I2L - Linux en réseau - TD3

Éric Leblond

14 décembre 2009

Introduction

Le but de ce TD est de travailler sur un fichier pcap pour déterminer les raisons d'un problème de performance. Le fichier pcap a été capturé sur un pare-feu en production. Il s'agit donc de données réelles. La seule modification consiste en un retrait des données des applications pour des raisons de confidentialité.

Le diagramme 1 représente l'architecture réseau (très simplifiée) dans laquelle est intégré le pare-feu :

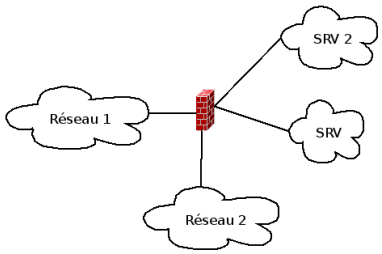

FIG. 1 – Architecture simplifiée

Comme ne le laisse pas apparaitre le schéma, les interfaces du pare-feu sont des vlans construites au dessus d'une interface bonding. On a une interface *bond0* construite à partir des interfaces *eth0* et *eth1*.

La problématique observée par les utilisateurs du réseau est un ralentissement et des pop-up indiquant des difficultés de récupération des messages sur le serveur Exchange (75.0.30.184). Une étude des paramètres de bases du pare-feu et une étude rapide de dump ciblé n'ont pas permis de trouver la raison du problème. En désespoir de cause, il a été réalisé un dump de l'ensemble du trafic réseau pendant une interruption assez longue.

La partie 1 contient des temps morts que l'on pourra exploiter en travaillant sur la partie 2.

1 Reconstitution du système

1.1 Installation de Virtualbox

On installera virtualbox et on créera une première machine virtuelle, nommé A, en debian lenny avec deux interfaces ethernet. Elles seront placés dans un réseau host nommé *interco*.

Créér ensuite une deuxième machine virtuelle, B, ayant une interface réseau connectée elle aussi au réseau *interco*.

1.2 Configuration réseau

Question 1 *Après avoir installé* ifenslave *sur les deux machines créer sur A une interface bond0 à partir des interfaces connectées au réseau* interco*.*

Question 2 *Numéroter l'interface bond0 et réaliser un ping entre les deux systèmes.*

Question 3 *Valider la redondance des liens en débranchant le cable d'une des interfaces de la machine A.*

2 Extraction de données significatives

2.1 Analyse préliminaire

On installera *wireshark* pour étudier le fichier pcap récupéré et on ouvrira le fichier dans la foulée.

Question 4 *Que remarque-t-on ?*

2.2 Focalisation sur le serveur

Question 5 *Extraire les données pour l'IP du serveur de messagerie et enregistrer le résultat dans un fichier séparé sur lequel on travaillera ensuite.*

Question 6 *Pourquoi les données restent encore inutilisables ?*

Question 7 *Extraire un sous-ensemble du fichier permettant d'obtenir un ensemble de paquets cohérents*[1].

2.3 Étude des données

Question 8 *Que permet de conclure l'étude des échanges du protocole TCP ?*

Question 9 *Extraire les flux non TCP et procéder à leur analyse. On veillera à détecter les paquets indiquants des problèmes de configuration réseau.*

2.4 Explication et résolution

L'un des coupable potentiel est donc le paquet suivant :

```
15:15:21.370814 IP (tos 0xc0, ttl 64, id 1660, offset 0, flags [none], proto ICMP (1), length 112)
    75.0.30.254 > 75.0.30.184: ICMP redirect 10.30.15.141 to host 10.30.15.141, length 92
IP (tos 0x0, ttl 127, id 24989, offset 0, flags [DF], proto ICMP (1), length 84)
    75.0.30.184 > 10.30.15.141: ICMP echo reply, id 19997, seq 0, length 64
```

Question 10 *Nonobstant le fait que* 75.0.30.254 *est une des IP du pare-feu et que* 10.30.15.141 *est l'IP du controleur de domaine, montrer que ce paquet permet d'expliquer les bloquages et les ralentissements réseaux.*

Question 11 *Proposer une résolution.*

Conclusion

Le paramétrage par défaut des systèmes réseau est suffisant tant que l'on ne pousse pas le vice trop loin.

3 Connexion de la machine A au réseau local

3.1 Préparation de A

Question 12 *Après avoir éteint la machine A, rajouter une interface réseau connecté à une interface locale* tap0.

Question 13 *Créer et numéroter une interface tun nommé* tap0 *avec l'utilitaire* tunctl. *On veillera à ce que l'utilisateur courant est accès à cette interface.*

Question 14 *Démarrer la machine A et numéroter la nouvelle interface puis vérifier la connectivité.*

[1] On pourra penser à descendre dans les couches du modèle OSI pour chercher un dénominateur commun aux paquets émis ou reçu par le serveur

3.2 Passage en bridge

Question 15 *Créer une interface bridge rassemblant votre interface physique ethernet et l'interface* tap0 *au moyen des* bridge-utils *puis vérifier avec tcpdump que la machine A a bien accés au réseau.*

Question 16 *Tenter de récupérer sur A une adresse avec DHCP.*

Question 17 *Pérenniser le setup réseau en écrivant un fichier* interfaces *reproduisant ce setup. On veillera à utiliser au maximum les fonctionnalités intégrées et à défaut les méthodes* pre-up *et associées.*