INF4420A
Sécurité informatique

Rapport de TP3

Présenté à
Corentin Bresteau

Par
Anthony Abboud (1681547)
Et
Riyad Lahmer (1917641)

5 Avril 2018

Question 1 - Découverte du réseau [/1.5]

a)

Poste admin : 192.168.212.124/24
ports : 135, 445,1026,139

Poste Internet : 192.168.214.128/24 et 123.45.67.128
port : aucun port

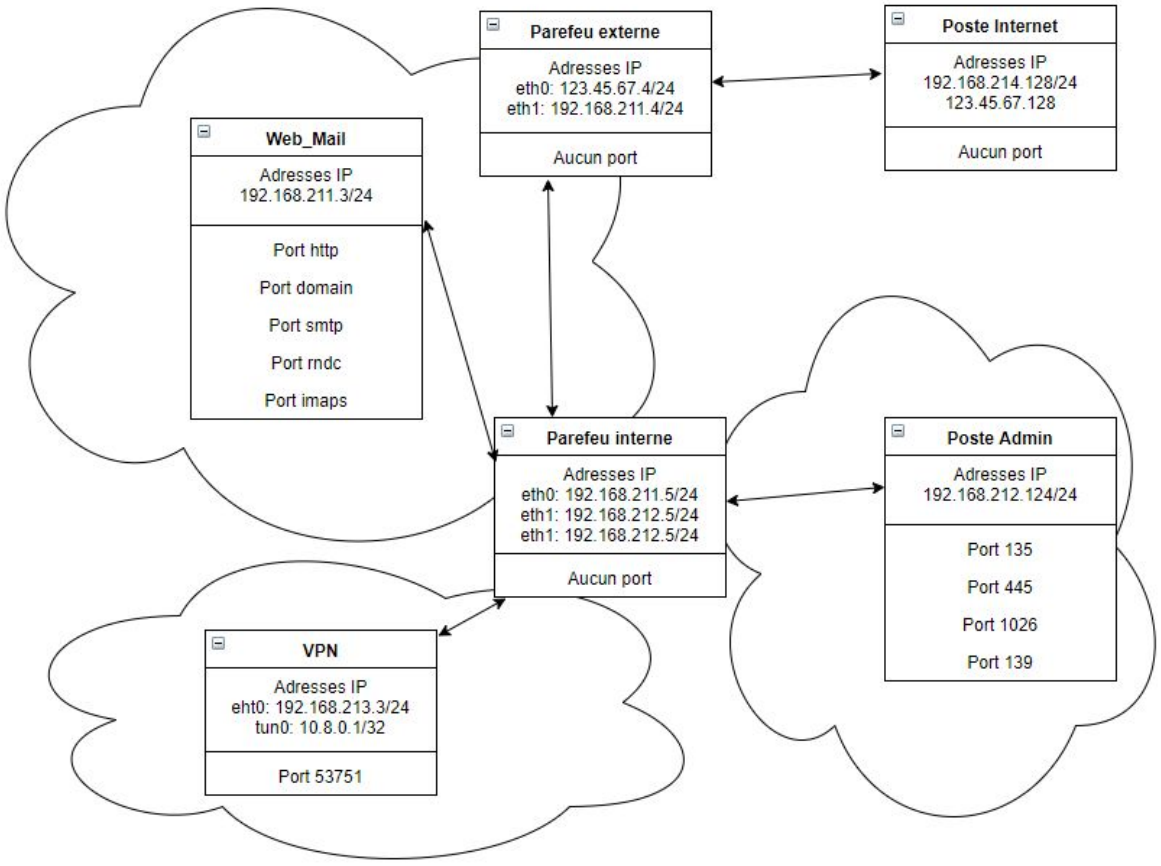
VPN : eht0 : 192.168.213.3/24
tun0 : 10.8.0.1/32
port : 53751

Web_Mail : 192.168.211.3/24
port : http, domain, smtp, rndc, imaps,

Parefeu externe :eth0 : 123.45.67.4/24
eth1 : 192.168.211.4/24
port : aucun port

parefeu interne : eth0: 192.168.211.5/24
eth1: 192.168.212.5/24
eth2: 192.168.213.5/24
port : aucun port

Le tout est représenté par le schéma retrouvé à la prochaine page.



b)

```
joe@localhost ~ $ sudo ifconfig eth0 123.45.67.128
joe@localhost ~ $ sudo ifconfig
Password:
Sorry, try again.
Password:
eth0      Link encap:Ethernet  HWaddr 00:0c:29:75:74:03
          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)
```

c)

C’est de la traduction d’adresse réseau, c’est-à-dire qu’il fait correspondre des adresses IP à d’autres. En d’autres termes, le NAT modifiera les informations d’adresse réseau contenues dans l’en-tête du paquet IP. Ainsi, il est possible de rassembler plusieurs adresses d’un réseau privé et de les relier à une seule adresse externe publique visible sur tout l’Internet.

```
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
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
```

Question 2 - Nmap [/2]

a)
secsi.com et mail.secsi.com possedent la meme adresse IP : 123.45.67.4

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

Name:   secsi.com
Address: 123.45.67.4

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

Name:   mail.secsi.com
Address: 123.45.67.4
```

b)

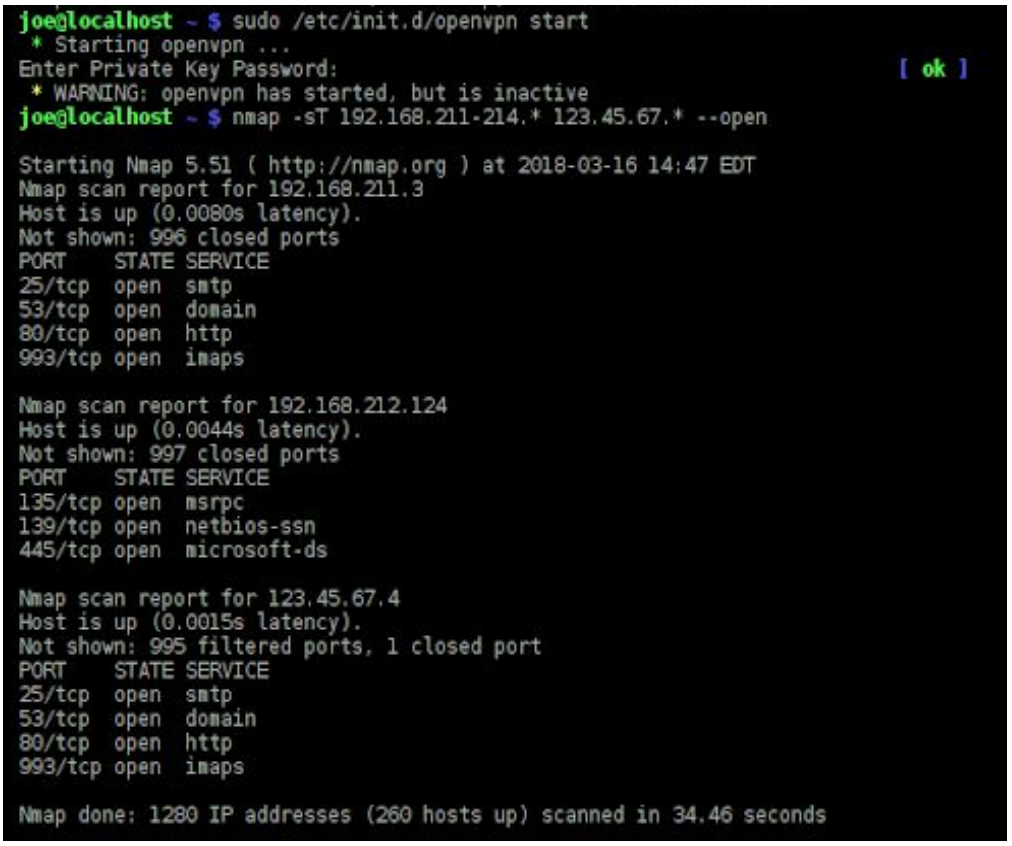
```
joe@localhost ~ $ nmap -sT 192.168.211-214.* 123.45.67.* --open

Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-16 14:46 EDT
Nmap scan report for 123.45.67.4
Host is up (0.0015s 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 19.59 seconds
```

-sT : scan technique connect

--open : only show open ports (or possibly open)

Donc, cette commande affiche tous les ports ouverts servant à la communication entre les adresses 192.168.211-214.* et 123.45.67.*.

c)



Un VPN est un service qui nous permet de créer une connexion sécurisée (un tunnel) vers un autre réseau sur l'Internet. On a donc un nouveau résultat avec la même commande nmap utilisée précédemment, avec des informations sur les machines Web_mail et Poste Admin

d)

Le port rndc n'est pas affiché dans la commande nmap pour la machine Web_mail.
Le port 1026 n'est pas affiché dans la commande nmap pour la machine Poste Admin.
La raison pour laquelle ces ports n'apparaissent pas dans le résultat de la commande, est parce que nmap dans sa configuration par défaut ne scanne que 1000 ports (les plus utilisés). Pour scanner tous les ports d'une machine, il faut utiliser l'option *-p 1-65535*.

e)

Dans le cas du NAT, la vraie adresse des machines à l'intérieur du réseau n'est pas visible car il y a translation, de même que leur ports. Elle sont donc protégé contre le balayage de port.

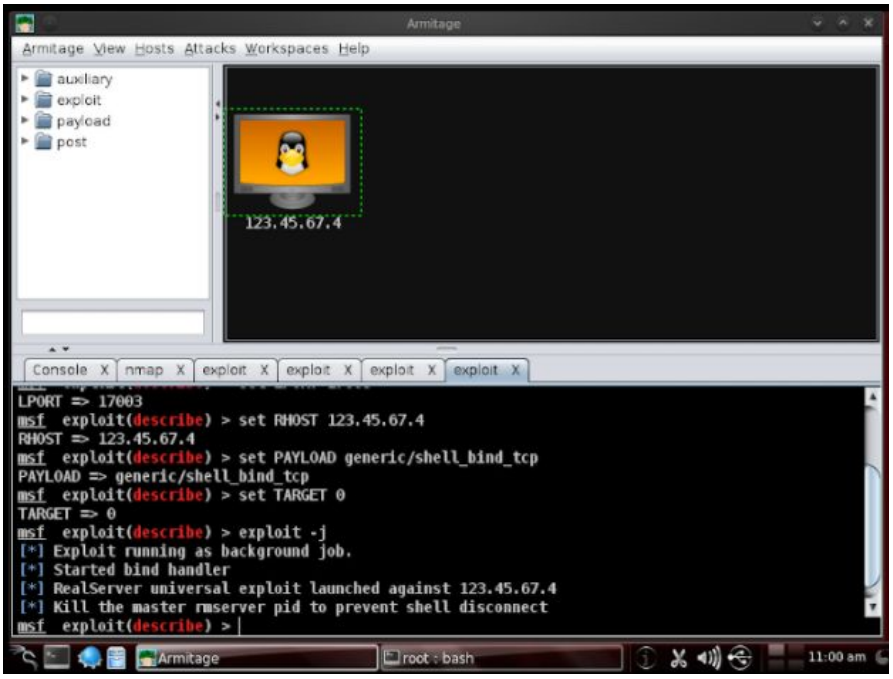
f)

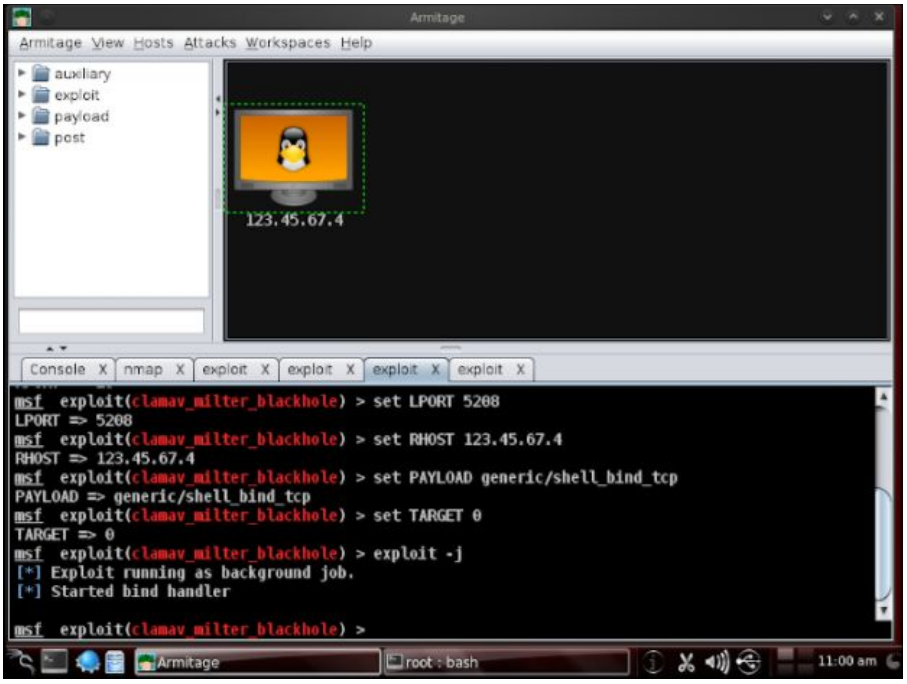
Pour le premier nmap, on met un IDS au niveau du parefeu externe. Pour le second nmap, on peux en placer 2, un au niveau du parefeu externe, et un au niveau du VPN.

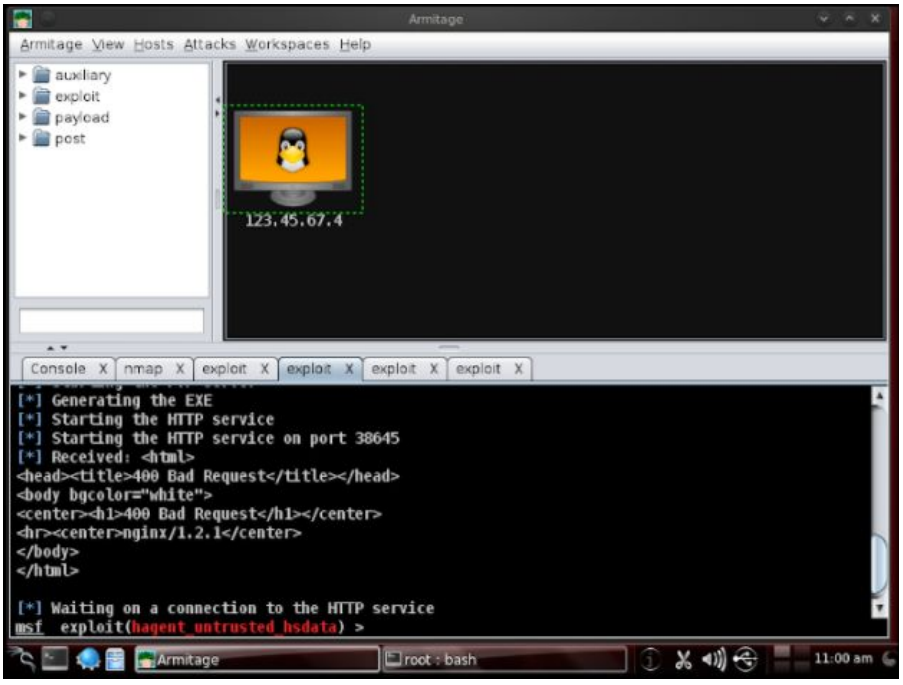
Question 3 - L'email de trop

Utilisation d'Armitage

a)





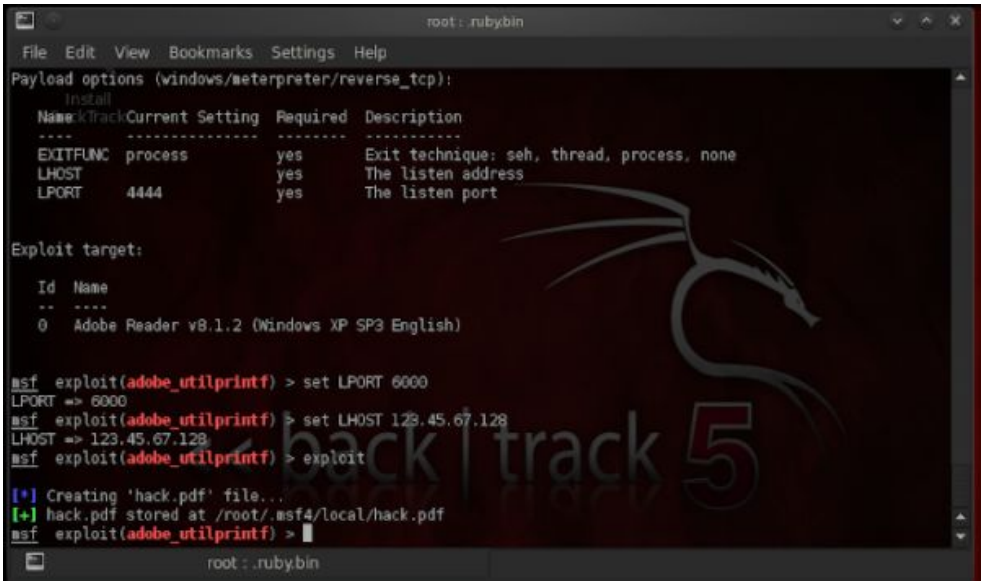


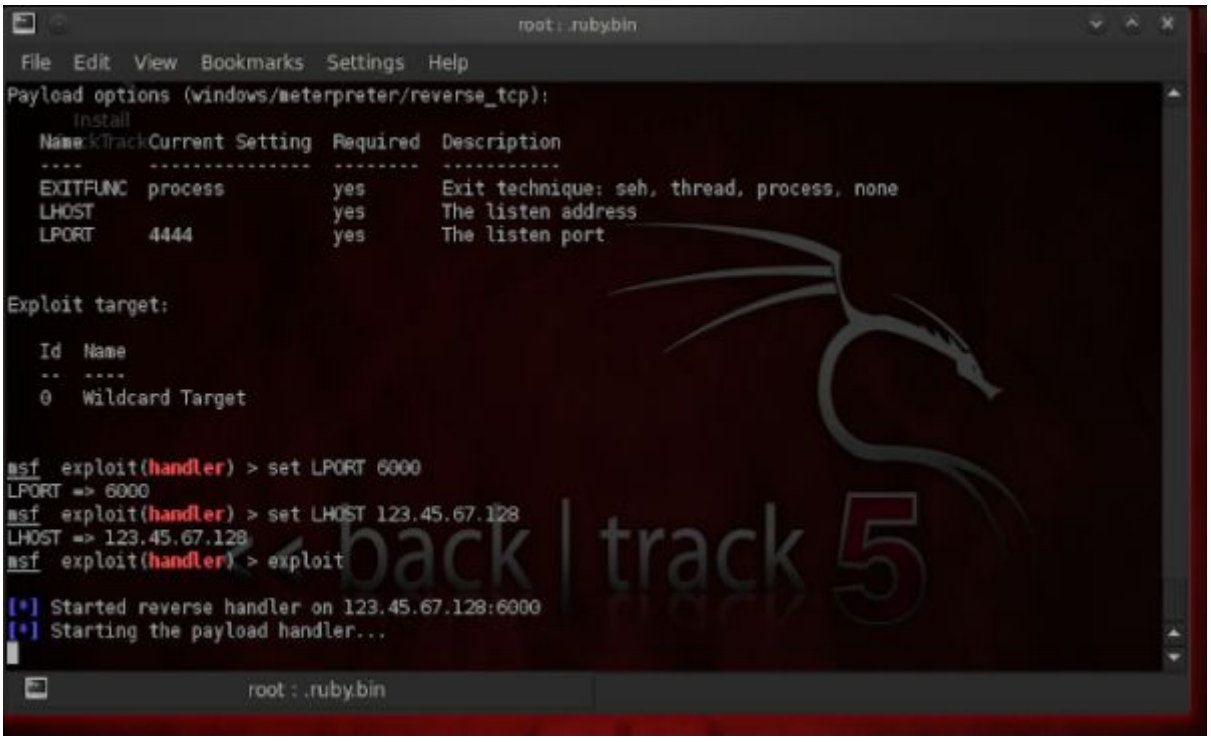
Comme on peut le voir sur chacune des captures d'écran, aucun exploit ne semble être possible.

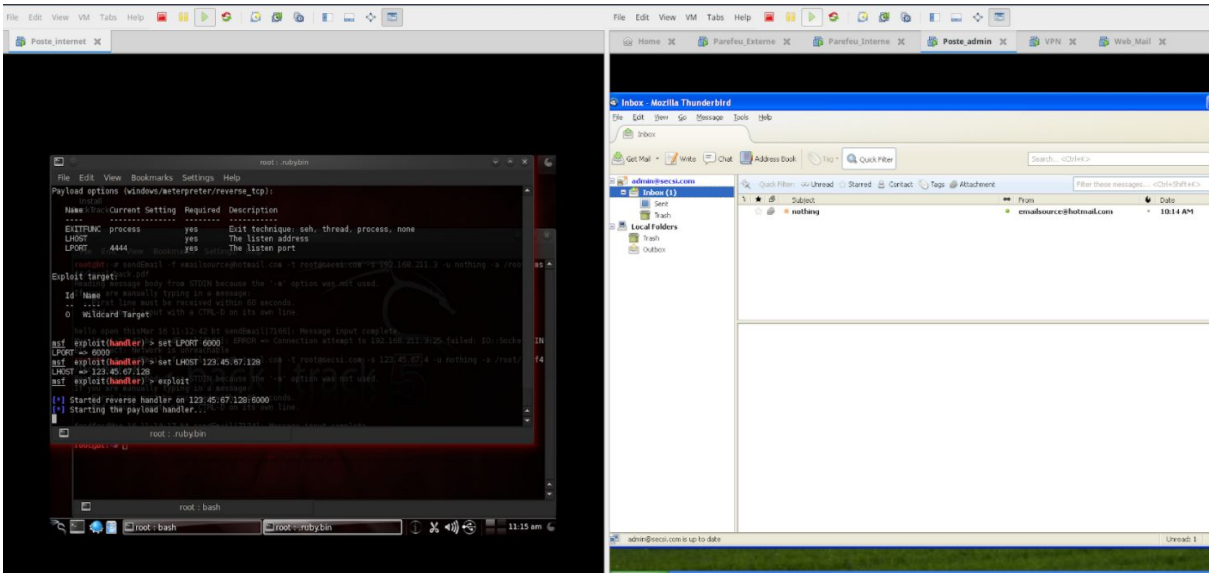
<u>Utilisation de msfconsole</u>

b)
Le bind_tcp ouvre un port sur la machine victime et attend qu'une connexion soit initialisée depuis l'attaquant. Alors que dans le cas du reverse_tcp, la connexion est initalisé du coté de la victime. Dans le cas du bind_tcp, si la machine n'est pas joignable pour une quelconque raison, il est impossible d'établir une connexion.

c)

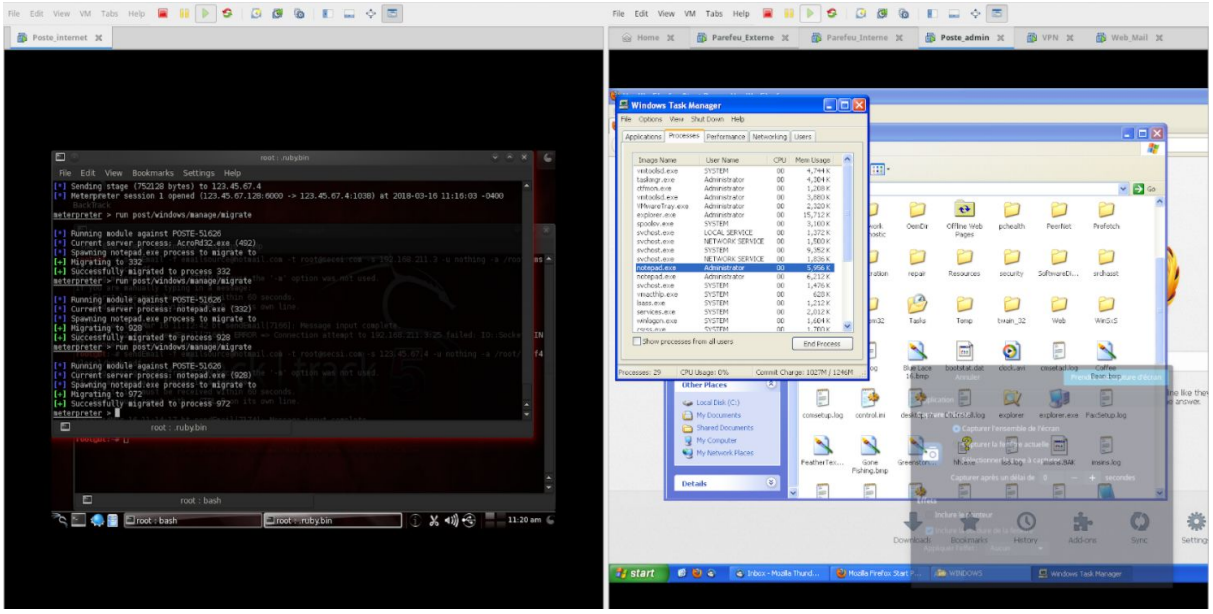






Le pdf ne répond pas sur le poste admin.
Sur msfconsole, une session meterpreter est crée, on a accès à la machine victime via un shell Windows.

d)



Le pdf s’est fermé, un processus notepad.exe s’est activé

e)

On aura beau ajouté des couches de sécurité dans notre réseaux et sur nos machines, si l’utilisateur final n’est pas sensibilisé aux risques présent sur Internet, il peut commettre une erreur (en ouvrant une pièce jointe infecté par exemple) et mettre en péril ses données ou celle de l’entreprise.