Connection à un serveur distant avec SSH et administration Linux

Modalités

- Travail individuel / Binôme en autonomie
- Durée : 8 heures (suggéré comme une journée complète ou 2 demi-journées).
- Prérequis : Connaissances basiques des systèmes d'exploitation basés sur Unix/Linux, notions de base en réseau.
- Outils requis : Machine sous Linux (Ubuntu)

Objectifs de l'activité

Découvrir les notions de SSH et pouvoir l'utiliser pour vous connecter à un serveur distant.

Compétences

- Comprendre comment fonctionne la connection en ssh à un serveur distant (les différentes étapes et méthodes utilisés comme le mode d'encryption et le mode de hachage)
- Comprendre les lignes de commandes utilisées (ssh et ses arguments)
- Configurer et sécuriser un serveur SSH.
- Établir des connexions sécurisées à des serveurs distants via SSH.
- Utiliser les techniques de transfert de fichiers via SSH.
- Gérer et comprendre les clés SSH pour une authentification sans mot de passe.
- Savoir utiliser les commandes de bases Linux

Consignes

1 — Le SSH, c'est quoi ?

Dans ce cours, on va vouloir administrer un serveur à distance et de manière sécurisé parce qu'on est des professionnels. Pour cela, on va utiliser le protocole SSH afin de se connecter à notre serveur distant.

SSH, ou Secure Shell, est un protocole cryptographique utilisé pour opérer des services réseau de manière sécurisée. Il a été inventé par Tatu Ylönen en 1995, en réponse à un piratage de mot de passe dans le réseau de son université.

SSH fonctionne en mode client-serveur. Le serveur SSH écoute sur un port spécifique, généralement le port 22, pour les connexions entrantes. Une fois la connexion établie, l'authentification est réalisée, soit par mot de passe, soit par clés publiques/privées. Après une authentification réussie, un shell sécurisé ou une session de commande est établie, permettant l'exécution de commandes à distance.

Pour ce faire, SSH utilise des mécanismes d'encryption symétriques et asymétriques. Ne vous inquiétez pas, SSH le fait automatiquement pour vous quand vous essayez de vous connecter à un serveur via SSH. Mais il est intéressant de comprendre le concept.

Livrables

- ➔ Quels sont les protocoles qui ont été remplacés par SSH ?
- ➔ Quelles sont les différents modes d'utilisation de SSH (notamment au niveau de la sécurité) ?
- ➔ Comment est établie une connection SSH entre un client et un serveur avec la méthode la plus sécurisé (faites un schéma)

2 — Connexion en réseau local

Maintenant que vous avez des connaissances théoriques par rapport au protocole SSH, on va passer à la pratique.

OBJECTIF

L'objectif de cette partie va être de pouvoir se connecter à la machine de votre binôme via SSH en utilisant le réseau local.
Vous devez mettre en place les différents éléments de la documentation afin de pouvoir vous connecter avec un système d'authentification par clés publique/privée.

Livrables

- ➔ Démonstration d'une connexion effective SSH entre votre machine et celle de votre binôme
- ➔ Démonstration de la création d'un fichier sur la machine de votre binôme depuis la votre

RESSOURCES

SSH - Doc Ubuntu https://doc.ubuntu-fr.org/ssh. Tous les éléments importants sont dans cette doc.

3 — Connexion à un serveur distant

Maintenant que vous avez réussi à vous connecter à la machine de votre binôme, vous allez essayer de vous connecter à un serveur distant. Votre formateur vous en a préparé un pour chacun de vous.
Suivez les instructions suivantes pour vous connecter au serveur en SSH à l'aide de votre paire de clé

- Demandez à votre formateur les informations suivantes :
  - Nom d'utilisateur
  - Mot de passe temporaire
  - Adresse IP du serveur distant
- Connectez-vous une première fois au serveur en utilisant le mot de passe temporaire fourni.
- À la première connexion, le serveur vous demandera de définir un nouveau mot de passe. Suivez les instructions à l'écran pour le faire.
- Utilisez la commande ssh-copy-id pour copier votre clé SSH publique sur le serveur. Lorsqu'il vous sera demandé, utilisez le nouveau mot de passe que vous avez défini pour autoriser la copie de la clé.
- Essayez de vous connecter de nouveau au serveur mais cette fois-ci sans utiliser de mot de passe. Si tout est bien configuré, la connexion devrait se faire automatiquement grâce à la clé SSH.

Vous êtes désormais connecté à votre serveur. Vous allez utiliser ce serveur pour tout le reste du module.

Nous allons maintenant revoir certaines commandes basiques de linux qui vous serviront pour la suite et dans votre vie de développeur. Pour cela, je vais vous faire une liste de commandes qui sont le plus souvent utilisées. N'hésitez pas à en proposer d'autres à votre formateur !

Catégorie	Ligne de commande
Navigation et Gestion de Fichiers	ls
	cd
	pwd
Manipulation de Fichiers et de Répertoires	cp
	mkdir
	touch
	mv
Affichage et lecture de contenu de fichier	cat
	less
	find
	grep
Transfert et Synchronisation de Fichiers	scp
	rsync
Éditeur de Texte	vim
	nano

Livrables

- ➔ Démonstration d’une connexion effective SSH entre votre machine et votre serveur

➔ Pour chaque ligne de commande listée plus haut, expliquez ce qu'elle fait et donner un exemple concret d'utilisation