PR6 – Programmation réseaux
TP n° 1 : Systèmes et réseaux

Exercice 1 : Authentification SSH par clef RSA

Vous souhaitez utiliser les services de `lucien` ou `nivose` à distance depuis une machine que nous nommerons A. Pour cela, il est nécessaire de configurer l'accès sécurisé `ssh`. L'idée est la suivante, `lucien` doit posséder la clé cryptographique publique de la machine A. Cette manipulation est donc à faire *pour toutes les machines A depuis lesquelles vous souhaitez travailler*. Sur A, générez la clé cryptographique avec la commande suivante :
`$ ssh-keygen -t rsa`
qui permet d'obtenir deux fichiers rangés dans le répertoire `.ssh` de votre répertoire privé. Le premier fichier est nommé `id_rsa` et appelé *clé privée*, le second `id_rsa.pub` et appelé *clé publique*. Ne confiez jamais la clé privée à qui que ce soit (considérez que c'est votre numéro de carte bleue). Par contre, vous pouvez confier la clé publique à qui désire vous faire confiance, par exemple `nivose` ! Allez sur `nivose`, placez-vous dans le répertoire `.ssh` de votre répertoire privé et éditez le fichier `authorized_keys`. Enlevez l'entrée précédente qui pouvait correspondre à votre machine A, s'il y en avait une. Et ajouter le contenu du fichier `id_rsa.pub` à la fin du fichier (attention au couper-coller qui ne respecte par toujours les terminaisons de ligne, le contenu doit être sur une seule ligne).
Vous pouvez dès maintenant vous connecter à distance à `lucien` via le protocole `ssh` (voir sur le wiki de l'UFR d'informatique la page `Guide : connexion à distance / SSH`).

N.B. : Si vous souhaitez réaliser la même opération depuis une machine qui ne se trouve pas sur le réseau de l'université, vous devez vous connecter à distance sur
`nivose.informatique.univ-paris-diderot.fr`
(la machine `lucien.infomatique.univ-paris-diderot.fr` n'acceptant pas les connexions à distance sans clé RSA).

Exercice 2 : Obtenir des informations sur le réseau

1. À l'aide de la commande `hostname`, déterminez l'identité de votre machine (son nom, son nom de domaine et son adresse réseau (IP)).
2. Utilisez la commande `ping` avec les arguments suivants `www.google.com` et `www.laplanete.uk`. Qu'en déduisez-vous ?
3. En utilisant successivement les commandes `host`, `nslookup` et `dig`, déterminez les adresses IPv4 et IPv6 de `www.informatique.univ-paris-diderot.fr`, puis de `www.free.fr`. Quels sont les noms d'hôtes associés aux adresses obtenues ?
4. Déterminez à l'aide de la commande `dig` comment connaître les serveurs de courrier électronique d'un réseau. Pour cela, regardez sur la page du manuel les types de requêtes proposées dans la rubrique SIMPLE USAGE. Déterminez ensuite les serveurs de courrier électronique des réseaux `informatique.univ-paris-diderot.fr` et `free.fr`.

Exercice 3 : Appels de services

Vous pouvez appeler des services à distance depuis votre machine en vous connectant au port correspondant à ces services. Pour cela vous pouvez utiliser la commande `telnet` (usage : `telnet machine service` où `service` peut être soit le numéro du service, soit le nom du service)

1. Déterminez le port associé au service `discard` (Indication : vous avez vu en cours où trouver la liste des services).
2. À l'aide de la commande `telnet`, déterminez l'heure (service `daytime`, dont la documentation est RFC 867) qu'il est sur la machine `lucien`. Appelez ce service à la fois par son nom et par son numéro de port et profitez en aussi pour aller voir la page Wikipedia de "Requests For Comments" pour connaître ce que sont les RFC. Consultez ensuite la documentation RFC 867.
3. À l'aide de la commande `telnet`, accédez au service `echo` (RFC 862) sur la machine `monjetas`. Tapez alors du texte avec des retours à la ligne. Comment pouvez quitter l'application `telnet` ?

Exercice 4 : Le service SMTP

Le protocole SMTP (*Simple Mail Transfer Protocol*, RFC 2821) sert à envoyer du courrier électronique (*e-mail*) à des utilisateurs locaux ou distants. Il s'agit d'un protocole dit *requête-réponse*, dans lequel le dialogue consiste pour le client à envoyer une commande au serveur puis à attendre la réponse de ce dernier, et à recommencer.

> **Remarque :** les techniques utilisées dans cette partie permettent, en théorie, d'envoyer des mails en se faisant passer pour quelqu'un d'autre. Une telle activité est totalement illégale, et nous vous déconseillons fortement de mettre à l'épreuve les capacités d'investigation de nos administrateurs système et réseau.

Les commandes SMTP les plus utiles sont les suivantes :

- « `HELO` *machine* » : à envoyer au début d'une connexion SMTP. La chaîne *machine* est le nom de l'hôte à partir duquel vous vous connectez.
- « `MAIL FROM:` *utilisateur* » : commence une transaction SMTP visant à envoyer un message. La chaîne *utilisateur* est l'adresse de l'auteur du message (de la forme `user@domain`).
- « `RCPT TO:` *utilisateur* » : déclare un destinataire de la transaction courante ; peut être répétée plusieurs fois.
- « `DATA` » : déclare le début de l'envoi du message, lequel commence à partir de la ligne suivante et se termine par une ligne ne contenant que le caractère point « `.` ».
- « `QUIT` » : termine une connection SMTP.

Le message passé à la commande « `DATA` » doit avoir le format défini par le document de normalisation RFC 2822. Il doit commencer par une série d'en-têtes (« `From:` », « `To:` », « `Subject:` », etc.) suivis d'une ligne vide, suivie du corps du message lui-même.

1. En vous connectant directement au port SMTP de `nivose` à l'aide de la commande « `telnet` », envoyez un mail à l'un de vos collègues.
2. Répétez l'expérience précédente en donnant des adresses différentes dans l'enveloppe (commande « `RCPT TO:` » de SMTP) et dans le message (entête « `To:` » de RFC 822). Que se passe-t-il ?