Auteur: P. Petit	*Titre: TD ASRA: introduction à l'utilisation de pf*	*Version: 1.2*
Date: 12/02/2018	Licence: Gnu Free Documentation Licence	Durée: 3h00

ASRA 02: Introduction à l'utilisation de packet filter, le filtre de packet d'OpenBSD

Objectifs

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

Configuration initiale

Ce TD est à réaliser avec quatre machines virtuelles:

- 3 machines virtuelle d'un unix de votre choix : A, B et C
- une machine virtuelle openbsd : FW

Prérequis

- configuration réseau d'une station unix (unix A, B, C et openBSD)
- notion théoriques sur les filtres de paquets à Etat
- analyse de trames et utilisation d'outil comme wireshark ou tcpdump (cf https://www.ibisc.univ-evry.fr/~petit/Enseignement/AdminSystem/Tuto-varies/tcpdump.html).

Outre les pages de manuel ad hoc, vous pourrez consulter la FAQ en français de packet filter à l'adresse http://www.openbsd.org/faq/pf/fr/index.html

Exercice 1: notions packet filter

1. La table FILTER de netfilter comprend 3 chaînes prédéfinies: INPUT, OUTPUT et FORWARD. Comment réaliser un travail similaire avec packet filter. Donnez quelques exemples de règles que vous écrirez pour netfilter et pour packet filter.

Exercice 2: étude de règles classiques

1. expliquer les règles packet filter suivantes :

groupe de règles No 1:
bloc in all
bloc out all
pass in on dc0 from 192.168.0.0/24 to 192.168.1.1 no keep state
groupe de règles No 2:
bloc in all
bloc out all
pass in on dc0 from 192.168.0.0/24 to 192.168.1.1
groupe de règles No 3:
my_ip="192.168.10.6"
if_in="dc0"
if_out="fxp0"
local_net="192.168.0.0/24"
bloc in all
block out all
block in quick from $local_net to $my_ip

```
pass in on $if_in from $local_net proto tcp flags S/SA to any port ssh
pass in on $if_in from $local_net proto tcp flags S/SA to any port domain
pass in on $if_in from $local_net proto udp to any port domain
```

Exercice 3: maquette 1: routage

1. on considère la maquette 1. Le routeur par défaut de B est 192.168.195.2 (routeur de la salle). Configurez le routage de façon à ce que les machines A, B, C et F puissent communiquer les unes avec les autres : on garantira que ping fonctionne entre toutes ces machines. Votre rapport contiendra une explication succincte de ce que vous avez fait ainsi qu'une copie des fichiers de configurations concernés.

Exercice 4: maquette 1: pare feu avec états

1. faites en sorte que packet filter soit actif sur la machine FW et configurez le en utilisant le suivi de session (keep state) de façon à ce que :
    - il soit possible de « pinger » B 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 A mais pas depuis C;
    - que A et C puisse faire des requêtes dns vers B.
2. testez la configuration de votre coupe feu avec les outils nmap et, éventuellement, 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 depuis C et depuis A vers B (configuration par défaut de nmap)
    - un scan de ports depuis C et depuis A vers B en imposant à nmap d'utiliser le port 22 comme port source puis 53 comme port source.

- l'option block-policy permet de définir le comportement à adopter en cas de blocage. Indiquez la différence entre les deux comportements et testez là.

Exercice 5: assainissement et mandataire syn

1. utiliser l'option « modulate state » au lieu de keep state dans la règle concernant ssh. Mettez en évidence[1] sur un exemple le travail réalisé par « modulate state »
2. utiliser l'option « synproxy state state » au lieu de keep state dans la règle concernant ssh. Mettez en évidence sur un exemple le travail réalisé par «synproxy state »
3. normalisation (scrub) : activez la fonctionnalité de normalisation sur tout le trafic routé par votre coupe feu. Mettez en évidence sur des exemples des transformations subies par les paquets.

1 En réalisant, par ex. 2 captures de trames.

Exercice 6: authpf

1. on souhaite autoriser certaines connexions après authentification des utilisateurs concernés. Utiliser authpf pour faire en sorte que les utilisateurs des postes windows aient toutes leurs connexions vers l'extérieur autorisées après qu'ils se soient authentifiés.

Vous utiliserez pour cela authpf:

- créer un utilisateur test
- créer un fichier vide /etc/authpf/authpf.conf
- créer un fichier /etc/authpf/authpf.rules contenant les règles à appliquer à tous les utilisateurs
- insérer une ancre nommée « authpf/* » dans le fichier ipf.conf à l'endroit où ces règles doivent s'appliquer
- définir /usr/sbin/authpf comme shell aux utilisateurs concernés avec la commande chsh