université de BORDEAUX

Master 1 *Sciences Technologies*

Année 2015-2016
Étape : Master Sciences Technologies (semestre 2)
Épreuve de : Administration des rseaux
Date : 10 Mai 2016
Heure : 14h00

Session de Mai 2016
UE : IN8W13
Durée : 1h30
Documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. Expliquer comment un paquet destiné à une machine faisant partie d'un réseau privé traverse les différents points de contrôle d'`iptables`. Il vous est particulièrement demandé de mettre en avant le moment où la translation d'adresse est faite. Deux cas seront à considérer, les paquets entrants vers le réseau et les paquets sortants du réseau.
2. Expliquer la différence entre une recherche itérative et une recherche récursive en `DNS`.
3. Quel est le rôle du transfert de ports (*port forwarding*) dans les mécanismes de translation d'adresses dynamique ?
4. Expliquer le rôle du service `portmap/rpcbind`.
5. Dans un réseau local, expliquer ce qui se passe lorsque deux machines ont la même adresse IP. Même question lorsqu'elles ont la même adresse physique (MAC).
6. Expliquer rapidement le fonctionnement du protocole `ARP`. Qu'apporte l'utilisation de caches dans des protocoles tels qu'`ARP` ou `DNS` ? Quels sont les problèmes posés par l'utilisation de tels caches ?

Exercices

1. Un système de translation d'adresses statique est utilisé pour donner accès à Internet à 2 postes de travail. Ce système disposant de deux adresses IP publiques associées de manière statique à chacune des adresses privées, combien de connexions TCP simultanées sur le port 80 du serveur web dont l'adresse IP est `74.125.230.210` peuvent être supportées au plus ? Expliquez. Nous considérerons le cas où le serveur web n'a pas de mécanisme lui permettant de limiter le nombre de connexions simultanées.
2. Un serveur FTP se trouve dans une DMZ qui est séparée d'Internet par un pare-feu pratiquant la translation d'adresses dynamique. Quel problème risque de survenir lors d'une connexion entre un client et le serveur FTP ? Dans le cas où la connexion serait impossible, proposer une solution. Il vous est demandé de considérer le cas du mode actif ainsi que celui du mode actif.
   Rappel : Le protocole FTP utilise deux connexions. La première dite de contrôle est faite généralement sur le port 21. La seconde, quant à elle sert à transférer les données. Elle est soit ouverte par le client après que le serveur lui ait indiqué le numéro de port correspondant (c'est le mode passif) ou par le serveur sur un port indiqué par le client (c'est le mode actif).

Problème

Soit le script de configuration d'`iptables` donné ci-dessous. Il correspond au réseau représenté par la figure 1 et est exécuté par la machine `immortal`.

```
#!/bin/sh
[1] iptables -F
[2] iptables -t nat -F

[3] iptables -P INPUT DROP
[4] iptables -P OUTPUT DROP
[5] iptables -P FORWARD DROP

[6] iptables -A INPUT  -i eth0 -j ACCEPT
[7] iptables -A INPUT  -i lo -j ACCEPT

[8] iptables -A OUTPUT  -o eth0 -j ACCEPT
[9] iptables -A OUTPUT  -o lo -j ACCEPT
```

```
[10] iptables -t nat -A POSTROUTING -s 192.168.0.0/28 -o eth1 -j MASQUERADE

[11] iptables -t nat -A POSTROUTING -s 192.168.0.254 -j SNAT --to-source 147.210.20.2
[12] iptables -t nat -A PREROUTING -d 147.210.20.2 -j DNAT --to-destination 192.168.0.254

[13] iptables -A FORWARD -i eth0  -s 192.168.0.0/24 -j ACCEPT
```

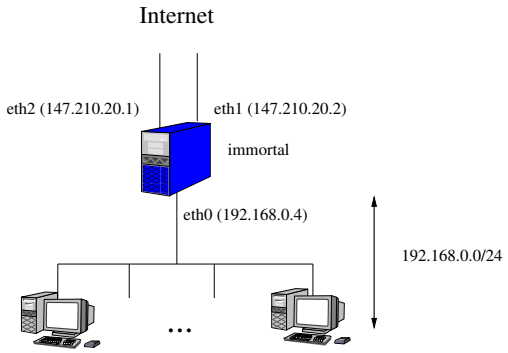

FIGURE 1 – Architecture du réseau.

1. Détailler les modification que subit un paquet (correspondant à une ouverture de connexion) envoyé par l'hôte 192.168.0.1 à la machine dont l'adresse IP est 74.125.206.99 sur le port 80. Ce paquet arrivera-t-il à destination ? Expliquer. Qu'en est il de la connexion correspondante ? pourra-t-elle être établie ? Dans le cas où elle ne le pourrait pas ajouter une (ou plusieurs) règles pour que ce soit possible.
2. Expliquer pourquoi le paquet envoyé par la machine par la machine dont l'adresse IP est 192.168.0.250 vers la machine d'adresse IP 74.125.206.99 ne peut pas arriver à destination. Proposer une solution.
3. Détailler les modification que subit un paquet (correspondant à une ouverture de connexion) envoyé par l'hôte 192.168.0.254 à la machine d'adresse IP 74.125.206.99 sur le port 80. Ce paquet arrivera-t-il à destination ? Expliquer.
4. Est ce que l'hôte dont l'adresse IP est 74.125.206.99 peut ouvrir une connexion sur le port 21 (ftp) du serveur dont l'adresse IP privée est 192.168.0.1 (on supposera qu'un serveur ftp est exécuté sur la machine correspondante) ? Que faut-il mettre en place dans le cas où cette ouverture de connexion ainsi que l'échange correspondant seraient impossibles ? Détailler dans ce cas les règles iptables correspondantes en les commentant.

   Remarque : À chaque question il est nécessaire de prendre en compte les modifications effectuées dans les questions précédentes.