TP 2 : Utilisation de SSH pour le transfert de fichier de façon sécurisée.

SSH (Secure Shell) est un protocole de communication sécurisé. Il permet de se connecter à une machine distante avec une liaison sécurisée.

Installation du client SSH

Le package **openssh-client** est installé par défaut sous Ubuntu.

Si ce n'est pas le cas, on peut installer le paquet ssh qui installe à la fois le "serveur" et le "client".

Sur une machine cliente, le serveur peut ne pas être indispensable.

Vérifier la version actuelle de ssh

ssh -V

Vérifier la version de la librairie ssl

dpkg -l libssl*

On peut également utiliser le client putty sous windows qui est une implémentation de ssh pour se connecter à distance sur une machine serveur.

Installation du serveur SSH

Installez le paquet **openssh-server** sur votre machine.

sudo apt-get install openssh-server

Activation/désactivation du service

Le serveur SSH fonctionne en tant que service qui par défaut après l'installation sera lancé au démarrage de la machine.

Il est possible notamment de l'activer ou l'arrêter ou de le relancer

Activer

sudo service ssh start

Arrêter

sudo service ssh stop

Relancer

sudo service ssh restart

Le port d'écoute du serveur, est par défaut le port 22.

Accès à distance à une machine en mode console

Pour ouvrir une session distante ayant un serveur SSH (important), la commande est la suivante :

ssh <nom_utilisateur>@<adresseIP> -p <num_port>

ou

ssh <nom_utilisateur>@<adresseIP>

Exemple :

Rester dans le repertoire /home/minterne de la machine interne et se connecter sur mfirewall

ssh mfirewall@10.2.0.2

Pour quitter la machine mfirewall, il faut saisir la commande :

exit

Copie d'un fichier/répertoire à distance

Ceci se fait en utilisant la commande scp

scp *source destination*

Exemples :

1-copier un fichier de la machine minterne vers mfirewall

scp essai1 mfirewall@10.2.0.2:/home/mfirewall

Vérifier que la copie est effective

2-copier un répertoire (nommé fichiers par exemple) de la machine minterne vers mfirewall

scp -r fichiers mfirewalll@10.2.0.2:/home/mfirewall

3-copier un fichier de mfirewall vers minterne tout en restant sur minterne

scp mfirewall@10.2.0.2:/home/mfirewall/essaiparefeu /home/minterne

Vérifier que la copie est effective

4-copier un fichier répertoire de mfirewall vers minterne tout en restant sur minterne

scp -r mfirewall@10.2.0.2:/home/mfirewall/nomrep /home/minterne

Authentification par un système de clés publique/privée

Tout le monde a tendance à employer l'authentification typique par *identifiant et mot de passe*. Cependant, si quelqu'un connaît votre mot de passe, la sécurité est compromise.

Comme parade, SSH offre l'**Authentification par clé publique/privée** au lieu des mots de passe « simples ».

De cette manière, il faut être en possession de deux informations pour se connecter (la clé privée et connaître le mot de passe de cette clé).

Avantages :

- Permet à un administrateur de se connecter à des centaines de machines sans devoir connaître des centaines de mots de passe différents ;
- Permet de ne pas avoir un mot de passe à saisir fréquemment.

Procédure :

Il va falloir créer un couple de clés.

Pour créer une clé utilisant le protocole de chiffrement RSA, **restez sur minterne** et tapez :

ssh-keygen -t rsa

Acceptez juste l'endroit par défaut et le nom du fichier: **~/.ssh**, (en validant sans rien saisir) puis choisir une *passphrase* (phrase de reconnaissance), par exemple, securite informatique

Une clé publique a été créée avec une nouvelle clé privée. Elles sont habituellement localisées dans le dossier caché **.ssh**, soit **.ssh/id_rsa.pub** pour la clé publique et **.ssh/id_rsa** pour la clé privée.

Il va falloir envoyer au serveur votre clé publique pour qu'il puisse l'utiliser pour chiffrer des messages.

L'utilisateur distant doit avoir cette clé (c'est une ligne de caractères en code ASCII) dans son fichier de clés d'autorisation situé à **~/.ssh/authorized_keys** sur le système distant. Employez la commande ***ssh-copy-id*** pour copier la clé publique vers le serveur distant.

ssh-copy-id -i ~/.ssh/id_rsa.pub mfirewall@10.2.0.2

ssh-copy-id est un script qui utilise ssh pour se connecter à une machine à distance en utilisant le mot de passe de l'utilisateur.

Vous devez alors donner le mot de passe *utilisateur* de l'ordinateur distant durant la copie de la clé. Après l'ajout de votre clé publique, vous devenez un hôte de confiance.

Pour vous connecter à mfirewall faire :

ssh mfirewall@10.2.0.2

Entrez votre **passphrase** pour vous connecter. Celle-ci sert à déchiffrer la *clé* privée.

Tester une copie de fichier appartenant à mfirewall depuis la machine interne par passphrase.

Sortir de mfirewall en tapant :

exit

Utiliser un agent ssh (Pour ne pas avoir à entrer la passphrase à chaque fois)

Comme vous l'avez constaté, si l'on protège son fichier contenant sa clé privée avec un mot de passe (passphrase), il faut donner ce mot de passe à chaque connexion. Une alternative est d'activer l'agent SSH qui garde en mémoire votre clé privée. Ensuite, cet agent réalise l'authentification pour l'ensemble des clients SSH que vous activez.

Ainsi, il ne vous demandera la passphrase qu'une fois au début. Ensuite, vous pourriez vous connecter autant de fois que vous le souhaitez à autant de serveurs que vous voulez sans avoir à entrer quoi que ce soit.

Procédure:

1-**Activer l'agent ssh**

Lancez :

ssh-agent

Cette commande affiche des variables d'environnement à déclarer et à exporter

Faites-le (copier et exécuter les différentes lignes)

2- Mettre ensuite les clés dans le cache de l'agent

Lancez :

ssh-add

Désormais vous n'aurez à entrer la passphrase qu'une seule fois durant une session.

Vous n'avez même plus besoin de vous connecter à la machine distante pour travailler

ssh mfirewall@10.2.0.2 ls