

**SECURE SHELL.**  
**<http://nassih.com>**  
**© MOHAMED NASSIH.**

## 1. Introduction.

L'administration et la maintenance des serveurs à distance est une opération très fréquente dans les environnements informatiques, l'un des protocoles les plus utilisés pour la connexion à distance est le protocole Telnet et les commande r-commandes comme rlogin. L'échange à l'aide de ces protocoles se fait en claire, même le mot de passe du super-utilisateur est transféré en clair.

Le protocole SSH est un protocole qui permet l'accès aux serveurs via Internet à travers une communication chiffrée. Il pourra aussi sécuriser d'autre protocole comme POP en utilisant la technique de retransmission de port.

SSH commence par créer une couche transport sécurisé, durant cette première étape le client et le serveur échangent les clés et négocient les protocoles d'authentification et de chiffrage à utilisés. La deuxième étape est l'étape d'authentification, en premier lieu le serveur et le client se mettent d'accord sur la méthode d'authentification qui pourra être utilisée telles que l'utilisation d'une signature chiffrée privée ou l'entrée d'un mot de passe. Après avoir effectué l'authentification avec succès, des canaux chiffrés sont créés entre le client et le serveur. Chaque canal s'occupe d'une session **SSH**.

## 2. L'implémentation de SSH.

SSH pourra être téléchargé à partir du site <http://www.openssh.com>. L'installation de SSH est simple. Il pourra être installé à partir d'un fichier rpm ou bien à partir des fichiers sources. Les fichiers que nous avons téléchargés sont openssh-3.5p1-6.i386.rpm, openssh-clients-3.5p1-6.i386.rpm, et openssh-server-3.5p1-6.i386.rpm. La figure 2.1 montre l'installation de ces trois rpms.

```
rpm -ivh openssh-3.5p1-6.i386.rpm
rpm -ivh openssh-clients-3.5p1-6.i386.rpm
rpm -ivh openssh-server-3.5p1-6.i386.rpm
```

**Figure 2.1 : l'installation de SSH.**

La commande service «sshd start» permet de démarrer le serveur SSH. La première fois qu'on se connecte au serveur SSH, le serveur pose la question suivante :

```
The authenticity of host '192.168.0.160' can't be established.  
RSA key fingerprint is 85:74:3a:c3:c5:cc:aa:ab:37:fc:e4:4a:83:e8:ac:05:78.  
Are you sure you want to continue connecting (yes/no)?
```

En répondant “yes”, le client ajoute le serveur à la liste des hôtes connus.

```
[root@SSH-Client root]# ssh 192.168.0.160  
The authenticity of host '192.168.0.160 (192.168.0.160)' can't be established.  
RSA key fingerprint is 85:74:c3:c5:cc:aa:ab:37:fc:e4:4a:83:e8:ac:05:78.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.0.160' (RSA) to the list of known hosts.  
root@192.168.0.160's password:  
Last login: Mon Sep  5 00:14:42 2005  
[root@ssh-server root]# _
```

**Figure 2.2 : la connexion au serveur SSH.**

Si pour un utilisateur donné, on ne veut pas qu'il fournisse un mot de passe à chaque fois qu'il se connecte au serveur, alors on pourra générer une paire de clés d'autorisation. Les clés doivent être générées pour chaque utilisateur.

```
[root@SSH-Client .ssh]# ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/root/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /root/.ssh/id_rsa.  
Your public key has been saved in /root/.ssh/id_rsa.pub.  
The key fingerprint is:  
a6:fb:a7:44:16:07:5d:00:21:7b:22:77:b5:fd:b8:41 root@SSH-Client  
[root@SSH-Client .ssh]#  
[root@SSH-Client .ssh]# ls  
id_rsa id_rsa.pub known_hosts  
[root@SSH-Client .ssh]# _
```

**Figure 2.3 : création des clés privée et publique pour un utilisateur.**

Une phrase d'identification (de passage) est nécessaire. La clé publique est créée dans le fichier /root/.ssh/id\_rsa.pub. la clé privée est créée dans le fichier /root/.ssh/id\_rsa.

Il faut copier le fichier qui contient la clé publique /root/.ssh/id\_rsa.pub dans le fichier /root/.ssh/authorized\_keys sur le serveur.

Lorsqu'on essaie de se connecter le système demande la phrase d'identification (voir la figure 2.4).

```
[root@SSH-Client .ssh]# ssh 192.168.0.160
Enter passphrase for key '/root/.ssh/id_rsa':
Last login: Mon Sep  5 01:46:22 2005 from 192.168.0.100
[root@ssh-server root]# _
```

**Figure 2.4 : l'accès au serveur SSH.**

Dans la phase de la création des clés de la figure 2.3, on pourra ne pas mettre la phrase d'identification et comme ça on pourra se loguer à distance sans mot de passe. Le problème est que cette phase sert à chiffrer la clé privé, et sans chiffrage, la clé pourrai être utilisé par un pirate qui aurai accès au système de fichier.