin/vsftpd /etc/vsftpd.conf

déc. 29 18:48:02 kali systemd[1]: Starting vsftpd FTP server...
déc. 29 18:48:02 kali systemd[1]: Started vsftpd FTP server.
```

- Retrouver sur la troisième machine les trames correspondant




Activities
Terminal
tps@tpsm: ~/Desktop
--------Packet---Starts----
08 00 27 09 b4 41 08 00 27 1a d9 9e 08 00 45 00 00 32 06 5c 40 00 80 06 71 13 c0 a8 01 04 c0 a8 01 02 c0 9f 00 15 04 4f a9 2a e2 b8 7d e8 50 18 40 11 e5 34 00 00 53 45 52 20 74 70 32 0d 0a
--------Packet---Ends-----
Destination MAC: 08 00 27 09 B4 41
Source MAC: 08 00 27 1A D9 9E
Protocol: 08 00
TTL: 128
Dest IP address: 192.168.1.2
Source IP address: 192.168.1.4
Source Port: 49311
Dest Port: 21
Not a UDP packet
Data Len : 10
USER tp2
login with USER and PASS.
****
a.o
a.c
sniffer
arptools
Corbeille
Nouveau dossier
Ninite_Chrome...
Google Chrome
Driver Booster 9
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\base-win2>ftp 192.168.1.2
Connecté à 192.168.1.2.
220 (vsFTPd 3.0.3)
Utilisateur (192.168.1.2:(none)) : tp2
331 Please specify the password.
Mot de passe :
230 Login successful.
ftp>
linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
└─$ sudo gedit /etc/vsftpd.chroot_list
** (gedit:4692): WARNING **: 18:47:20.336: Set document metadata failed: La d
┌──(base-linux㉿kali)-[/etc]
└─$ sudo service vsftpd restart
┌──(base-linux㉿kali)-[/etc]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor prese
Active: active (running) since Wed 2021-12-29 18:48:02 CET; 6s ago
Process: 4736 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exite
Main PID: 4738 (vsftpd)
Tasks: 1 (limit: 1071)
Memory: 696.0K
CPU: 5ms
CGroup: /system.slice/vsftpd.service
└─4738 /usr/sbin/vsftpd /etc/vsftpd.conf
déc. 29 18:48:02 kali systemd[1]: Starting vsftpd FTP server...
déc. 29 18:48:02 kali systemd[1]: Started vsftpd FTP server.
Cette copie
CTRL DROITE