Mise à niveau **Année 2022-2023**

Département Informatique, ENS Paris Saclay

SSH 2

Version α

Objectifs:

— Gérer des clés de chiffrement pour SSH

Exercices

Les trois exercices suivants utilisent tous trois `ssh-keygen`.

Exercice 1. Les connexions de la fiche précédente ont créé un fichier `~.ssh/known_hosts`. *(a.)* Cherchez le contenu de ce fichier pour l'hôte `ssh.dptinfo.ens-cachan.fr`. *(b.)* Vérifiez que si vous modifiez (la fin de) cette ligne (que vous pouvez trouver en éditant directement `known_hosts`), la connexion est maintenant refusée. *(c.)* Comment effacer la ligne pour accéder de nouveau au serveur ?

Exercice 2. Générez une paire de clefs (par exemple, rsa) sans mot de passe. En créant ou modifiant le fichier `~.ssh/authorized_keys` sur les machines du département, ainsi qu'éventuellement votre configuration SSH, faites en sorte de passer par cette clé pour vous connecter d'un serveur à l'autre. Limitez les hôtes autorisés pour la connexion par cette clef.

Note : Les machines du département ont toutes une IP commençant par `138.231.36.`, vous pouvez utiliser le masque `138.231.36.0/24`.

Exercice 3. Générez une nouvelle paire de clefs, cette fois-ci avec un mot de passe (de préférence différent de celui de votre compte machine). Utilisez cette paire pour vous connecter sur un serveur (trouvez le paramètre à utiliser pour spécifier la clé à utiliser dans la configuration de votre client SSH).

Pour ne pas avoir à réécrire le mot de passe pour plusieurs utilisations successives de `ssh` (et ses dérivés), vous pouvez utiliser `ssh-agent`.

Exercice 4. Trouvez comment démarrer l'agent, et démarrez-le. Ajoutez votre clé privée à mot de passe à l'agent, en précisant une durée limite d'utilisation. Vérifiez que vous pouvez ensuite faire plusieurs `ssh` (et dérivés) sans avoir à utiliser le mot de passe pendant la période choisie.

Attention : Pour le moment, il y a un nombre limité de connexions autorisées par minute sur la passerelle SSH. Il peut donc y avoir un échec après que vous avez corrigé l'erreur ; si c'est le cas, réessayez quelques minutes plus tard.