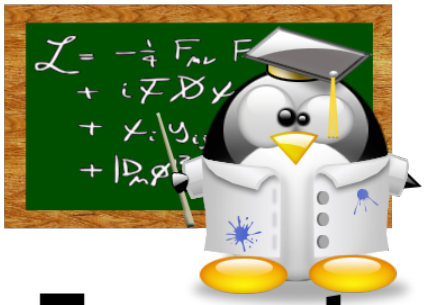

Formatux

Sécuriser le serveur SSH

Table des matières

Le serveur openSSH permet l’administration d’un serveur à distance.

Chapitre 1. Configuration

La configuration du serveur SSH se fait dans le fichier **/etc/ssh/sshd_config**.

Á chaque modification, il faut relancer le service :

```
service sshd restart
```

Chapitre 2. Changer le port d'écoute et la version du protocole

Il est préférable de changer le port par défaut (22) par un port connu de vous seul et de n'utiliser que la dernière version du protocole :

```
Port XXXX
Protocol 2
```

Chapitre 3. Utilisation de clefs privées/publiques

Dans la mesure du possible, utilisez un couple de clef privée/publique pour l'accès au serveur, et désactivez les autres possibilités de connexion (authentification par utilisateur + mot de passe) :

```
PasswordAuthentication no
RSAAuthentication yes
PubkeyAuthentication yes
```

Chapitre 4. Limiter les accès

Il est possible de limiter les accès directement dans la configuration du service avec la directive AllowUsers :

```
AllowUsers antoine
```

Il est également possible de limiter les accès par adresse IP via TCP Wrapper. Par exemple, refusez tous les accès dans le fichier /etc/hosts.deny :

```
sshd: ALL
```

et n'acceptez dans le fichier /etc/hosts.allow que les connexions depuis des adresses IP validées :

```
sshd: 192.168.1. 221.10.140.10
```

Voir la configuration de TCP Wrapper pour plus d'informations.

Chapitre 5. Interdire l'accès à root !!!

La mesure essentielle à prendre est d'interdire l'accès direct à root au serveur ssh :

```
PermitRootLogin no
```

et d'utiliser les possibilités offertes par le fichier sudoers pour permettre aux utilisateurs administrateurs de lancer des commandes d'administration.

Chapitre 6. Sécurité par le parefeu

Il est également important de limiter les accès aux services grâce au pare-feu et de bannir les adresses IP tentant des attaques par dictionnaire.