Travaux Pratiques R&T 2ème année
Durée : 3 heures
TP R2b – SECURITE RESEAUX
Filtrage Iptables

Noms :Rabenejamina Solohaja, Tharic Faris
Groupe :TP4 groupe5
Date : 24/10/14

Objectifs du TP

– Mise en œuvre des fonctions d'IPTABLES (filtrage, translation d'adresse…) sous linux en configurant une machine en tant que firewall pour une machine cliente.

Pour aide :
(Pour supprimer une règles on peut taper la commande suivantes :
iptables -L –line-numbers : pour avoir le numéro de la ligne puis la commande :
iptables -D OUTPUT/INPUT ou FORWARD numero de la ligne)

Pour l'ensemble des questions suivantes vous décrirez votre façon de procéder dans votre compte rendu de TP.

1. Effacez toutes les règles de toutes les chaînes dans toutes les tables.

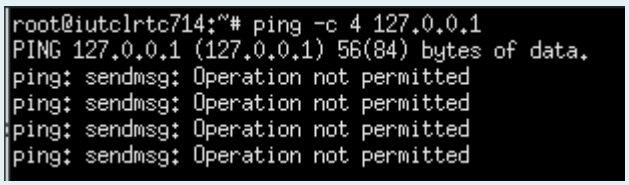
```
Pour effacer toutes les règles de toutes les chaîne dans toutes les
tables on tape les commandes suivantes :
iptables -X (supprime les chaines)
iptables -F (supprime toutes règles une par une)
```

2. Eliminez tous les paquets par défaut.

```
Pour éliminer tous les paquets par défaut on tape les commandes
suivantes :
iptables -P INPUT DROP (les paquets entrants)
iptables -P OUTPUT DROP (les paquets sortants)
iptables -P FORWARD DROP (les paquet qui vont transiter)
```

3. Faites un ping en local, résultat ?

```
On voit que les ping ne sont plus permis car on a interdit le trafic avec
les commande vu dans 2
```



4. Autorisez les paquets provenant du local host

pour autoriser les paquets provenant du localhost on tape la commande suivante:
iptables -A INPUT -s localhost -j ACCEPT

-A : ajouter une règle
-j : ce qu'il faut si le paquet correspond à la règle.

5. Autorisez les paquets à destination de local host

pour autoriser les paquets à destination du localhost on tape la commande suivante :
iptables -A OUTPUT -d localhost -j ACCEPT

6. Testez ping localhost, résultat ?

On voit que le ping fonctionne quand on ping en local :

```
root@iutclrtc714:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.025 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.049 ms
64 bytes from 127.0.0.1: icmp_req=3 ttl=64 time=0.047 ms
```

7. Autorisez les échanges avec le réseau local. Test ? Résultat?

Pour autoriser les échanges avec le réseau local on tape les commandes suivantes :
-iptables -A INPUT -s 192.168.108.0/24 -j ACCEPT (pour autorisé les paquets entrant provenant du réseau local le réseau ayant pour adresse 192.168.108.0/24).

-iptables -A OUTPUT -d 192.168.108.0/24 -j ACCEPT (pour autorisé les paquets sortant à destination du réseau local le réseau ayant pour adresse 192.168.108.0/24).

Pour tester que cela marche bien nous pouvons réalisé un ping de la machine ou on réalisé iptables vers une autre machine du réseau local(1). Puis un ping de la machine du réseau local vers la machine ou est configurer iptables (2).
Ici on voit que la machine peut échanger avec le réseau local.

(1)l'adresse ip de la machine client est 192.168.108.88 (ping à partir pc serveur).

```
root@iutclrtc714:~# ping 192.168.108.88
PING 192.168.108.88 (192.168.108.88) 56(84) bytes of data.
64 bytes from 192.168.108.88: icmp_req=1 ttl=64 time=0.442 ms
64 bytes from 192.168.108.88: icmp_req=2 ttl=64 time=0.295 ms
64 bytes from 192.168.108.88: icmp_req=3 ttl=64 time=0.263 ms
```

(2) l'adresse ip de la machine avec iptables est de 192.168.108.94

```
root@iutclrtc708:~# ping -c 4  192.168.108.94
PING 192.168.108.94 (192.168.108.94) 56(84) bytes of data.
64 bytes from 192.168.108.94: icmp_req=1 ttl=64 time=0.234 ms
64 bytes from 192.168.108.94: icmp_req=2 ttl=64 time=0.288 ms
64 bytes from 192.168.108.94: icmp_req=3 ttl=64 time=0.285 ms
64 bytes from 192.168.108.94: icmp_req=4 ttl=64 time=0.286 ms

--- 192.168.108.94 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.234/0.273/0.288/0.025 ms
```

8. Autorisez les échanges sur le net.

Pour autoriser les échanges sur le net il faut taper la commande :
iptables -A INPUT -p ip -j ACCEPT
iptables -A OUTPUT -p ip -j ACCEPT

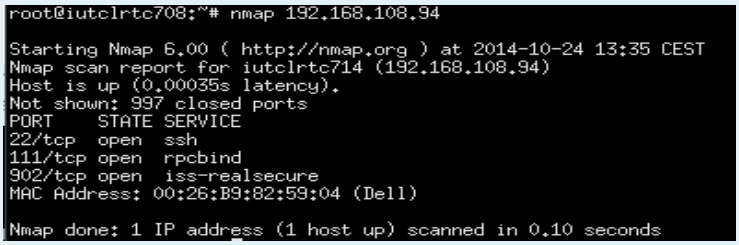
Maintenant la machine ou est configurer iptables peut aller sur internet

9. A partir de la machine cliente, faites un nmap. Résultat ?

Il faut vérifier si nmap est installé sur la machine client pour cela on peut taper la commande suivante : apt-cache policy nmap

Ici on voit que nmap n'est pas installé donc on tape la commande : apt-get install nmap pour l'installé.

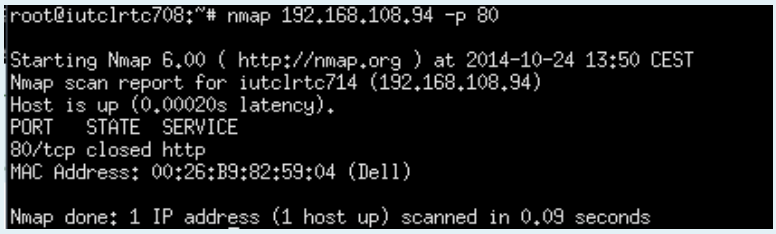
Le résultat de la commande nmap fait à partir de la machine client est :



192.168.106.94 : adresse ip de la machine serveur(ou iptable est configuré) la commade nmap @ip montre les ports qui sont ouvert (open). Ici on voit que les ports autres que les port tcp sont fermé.

10. A partir de la machine cliente, faites un nmap sous le port 80. Résultat ?

On tape la commande 192.168.108.94 -p 80



ici on voit que le port 80 est closed c'est à dire que le port est ouvert mais aucun service ne lui est associé (ici par exemple on n'a pas de serveur apache qui va utilisé le port 80 donc il nous indique closed).

Mode suivi de connexion :

11. Expliquez à quoi sert ce mode.

```
Mode suivi de connexion sert à inspecter et restreindre la connexion aux
services disponibles dans un réseau interne selon l’état de connexion du
paquet.
État du paquet (exemple) :-New :demande de nouvelle connexion
                          -ESTABLISHED:paquet qui fait partie d'une
connexion existante.
                          -RELATED:paquet qui demande une nouvelle
connexion et qui fait partie d'une connexion existant.
                          -INVALID:paquet qui ne fait pas partie d'aucune
connexion dans la table de suivi de connexion.
```

12. Appliquez le à votre cas. Testez, résultat ?

```
Ici pour l'appliquer on peut tape la commande suivante sur le serveur
(iptable) :
pour cela il faut taper la commande :

iptables -A INPUT -m state –state  New,ESTABLISHED,RELATED,INVALID -j
ACCEPT
iptables -A INPUT -m state –state  New,ESTABLISHED,RELATED,INVALID -j
ACCEPT

Puis il faut enlever les règles que nous avons mis dans 8. (pour pouvoir
aller sur internet) avec la commande
iptables -D INPUT 3    3: numero de la ligne ou est defini la règle que
nous avons mis dans la question 9.
iptables -D INPUT 3    3: numero de la ligne ou est defini la règle que
nous avons mis dans la question 9.

Cela nous permet d'avoir encore internet mêle si les règles ont été
supprimer grâce à la suivi de connexion.
```

Masquerading :

13 – Autorisez le forwarding sur votre machine. Commande ?

Pour autorisé le forwarding sur la machine on tape les commandes suivantes:

```
iptables -A FORWARD -d localhost -j ACCEPT
iptables -A FORWARD -s localhost -j ACCEPT
```

```
root@iutclrtc714:~# iptables -A FORWARD -d localhost -j ACCEPT
root@iutclrtc714:~# iptables -A FORWARD -s localhost -j ACCEPT
root@iutclrtc714:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  localhost            anywhere
ACCEPT     all  --  192.168.108.0/24     anywhere
ACCEPT     all  --  anywhere             anywhere             state INVALID,NEW,
RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             localhost
ACCEPT     all  --  localhost            anywhere

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             localhost
ACCEPT     all  --  anywhere             192.168.108.0/24
ACCEPT     all  --  anywhere             anywhere             state INVALID,NEW,
RELATED,ESTABLISHED
```

14 – Expliquez à quoi sert le masquerading et appliquez le à votre situation pour le trafic provenant de la machine cliente. Utilisez *wireshark* pour vérifier le fonctionnement de MASQUERADE.

Commande ? Capture *wireshark* + commentaires.

```
MASQUERADE sert à faire un translation vers l'adresse ip de l'interface de
sortie.
On peut dire qu'elle fait le NAT.
Pour l'appliquer dans notre cas il faut relier le pc client avec le pc
serveur, mettre leur interface dans le même plage ici on a décidé de les
mettre (eth3 de nos deux pc) dans le réseau 10.0.0.0/24
sur le pc client on fait ifconfig eth3 10.0.0.3/24
# route add default gateway 10.0.0.1
pc serveur 10.0.0.1/24
iptables -A INPUT -s 10.0.0.0/24-j ACCEPT
iptables -A OUTPUT -d 10.0.0.0/24-j ACCEPT
il faut aussi penser à faire :
iptables -P FORWARD ACCEPT

maintenant il faut autoriser le routage sur pc serveur pour cela on tape la
commande(sur le pc serveur)
echo>1 /proc/sys/net/ipv4/ip_forward

puis il faut taper la commande :
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```