M2103 TD5 :
Filtrage iptables

1. filtrage généralités

1. A votre avis à quoi correspond une politique par défaut en terme de filtrage ?
   Soit on accepte tout et on rejette par exception
   Soit on refuse tout et on accepte par exception
2. Rappeler les 5 chaînes présentes dans le modèle d'iptables ainsi que leur structure ?
   INPUT OUTPUT FORWARD PREROUTING POSTROUTING
3. A quoi correspond une table ?
   C'est un système d'évaluation de règles. Lorsqu'un paquet arrive sur un hook netfilter le paquet est évalué en fonction de chaines présentes dans chaque table.
4. Donner le nom des différentes tables présentes par défaut dans iptables.
   Conntrack Mangle Filter Nat
5. Peut-on rajouter des tables ? Oui
   A quoi cela peut il servir ? Pour créer ses propres chaines « proprement ».
6. Quels sont à votre avis les caractéristiques d'un bon logiciel de filtrage ?
   Mémoire (protocoles non linéaires comme H323) afin de faire du stateful
   capacité à travailler du n2 ethernet au n7 de la couche OSI
   capacité à reconnaître des protocoles (par exemple un tunnel qui passe par le port 53 UDP doit être bloqué par un firewall de nouvelles générations)
7. Pourquoi l'interface en ligne de commande est-elle utile au niveau d'iptables ?
   Il faut communiquer avec le kernel et netfilter depuis le userland.(interface utilisateur)

2. Quelques règles à expliquer

Donner la signification des règles suivantes :

1. iptables -L
   Liste les chaines pout la table filter (le -t filter est
2. iptables -F
   flush une chaine
3. iptables -t NAT -F
   flush toutes les chaines de la table NAT
4. iptables --policy INPUT DROP
   Par défaut on droppe les paquets
5. iptables -A INPUT -s 193.48.143.10 -j ACCEPT
   On ajoute une règle dans la table INPUT qui consiste à accepter tous les paquets de l'ip 192.48.143.10
6. iptables -A INPUT -i lo -j DROP
   On rajoute une règle dans la table INPUT qui va consister à dropper tous les paquets à destination de l'interface de loopback lo
7. iptables -A INPUT -p ICMP -j ACCEPT
   On rajoute une règle dans la table INPUT qui va accepter le protocole ICMP
8. iptables -A INPUT -p udp --dport 22 -j ACCEPT
   On rajoute une règle dans la table INPUT qui va accepter les paquets UDP sur le port 22
9. iptables -A INPUT -p tcp --dport 22 -j ACCEPT
   idem que 8 en TCP = protocole ssh
10. iptables -A INPUT -p tcp --tcp-flags SYN,FIN,ACK SYN -j ACCEPT
    accepte la poignée de main TCP et l'initialisation d'une connexion.
11. iptables -A INPUT -j LOG --log-level debug
    loggue tous les accès en INPUT
12. iptables -A INPUT -j LOG --log-level debug --log-prefix "PAQUET ENTRANT "
13. iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
14. iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
    13 est l'ancienne facon de faire du suivi de connexion établie

3. Création d'une nouvelle table personnalisée

Expliquer la signification des lignes comprises dans un script bash :

```
#!/bin/bash
iptables -N LOGACCEPT
iptables -A LOGACCEPT -j LOG --log-prefix "LOGACCEPT: "
iptables -A LOGACCEPT -j ACCEPT

iptables -N LOGDROP
iptables -A LOGDROP -j LOG --log-prefix "LOGDROP: "
iptables -A LOGDROP -j DROP

iptables -A INPUT -s 193.48.143.10 -j LOGACCEPT
iptables -A INPUT -j LOGDROP
```

4. Sur la chaîne FORWARD

1. Que font les 2 lignes suivantes ?
   iptables -A FORWARD -i eth1 -j ACCEPT
   iptables -A FORWARD -o eth1 -j ACCEPT
   Accepte le routage des paquets sur la carte eth1 (en entrée et ensortie de l'interface)
2. Pourquoi aucune table n'est précisée ?
   La table filter est la table par défaut

5. Un peu de NAT

Quelle est la signification des commandes suivantes

1. iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4
   source nat qui transforme les ip « externes » en 1.2.34
2. Si on souhaite que l'adresse de sortie soit choisie dans la plage 1.2.3.4 à 1.2.3.8 proposer une modification de la commande précédente

```
>iptables -t nat -A POSTROUTING -o eth0  -j SNAT --to-source 1.1.1.4-1.1.1.8
```

3. iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to 1.2.3.4 :1-1023
   source nat sur les ports 1-1023
4. iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 5.6.7.8
   dnat des adresses internes source transfomées en 5.6.7.8
5. iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to 5.6.7.8 :8080
   dnat port 80 vers le prort 8080 de 5.6.7.8 (on accède au port 8080 sur une ip externe)