

Travail pratique 3

Présenté à M. Bresteau  
INF4420A Sécurité informatique

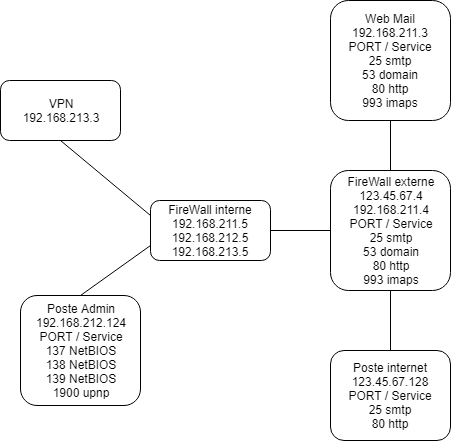
Fait par :

Étienne Asselin 1773922  
Vincent Rodier 1744784  
Groupe laboratoire B1-9

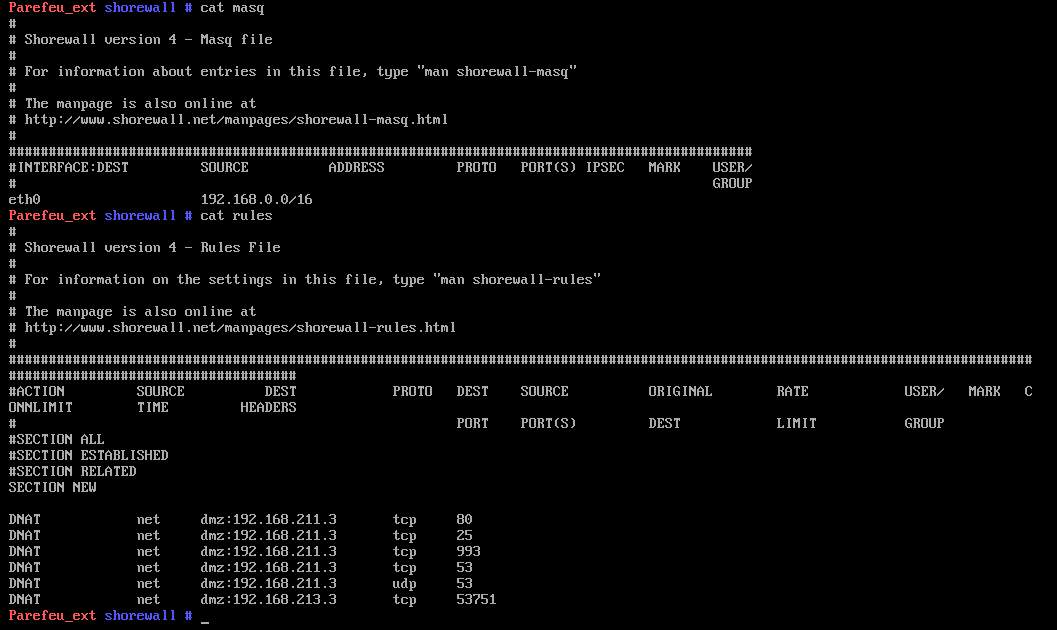
Le vendredi 30 mars 2018  
École Polytechnique de Montréal

# 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?



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.

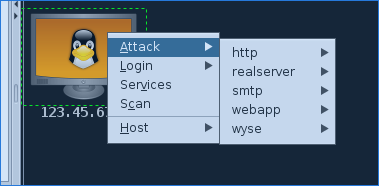
DEST : Pour la destination dmz :192.168.211.3, le but de dmz est d’isoler les systèmes du réseau local des serveurs qui sont exposés sur internet. Ainsi, si un des serveurs est compromis, il reste encore un firewall ente le système compromis et les systèmes locaux.

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

D-PORT : Signifie le port de destination.

# Question 3

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

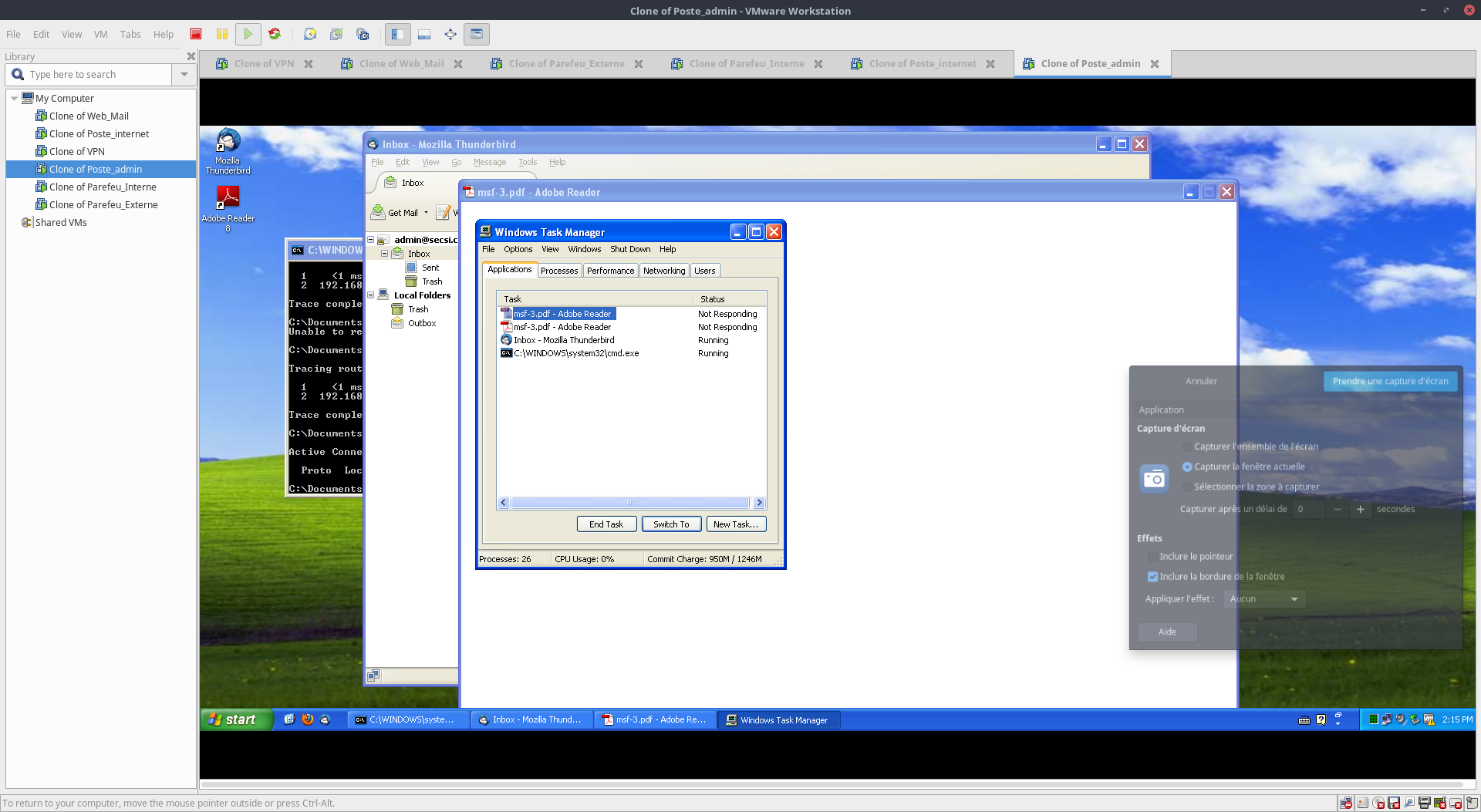
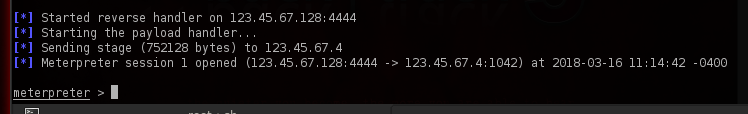


Nous sommes en mesure de voir les différents ports ouverts de la machine cependant nous sommes incapables de prendre le contrôle de celle-ci.

## 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.