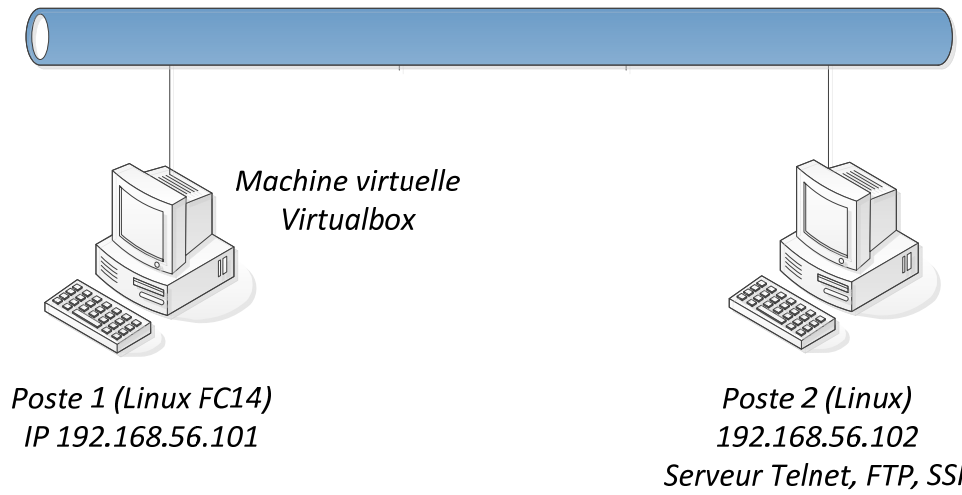
Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°3

Telnet, FTP et SSH

a) Configuration des machines



Dans ce TP, vous allez utiliser les machines virtuelles FC14 Client et Serveur

- **Login** : etu **password** : etu&reseaux
- Vous allez installer et configurer les 3 serveurs : Telnet, FTP et SSH
- Vous allez utiliser WireShark pour capturer les trafics qui circulent entre les deux machines

1. COMMANDES SYSTEMES & RESEAUX

1.1 – Quelle commande permet de visualiser l'adresse MAC (Physique) et l'adresse IP (logique) de votre station ?

1.2 – A partir de votre terminal, exécuter la commande "**ping**" avec une station voisine. Quelle commande système permet de visualiser les adresses MAC et IP des hôtes avec lesquelles vous avez échangés des trames ?

1.3– Editer le fichier système suivant et expliquer son rôle et son utilité:

- nano /etc/hosts

1.4- Trouver le numéro de port par défaut utilisé par les applications suivantes : Telnet, FTP, SSH, HTTP, HTTPS, DNS, SMTP, IMAP, SNMP.

- nano /etc/services

2. Server telnet

2.1 – Vérifier que le serveur Telnet est à l'écoute des nouvelles connections

2.2– Lancer Wireshark pour capturer les trames échangées entre le client et le serveur TELNET. Ensuite, connectez-vous au serveur TELNET :

telnet 192.168.56.102

Après l'authentification, utiliser les commandes

1. *ls*
2. mkdir test_telnet
3. cd test_telnet
4. nano fichier.txt
   Je suis le/la plus beau/belle du quartier. Beaucoup plus que
   Appuyer sur ctrl+x pour quitter le mode d'édition et enregistrer les modifications.
5. Ensuite, ″su″ et entrer le mot de passe de l'utilisateur root.

2.3 - Quel est le numéro du port utilisé par le serveur TELNET ? Quel est le protocole de transport utilisé par TELNET ?

2.4- Via le logiciel Wireshark, retrouvez votre login et mot de passe. Est-il lisible ? Retrouver aussi le résultat de votre commande ″ls, cd, nano, etc.″. Sont-ils lisibles par un MITM ?

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°3

3. Serveur FTP : File Transfer Protocol

2.1 – Vérifier que le serveur FTP est à l'écoute des nouvelles connections

3.2 – Lancer Wireshark et commencer à capturer les trames échangées entre le client et le serveur FTP. Ensuite, connectez-vous au serveur FTP via l'interface graphique du gftp/filezila. Déposer le fichier ″file1.txt″ sur le serveur. Le contenu du fichier ″file1.txt″ est :

$echo ″ceci est un message classé secret défense″ > file1.txt
$echo ″mon numéro de compte : 123456789″ >> file1.txt

Lancer le client gftp : Applications => internet => gftp
Ou le client filezilla : Applications => internet => Filezilla

3.3 - Quel est le numéro du port utilisé par le serveur ? Quel est le protocole de transport utilisé par FTP ?

3.4- Via le logiciel Wireshark, et des messages capturés, retrouver votre login et mot de passe. Sont-ils lisibles ? Retrouver aussi le contenu du fichier "file1.txt". Est-il lisible ? Expliquer la démarche

4. SSH: Secure SHell

Le protocole SSH (Secure SHell) permet à des utilisateurs d'accéder à une machine distante à travers une communication chiffrée (appelée tunnel).

4.1- Votre serveur sshd est-il actuellement en exécution sur la machine virtuelle ? Comment feriez-vous pour arrêter ou démarrer ce service ?

4.2- SSH est basé sur une architecture client/serveur. Sur quel port écoute le serveur SSH?

4.3 - Lancer Wireshark pour capturer le trafic. Essayez de vous connecter sur le serveur à l'aide de la commande ***ssh***.
Syntaxe : ***ssh etu@192.168.56.102***, *etu* étant un compte valide défini sur le serveur. A la place du @IP_serveur, utiliser l'adresse IP de votre serveur (voir le résultat de la commande ***ifconfig***), ou bien renseigner l'adresse IP et le nom du serveur dans le fichier /etc/hosts
Note : créer votre compte utilisateur sur le serveur et sur le client avant d'établir la connexion. (useradd user1 ; passwd user1), sinon utiliser un compte existant.

```
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be
established.
RSA key fingerprint is 53:b4:ad:c8:51:17:99:4b:c9:08:ac:c1:b6:05:71:9b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.17.129 (RSA) to the list of known hosts
user@172.16.17.130's password: (enter the password)
[user1@server]$
```

Transferts des fichiers avec scp et sftp

scp (secure copy) et sftp (secure ftp), permettent de copier des fichiers et des arborescences, en utilisant ***ssh*** pour sécuriser les transferts

Syntaxe générale:

scp [-r] source destination, où ***source*** et ***destination*** désigne l'ensemble des fichiers à copier ou le répertoire d'accueil.

Exemples:

scp user@serveur:fichier rep-local, pour copier du serveur distant le fichier vers le répertoire rep d'accueil **rep-local**

scp -r fichiers-locaux user@serveur:rep-distant, pour copier les **fichiers-locaux** vers le répertoire situé sur le serveur distant

1. Effectuez les copies suivantes en expliquant la commande et son utilité. Vérifiez les résultats. Vous devez adapter la commande en utilisant un utilisateur existant.

scp /etc/services etu@192.168.56.102:

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Réseaux avancés

TD/TP n°3

2. Dans votre répertoire home d'un utilisateur existant, exécuter les commandes suivantes :

```
mkdir test/
cd test
touch file1.txt
echo `` hello `` > file2.txt
netstat –ant >  file3.txt
route –nr > file4.txt
```

Ensuite utiliser la commande **scp** pour copier le répertoire ***test*** sur le serveur.

3. Testez des transferts des fichiers précédents entre le client et le serveur avec l'application ***sftp***.

4. Est-il possible de récupérer votre login et votre password via Wireshark ? Si oui expliquer la démarche ?

5. Est-il possible de récupérer le contenu des fichiers (file1.txt, file2.txt, file3.txt, file4.txt) ? Si oui expliquer la démarche.

6. Que préférez-vous pour le transfert de vos fichiers (FTP ou SFTP) ? expliquer pourquoi ?