

SECURiSER SSH

Résumé

Cette documentation est une notice pour l'amélioration de la sécurité de votre serveur ssh. Elle ne prêtant pas donner une installation inviolable.

La dernière version de cette documentation est disponible en ligne :
http://www.pileouface.org/linux/documentation/securiser_ssh.pdf

Copyright

Auteur : Loïc Brayat, loack@pileouface.org

[Ce document peut être utilisé selon les termes de la Licence Publique Générale de GNU version 2 ou suivante.](#)

Il est permis de produire et distribuer des copies conformes de ce document à condition que la présente notice de copyright et la présente notice de permission soient préservées sur toutes les copies.

Il est permis de copier et distribuer des versions modifiées de ce document selon les conditions d'une copie conforme, à condition que le travail dérivé résultant soit entièrement distribué selon les termes d'une notice de permission identique à celle-ci.

Table des matières

Résumé.....	2
Copyright.....	2
I\ Fonctionnement général.....	3
II\ Actions à effectuer.....	4
1. Interdire la connexion en root.....	4
2. Interdire / autoriser des adresses IP à se connecter.....	4
3. Interdire / autoriser des utilisateurs à se connecter.....	4
4. Changer le port de connexion.....	4
5. Remplacer l'authentification par mot de passe par celle par clefs.....	4
III\ Remarques.....	5
IV\ Sources.....	5

I\ Fonctionnement général

1. Le serveur (démon sshd) écoute par défaut sur le port 22
2. Le client et le serveur s'échangent des chaînes d'identification pour déterminer les versions respectives de SSH
3. Le serveur transmet sa clé de machine, "host-key", pour s'authentifier, puis une clé de serveur, "server-key" (regénérée toutes les heures) qui va servir à l'échange de la clé de session
4. Le client génère et envoie une clé de session
5. Le canal est maintenant chiffré suivant un algorithme négocié
5. Vient ensuite la phase d'authentification de l'utilisateur avec deux procédés principaux :
 - * par mot de passe "classique"
 - * par clés associées à l'utilisateur

III Actions à effectuer

1. Interdire la connexion en root

PermitRootLogin no" dans /etc/ssh/sshd_config

2. Interdire / autoriser des adresses IP à se connecter

Voir "AllowHosts" et "DenyHosts"dans /etc/ssh/sshd_config

3. Interdire / autoriser des utilisateurs à se connecter

Voir «AllowUsers», «DenyUsers», «AllowGroups» et «DenyGroups» dans /etc/ssh/sshd_config

4. Changer le port de connexion

Voir «Port» dans /etc/ssh/sshd_config

5. Remplacer l'authentification par mot de passe par celle par clefs

- Configuration du serveur :

Autoriser l'identification par clefs : "RSAAuthentication yes"

Interdire l'identification par mot de passe :

"IgnoreRhosts yes"

"RhostsAuthentication no"

"PasswordAuthentication no"

- Configuration du client Linux :

Création des clefs : "ssh-keygen -t rsa"

Prise en compte de la clef publique par le serveur : Copier le fichier généré (.pub) au fichier authorized_keys de l'utilisateur sur le serveur.

Test de la connexion : "ssh -i ~/.ssh/clef_privee [login@]serveur"

- Configuration du client Windows :

Création des clefs: "puttygen.exe"

Prise en compte : Concatener la clef notée sous "Public key for pasting into OpenSSH authorized_keys2 file" au fichier authorized_keys.

Test de la connexion :

Lancer l'agent Ssh (pageant.exe) et lui donner la clef privée.

Lancer Putty (auto-login username, ssh2, allow agent forwarding, Private key filename)

III\ Remarques

1. Les clefs privées ne doivent surtout pas être diffusées
2. Les clefs sont générées pour une machine. Si un utilisateur doit pouvoir accéder à une même cible à partir de plusieurs postes, il lui faudra plusieurs paires de clefs.

IV\ Sources

<http://securite.univ-rennes1.fr/SSH/Utilisation.html>

<http://www.ac-creteil.fr/reseaux/systemes/linux/outils-tcp-ip/Ssf.html>