TD M2102 - Architecture des réseaux
Configuration réseau – Sécurité réseau

(Adaptation de TDs écrits par Vincent Autefage basés sur l'environnement virtuel NEmu)

Gestion du réseau virtuel

Ce TP tourne sur un réseau virtuel basé sur l'émulateur de machine virtuelle QEMU.

Michel Billaud, enseignant au département, a développé une sur-couche QS, installée dans /net/adm sur les machines du département, qui permet de configurer et manipuler de tels réseaux virtuels basés sur QEMU.

Au département, la machine virtuelle de base tourne sous une distribution allégée de debian.

Pendant la simulation :

- Vous êtes administrateur de la machine virtuelle : compte **root** et mot de passe **plop**
- La souris est parfois « capturée » par le simulateur quand vous cliquez dans une fenêtre, tapez Ctrl-Alt pour la libérer
- Vous disposez d'éditeurs de texte simples : nano ou jed (Ctrl-x s pour sauver, Ctrl-x c pour quitter)
- Redémarrez une machine par **reboot**
- Arrêtez proprement une machine par **halt**
-
- Le montage **/mnt** permet de copier des fichiers depuis/vers la racine de votre compte local
-
- Pour des manipulations avancées :
  - Démarrez l'interface graphique par **startx**
  - Par bouton droit, vous avez accès à diverses applications : interpréteur de commandes, navigateur, « sniffeur » (wireshark), etc…

Installation : exécutez le script

~/Bibliotheque/M2102 – Architecture des reseaux/ installer-tp-routagehack.sh

(cela a pour effet de copier le fichier tp-routagehack.tgz dans votre répertoire ~/QS)

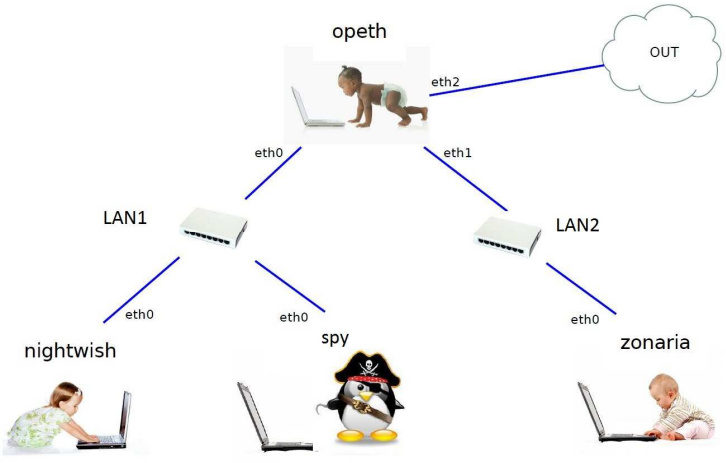
Simulation : exécutez la commande

qs-run tp-routagehack

(cela a pour effet de créer une session de travail dans le répertoire /tmp de la machine locale, et de lancer le réseau de machines virtuelles)

Topologie du réseau virtuel :

Le réseau est composé de deux réseaux locaux LAN1 et LAN2 interconnectés par un routeur (*opeth*), l'un avec les postes *nightwish* et *spy*, et l'autre avec le poste *zonaria*. Le routeur *opeth* est également relié à internet.



Les machines virtuelles vous sont livrées *nues*. C'est-à-dire qu'elles disposent uniquement des réglages élémentaires du système.
C'est donc à vous de faire le reste ☺

Première Partie : Configuration réseau

1. Un peu d'administration système : ajout d'un utilisateur

Les machines étant neuves, le seul compte existant est celui de l'administrateur.

1- Identifiez vous donc en tant que *root* (rappel : le mot de passe est *plop*).

2- Ajoutez un nouvel utilisateur sur une des machines à l'aide de la commande **adduser** :

adduser <nomlogin>

3- Tentez de vous connecter sur le compte de votre nouvel utilisateur à l'aide de la commande **login** :

login <nomlogin>

4- Revenez sur le compte de l'administrateur en quittant le compte courant avec la commande **exit**.

2. Choix de l'adressage IP

Vous allez maintenant choisir les adresses IP attribuées à chacun de vos sous-réseaux locaux LAN1 et LAN2, ainsi qu'aux machines.

5- Le masque de sous-réseau sera le même pour les 2 sous-réseaux : **255.255.255.0**.
Qu'est-ce que cela signifie ?

6- Choisissez pour chaque sous-réseau une adresse IP privée commençant par **192.168** :

Adresse de LAN1 : ……
Adresse de LAN2 : ……

7- Choisissez en conséquence les adresses IP des machines :

eth0 de opeth : ……
eth0 de nightwish : ……
eth0 de spy : ……
eth1 de opeth : ……
eth0 de zonaria : ……

Conseil : reportez ces numéros sur le schéma du réseau pour plus de lisibilité pour la suite du travail.

3. Configuration et tests

Vous allez maintenant réaliser la configuration réseau des machines pour qu'elles puissent toutes communiquer entre elles.

8- Attribuez les adresses IP aux interfaces de chaque machine à l'aide de la commande **ifconfig** :
Exemples de syntaxe :

ifconfig
ifconfig <iface> <@IP> netmask <netmask>
ifconfig <iface> up
ifconfig <iface> down

Exemple d'utilisation :

ifconfig eth0 192.168.0.1 netmask 255.255.255.0

9- Testez votre configuration à l'aide de la commande **ping** :

ping <@IP> *(ctrl C pour stopper)*
ping –c1 <@IP> *(pour envoyer un seul paquet)*

Attention : à ce stade, la communication entre les machines du LAN1 (*nightwish* et *spy*) et celle du LAN2 (*zonaria*) est impossible car *opeth* rejette les paquets qui ne lui sont pas directement destinés.

10- Pour régler le problème, vous allez indiquer au système de la machine *opeth* qu'il doit transmettre les paquets qui ne lui sont pas destinés, c'est-à-dire qu'il doit agir comme un routeur, grâce à la commande :

sysctl –w net.ipv4.ip_forward=1

Pourquoi ne peut-on toujours pas faire communiquer *nightwish* et *zonaria* (ou *spy* et *zonaria*) ?

11- Indiquez sur *nightwish*, *spy* et *zonaria* que *opeth* doit être leur passerelle par défaut grâce à la commande **route** :
Exemples de syntaxe :

```
route -n
route add default gw <@IP passerelle>
route del default gw <@IP passerelle>
```

Exemple d'utilisation :

```
route add default gw 192.168.0.1
```

12- Testez maintenant la communication entre *nightwish* et *zonaria* (ou *spy* et *zonaria*) à l'aide de la commande **ping**. Testez également la connexion à distance avec la commande **ssh** et les comptes utilisateurs que vous avez créés au début de la séance.

13- L'interface **eth2** d'*opeth* est reliée à un routeur « virtuel » qui est lui même connecté à internet.
Enregistrez *opeth* auprès de ce routeur et activez le NAT à l'aide des commandes suivantes (sur *opeth*) :

```
dhclient eth2
iptables -t nat -A POSTROUTING --source 192.168.0.0/16 -j MASQUERADE
```

Vous obtenez ainsi automatiquement une adresse IP et une passerelle par défaut, et le NAT est activé.

14- Tentez d'effectuer la commande suivante pour vérifier que *opeth* a bien accès à internet :

```
wget www.labri.fr
```

15- Recopiez le contenu du fichier **/etc/resolv.conf** (sur *opeth*) sur toutes les autres machines. Ceci permet de leur indiquer le serveur DNS à utiliser.

16- Effectuez le test du **wget** sur chaque machine pour vérifier leur accès à internet.

Deuxième Partie : Sécurité réseau

L'objectif est de vous initier à certaines techniques dites d'*attaque* afin de vous faire prendre conscience de l'importance de la sécurité en informatique. L'utilisation des outils présentés ici dans un autre cadre et notamment au sein de l'université sera très sévèrement punis tant sur le plan universitaire que pénal.

1. Que dit le droit pénal ?

Article 323-1 : *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.*
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-2 : *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.*

Article 323-3 : *Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.*

Article 323-3-1 : *Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.*

L'article 323 du code pénal comporte d'autres alinéas qui durcissent le tableau dressé ci-dessus.

2. Mise en place d'une attaque de type « *man in the middle* »

ARP

Lorsque une machine fait une requête à une autre machine sur un même réseau local, la machine appelante effectue une requête **arp** de manière à acquérir l'adresse physique (appelée aussi MAC) de la machine qu'elle cherche à joindre. Cette association IP/MAC est gardée en cache quelque temps dans une table de correspondance.

1- Consultez la table de correspondance entre adresse IP et MAC d'une ou plusieurs machines grâce à la commande :

```
arp -n
```

Principe de l'attaque

Les requêtes/réponses **arp** étant faites en *broadcast*, le principe est de *spoofer*, c'est-à-dire inonder la victime (ici *nightwish*) de réponses **arp** de manière à lui faire croire que l'adresse IP de la passerelle (ici *opeth*) qu'il souhaite contacter correspond à notre machine pirate (ici *spy*). Il faut ensuite transmettre ses requêtes à la véritable passerelle. De cette manière, notre machine pirate jouera le rôle de relais entre la victime et l'extérieur. Nous pourrons ainsi espionner toutes ses communications.

A l'abordage !

2- Passez tout d'abord en mode graphique sur *spy* grâce à la commande **startx**.

3- Sur *spy*, ouvrez un terminal et commencez par activer l'*IP forwarding* pour qu'elle se comporte comme un routeur.

4- Utilisez la commande **arpspoof** de manière à réaliser le *man in the middle* :

```
arpspoof –t <@IP victime> <@IP vraie passerelle>
```

5- Ouvrez maintenant l'utilitaire **wireshark** (dans un nouveau terminal) afin de capturer le trafic qui passe sur votre interface réseau :

```
wireshark –i eth0 -k
```

Vous pourrez constater le florilège de paquets **arp** que vous êtes honteusement en train d'émettre...

6- Lancez une session graphique ainsi que le navigateur web sur *nightwish* et baladez vous un peu sur la toile...
Vous constaterez que *spy* trace tout ce que fait *nightwish* . Nous avons donc réussi !

7- Quels types de trames peut-on voir transiter ?

8- À quelles couches du modèle OSI appartiennent elles ?

9- Lorsque *nightwish* contacte un serveur web, plusieurs **GET** apparaissent. Pourquoi ?

10- Comment *nightwish* pourrait-il se rendre compte de cet ignoble complot ?

11- Éteignez chaque machine correctement à l'aide de la commande **halt**.

3. Bilan

Vous avez pu constater la facilité ainsi que l'efficacité de cette méthode. En conclusion, nous pouvons affirmer qu'une adresse IP ne fait pas foi sur l'identité d'un interlocuteur.
Il existe néanmoins des solutions qui permettent de détecter ce genre d'attaque, comme :
arpwatch (http://ee.lbl.gov) ou encore **arpalert** (http://www.arpalert.org/arpalert.html).