Améliorer la sécurité d'OpenSSH

OpenSSH est le couteau suisse pour les connexions à distance : il fournit un shell sur votre machine distante et permet de transférer des données de manière sécurisée et chiffrée, que ce soit des commandes, des fichiers, des sessions X11 ou VNC, des données via rsync, etc.

OpenSSH est si performant qu'il peut être considéré comme un VPN (Virtual Private Network) simplifié.

Slackware propose OpenSSH bien sûr, et la configuration par défaut est déjà sécurisée. Cette page a été créée pour vous montrer quelques simples astuces de configuration à apporter à la configuration par défaut pour en améliorer la sécurité.

Vous aurez besoin de savoir comment utiliser un éditeur de texte pour suivre ce HOWTO. Si vous êtes un débutant complet, essayez `nano`. Une fois que vous vous sentez en confiance, vous pourrez utiliser quelque chose de plus avancé...

Les fichiers de configuration de SSH - où trouver plus d'information

Les fichiers de configuration d'OpenSSH se trouvent dans le répertoire `/etc/ssh/`. Le plus important est `/etc/ssh/sshd_config`, qui est celui que nous allons modifier ici.

La documentation d'OpenSSH est bien faite et très complète, vous pouvez utiliser la commande `apropos openssh` ou `man -k openssh` et lire les différentes pages de manuel, qui sont beaucoup plus détaillées que cette page de wiki.

Modifier le fichier sshd_config

La première règle, avant de modifier un fichier de configuration important est d'en créer une copie de sauvegarde. Par exemple :

```
# cp -v /etc/ssh/sshd_config /etc/ssh/sshd_config.ORIG.20120826
```

La commande ci-dessus copiera le fichier `sshd_config` et ajoutera l'extension `.ORIG` (pour original, bien sûr) et comporte également la date de modification. Sans être parfait, ce système assure que vous pourrez toujours revenir à une version précédente d'un fichier important en utilisant la commande suivante :

```
# cp -v /etc/ssh/sshd_config.ORIG.20120826 /etc/ssh/sshd_config
```

Veuillez noter que ceci n'est qu'une suggestion, bien sûr, et il est fortement recommandé pour les administrateurs systèmes devant gérer de larges installations, avec des centaines de serveurs de regarder du côté de Puppet ou autres gestionnaires de configurations distribuées.

Maintenant éditez le fichier `/etc/ssh/sshd_config` avec votre éditeur favori et modifiez les lignes

suivantes :

Modifier le port par défaut de SSH

Par défaut, OpenSSH écoute sur le port 22. Il est parfois conseillé de changer ce port par défaut pour un autre, tel que 2222 ou 4242. Ce n'est pas une mauvaise idée, mais vous devez vous souvenir qu'une analyse de votre machine avec un programme comme `nmap` révèlera ce nouveau port rapidement. Cela peut donc ralentir certaines attaques contre votre machine, mais pas les bloquer complètement.

Si vous voulez changer le port, cherchez l'option `Port` dans `sshd_config`, qui se trouve habituellement en début du fichier et modifiez-en la valeur.

Par exemple :

```
Port 22
```

Peut être changé en :

```
Port 4242
```

Interdire l'accès root à votre machine

C'est probablement le changement le plus simple et le plus important que vous pouvez effectuer pour améliorer la sécurité de votre machine : interdisez à l'utilisateur `root` d'accéder à votre machine par SSH. Pour cela, cherchez la ligne suivante dans `sshd_config` :

```
PermitRootLogin yes
```

Et modifiez la en :

```
PermitRootLogin no
```

Si vous appliquez le changement ci-dessus, vérifiez que vous avez au moins un utilisateur sur votre machine qui puisse utiliser `su` (switch user - changer d'utilisateur) pour passer `root` ou utilisez `sudo` pour des permissions plus spécifiques. La meilleure façon d'administrer un serveur via SSH est d'avoir un utilisateur membre du groupe `wheel`, qui pourra utliser `sudo` et `su` pour devenir `root` lorsque nécessaire.

Puisque la plupart des personnes qui essayent de pirater votre machine via des scripts automatiques utilisent le compte `root`, vous êtes tranquille, étant donné que cet accès est fermé.

Améliorer la sécurité des comptes et des délais de connexion

Avant et après l'option `PermitRootLogin`, vous trouverez d'autres permissions que nous allons

détailler rapidement ici :

- `LoginGraceTime` permet d'augmenter ou diminuer le temps laissé à l'utilisateur pour se connecter sur la machine. Il peut être limité sans risque à cinq minutes de la manière suivante :

```
LoginGraceTime 5m
```

- `MaxAuthTries` est utilisé pour augmenter ou diminuer le nombre de tentatives autorisées à un utilisateur pour s'authentifier correctement sur la machine. Cela peut être limité à trois tentatives de la façon suivante :

```
MaxAuthTries 3
```

Interdire la transmission X11

À moins que vous n'ayez besoin d'X11 via SSH, vous pouvez raisonnablement désactiver l'option suivante :

```
X11Forwarding no
```

Veuillez noter que désactiver X11 n'affecte pas VNC via SSH, par exemple. Dans la plupart des cas, il est toujours bon de désactiver les services inutiles.

Limiter les connexions SSH aux utilisateurs autorisés

Si vous êtes sûr que seuls certains utilisateurs ont besoin de se connecter à votre machine via SSH, vous pouvez les indiquer via l'option `AllowUsers`. Tous les utilisateurs, et seulement ceux-ci, listés après l'option seront en mesure de se connecter à votre machine via SSH.

```
AllowUsers jacques sauvegarde beatrice
```

Dans l'exemple ci-dessus, seuls les utilisateurs `jacques`, `beatrice` et `sauvegarde` pourront utiliser SSH vers cette machine. L'accès sera interdit pour tous les autres utilisateurs. Bien sûr, vous devez utiliser cette option de manière prudente et vérifier qu'au moins un utilisateur est mentionné...

Relancer le serveur SSH

Dernière chose à effectuer, pour être sûr que votre nouvelle configuration est prise en compte par le serveur SSH vous devez le relancer par la commande suivante :

```
# /etc/rc.d/rc.sshd restart
```

Votre nouvelle configuration, légèrement plus sécurisée, est maintenant appliquée. Félicitations !

À consulter également

- OpenSSH manual pages (on-line)

Sources

- Originally written by User Noryungi
- Translated into French by Ellendhel
- With a few changes by User Noryungi

security