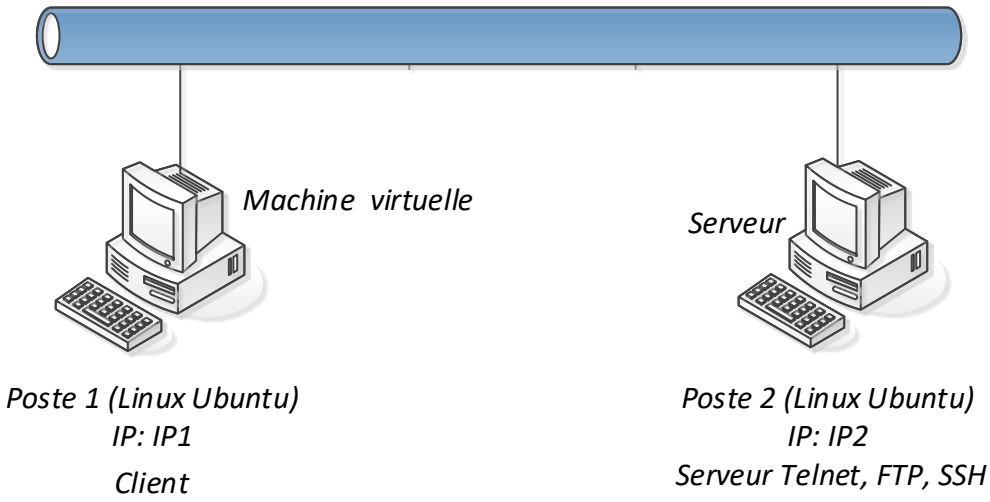
Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 Informatique – Sécurité et Réseaux

TD/TP n°3

Telnet, FTP et SSH

a) Configuration des machines



- Dans ce TP, on va utiliser 3 Serveurs (telnet, FTP et SSH).
- Pour accéder aux machines virtuelles : https://vdi.ens.math-info.univ-paris5.fr/

1. Commandes systèmes et réseaux

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

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 ?

3. Avec un éditeur de texte de votre choix, ouvrez le fichier : /etc/services et identifier le numéro le numéro de port utilisé par défaut par les applications suivantes : Telnet, FTP, SSH, HTTP, HTTPS, DNS, SMTP, IMAP, SNMP. □

Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 Informatique – Sécurité et Réseaux

TD/TP n°3

2. Server telnet

1. Vérifier que le serveur Telnet est à l'écoute des nouvelles connections

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

$telnet @IP2

Après l'authentification, utiliser les commande ″ls″, ″pwd″, ″mkdir test″, ″cd test″, ″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

3. Quel est le numéro du port du serveur ? Quel est le protocole de transport utilisé par telnet ? donner la commande permettant de vérifier que le serveur écoute sur ce port ?

4. Via le logiciel Wireshark, retrouvez votre login et mot de passe. Est-il lisible ? Retrouver aussi le résultat de vos commandes ″ls″, ″pwd″, etc. Sont-ils lisibles par un MITM ?

3. Server FTP: File Transfer Protocol

1. Vérifier que le serveur FTP est à l'écoute des nouvelles connections

2. Lancer Wireshark et commencer à capturer les trames échangées entre le client et le serveur FTP. Ensuite, connectez-vous au serveur FTP. 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

3. Quel est le numéro du port utilisé par le serveur ? Quel est le protocole de transport utilisé par FTP ?

4. Au moyen du 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

5. http : Hypertexte Transfer Protocol

Lancer Wireshark et commencer à capturer les trames échangées entre un navigateur web et internet. Ouvrez un navigateur web et accéder au site : http://zero.webappsecurity.com/. Entrer un identifiant et un mot de passe de votre choix (par hasard).

1. Quel est le numéro du port utilisé par le serveur http ? Quel est le protocole de transport utilisé par http ?

2. Au moyen du logiciel Wireshark, et des messages capturés, retrouver votre login et mot de passe. Est-il lisible ? Expliquer la démarche

6. SSH: Secure SHell

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

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

Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 Informatique – Sécurité et Réseaux

TD/TP n°3

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

3. Lancer Wireshark pour capturer le trafic. Essayer de vous connecter sur le serveur à l'aide de la commande ***ssh***.

Syntaxe : ***ssh user@IP2***, *user* étant un compte valide défini sur le serveur. A la place du nom du serveur, utiliser l'adresse IP de votre serveur.

```
The authenticity of host 'IP2' 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 IP2 (RSA) to the list of known hosts
user@172.16.17.130's password: (enter the password)
[user1@server]$
```

Est-il possible de récupérer votre login et votre mot de passe via Wireshark ? Est-ce possible de retrouver aussi le résultat de votre commande ″ls″. Si oui expliquer la démarche ? Est-il lisible ?

Transferts des fichiers aec 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@sIP2:fichier rep-local, pour copier du serveur distant le fichier vers le répertoire rep d'accueil local

scp -r fichiers-locaux user@IP2:rep-distant, pour copier les fichiers locaux vers le répertoire situé sur le serveur distant

1. Effectuez les copies suivantes et vérifiez les résultats

scp /etc/services user@IP2:/home/votre_compte/

2. Dans votre répertoire home, exécuter les commandes suivantes sur machine contenant le client :

```
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, file2, file3, file4) ? Si oui expliquer la démarche.

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