M1 Informatique Réseaux et systèmes
TP3 – TP4

Gaétan Richard
gaetan.richard@unicaen.fr

09/2017

1 Introduction

Le but premier est de configurer un réseau minimal. On s'intéressera particulièrement dans cette partie à l'aspect routage. On pourra reprendre le réseau du T.P. 1, afin d'arriver au réseau décrit en figure 1.

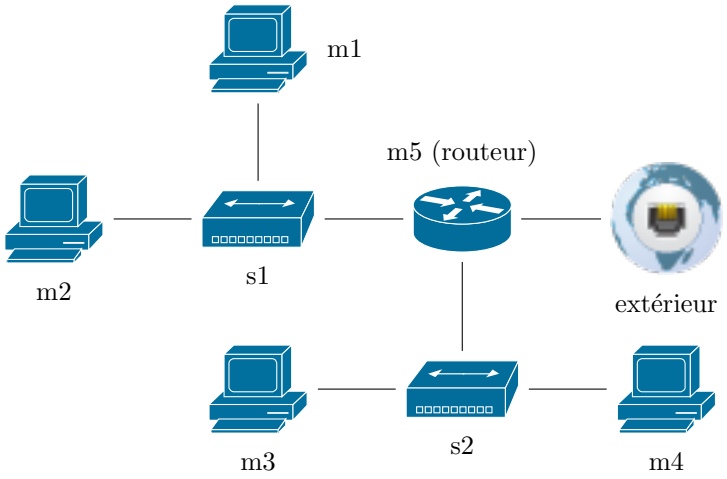

FIGURE 1 – Notre réseau de test

Note : en IPv4, vous pouvez continuer à prendre des réseaux privés (des /24 de préférence). Pour IPv6, voir plus bas le paragraphe 3.

Ce réseau sera également utilisé pour les T.P. suivants. Pensez à le sauvegarder !

2 Routage statique IPv4

Vérifiez que la configuration IPv4 est toujours fonctionnelle et corrigez la au besion.w

3 IPv6

3.1 Adresses fixes

Maintenant, on se donne pour chaque étudiant une classe ipv6 allant de `2001:660:7101:0011::/64` à `2001:660:7101:001F::/64`. Ajouter la configuration statique en IPV6 sur les machines m1 à m4 et configurer les tables de routages avec une route par défaut pour les machines m1 à m4, et plus en détail celle du routeur m5 (on pourra utiliser l'option `-A inet6` de la commande `route`, ou mieux la commande `ip`).

Attention ! Comme on a deux sous-réseaux, il faut “diviser” le /64 fourni. On utilisera pour cela deux /65 comme vu en exercice. Si on prévoit un réseau de plus, il faudra diviser en 3, 4, ...

La configuration externe est fournie par radvd. L'adresse obtenue n'est pas routée (adresse d'interconnection).

3.2 Connexion externe

Pour la suite, nous allons manipuler des services qui sont disponibles par l'intermédiaire de `Quagga` dont la configuration est présente dans `/etc/quagga/`.

Il reste à indiquer au reste du monde que vous disposez des machines dans le préfixe qui vous a été attribué. Pour cela, nous utiliserons le protocole *RIPng*. Nous allons maintenant annoncer notre préfixe en utilisant *RIPng*. Pour cela, il faut modifier le fichier `/etc/quagga/ripngd.conf`. Vous trouverez un exemple de configuration à l'emplacement `/usr/share/doc/quagga/examples/`.

Une fois la configuration effectuée et `Quagga` relancé (par l'intermédiaire de **/etc/init.d/quagga restart**), les routeurs devraient commencer à s'échanger leurs routes et au bout de quelques instants, il devrait être possible de se connecter aux machines en utilisant les adresses de ces préfixes.

Il ne faut bien sur pas oublier d'activer le forwarding des paquets ipv6 sur m5.

Vérifiez que tout fonctionne au niveau réseau :

— Pinger une machine sur Internet ;
— Consuluter un site web ;
— Faite un ssh depuis la machine physique dans le réseau `etu.info.unicaen.fr` vers m1 en IPv6.

3.3 Sécurisation

Activez l'extension IPv6 privacy pour ne pas avoir votre adresse MAC dans l'adresse IP construite par radvd.

3.4 Retour vers le passé

Mettez en place un seveur dhcp (v4 puis v6) sur m5 pour configurer m3 et m4. Peut-on utiliser *radvd* ?

4 Système

Nous allons regarder les actions effectuées depuis le début de l'année sur une machine virtuelle du réseau. Pour cela, vous allez vous connecter sur *m5* et analyser les différents fichiers afin de répondre aux questions.

Pour analyser les fichiers, on pourra utiliser la commande **grep** ou la commande **awk**.

4.1 /var/log

En analysant les fichiers de *var/log*, déterminer la date d'installation de m5 ainsi que toutes les connexions qui ont eu lieu sur cette machine.

Déterminer tous les services ayant laissé des traces dans les logs.

Essayer de faire une connexion ssh avec un login et mot de passe invalide. Ceci se retrouve-t-il dans les logs.

4.2 binaires

Comparer les sommes *md5* des différents binaires (**ls**,**ps**, ...) sur la machine avec ceux de vos voisins.

Installer le paquet *chkrootkit* et lancer le programme. Expliquer ce que fait ce programme.

4.3 Historique

À l'aide de la commande fin, trouver tous les fichiers modifiés dans `/etc` depuis début novembre.

En analysant l'historique de l'utilisateur root, confirmer les question déjà obtenues.

4.4 Sur votre site universitaire

À partir de ce moment, on se place simplement sur les machines étudiant.
Si cela est disponible, essayer d'atteindre l'adresse `https://nn^o etu.users.info.fr/myadmin`.
Commenter.

4.5 Masquage

On se donne le fichier C suivant :

```
#define _GNU_SOURCE
#include <sys/types.h>
#include <sys/dir.h>
#include <unistd.h>
#include <errno.h>
#include <dirent.h>
#include <dlfcn.h>


static  struct dirent *  (*old_readdir)(DIR *dirp) = NULL;

int errno;
struct dirent * temp ;

struct dirent * readdir(DIR *dirp)
{
  if (old_readdir == NULL)
    {
      old_readdir = dlsym(RTLD_NEXT, "readdir");
    }

  temp=old_readdir(dirp);
  if ((temp != NULL) && (strncmp(temp->d_name,"toto",255)==0))
    {
      temp=old_readdir(dirp);
    }
  return(temp);

 }
```

Compiler ce programme à l'aide de la commande **gcc -shared -Wl,-soname,libfuncs.so.1 -fPIC -o libfuncs.so.1.0** ***fichier.c***. Puis créer deux liens symboliques à l'aide des commandes **ln -s libfuncs.so.1.0 libfuncs.so.1** et **ln -s libfuncs.so.1 libfuncs.so** ainsi qu'un fichier ou dossier toto.

Dans un terminal temporaire et dans le dossier ou se trouve cette librairie, modifier les variables d'environnement comme suit :

— **export LD_LIBRARY_PATH=‘pwd‘**
— **LD_PRELOAD=libfuncs.so.1**

Comparer alors les résultats de la commande **ls** et expliquer ce que fait le programme. Observer en particulier le résultat de la commande **ldd**

4.6 strace

En utilisant la commande **strace**, observer le fonctionnement de la commande **ps**.
Essayer ensuite de modifier cette commande de différentes façon afin de cacher des processus.