

**INF4420A - Sécurité informatique**

**Automne 2018**

**TP  No. [3]**

**Groupe [2]**

**[1972528] – [Manuel Rodriguez]**

**[1748125] – [David Tremblay]**

**Soumis à : Mikaela Stéphanie Ngamboe Mvogo**

**[26-11-2018]**

**Question 1 – Découverte du réseau**

a)

Nous utilisons la commande **ifconfig** sur les machines Linux connectées sur le root pour obtenir les adresses IP. Si l'utilisateur n’est pas root, nous utilisons la commande **/sbin/ifconfig**. Dans les 2 cas, nous utilisons la commande **netstat -l** pour obtenir la liste des ports ouverts. Pour les machines Windows, nous utilisons plutôt les commandes **ipconfig** et **netstat -a** sur un terminal powershell.

**Poste\_internet:**

Adresse IP:

* eth0: 123.45.67.128

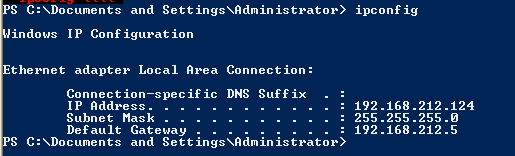
Port:

Aucun port ouvert

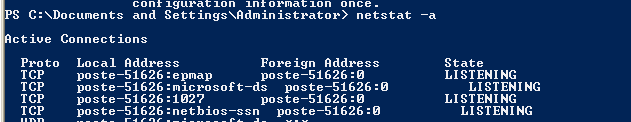
**Poste\_admin:**

Adresse IP:

* eth0: 192.168.214.124



Port:



**Web\_Mail:**

Adresse IP:

* eth0: 192.168.211.3

Port:



**Parefeu\_Interne:**

Adresse IP:

* eth0: 192.168.211.5
* eth1: 192.168.212.5
* eth2: 192.168.213.5

Port:

Aucun port ouvert

**Parefeu\_Externe:**

Adresse IP:

* eth0: 123.45.67.4
* eth1: 192.168.211.4

Port:

Aucun port ouvert

**VPN:**

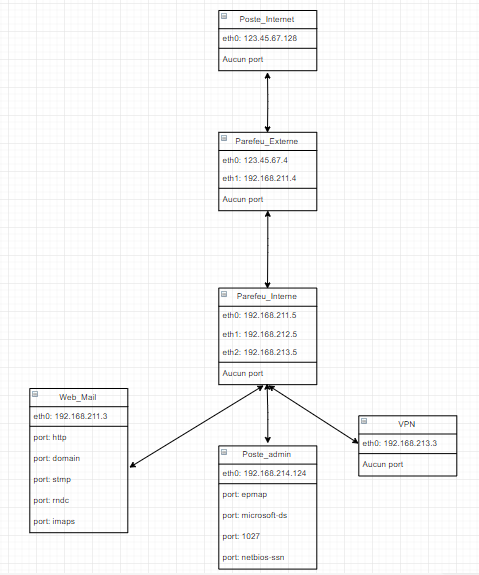
Adresse IP:

* eth0: 192.168.213.3

Port:

Aucun port ouvert

Voici un schéma qui montre l’ensemble du réseau:



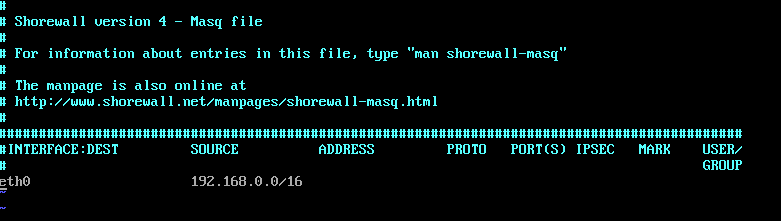
b)

Notre adresse IP est déjà correcte comme tel qu’illustré ci-dessous.

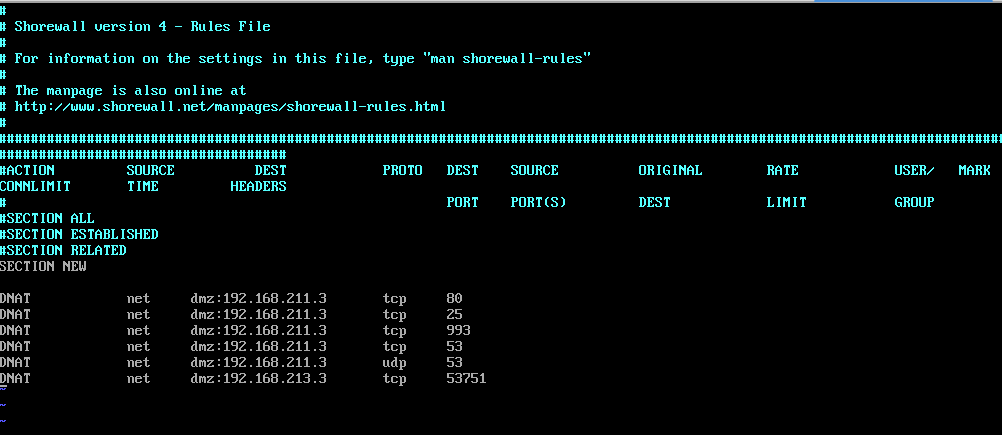


c)

Fichier masq:



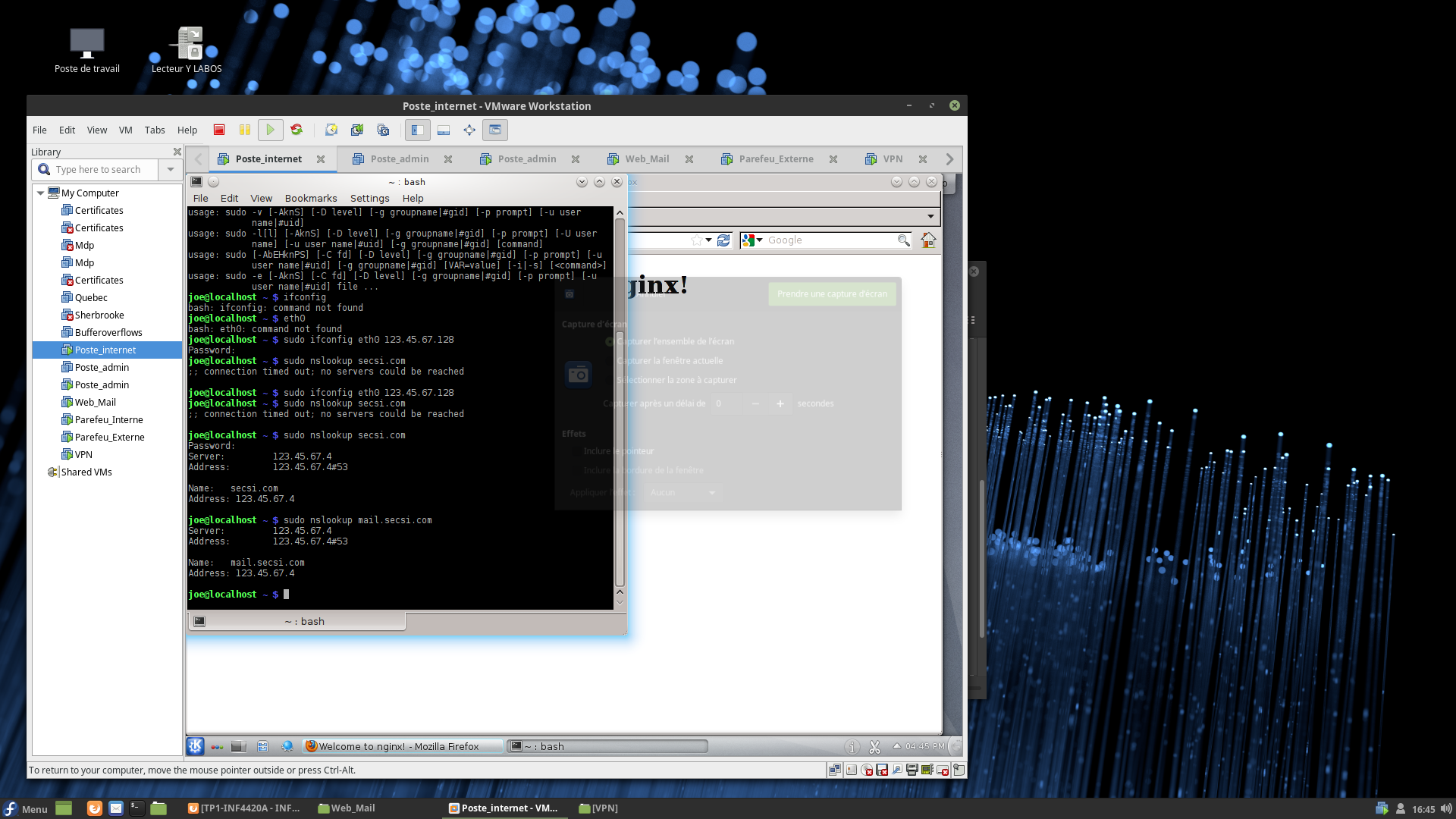
Fichier rules:



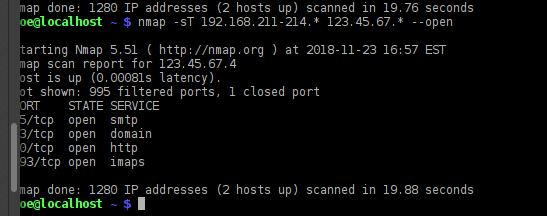
Un service NAT (Network Address Translation) est un service qui fait correspondre des adresses IP à d’autres adresses IP. L’utilisation la plus répandue est de pouvoir avoir qu’une seule adresse externe publique visible sur Internet mais plusieurs adresses IP interne. Dans le cas du TP, la compagnie *Secsi* n’a qu’une seule adresse IP externe publique mais les VMs ont des adresses IP différentes qui seront traduite à l’aide du service NAT lorsque ces machines veulent communiquer avec le Web.

**Question 2 – Nmap**

1. En utilisant *nslookup* on remarque que l’adresse IP des domaines secsi.com et mail.secsi.com est la même. Cette adresse IP est **123.45.67.4**.



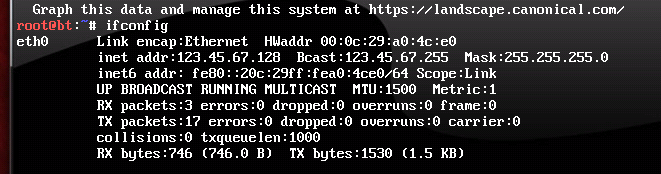
1. Nmap (Network Mapper, en anglais) est une commande qui effectue un audit réseau et un mappage. D'autre part, --open affiche seulement les ports ouverts et -sT est un type d’audit par connexion. Donc, cette commande affiche les ports ouverts entre 192.168.211-214.\* et 123.45.67.\*.



1. Un VPN (Virtual Private Network, en anglais) est un service qui nous permet de créer une connexion sécurisée pour nous connecter à Internet en utilisant un autre réseau que le nôtre, simulant un tunnel. On a utilisé la même commande qu’avant mais maintenant on peut voir l’info des machines Web\_mail et Poste\_Admin.
2. La différence entre le schéma de réseau qu’on a fait à la première question et les informations obtenues avec nmap est que les ports rndc et 1026 ne sont pas affichés par nmap pour les machines Web\_mail et Poste\_Admin. La raison est que nmap ne scanne que 1000 ports par défaut, donc si on veut avoir le schéma complet, il faudrait ajouter à la commande combien de ports on veut faire au balayage.
3. L’avantage du NAT est que la vraie adresse des machines n’est pas visible parce qu’il y a translation et il en va de même pour les ports. Ce n’est pas le cas pour un balayage de ports.
4. Dans le premier cas d’utilisation il suffit de placer un IDS pour détecter le balayage de ports au niveau du pare-feu externe parce que c’est le seul point d'entrée. Pour le deuxième cas d’utilisation il faudrait placer un IDS au niveau du pare-feu externe et au niveau du VPN.

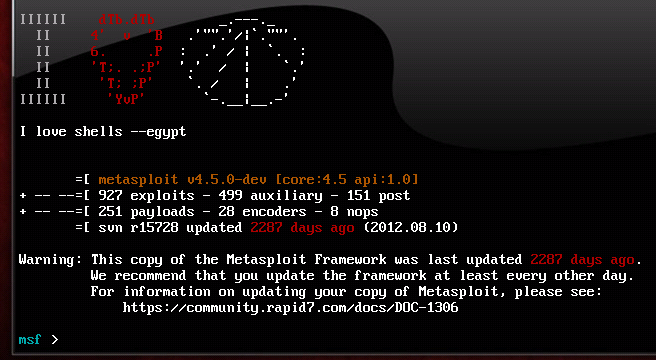
**Question 3 – L’email de trop**

Nous pouvons constater que notre adresse IP ne nécessite pas d’être changée.



a)

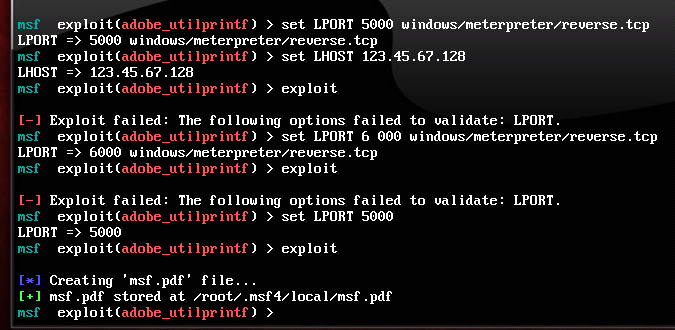
On a lancé Armitage mais aucun exploit semble être possible. Nous lançons maintenant *msfconsole*.



b)

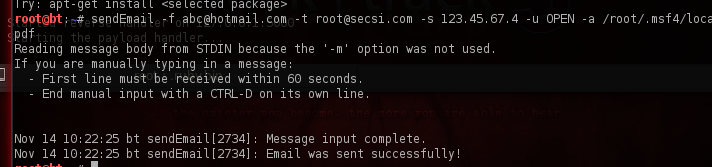
Utiliser le reverse\_tcp permet d’initialiser une connexion du côté de la machine qu’on tente d’attaquer. Au contraire, utiliser bind\_tcp nécessite une initialisation de la connexion du côté de l’attaquant. Bind\_tcp ouvre également un port sur la machine victime.

Nous lançons les exploits *adobe\_utilprintf*  ainsi que *handler*.



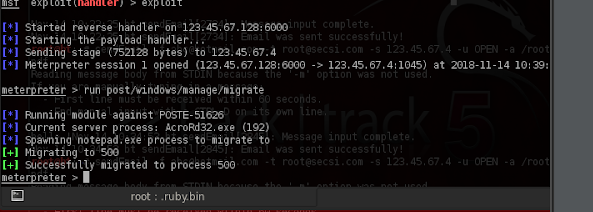


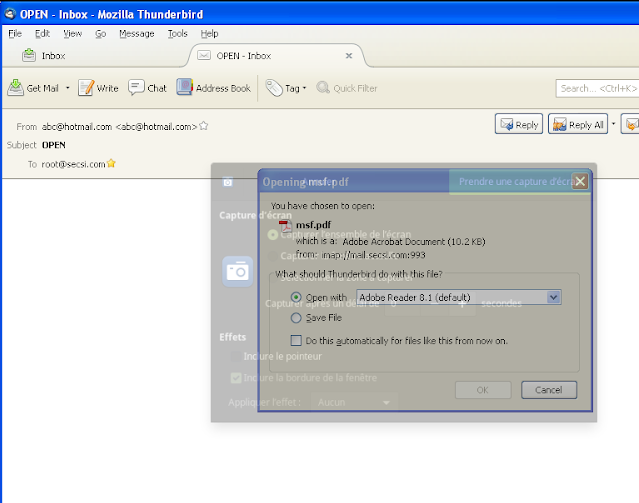
Puis, nous envoyons un courriel contenant notr pdf créé précédemment.



c)

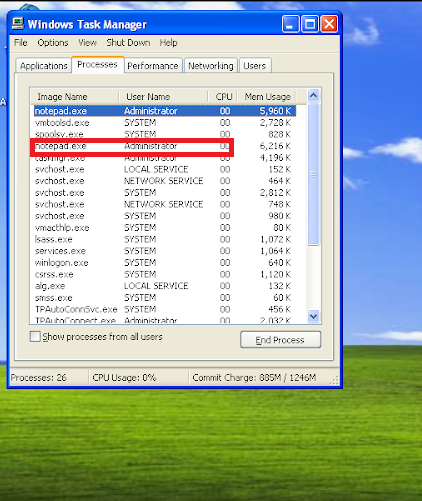
Le poste internet fige lorsqu’on ouvre le fichier pdf et une session meterpreter s’ouvre sur notre msfconsole.





d)

On ouvre un processus notepad.exe sur le poste de la victime. Ici, ce processus est inoffensif mais on pourrait imaginer un scénario où on exécuterait un processus beaucoup plus dangereux.



e)

Cette question permet de constater qu’aucun ordinateur n’est réellement totalement protéger d’une attaque. On pourrait avoir les meilleurs pare-feux et mesures de sécurité mais si au final l’utilisateur n’est pas conscientisé aux dangers potentiels, l’ordinateur peut facilement être attaqué. L’installation de logiciels malveillants ou l’ouverture de pièces jointes en sont des exemples très répandus.