

Hébergement

une ballade dans les nuages



Accès à distance

Quand un **systeme** tourne sur une machine **virtuelle** il n'a généralement **pas d'interface** utilisateur

Il n'est accessible que par le réseau.

→ Outils d'administration distante

Accès à distance

RPC

Remote Procedure Call

Protocole réseau de type client/serveur

Permettant l'exécution de programme
prédéfinis sur une machine distante

- Possibilités **restreintes**
- Interface conçue pour des
programmes pas pour des humains

Accès à distance ssh

Secure shell

Protocole réseau de type client/serveur

Permettant l'exécution d'un

interpréteur de commande sur une
machine distante

- Possibilités infinies
- Interface conçue pour des humains,
mais utilisable aussi par des
programmes

Accès à distance ssh

Secure ?

ssh remplace telnet (terminal network)
ou rsh (remote shell)

en ajoutant le chiffrement de la
communication.

Il utilise toutes les méthodes
modernes de chiffrement afin de
sécuriser l'échange.

Accès à distance ssh

Secure ?

ssh offre les sécurités suivantes :

- Chiffrement de la communication
- Authentification forte
- Détection d'une usurpation de l'adresse du serveur distant (attaque du type « man in the middle »)

Accès à distance

ssh

Shell ?

ssh offre les services suivants :

- Shell distant
- Transfert de fichiers SFTP (secure file transfert protocol : remplace et sécurise FTP)
- Redirections chiffrées de flux réseaux (fonction de VPN et firewall)

Accès à distance

ssh : shell

ssh propose deux modes de fonctionnement :

- Shell **interactif**
- Exécution directe de commandes

Authentication

SSh propose plusieurs systèmes d'authentification :

- login/mot de passe
- Paire de Clés cryptographique

Authentication ~~forte~~

login/mot de passe

- Idem ouverture de session
- Problème de la **force** du mot de passe
- **Pas automatisable** fiablement et facilement

Authentification **forte**

Paire de Clés cryptographique

- Combinaison de **deux** clés
 - Une sur le serveur : la clé **publique**
 - Une sur le client la : clé **privée**
- ssh vérifie la correspondance entre les deux clés pour autoriser l'accès
- Totalement **automatisable**
- Il faut **plusieurs années** de calculs pour **casser** les clés

SAÉ 105

Dans la SAÉ105 **ssh** sera votre **seul** moyen d'accès au serveur mutualisé qui hébergera votre site.

Nous ferons un **TD** sur l'utilisation de **ssh** : création de clés, configuration...

Je vous fournirai une paire de **clés** (via **moodle**) pré-**installée** sur le serveur.