Travail pratique 3

Présenté à M. Bresteau
INF4420A Sécurité informatique

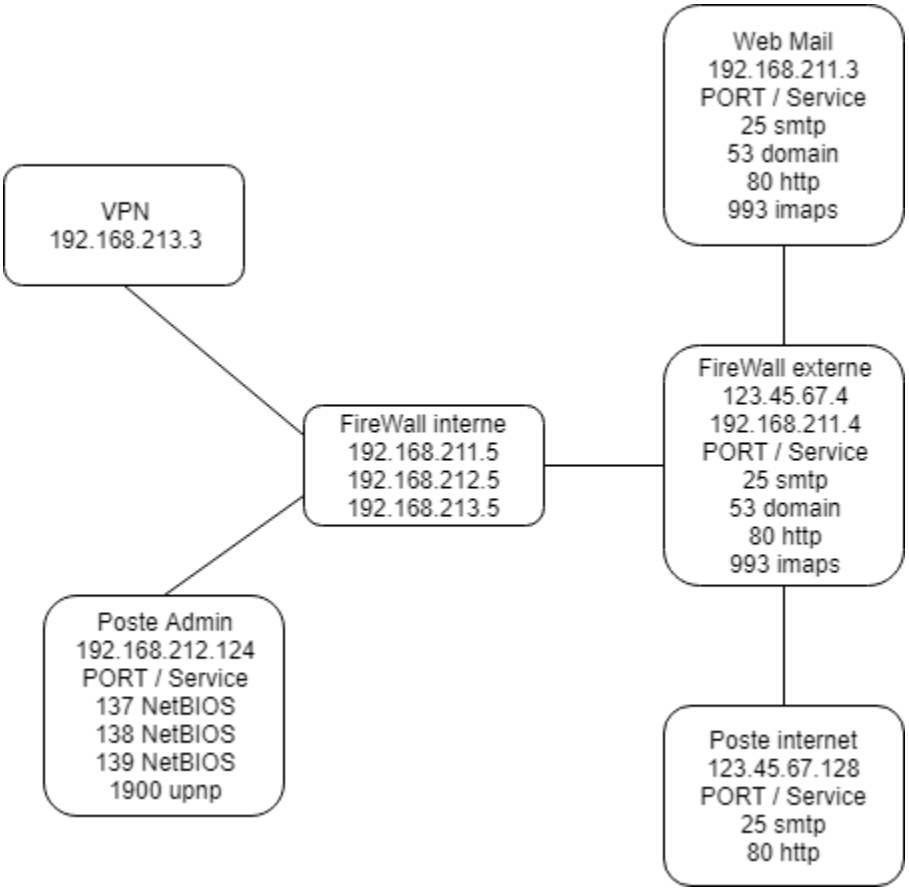
Fait par :

Étienne Asselin 1773922
Vincent Rodier 1744784
Groupe laboratoire B1-9

Le vendredi 30 mars 2018
École Polytechnique de Montréal

Question 1

A - Faites un schéma de ce réseau le plus complet possible (machines, adresses IP, ports ouverts et services utiles)



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?

```
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
Parefeu_ext shorewall # _
```

Le NAT permet de faire le lien entre une adresse IP de source interne en adresse IP globale. Dans ce cas si, le masque est 192.168.0.0/16. Ceci implique que les adresses du sous réseau privées sont de 192.168.0.0 à 192.168.255.255. Les instructions dans le fichiers /etc/shorewall permettent de faire la traduction d'adresse réseau de destination.

ACTION	SOURCE	DEST	PROTO	D-PORT
DNAT	Net	Dmz :192.168.211.3	Tcp / udp	80, 25 …

ACTION : L'action DNAT permet de transférer la demande à un autre système (192.168.211.3).

SOURCE : La source Net veut dire que la requête vient de l'extérieur du réseau privée.

DEST : Pour la destination dmz :192.168.211.3, le but de dmz est d'isoler les systèmes du réseau local des serveurs qui sont exposés sur internet. Ainsi, si un des serveurs est compromis, il reste encore un firewall ente le système compromis et les systèmes locaux.

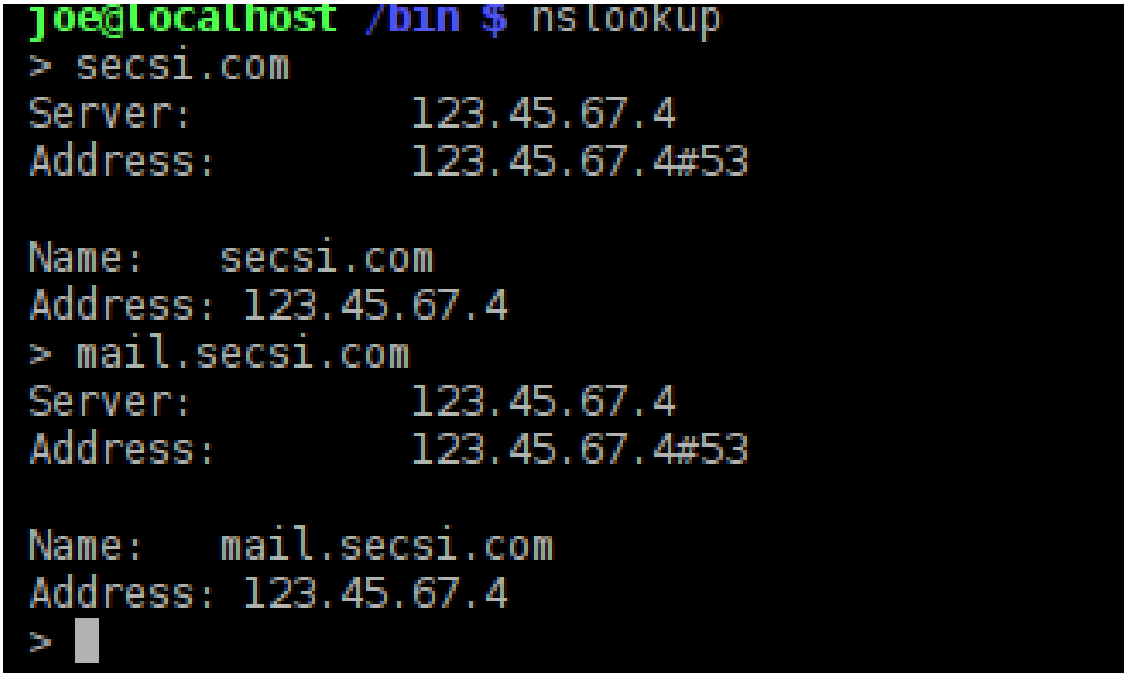
PROTO : Signifie le protocole de communication soit TCP ou UDP.

D-PORT : Signifie le port de destination.

Question 2

A - À quelle adresse IP correspondent le domaine secsi.com et le serveur mail mail.secsi.com

L'adresse IP de correspondant au domaine secsi.com est le même que le celui du serveur mail mail.secsi.com soit 123.45.67.4.



B - Lancez la commande « nmap –sT 192.168.211-214.* 123.45.67.* --open » en tant qu'utilisateur joe. Que fait cette commande? Expliquez le résultat.

La commande est utilisée afin de déterminer quels ports sont ouvert sur un réseau. Cette commande nous informe de plusieurs choses sur ces ports comme par exemple les services disponibles sur ces ports ainsi que le système d'exploitation de l'hôte offrant ce service. L'option « sT » de nMap spécifie de faire un scan en essayant d'ouvrir une connexion TCP sur les ports. Les deux adresses suivant le paramètre « sT » spécifie à nMap sur quelle plage d'adresse la tentative de connexion TCP devrait se faire. Dans le cas de la première adresse spécifier, on scan les ports sur toutes les adresses IP entre 192.168.211.0 et 192.168.214.255. Le tiret dans le 3^{ième} octet veut donc simplement dire que l'on veut faire le scan entre les deux valeurs spécifier. L'étoile à la fin des deux adresses IP signifie que toutes les possibilités doivent être tester entre 0 et 255. Finalement, l'option « --open » permet de filtrer les résultats que nMap donne afin d'afficher seulement les ports qui sont ouvert auquel il est possible de se connecter.

Le résultat nous montre que les ports ouverts et disponibles depuis le réseau du Poste_internet sont tous disponibles depuis l'adresse 123.45.67.4. Tous les ports ouverts et disponibles sont ceux que le service NAT du pare-feu externe redirige.

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

Starting Nmap 5.51 ( http://nmap.org ) at 2018-03-16 12:23 EDT
Nmap scan report for 123.45.67.4
Host is up (0.0013s 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 19.83 seconds
```

C - Que fait un service VPN? Expliquez le nouveau résultat.

Un VPN permet de créer un réseau virtuel privé qui redirige en quelque sorte le trafic. Maintenant, si le Poste_internet veut faire une requête, il doit passer par le VPN en premier lieu. C'est pour cela que maintenant que tout passe par le VPN que le Poste_internet n'est plus capable de voir les ports ouverts de l'adresse IP 123.45.67.4.

```
joe@localhost / $ sudo /etc/init.d/openvpn start
Password:
 * 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 2018-03-16 14:28 EDT
Nmap done: 1280 IP addresses (1 host up) scanned in 15.12 seconds
```

D - Comparez les informations obtenues à l'aide de nmap à votre schéma du réseau. Expliquez les différences.

La différence entre les deux nMap est que la première fois, le Poste_internet ainsi que le pare-feu externe étaient tous deux dans le même réseau soit 123.45.67.0/24 tandis qu'une fois le VPN ouvert, les deux ordinateurs n'étaient plus dans le même réseau local à cause du niveau d'abstraction que le VPN apporte. Donc la première fois que la commande nMap fut lancer, le Poste_internet à pus voire les ports d'ouvert tandis que la deuxième fois il n'a pas eu cette occasion.

E - Quel est l'avantage du NAT contre un balayage de ports?

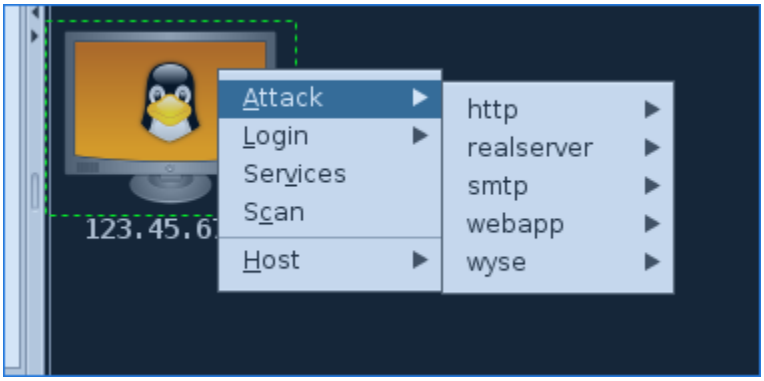
Le NAT peut appliquer des restrictions qui font en sorte qu'il présente certains ports selon la provenance de la requête. Ainsi un balayage des ports provenant de l'extérieur du réseau peut être prévenue.

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

Ajouter un IDS à mon pare-feu externe aurait permis de détecter le balayage de ports.

Question 3

Comme vu au TP2, lancez Armitage et essayez de prendre le contrôle des machines accessibles. a) Quel est le résultat ?

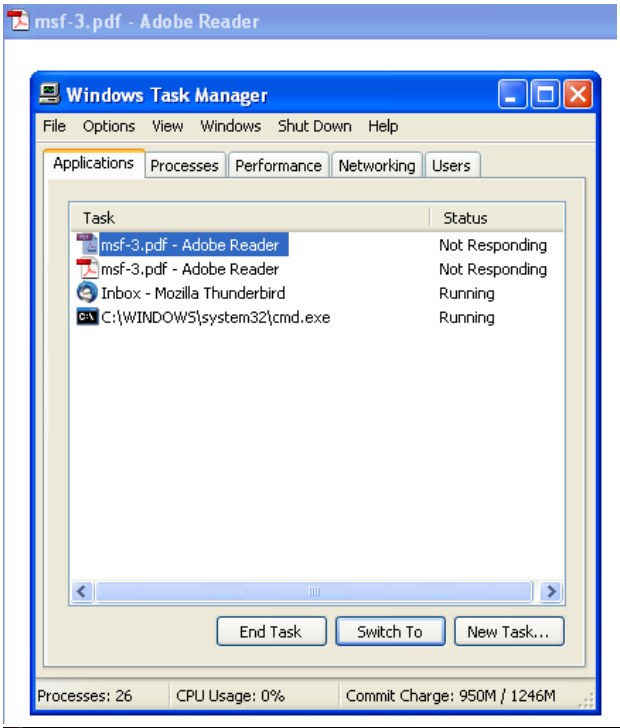


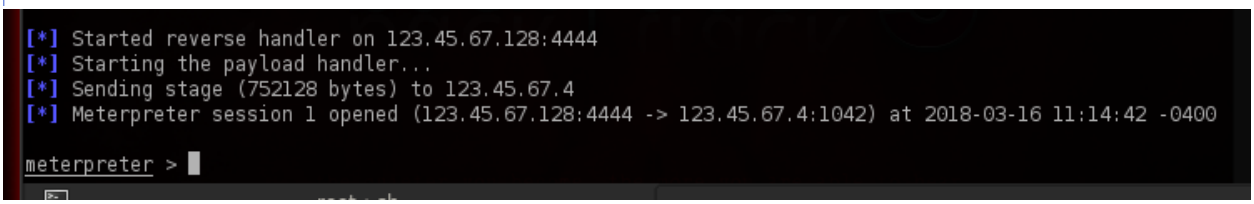
Nous sommes en mesure de voir les différents ports ouverts de la machine cependant nous sommes incapables de prendre le contrôle de celle-ci.

b) Pourquoi choisir le payload reverse_tcp plutôt que bind_tcp ?

La méthode reverse tcp permet d'attendre une réponse lorsque la victime ouvre la pièce jointe infectée. Quant à la méthode bind tcp, celle-ci écoute constamment la victime jusqu'à ce que qu'elle ouvre la pièce jointe. La première méthode est favorable puisqu'elle permet d'attendre une seule réponse au lieu de faire une multitude de requête infructueuse.

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





Sur le poste admin, le programme Adobe Reader a un statut d'aucune réponse (gelé), tandis que sur le poste internet nous voyons que l'utilisateur a ouvert la pièce jointe et que nous sommes prêts à passer à l'action.

d) Que s'est-il passé sur la Poste_admin ? Expliquez.

Le programme Adobe Reader s'est arrêté et nous ne voyons aucune trace que nous avons subis une attaque.

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

Le serveur web laisse transiter n'importe quel fichier avec n'importe quel code à l'intérieur. Ainsi, les mesures de sécurité ne sont pas très bonnes. Il faudrait implémenter un système que reconnait les Payload, dont le code est malicieux. Pour conclure, peu importe le niveau de logiciel de sécurité, un utilisateur imprudent reste la plus grande menace pour un système.