# OpenSSH

## Nouveautés et Principes de durcissement

Présentation pour le groupe SUR

11/03/2008

Saâd Kadhi -- HAPSIS

# Agenda

★ Rappels

★ Les nouveautés

★ Principes de durcissement


# Rappels

# Né En 1999

★ OpenSSH est un "chantier" du projet OpenBSD

★ OpenSSH a été créé en octobre 1999

- A partir de OSSH, lui-même basé sur SSH1 1.2.12

# Projet OpenBSD ?

★ Initié par Theo de Raadt le 14 octobre 1995, en même temps que l'OS éponyme

★ Compte env. 90 développeurs actifs

★ Chantiers : OpenSSH, OpenBSD, OpenNTPD, OpenBGPD/OpenOSPFD, OpenCVS

# La Sécurité Est Très Importante

★ Approche proactive de la sécurité

★ Audit permanent du code par une équipe de 6 à 12 développeurs suivant les disponibilités

★ Mise à disposition de correctifs très rapide dans la plupart des cas

# Deux Variantes

★ OpenSSH pour OpenBSD
(openssh-4.7.tgz)

★ Portable OpenSSH pour les autres
(openssh-4.7p1.tgz

★ Portable OpenSSH = OpenSSH +
couche de portabilité

# Composants

★ Client/serveur : ssh et sshd

★ SFTP : sftp et sftp-server

★ Outils complémentaires : ssh-add, ssh-agent, ssh-keygen, ssh-keyscan, scp


# Les Nouveautés

# Jeu, Set et Match

★ Depuis OpenSSH 4.4 (septembre 2006), on a la possibilité de recourir à la directive Match pour modifier quelques éléments de configuration par utilisateur/groupe/hôte/adresse IP

# Match et Directives

★ 15 directives modifiables à l'aide de `Match`

★ `AllowTcpForwarding`, `Banner`, `ForceCommand`, `GatewayPorts`, `GSSApiAuthentication`, `KbdInteractiveAuthentication`, `KerberosAuthentication`, `PasswordAuthentication`, `PermitOpen`, `PermitRootLogin`, `RhostsRSAAuthentication`, `RSAAuthentication`, `X11DisplayOffset`, `X11Forwarding`, et `X11UseLocalHost`.

# ForceCommand

★ ForceCommand est apparue en même temps que Match

★ C'est l'équivalent de l'option cmd= acceptée au niveau de authorized_keys

★ Force l'exécution de la commande spécifiée

# PermitOpen

★ PermitOpen est aussi apparue dans OpenSSH 4.4

★ C'est l'équivalent de l'option permitopen= acceptée au niveau de authorized_keys

★ Permet de contrôler les forwardings établis par un utilisateur

# OpenSSH 4.7

★ Améliorations des performances dans les environnements utilisant des BDP (Bandwidth Delay Products)

★ Améliorations des performances hmac-md5

★ Intégration d'un nouvel algorithme MAC (UMAC64, RFC4418)

# Comment Confiner Un Utilisateur ?

★ Pour confiner les utilisateurs à une sous-arborescence donnée : rssh, scponly, ou jouer avec cmd= & co. en préfixe de clé publique (authorized_keys)

★ Solutions relativement difficiles à mettre en oeuvre et à maintenir

# Mise En Cage En Natif

★ Il existe désormais une "voie du milieu" : la directive ChrootDirectory

★ Utilisée en combinaison avec la directive Match

```
# override default of no subsystems
#Subsystem      sftp    /usr/libexec/sftp-server
Subsystem       sftp    internal-sftp

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       ForceCommand cvs server

Match User poop
        ForceCommand internal-sftp
        ChrootDirectory /home/chroot
```

# Objectifs

★ Cette directive répond à un besoin très précis : permettre le transfert de fichiers via SFTP mais en le confinant à un répertoire donné

★ Elle appelle chroot(2) et ne nécessite aucune configuration additionnelle

# Pourquoi Ca Marche ?

★ Cette directive s'appuie sur une version "interne" du sous-système SFTP, disponible "dans" sshd

★ internal-sftp au lieu de /usr/libexec/sftp-server

# Intérêts

★ Tirer bénéfice de chroot(2) sans les inconvénients associés à la mise en place

★ Tout est configurable dans sshd_config

★ Configurable par utilisateur/groupe

# Autres Utilisations

★ Possibilité d'utiliser ChrootDirectory pour les sessions interactives ou scp

★ Mais ceci nécessite la mise en place de l'environnement chroot (pourquoi vous ne souriez plus ?)

# Disponible ...

★ Ou pas. Enfin ... bientôt

★ ChrootDirectory est déjà dans la version de développement d'OpenSSH depuis le 08/02/2008 et dans les snapshots d'OpenBSD 4.3

★ Elle sera incluse dans la prochaine version (4.8, 4.8p1) prévue début mai


# Principes De Durcissement

# Petit Retour d'Experience

★ Passons en revue quelques principes de durcissement et leur applicabilité sur le terrain...

# Remerciements

★ Merci à vous pour m'avoir accordé un peu de "temps disponible du cerveau"

★ Et comme il est de coutume maintenant : Toumani Diabaté et Eric Bibb pour la musique

# Intervenant

★ Saâd Kadhi, consultant sécurité,
HAPSIS (http://www.hapsis.fr/)

# Informations Utiles

★ Vous pourrez bientôt télécharger cette présentation en ligne

- http://saad.docisland.org/docs/
- http://www.ossir.org/

★ Questions ? Commentaires ?

- saad@docisland.org

# Licence

★ Creative Commons Attribution-NonCommercial 2.5

- http://creativecommons.org/licenses/by-nc/2.5/