TUTORIEL : Débuter avec SSH

Tutoriel réalisé par Maurice Vidal et Romain Prunac le 12/04/12

L'objectif présenté ici est de mettre en place une connexion sécurisée entre un client et un serveur à travers une zone non fiable (Internet) grâce à un tunnel crypté. Nous nous serviront d'un système de clé SSH qui servira à nous authentifier : une clé privée que nous garderons sur le poste local, et une clé publique que nous mettrons dans le serveur.

Nous allons prendre comme exemple, le poste distant de l'association *pvm3.tetaneutral.net* (qui jouera le rôle du serveur), et comme poste local, *pc_local*.

Sur le poste distant il faut installer le package openssh-server :
 # aptitude install openssh-server

Et sur le poste local il faut installer le package openssh-client :
 # aptitude install openssh-client

Configuration du poste local :

Nous allons commencer par générer une clé SSH.

 # ssh-keygen
(/root/.ssh/id_rsa) :
enter passphrase :
enter same passphrase :

Par défaut la clé publique sera créée au nom de /root/.ssh/id_rsa.pub et la clé privée au nom de /root/.ssh/id_rsa.

En laissant chacun de ces champs vides, le chemin sera celui utilisé par défaut et aucune passphrase ne sera nécessaire. La passphrase sert uniquement à protéger la clé privé si on craint de ne pas la garder en sûreté sur son poste local.

On vérifie que les clés soient bien créées (exemple type) :

 # ls /root/.ssh/
id_rsa id_rsa.pub know_hosts

Configuration du poste distant :

Nous allons modifier le fichier de configuration se trouvant dans /root/.shh/authorized_keys pour venir y ajouter la clé publique (id_rsa.pub) du poste local, ce lui permettra de venir se connecter au serveur

Si nous avons récupéré la clé publique sur le serveur, nous pouvons l'insérer dans le fichier des clés autorisées :
 # cat id_rsa.pub >> ~/.ssh/authorized_keys

Le fichier de configuration pour le démon SSHD se situe à /etc/ssh/sshd_config, on le modifie pour améliorer la sécurité. Quelques options importantes :

ListenAddress X.X.X.X:X	Change le port d'écoute, ainsi l'intrus ne peut être complètement sûr de l'exécution d'un démon SSHD (c'est de la sécurité par l'obscurité).
Protocole 2	Désactiver le protocole version 1, car il a des défauts de conception qui facilite le crack de mots de passe.
PermitRootLogin no	Cette option permet de ne pas autoriser la connexion en root sur la machine.
PermitEmptyPasswords no	Les mots de passe vides sont un affront au système de sécurité.
PasswordAuthentication yes	Il est plus sûr d'autoriser l'accès à la machine uniquement aux utilisateurs avec des clés SSH placées dans le fichier /root/.ssh/authorized_keys, il faut donc placer cette option à "no".
SyslogFacility AUTH et LogLevel INF	Ce sont des fichiers journaux.

Une fois le fichier de configuration prêt, il ne reste plus qu'à relancer le service :
 # /etc/init.d/ssh reload

Commandes utiles :

Se connecter en SSH sur le port 443 de la machine pvm3 de tetaneutral.net :
 # ssh -p 443 root@pvm3.tetaneutral.net

Copier le fichier distant /var/log/mail.log sur son poste local (il ne faut pas être connecté en SSH) :
 # scp -p 443 root@pvm3.tetaneutral.net:/var/log/mail.log /tmp/