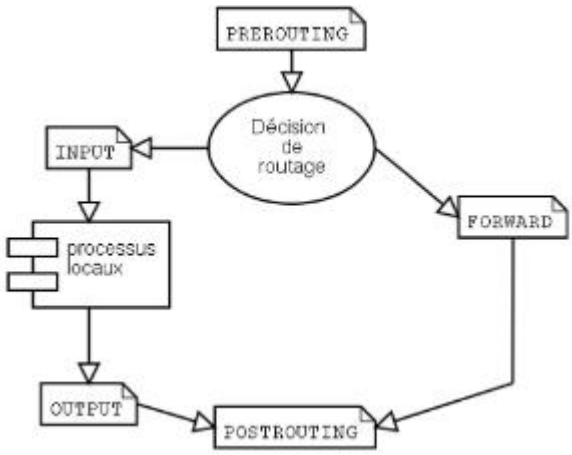
TP ITC7-2 Réseaux

Mickaël CHOISNARD, Benoit DARTIES, Arnaud DA COSTA

Exercice 1 **iptables (Netfilter)**

Le schéma suivant décrit brièvement le cheminement des paquets au sein d'une machine Linux.

Une documentation plus conséquente est disponible à cette adresse : http://www.linux-france.org/prj/inetdoc/guides/iptables-tutorial/



Iptables permet le filtrage de paquet avec la table filter (chaîne INPUT, OUTPUT, FORWARD), permet la translation d'adresse avec la table nat (chaîne PREROUTING, OUTPUT, POSTROUTING) et permet la modification de paquets avec la table mangle.

1. Comment définir la politique par défaut d'une chaîne iptables (INPUT, OUTPUT, FORWARD) ?
2. Proposer une politique par défaut pour les chaînes INPUT, OUTPUT, FORWARD dans les deux cas suivants :
    a. Machine de bureau
    b. Routeur filtrant
3. Comment autoriser les paquets ayant pour port source le port 80 à entrer sur une machine ?
4. Comment autoriser les paquets ayant pour port source le port 80 à traverser sur une machine ?
5. Comment autoriser les paquets ayant pour port source le port 53 et ayant pour adresse source 193.50.50.2 à entrer sur une machine ?
6. Comment autoriser les paquets ayant pour port source le port 53 et ayant pour adresse source 193.50.50.2 à traverser sur une machine ?

7. Comment n’autoriser en entré QUE les paquets relatifs à une connexion déjà existante ?
8. Comment n’autoriser en traversée QUE les paquets relatifs à une connexion déjà existante ?
9. Quel outil peut être utilisé pour connaître les ports qui sont utilisés pendant un temps donné (par exemple pendant une navigation web) ?

Exercice 2 **manipulation iptables**

En utilisant la politque par défaut à DROP, faire en sorte de pouvoir :

1. pouvez visualiser les pages web des autres serveurs depuis votre serveur (en utilisant l'adresse IP)
2. pouvez visualiser les pages web des autres serveurs depuis votre client (en utilisant l'adresse IP)
3. pouvez visualiser la page d'accueil de google depuis votre serveur (en utilisant l'adresse IP)
4. pouvez visualiser la page d'accueil de google depuis votre client (en utilisant l'adresse IP)
5. pouvez visualiser la page d'accueil de google depuis votre serveur (en utilisant le nom www.google.fr)
6. pouvez visualiser la page d'accueil de google depuis votre client (en utilisant le nom www.google.fr)
7. Ecrire un script pour stocker vos règles de filtrage.
8. Ecrire un script pour effacer vos règles de filtrage et autoriser tout le trafic réseau
9. En sachant que les serveurs web écoutent sur le port 80 par défaut, déterminer à quoi sert l’information contenue dans le fichier /etc/services

Exercice 3

1 - est-il possible, avec iptables, de limiter (par heure par exemple) le nombre de paquet arrivant sur un port donné ?

2 - est-il possible, avec iptables, de limiter (par heure par exemple) le nombre de paquets arrivant sur un port donné en provenance de 3 sources connues à l'avance ?

3 - est-il possible, avec iptables, de limiter (par heure par exemple) le nombre de paquets arrivant sur un port donné en provenance de X sources inconnues à l'avance ?

4 - Appliquer sur un client les règles qui suivent, puis essayez ensuite de vous connecter 4 fois de suite depuis la même machine à ce client. Que se passe-t-il à partir de la 4ème tentative ?

```
# Generated by iptables-save v1.4.2 on Wed Jun  9 14:27:04 2010
*filter
:INPUT ACCEPT [22234083:52627703270]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [18775047:65997250069]
:LGRDP - [0:0]
:LOGDROP - [0:0]
-A INPUT -p tcp -m tcp --dport 22 -j LOGDROP
-A INPUT -p tcp -m tcp --dport 3389 -j DROP
-A LGRDP -p tcp -m limit --limit 5/min -j LOG --log-prefix "Denied RDP : "
--log-level 7
-A LGRDP -j DROP
-A LOGDROP -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --
name SSH --rsource
-A LOGDROP -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update
--seconds 60 --hitcount 4 --name SSH --rsource -j LOG --log-prefix "SSH
SCAN blocked: " --log-level 6
-A LOGDROP -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update
--seconds 60 --hitcount 4 --name SSH --rsource -j DROP
-A LOGDROP -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
COMMIT
# Completed on Wed Jun  9 14:27:04 2010
```

5 - Expliquer chacune des lignes de règles ci-dessus

6 - qu'est-ce que le port knocking ?

7 - Expliquer ce que fait le script suivant (source : http://www.debian-administration.org/articles/268)

```
# Netfilter/IPtables - example of multiple-port knocking
# Note: Knock ports 100,200,300,400 to open SSH port for 5 seconds.
# Nice thing to knock TCP with is `telnet' program:
# $> alias k='telnet ip_address_or_hostname'
# $> k 100 ; k 200 ; k 300 ; k 400 ; ssh ip_address_or_hostname
# Then press Ctrl-C 4 times. That's all. Enjoy.

HOST_IP="12.34.56.78"

/sbin/iptables -N INTO-PHASE2
/sbin/iptables -A INTO-PHASE2 -m recent --name PHASE1 --remove
/sbin/iptables -A INTO-PHASE2 -m recent --name PHASE2 --set
/sbin/iptables -A INTO-PHASE2 -j LOG --log-prefix "INTO PHASE2: "

/sbin/iptables -N INTO-PHASE3
```

```
/sbin/iptables -A INTO-PHASE3 -m recent --name PHASE2 --remove
/sbin/iptables -A INTO-PHASE3 -m recent --name PHASE3 --set
/sbin/iptables -A INTO-PHASE3 -j LOG --log-prefix "INTO PHASE3: "

/sbin/iptables -N INTO-PHASE4
/sbin/iptables -A INTO-PHASE4 -m recent --name PHASE3 --remove
/sbin/iptables -A INTO-PHASE4 -m recent --name PHASE4 --set
/sbin/iptables -A INTO-PHASE4 -j LOG --log-prefix "INTO PHASE4: "

/sbin/iptables -A INPUT -m recent --update --name PHASE1

/sbin/iptables -A INPUT -p tcp --dport 100 -m recent --set --name PHASE1
/sbin/iptables -A INPUT -p tcp --dport 200 -m recent --rcheck --name PHASE1
-j INTO-PHASE2
/sbin/iptables -A INPUT -p tcp --dport 300 -m recent --rcheck --name PHASE2
-j INTO-PHASE3
/sbin/iptables -A INPUT -p tcp --dport 400 -m recent --rcheck --name PHASE3
-j INTO-PHASE4

/sbin/iptables -A INPUT -p tcp -s $HOST_IP --dport 22 -m recent --rcheck --
seconds 5 --name PHASE4 -j ACCEPT
```

Exercice 4 **Translation d'adresses**

1. Créer un alias 172.24.24.xx sur la carte publique
2. Vérifier sur votre serveur l'adresse d'un client
3. Mettre en place du NAT entre le client et l'Alias : accéder au serveur web d'une autre groupe et vérifier quelle est l'adresse source vue par le serveur web
4. Limiter les ports du NAT entre le client et l'IP publique