TP Filtrage

Un pare-feu (ou Firewall) est un dispositif logiciel permettant de filtrer les paquets réseau afin de mettre en place une politique de sécurité. Un pare-feu peut être avec états (stateful firewall) (il mémorise l'état des connexions, en vérifie la conformité et applique des règles adaptées) ou sans état (stateless firewall) (il applique des règles sur chaque paquet de manière indépendante).

Le pare-feu linux (appelé iptables) est sans état.

1) Le filtrage des paquets

Le programme iptables sert à manipuler les règles de filtrage de paquets au niveau du noyau Linux. Il permet de configurer un pare-feu.
Le noyau dispose de listes de règles appelées des **chaînes**. Les règles **sont analysées les unes à la suite des autres dans l'ordre de leur écriture**. Dès qu'une règle peut s'appliquer à un paquet, elle est déclenchée, et la suite de la chaîne est ignorée. Les chaînes sont regroupées dans des **tables**. Il existe trois tables :

- Table **NAT** (*Network Address Translation*) : elle est utilisée pour la translation d'adresse ou la translation de port. Deux types de chaînes s'appliquent à cette table :
  - PREROUTING
  - POSTROUTING

- Table **FILTER** : c'est la table par défaut. Elle contient toutes les règles de filtrage. Trois types de chaînes s'appliquent à cette table :

INPUT pour les paquets entrants dans la machine,
_ OUTPUT : pour les paquets g_en_er_es localement,

  - .
  - OUTPUT
  - FORWARD : pour les paquets rout_es _a travers la machine
- Table **Mangle** : contient les règles de modification des paquets.

❖ **Les opérations servant à gérer les chaînes entières** (les 3 chaînes intégrées INPUT OUTPUT FORWARD ne peuvent pas être effacées) :

Créer une nouvelle chaîne utilisateur	-N	iptables -N test
Supprimer une chaîne utilisateur vide	-X	iptables -X test
Changer la police d'une chaîne intégrée	-P	iptables -P FORWARD DROP
Afficher les règles d'une chaîne ou de toutes les chaînes sous forme numérique	-L -n	iptables -L INPUT iptables -L iptables -nL
Supprimer les règles d'une chaîne ou de toutes les chaînes	-F	iptables -F INPUT iptables -F

❖ **Les moyens pour manipuler les règles à l'intérieur d'une chaine**

Ajouter une nouvelle règle à une chaîne	-A	iptables -A INPUT -s 0/0 -j DENY
Insérer une nouvelle règle à une position quelconque de la chaîne	-I	
Remplacer une règle à une position quelconque de la chaîne	-R	
Supprimer une règle à une position quelconque de la chaîne	-D	iptables -D INPUT 1
Supprimer la première règle vérifiée dans la chaîne	-D	iptables -D INPUT -s 127.0.0.1 -p icmp -j DENY

❖ QUELQUES PARAMETRES DE CIBLE : Les cibles sont précisée en fin de commande par l'option --jump (ou –j)

Les adresses IP source (option –s ou --source) et destination (option –d ou --destination) peuvent être spécifiées :

•en utilisant le nom complet

•en utilisant l'adresse IP, comme 195.221.42.159

•en indiquant un groupe d'adresse IP, comme 195.221.42.0/255.255.255.0 (c'est-à-dire toutes les adresses du réseau 195.221.42.0) ou en notation condensé 195.221.42.0/24)

•en désignant n'importe quelle machine : 0.0.0.0/0 ou 0/0

Test	Option Complète	Option Abrégé	Valeurs
Adresse IP Source	--source *@IP*	-s @IP	@IP = IP en Décimal
Adresse IP Destination	--destination *@IP*	-d @IP	@IP = IP en Décimal
Interface d'entrée	--in-interface *Interface*	-i *Interface*	Interface = eth0, ppp0, ...
Interface de sortie	--out-interface *Interface*	-o *Interface*	Interface = eth0, ppp0, ...
Protocole	--protocol *Proto*	-p *Proto*	Proto = udp, tcp, icmp ou all
Port source	--source-port *Port*	--sport *Port*	Port = N° de port ou Nom du service associé 25:110 teste tous les ports de 25 à 110 -m muliport -sport 53,80 teste les ports 53 et 80
Port destination	--destination-port *Port*	--dport *Port*	Port = N° de port ou Nom du service associé 25:110 teste tous les ports de 25 à 110 -m muliport -sport 53,80 teste les ports 53 et 80
Etat du paquet	--state *Etat*		Etat = NEW, ETABLISHED, RELATED ou INVALID

Mise en place de règles de filtrage

Pour apprendre à manipuler les règles de filtrage, nous allons commencer par bloquer le ping sur l'adresse de bouclage (127.0.0.1) de chaque machine.

1) Vérifiez que votre interface de bouclage fonctionne correctement (0% des paquets perdus) :

ping –c 1 127.0.0.1

2) Créez une nouvelle chaîne utilisateur nommée LOG_DROP pour à la fois rejeter les paquets et enregistrer dans le journal (fichier /var/log/messages) les paquets rejetés.

iptables –N LOG_DROP

iptables –A LOG_DROP –j LOG

iptables –A LOG_DROP –j DROP

3) Appliquez un filtre sur la chaîne d'entrée INPUT :

iptables –A INPUT –p icmp –s 127.0.0.1 –j LOG_DROP

4) Vérifiez que votre modification a bien été prise en compte en affichant la chaîne INPUT :

iptables –L INPUT

5) Ouvrez un autre shell dans un terminal, puis tapez la commande :

tail –f /var/log/messages

Dans le terminal initial, essayez de faire à nouveau le ping ; la connexion ne doit pas pouvoir aboutir (100% des paquets perdus). Observez les messages qui s'affichent au fur et à mesure dans le terminal dans lequel vous avez lancé la commande tail.

6) Interdisez maintenant en TCP :

- l'accès aux paquets venant du port 80 (réponses http)
- l'accès aux paquets allant vers le port 80 (requêtes http)

7) Effacez les règles précédentes

8) Maintenant le poste de travail devient serveur web exclusivement. Il ne peut rien faire d'autre. Ecrivez les règles.