# Admin Linux Fiche 4 : SSH

## 1 SSH

Les systèmes Linux actuels sont le plus souvent gérés en ligne de commande (pas d'interface graphique) et à distance. Pour ce faire, on utilisait *telnet* mais ce protocole a le gros inconvénient de ne rien crypter. Une simple écoute réseau permet alors de récupérer le mot de passe root. SSH est venu remplacer *telnet.*

### 1.1 Fonctionnement

Nous ne donnerons ici qu'un résumé du fonctionnement du protocole SSH, celui-ci étant abordé par le cours théorique. Le protocole SSH effectue un échange de clés de chiffrement avant d'utiliser ces dernières pour crypter toutes les communications entre le client et le serveur. Le port 22 est le port par défaut utilisé par SSH.

SSH est un service qui est initialisé/démarré par systemd.

### 1.2 Installation

```
apt-get install ssh
```

### 1.3 Configuration

Le fichier de configuration client est : /etc/ssh/ssh_config

Le fichier de configuration serveur est : /etc/ssh/sshd_config

Par défaut, SSH est installé pour permettre une authentification par login et mot de passe pour tout les utilisateurs présents sur le serveur (y compris root).

Après avoir effectué une modification dans un fichier de configuration, il faut redémarrer le service pour que les modifications soient prises en compte.

```
/etc/init.d/ssh restart
OU
service ssh restart
OU
systemctl restart ssh
```

### 1.4 Utilisation

Le client SSH a besoin des informations suivantes : un nom de machine ou une adresse IP, un login et un mot de passe. On peut remplacer l'authentification par login/mdp par une clé.

Comme client SSH, vous connaissez sans doute déjà le client SSH Windows par excellence : *Putty.*

Sous Linux :

```
ssh nomutilisateur@nommachineOUadresseIP
```

## 1.5 Sécurité

Il est possible de configurer le serveur SSH pour interdire l'usage du compte root pour les connexions SSH. L'option « PermitRootLogin » doit être positionnée à « No » dans le fichier de configuration du serveur SSH.

Il également possible de restreindre l'utilisation que depuis certaines machines et qu'avec certains utilisateurs.

```
AllowUsers olivier@192.168.1.*
AllowUsers admin bob
```

Ici les utilisateurs admin et bob sont uniquement autorisés et l'utilisateur olivier depuis le sous-réseau 192.168.1.0/24

## 1.6 Copie de fichiers

Il est à noter que dès que vous avez un accès SSH, vous pouvez copier des fichiers entre votre machine hôte et invitée via SCP/SFTP. Ceci peut se faire avec le logiciel WinSCP (Windows) ou Cyberduck(Mac).