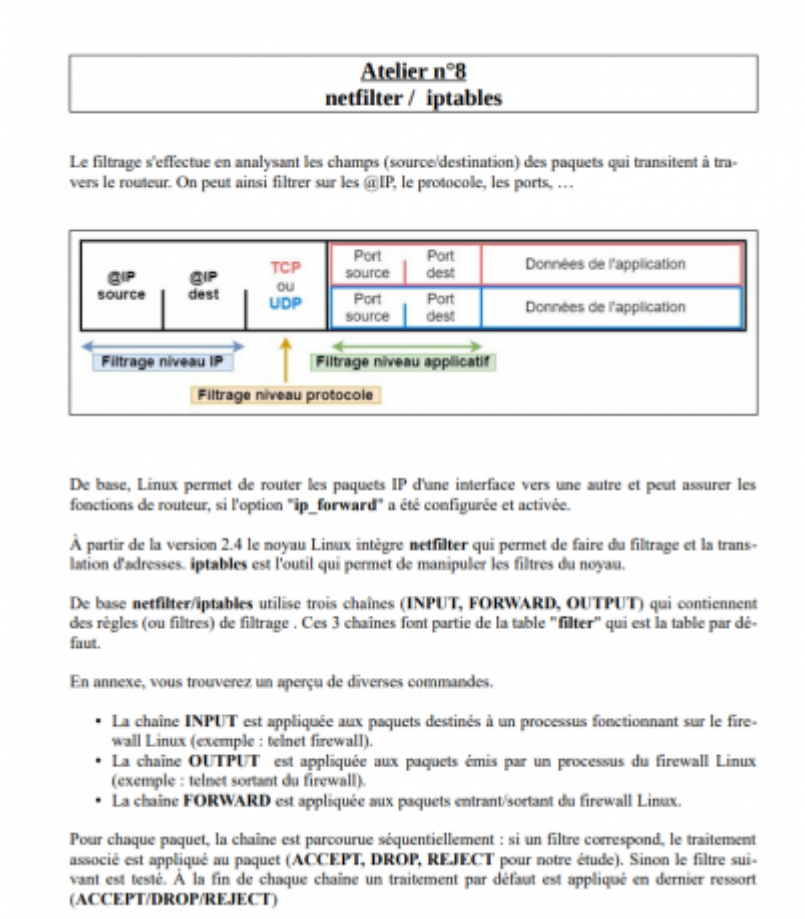
Aller au contenu

Atelier n° 8 netfilter / iptables

Lecon :



Atelier n°8
netfilter / iptables

Le filtrage s'effectue en analysant les champs (source/destination) des paquets qui transitent à travers le routeur. On peut ainsi filtrer sur les @IP, le protocole, les ports, …

De base, Linux permet de router les paquets IP d'une interface vers une autre et peut assurer les fonctions de routeur, si l'option "**ip_forward**" a été configurée et activée.

À partir de la version 2.4 le noyau Linux intègre **netfilter** qui permet de faire du filtrage et la translation d'adresses. **iptables** est l'outil qui permet de manipuler les filtres du noyau.

De base **netfilter/iptables** utilise trois chaînes (**INPUT, FORWARD, OUTPUT**) qui contiennent des règles (ou filtres) de filtrage . Ces 3 chaînes font partie de la table "**filter**" qui est la table par défaut.

En annexe, vous trouverez un aperçu de diverses commandes.

- La chaîne **INPUT** est appliquée aux paquets destinés à un processus fonctionnant sur le firewall Linux (exemple : telnet firewall).
- La chaîne **OUTPUT** est appliquée aux paquets émis par un processus du firewall Linux (exemple : telnet sortant du firewall).
- La chaîne **FORWARD** est appliquée aux paquets entrant/sortant du firewall Linux.

Pour chaque paquet, la chaîne est parcourue séquentiellement : si un filtre correspond, le traitement associé est appliqué au paquet (**ACCEPT, DROP, REJECT** pour notre étude). Sinon le filtre suivant est testé. À la fin de chaque chaîne un traitement par défaut est appliqué en dernier ressort (**ACCEPT/DROP/REJECT**)

iptables -t nat -F (supprime toutes les regles de la table nat)
iptables -A INPUT-s 202.54.1.2 -j DROP (bloque l'adresse ip 202.54.1.2)
iptables -D INPUT -s 202.54.1.1 -j DROP (supprimer la regle qui permetter de bloquait l'adresse 202.54.1.2)

Script firewall sur le serveur
:

```
#!/bin/bash
iptables -F #suppression des tables
iptables -t nat -F  #suppression de la tables nat
iptables -P INPUT ACCEPT  #accepte les connexions entrantes
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT #accepter les connexions sortantes

#tous refuser (les connexions entrantes)
iptables -P INPUT DROP #refuser les connexions entrantes

#accepter ces connexions
#iptables -A INPUT -P tcp --dport 2222 -j ACCEPT
iptables -A INPUT -p tcp --dport 53 -j ACCEPT #connexions entrante sur le port 53 autoris
iptables -A INPUT -p tcp --dport 80 -j ACCEPT #connexions entrante sur le port 80 autoris
iptables -A INPUT -p tcp --dport 21 -j ACCEPT #connexions entrante sur le port 21 autoris
iptables -A INPUT -p icmp -j ACCEPT #ping depuis 10.31.112.0 autorisé
iptables -A FORWARD -p icmp -j ACCEPT #ping autorise
iptables -A INPUT -p icmp -j ACCEPT #ping entrant autorisé
iptables -A INPUT -i lo -j ACCEPT #autorise la machine a se contacter
iptables -A INPUT -p tcp --dport 8001 -j ACCEPT #autorise les connexions entrante sur le
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p udp --dport 443 -j ACCEPT
iptables -A INPUT -p udp --dport 80 -j ACCEPT
```

```
#iptables -A INPUT -p tcp --dport
#iptables -A OUTPUT -o lo -j ACCEPT
#iptables -t nat -A POSTROUTING -p icmp -s 10.31.112.254 -j ACCEPT

#accepter les adresse ip entre 20 et 50 a se connecter en ssh
iptables -A INPUT -p tcp -m iprange --src-range 10.187.20.20-10.187.20.54 --dport 2222 -j
iptables -A INPUT -p tcp -s 10.31.112.254 --dport 2222 -j ACCEPT #autorise la connexion e
iptables -A INPUT -p tcp -s 10.31.112.254 -m state --state NEW,ESTABLISHED -j ACCEPT #aut
#range of ip authorized 10.187.20.20 to 10.187.20.50 in port 2222

#regles pour télécharge avec apt-get
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT #autorise le retour des
iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT

#iptables -A INPUT -p tcp --dport 2222 -j ACCEPT
#iptables pour les conteneur
iptables -A INPUT -p tcp -s 10.31.112.53 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -s 10.31.112.21 --dport 21 -j ACCEPT
iptables -A INPUT -p tcp -s 10.31.112.80 --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.112.53 --dport 53 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.112.21 --dport 21 -j ACCEPT
iptables -A OUTPUT -p tcp -s 10.31.112.80 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.112.53 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.112.21 --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.112.80 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.112.36 --dport 3306 -j ACCEPT
```

Script bash sur le routeur pour le firewall :

```
#!/bin/bash
#!/bin/bash
iptables -F #suppression des tables
iptables -t nat -F  #suppression de la tables nat
iptables -P INPUT ACCEPT  #accepte les connexions entrantes
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT #accepter les connexions sortantes

#tous refuser (les connexions entrantes)
iptables -P INPUT DROP #refuser les connexions entrantes
iptables -P OUTPUT DROP #refuser les connexions sortantes

#accepter ces connexions
#iptables -A INPUT -P tcp --dport 2222 -j ACCEPT
iptables -A INPUT -p tcp --dport 53 -j ACCEPT #connexions entrante sur le port 53 tcp aut
iptables -A INPUT -p udp --dport 53 -j ACCEPT #connexions entrante sur le port 53 udp aut
iptables -A INPUT -p tcp --dport 53 -j ACCEPT #connexions entrante sur le port 53 tcp aut
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT #connexions sortante sur le port 53 tcp au
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT #connexions sortante sur le port 53 udp au
iptables -A FORWARD -p tcp --dport 80 -j ACCEPT #connexions entrante sur le port 80 autor
iptables -A FORWARD -p tcp --dport 21 -j ACCEPT #connexions entrante sur le port 21 autor
iptables -A INPUT -p icmp -j ACCEPT #ping autorisé
iptables -A FORWARD -p icmp -j ACCEPT #ping autorisé
iptables -A OUTPUT -p icmp -j ACCEPT #ping autorisé
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT #permet au paquet de rev
iptables -A INPUT -i lo -j ACCEPT #autorise la machine a se contacter
iptables -A OUTPUT -o lo -j ACCEPT #autorsie la machine a se contacter
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT #connexions sortante  sur le port 443 aut
iptables -A FORWARD -p tcp --dport 443 -j ACCEPT #connexions sur le port 443 autorisé a a
iptables -A FORWARD -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp --dport 8001 -j ACCEPT
iptables -A INPUT -p tcp --dport 8001 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 8001 -j ACCEPT
iptables -A FORWARD -p tcp --dport 53 -j ACCEPT #pour acceder au site web (resolution de
iptables -A FORWARD -p udp --dport 53 -j ACCEPT #pour acceder au site web (resolution de


#iptables -t nat -A POSTROUTING -p icmp -s 10.31.112.254 -j ACCEPT

#accepter les adresse ip entre 20 et 50 a se connecter en ssh
iptables -A INPUT -p tcp -s 10.31.112.1 --dport 22 -j ACCEPT #accepter connexion sur ssh
```

```
iptables -A OUTPUT -p tcp -s 10.31.112.1 --dport 22 -j ACCEPT #accepter connexion sur ssh
iptables -A INPUT -p tcp -m iprange --src-range 10.187.20.20-10.187.20.54 --dport 22 -j A
iptables -A OUTPUT -p tcp -m iprange --src-range 10.187.20.20-10.187.20.54 --dport 22 -j
iptables -A INPUT -p tcp -s 10.31.112.1 -m state --state NEW,ESTABLISHED -j ACCEPT #accep
iptables -A INPUT -p tcp -m iprange --src-range 10.187.20.10-10.187.20.54 -m state --stat
iptables -A OUTPUT -p tcp -m iprange --src-range 10.187.20.10-10.187.20.54 -m state --sta
iptables -A OUTPUT -p tcp  -m state --state NEW,ESTABLISHED -j ACCEPT #autorise les conne
iptables -A INPUT -p tcp  -m state --state NEW,ESTABLISHED -j ACCEPT #autorise les connex
#range of ip authorized 10.187.20.20 to 10.187.20.50 in port 2222

#iptables pour les conteneurs
iptables -A FORWARD -p udp -s 10.31.112.53 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.112.21 --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.112.80 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.31.112.36 --dport 3306 -j ACCEPT

#iptables pour le serveur
iptables -A FORWARD -p tcp -s 10.31.112.1 --dport 2222 -j ACCEPT
iptables -A FORWARD -p tcp -m iprange --src-range 10.187.20.20-10.187.20.54 --dport 2222
```

sisr1-g7/mission_8.txt · Dernière modification: 2021/05/11 13:35 de h-benzahaf