Sécurité des Réseaux - TP

Iptables

Monroe Samuel

30 décembre 2015

1 Exercices de Théorie

1.1 Exercice 1

Les trois chaînes ont une policy de DROP par défaut.

— INPUT : Accepte du ICMP peu importe les conditions
— FORWARD : Accepte de l'udp depuis 192.168.1.10 vers n'importe où, et accepte de l'udp depuis n'importe où vers 192.168.1.10
— OUTPUT : Pas de règle

1.2 Exercice 2

Les commandes font un **flush** de toutes les règles précédentes, mettent une **policy** de drop par défaut sur toutes les chaînes, ajoutent sur **INPUT** l'acceptation de messages ICMP echo-request.
Sur **OUTPUT**, accepte les messages ICMP

1.3 Exercice 3

La chaîne **PREROUTING** a une policy d'acceptation par défaut.
La chaîne **POSTROUTING** a une policy d'acceptation par défault, et une règle de NAT qui modifie les adresses IP source du réseau local vers n'importe quelle destination.
La chaîne **OUTPUT** a une policy d'acceptation par défaut.

1.4 Exercice 4

Flush de toutes les règles précédentes, et ajout d'une policy **DROP** par défaut sur les trois chaînes.
Ajoute une règle d'acceptation en INPUT de nouvelles connexions ou de connexions établies sur les ports 80 et 443 (HTTP(S))
En **OUTPUT**, règle d'acceptation de toute connexion en état établie.

1.5 Exercice 5

— Flush de la chaîne **Forward**
— Ajout d'une règle d'acceptance sur forward
— Sur la table NAT, la chaîne **PREROUTING** est créditée d'une règle de NAT dynamique pour NAter les adresses du LAN.

1.6 Exercice 6

On flush les trois chaînes de la table **FILTER**, et on leur ajoute une policy d'acceptation.
On flush la chaînes **POSTROUTING** de la table **NAT**, et on ajoute une règle qui va modifier (**SNAT**) l'adresse source publique à une adresse publique dans un range de 10 adresses.

1.7 Exercice 7

On flush les trois chaînes de la table **FILTER**, et on leur ajoute une policy d'acceptation.
On flush la chaînes **PREROUTING** de la table **NAT**, et on ajoute une règle qui va modifier (**DNAT**) l'adresse de destination publique à une adresse privée port 80.

1.8 Exercice 8

On ajoute des règles en INPUT et OUTPUT, pour l'interface ppp0 en sortie et en entrée, qui vont accepter le protocole DNS port 53 en TCP et en UDP.

1.9 Exercice 9

1. Active le routage ipv4
2. Flush de toutes les règles
3. Création d'une chaîne personelle LOG_DROP, on spécifie que les outputs de cette chaîne vont avoir un préfixe textuel et on spécifie également que tout paquet amené sur cette chaîne doit être droppé.
4. Création d'une chaîne personelle LOG_ACCEPT, on spécifie que les outputs de cette chaîne vont avoir un préfixe textuel et on spécifie également que tout paquet amené sur cette chaîne doit être accepté.
5. Les policies sur les chaînes **INPUT, OUTPUT, FORWARD** sont mise à **DROP**.
6. Sur la chaîne **INPUT**, l'interface l0 en input est mise à **ACCEPT**, et sur la chaîne **OUTPUT**, l'interface l0 en output est mise à **ACCEPT**
7. Sur la chaîne **FORWARD**, ACCEPT en input sur la eth1 et output sur ppp0, et inversément. De plus, sur la tâble nat chaîne **POSTROUTING**, une règle NAT les adresses du réseaux local.

8. Sur la chaîne **OUTPUT**, on accepte en sortie de l'interface ppp0, les connexions en état nouveau ou établie sur le port 80.
   Sur la chaîne **INPUT** ; on accepte en entrée de l'interface ppp0 les connexion établies sur le port 80.
   Enfin, sur la tâble NAT chaîne **PREROUTING**, la règle NATe l'adresse destination des paquets en entrée de l'interface eth1 sur le port 80 vers l'adresse 192.168.2.1 port 3128.

9. Sur la tâble NAT chaîne **PREROUTING**, la règle NATe l'adresse destination 42.42.42.42 port 80 vers l'adresse 192.168.1.2 port 80.
   Sur la chaîne **FORWARD**, on accepte les paquets entrants sur ppp0 à destination du port 80 pour des connexions NEW ou ESTABLISHED.
   Sur la chaîne **FORWARD**, on accepte les paquets sortants sur ppp0 à destination du port 80 pour des connexions ESTABLISHED.
   Sur la table **NAT**, chaîne **POSTROUTING** on NATe les paquets du LAN.

10. Sur la chaîne **FORWARD**, on accepte les paquets entrants sur eth1 pour le port 80 entrant pour des connexions nouvelles ou établies.
    On accepte également les paquets entrants sur eth1 pour le port 80 sortant pour des connexions établies.

11. Sur la chaîne **INPUT**, on transfère à la liste LOG_ACCEPT les paquets entrants sur eth1, depuis 192.168.2.42 à destination du port 22 pour des nouvelles connexions ou établies.
    Sur la chaîne **OUTPUT**, on transfère à la liste LOG_ACCEPT les paquets sortants sur eth0, vers l'adresse 192.168.2.42 port 200, pour des connexions établies.

12. On jump les trois chaînes de la table **filter** sur LOG_DROP.

2 Laboratoire

1. Les trois commandes suivantes ajoutent une policy d'acceptation pour tout paquet :

   — iptables -P INPUT ACCEPT
   — iptables -P OUTPUT ACCEPT
   — iptables -P FORWARD ACCEPT

2. Rejet de tout le traffic, et logging des outputs, les commandes fonctionnent et on observe bien les rejets dans /var/log/messages

   — iptables –flush (flush de toutes les règles)
   — iptables -N LOGS (création d'une liste custom LOGS)
   — iptables -P INPUT DROP
   — iptables -P OUTPUT DROP
   — iptables -P FORWARD DROP
   — iptables -A INPUT -j LOGS (jump da la liste dans logs)
   — iptables -A OUTPUT -j LOGS
   — iptables -A FORWARD -j LOGS
   — iptables -A LOGS -m limit -j LOG –log-prefix "IPTables-Dropped : " –log-level 4
   — iptables -A LOGS -j DROP

3. Remise du firewall dans sa config par défault, configurer le firewall pour empêcher toute requête html vers pc3 qui possède un site web.

   Le serveur web du PC3 affiche une page html avec "It works ! ".

   — iptables -A INPUT -p tcp –destination-port 80 -j DROP
   — iptables -A OUTPUT -p tcp –destination-port 80 -j DROP
   — iptables -A FORWARD -p tcp –destination-port 80 -j DROP

4. Dans l'exercice précédent, la policy par défaut était ACCEPT donc je garde ici la configuration précédente.
   Cette commande permet toujours le ping par PC4, mais le subnet précisé ne peut plus pinguer PC3.

   — iptables -A FORWARD -p icmp -s 192.168.2.0/24 -d 192.168.1.3 -j DROP

5. Ici encore, je garde la configuration de policy d'acceptance par défaut, pour bien voir que les échecs et l'acceptance sont dûs à mes règles.

   Je précise d'abord une règle d'accès pour le PC2 sur l'interface du côté de PC2, ensuite un refus pour tout autre source.
   Ensuite on rejette le reste dans la liste LOGS, qui elle-même rejera un jump sur drop.

   — Flush puis acceptance par défaut.
   — iptables -A INPUT -i eth0 -p tcp –destination-port 22 -s 192.168.2.2/24 -d 192.168.2.200/24 -j ACCEPT
   — iptables -A OUTPUT -p tcp –source-port 22 -d 192.168.2.2/24 -j ACCEPT
   — iptables -A INPUT -j LOGS
   — iptables -A OUTPUT -j LOGS
   — iptables -A LOGS -m limit -j LOG –log-prefix "IPTables-Dropped : " –log-level 4
   — iptables -A LOGS -j DROP