I2L - Linux en réseau - TD2

Éric Leblond

30 novembre 2009

Introduction

Le but de ce TD est de travailler sur les capacités de filtrage de GNU/Linux. On abordera ensuite la mise en place d'une politique de routage avancée.

1 Utilisation de netem

Netem est une discipline de QoS développé par Stephen Hemminger. Elle permet de simuler des problèmes réseaux sur un lien standard.

Télécharger lagfactory.sh depuis la page http ://software.inl.fr/trac/wiki/LagFactory.

Ce script a été développé pour faciliter l'utilisation des fonctionnalités de Netem.

Question 1 *Paramétrer le script pour avoir 10% de perte de paquets et un temps de transmission de 1s sur l'interface réseau connecté à l'université.*

Question 2 *Lister la discipline appliquée sur l'interface*

Question 3 *Lister les règles iptables et les commenter.*

2 Utilisation de Netfilter

2.1 Introduction

La couche Netfilter intégrée au noyau propose une couche de filtrage complète permettant de réaliser des politiques de filtrages avancées.

Les outils nécessaires à ce TD sont principalement *tcpdump*, *iptables* et *ip*. On veillera donc à installer les paquets nécessaires :

```
# apt-get install tcpdump iproute2
```

Le premier TD sur iptables vous a montré les bases de Netfilter.

2.2 Politique avancée

Question 4 *En utilisant une négation, limiter le trafic de l'utilisateur root au réseau local*

La méthode précédente nous oblige à connaitre le réseau local. Il peut donc être intéressant de supprimer cette dépendance :

Question 5 *En utilisant la target TTL, limiter le trafic de l'utilisateur root au réseau local*

2.3 Suivi de connexions

Installer libnfnetlink, libnetfilter_conntrack et les conntrack-tools sur votre système.
Visualisation des événements avec conntrack -E

Question 6 *Pourquoi y a-t-il deux couples de coordonnées IP ?*

Ouvrir une connexion vers un serveur (type ssh) et supprimer l'entrée avec l'option -D de l'outil conntrack.

Question 7 *Que se passe-t-il ?*

Question 8 *Mettre en place un jeu de règle suffisamment strict pour éviter le "problème" précédent ?*

3 Routage avancé

3.1 Manipulation de ip

Question 9 *Récupérer la route utilisée pour aller vers* 1.2.3.4 *grâce à* ip.

Question 10 *Lister le cache de routage et le vider.*

Question 11 *Interdire le routage des IPs* 192.168.44.0/24 *sur la table principale.*

3.2 Routage différencié

Question 12 *Ajouter un alias à l'interface* eth0 *dans le réseau* 192.168.33.0/24.

Question 13 *Déclarer une nouvelle table de routage où la route par défaut est* 192.168.33.1.

Question 14 *Ajouter une règle pour que les paquets provenant du réseau* 192.168.33.0/24 *soit routés sur cette table.*

Question 15 *Tester avec* netcat *les propriétés de routages en emettant une connexion vers le réseau 192.168.44.0/24 depuis une IP du réseau 33.*

Question 16 *Émettre une connexion vers l'extérieur depuis une IP du réseau 33 et valider la route prise grâce à* tcpdump.

3.3 Netfilter et routage

Question 17 *Router l'ensemble des paquets marqués 1 par cette passerelle.*

Question 18 *Router l'ensemble des flux web vers cette passerelle.*

Question 19 *En utilisant les questions de 3.3, indiquez les commandes à utiliser pour répartir les flux entre deux liens internets.*

4 Mise en place de Nulog 2

Le but des exercices est d'installer Nulog2 :

`http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/NuLog2`

4.1 Récupération des sources

On commencera par récupérer les sources de Nulog2.

4.2 Installation de Ulogd

```
# apt-get install ulogd
```

4.3 Configuration

On crée la table MySQL en utilisant ipv4.mysql contenu dans les sources de Nulog2 :

```
mysqladmin create ulogd
cat scripts/ipv4.sql | mysql ulogd
```

Question 20 *Configurer ulogd pour supporter l'export vers la table ulogd.*

4.3.1 Migration des règles de log

Question 21 *On utilisera `iptables -R` pour remplacer les règles en LOG par des règles en NFLOG*

Question 22 *Vérifier le remplissage de la table en comptant le nombre d'entrée contenues.*

4.4 Installation de Nulog2

Question 23 *Utiliser l'url suivante pour installer nulog2 :*

`http://software.inl.fr/trac/trac.cgi/browser/mirror/edenwall/nulog2/trunk/INSTALL`

5 Question subsidiaire

NuFW permet d'apposer une marque sur les paquets suivant des critères variés lors de la décision de filtrage (Équivalent d'un -j ACCEPT).

Question 24 *Décrire la méthode permettant de réaliser un proxy transparent suivant une marque apposée sur les paquets. Si la marque vaut 0 le paquet sort en direct, si il vaut 1 il est redirigé vers le proxy. On notera précisément l'enchainement des règles.*