Auteur: P. Petit	*Titre: TD ASRA: introduction à l'utilisation de netfilter*	*Version: 1.0*
Date: 31/02/2007	Licence: Gnu Free Documentation Licence	Durée: 3h00

ASRA 01: Introduction à l'utilisation de netfilter

Objectifs

- comprendre l'utilisation de base de netfilter
- utilisation des outils nmap, hping et ethereal/tcp dump pour le debugging

Configuration initiale

Ce TD est à réaliser avec quatre machines linux debian.Sarge (cf maquette 1)

Prérequis

- configuration réseau d'une station unix (debian sarge)
- notion théoriques sur les filtres de paquets à Etat, sur les tables netfilter (input, output, forward)
- analyse de trames et utilisation d'outil comme ethereal ou tcpdump.

Exercice 1: notions netfilter

1. La table FILTER comprend 3 chaînes prédéfinies. Citez ces trois chaînes et expliquez les types de paquets concernés par chaque chaîne en vous appuyant sur des exemples (utilisez le réseau de la maquette 1 pour éviter d'avoir à décrire le réseau sur lequel vous vous appuyez
2. Quelle différence (comportement, cas d'utilisation, ...) y a-t-il entre les cibles DROP et « REJECT --reject-with tcp-reset. » ?

Exercice 2: étude de règles classiques

1. expliquer les règles netfilter suivantes :

groupe de règles No 1:

```
iptables -A INPUT -p TCP  --dport 22 -j ALLOWED
```

groupe de règles No 2:

```
iptables -A INPUT -p ICMP --icmp-type 8 -j ACCEPT
iptables-A INPUT -p ICMP --icmp-type 11 -j ACCEPT
```

groupe de règles No 3 (quelle différence avec le groupe 2 ?):

```
iptables -N icmp_packets
iptables -A icmp_packets -p ICMP --icmp-type 8 -j ACCEPT
iptables -A icmp_packets -p ICMP --icmp-type 11 -j ACCEPT
iptables -A INPUT -p ICMP -j icmp_packets
```

groupe de règles No 4:

```
iptables -N allowed
iptables -A allowed -p TCP --syn -j   ACCEPT
iptables -A allowed -p TCP -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A allowed -p TCP -j DROP
```


Auteur: P. Petit	*Titre: TD ASRA: introduction à l'utilisation de netfilter*	*Version: 1.0*
Date: 31/02/2007	Licence: Gnu Free Documentation Licence	Durée: 3h00

Exercice 3: fichier de règles classique

Récupérer le fichier rc.firewall (http://iptables-tutorial.frozentux.net/scripts/rc.firewall.txt) et expliquer le travail réalisé par les divers sous-sections de la section 4 du fichier.

Exercice 4: maquette 1: pare feu sans états

1. faites en sorte que netfilter soit actif sur la machine F et configurez le SANS UTILISER le suivi de session (ip_conntrack et ipt_state) de façon à ce que :
   - il soit possible de « pinger » B et internet depuis A et C;
   - que les hôtes C et A ne puissent pas être « pinger » depuis B ou internet.;
   - qu'il soit possible d'établir des connections ssh sur B depuis C mais pas depuis A;
   - que A et C puisse faire des requetes dns B et vers internet.
2. testez la configuration de votre coupe feu avec les outils nmap et hping2. Vous indiquerez dans votre compte-rendu de TP les commandes utilisées, le résultat de ces commandes et vos commentaires. Quand c'est pertinent, vous pourrez aussi vous appuyer sur des analyses de trames en précisant à chaque fois sur quel hôtes elles ont été réalisées. On pratiquera notamment :
   - un scan de ports de C et A depuis B (configuration par défaut de nmap)
   - un scan de ports de C et A depuis B en imposant à nmap d'utiliser le port 22 comme port source puis 53 comme port source.

Exercice 5: maquette 1: pare feu à états

reprendre l'exercice précédent en activant et en utilisant les fonctionnalités de suivi d'état de netfilter.

Exercice 6: journalisation, entrées de la table de suivi d'états

1. affichez la liste des règles ainsi que le nombre de paquets passés par chaque règles.
2. comment consulte-t-on les tables du suivi de connexion ? Utilisez hping pour montrer l'évolution de l'état interne d'une connexion tcp (votre compte-rendu contiendra la commande hping et l'entrée modifiée de conntrack). Comparez ces états internes avec ceux que l'on peut manipuler Ces états internes sont-ils équivalents à ceux que l'on peut manipuler via iptables -m state ?
3. A quoi sert la cible LOG ? Mettez là en application pour journaliser tous les paquets venant de B non autorisés à passer FW. Faites en sorte qu'elle soit utilisée et montrez l'une des entrées correspondantes des journaux. Quelle est la taille de cette entrée (un minorant à la louche en octets suffira) ? Si B se met à envoyer une centaine de paquets udp non autorisés à passer FW par seconde, quelle sera la taille du journal concerné au bout de 10mn, au bout d'une heure, au bout de 24h00 ? expliquez comment résoudre ce problème. Mettez la solution en application.