JUNIA Grande école d'ingénieurs
HEI·ISEN·ISA

Thème

La cryptographie : exploration du protocole SSH

Etudiants : Marc BAYART - Axel DERLY - Allan MATANGA - Clément ZAJAC
Encadrants : Gabriel CHENEVERT - Mounia ZAYDI
Date de soutenance : 20 octobre 2023

Résumé :

Dans ce rapport, nous allons explorer en détail le protocole SSH (Secure Shell). Tout d'abord, nous aborderons les aspects théoriques du protocole SSH, en mettant en lumière son importance cruciale pour la sécurité des systèmes d'information. Nous allons également examiner son fonctionnement au sein de la couche transport du modèle OSI, en particulier en utilisant des protocoles comme TCP. SSH repose sur des principes fondamentaux de cryptographie, en faisant usage à la fois de chiffrement symétrique et asymétrique.

Dans une seconde phase, nous allons mettre en pratique nos connaissances en configurant un serveur SSH ainsi qu'un client sur un système d'exploitation Linux. Notre objectif est de démontrer concrètement le fonctionnement du protocole et de mettre en œuvre les compétences acquises. Nous serons en mesure de créer un environnement adéquat et de mettre en place une communication sécurisée entre les différentes machines de notre réseau local grâce à SSH.

Ce rapport permettra une meilleure compréhension du protocole SSH, de son rôle dans la sécurité des systèmes, et de sa mise en pratique sur des plateformes Linux.

Introduction :

Contexte

La sécurité des systèmes représente un enjeu majeur dans un monde de plus en plus interconnecté et numérique, où les menaces potentielles sont en constante évolution, allant des cyberattaques sophistiquées à la protection de la vie privée des individus, et où la confiance dans les systèmes informatiques et les communications est essentielle pour le fonctionnement de la société et de l'économie mondiale.

Le principe de la cryptographie est de sécuriser la communication entre deux individus. Sécuriser une communication est décrit par plusieurs principes :
Dans un premier temps il faut empêcher l'interception de ce message par une personne tierce, et que cette dernière puisse lire le contenu du message. Dans un second temps, il faut empêcher la modification du message par une personne tierce : c'est la confidentialité. Il faut également empêcher qu'une personne tierce puisse injecter un faux message afin d'empêcher l'usurpation d'identité. Et pour finir, il faut également empêcher qu'un message puisse être envoyé de nouveau par une personne tierce.

Les objectifs

Durant cette étude, nous avons différents objectifs à atteindre dans le but de mieux comprendre le protocole SSH et ses utilisations, et cela passe par :

- La compréhension des principes de base du protocol
- L'identification du rôle du protocol SSH dans la sécurité des communications
- La configuration d'un serveur SSH pour permettre des connexions sécurisées.
- La recherche sur des mécanismes d'authentification et de sécurité de SSH.

Sommaire

Chapitre 1 : Cadrage du projet

Choix de la thématique :

Nous avons choisi d'étudier le protocole SSH car ce protocole de communication communément utilisé dans les domaines de l'administration système, la gestion de serveurs, le développement web etc. Le SSH intervient pour chiffrer les données, permettre une gestion efficace, à distance des différents systèmes, permet d'automatisation de tâches, tout en s'intégrant à de nombreux outils.

Planification des activités :

Pour le projet qui s'étalait sur une durée de 4h, il n'a pas été nécessaire de mettre en place une gestion de projet à proprement parler, ou d'outils pour réaliser celle-ci. Nous avons opté pour la simplicité.
Une réunion d'une demi heure à été faites avant pour cadrer le sujet et répartir les tâches selon la manière suivante :

Travail par binôme :

- Axel et Marc
- Allan et Clément

3 tâches sur lesquels travailler :

- Réalisation des recherches : binôme Allan / Clément
- Mise en oeuvre pratique selon les objectifs définis : binôme Axel / Marc
- Réalisation du PPT pour la soutenance : tous ensemble

Chapitre 2 : Concepts fondamentaux, recherche et apprentissage :

Qu'est ce que le SSH ?

SSH (secure shell) est un protocole pour garantir une communication sécurisée entre différents appareils d'un réseau. Il est majoritairement utilisé pour de l'administration à distance des ordinateurs d'un système informatique

Quel est son rôle dans la sécurité des communications?

Le rôle du protocole SSH est de garantir la sécurité des données transitant entre les éléments du SI. Il permet de chiffrer les informations, de permettre l'intégrité des données et d'authentifier le client ainsi que le serveur grâce à des mots de passe ou une clé d'authentification. Cela permet de lutter contre les attaques du type MITM(Man-in-the-middle).

Quelles sont les méthodes de chiffrement du SSH ?

SSH utilise deux méthodes de chiffrement :

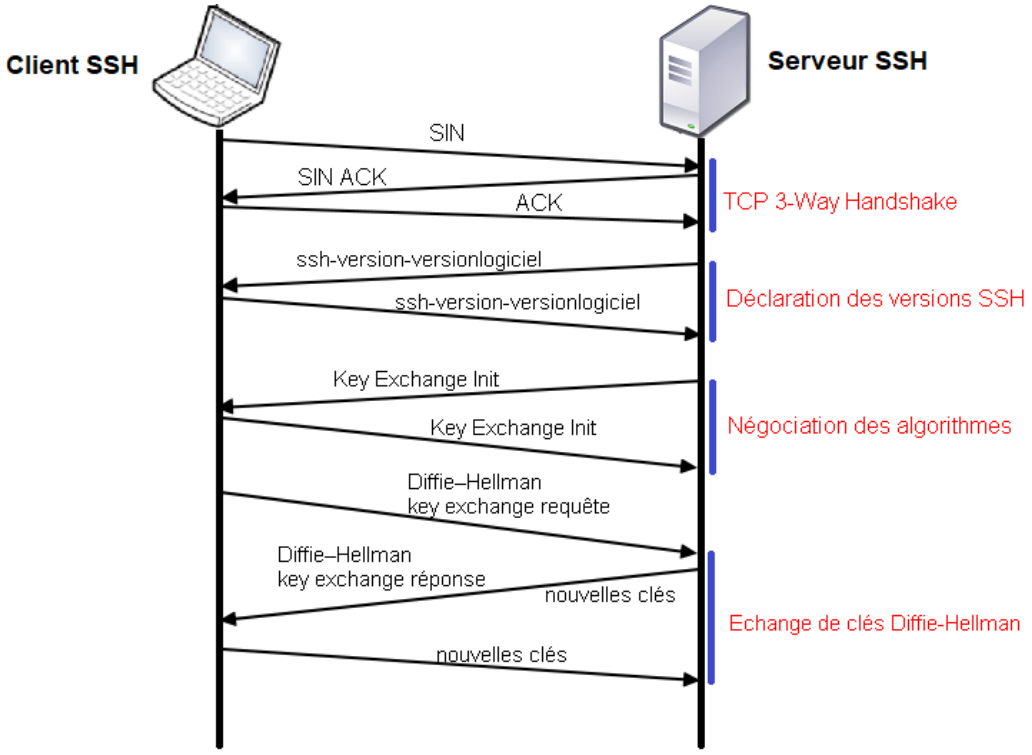
- Le chiffrement symétrique : AES (Advanced Encryption Standard), chacha20-poly1305
- Le chiffrement asymétrique : RSA, ECDSA

Le chiffrement asymétrique est majoritairement utilisé pour l'authentification des différentes parties prenantes alors que le chiffrement symétrique est utile pour le transit des données.

Le chiffrement symétrique est une technique qui consiste à utiliser une clé commune entre deux postes afin de chiffrer les données entre deux points. Il est pratique pour sécuriser une communication, le point fort est la rapidité du processus pour des échanges de gros volumes de données. Cependant il est nécessaire que la clé secrète ne soit pas compromise.

Le chiffrement asymétrique est une autre technique de chiffrement qui utilise deux clés distinctes : une clé publique et une clé privée. Ces deux clés sont mathématiquement liées. Le chiffrement est effectué avec la clé publique alors que le déchiffrement est fait avec la clé secrète.

Fonctionnement du protocol :



Le TCP 3-Way Handshake

1. **SYN (Synchronize)** : Le client envoie un paquet SYN pour initialiser la connexion TCP avec le serveur SSH.
2. **SYN-ACK (Synchronize-Acknowledgment)** : Le serveur répond avec un paquet SYN-ACK pour confirmer la demande de connexion et établir une session TCP.
3. **ACK** : Le client répond ensuite avec un paquet ACK pour confirmer la réception du paquet SYN-ACK

La déclaration des versions SSH

4. **SSH Version Exchange** : Après l'établissement de la session TCP, le client et le serveur SSH s'envoient mutuellement des informations de version du protocole SSH pour choisir la version à utiliser. Le client cherche à utiliser la version la plus récente et sécurisée commun aux deux parties.

Négociation des algorithmes

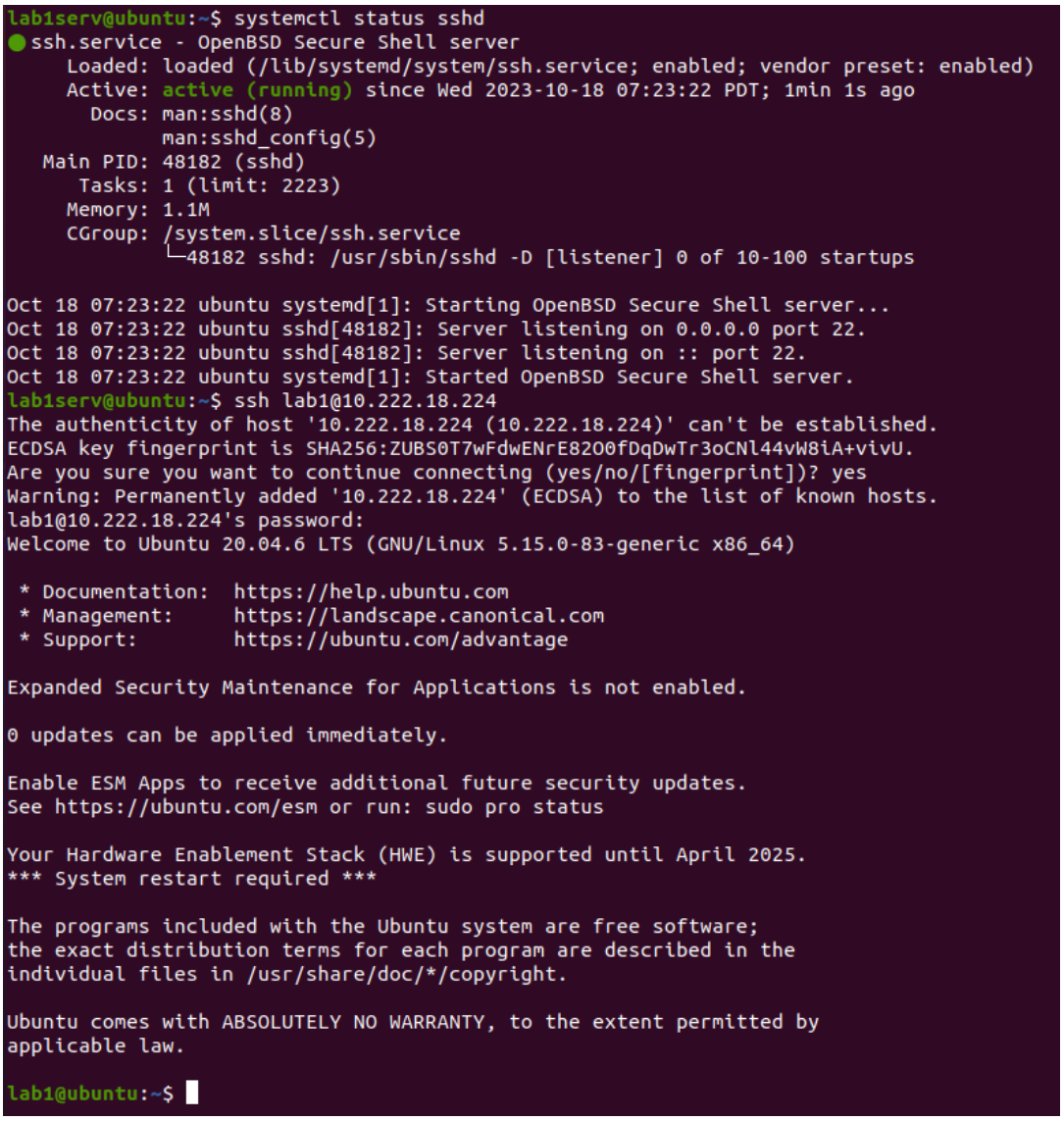
5. **Key Exchange (Échange de clés)** : Une fois la version du protocole SSH négociée, les parties entament l'échange de clés pour établir une session sécurisée. Le processus inclut des étapes telles que l'envoi de "KEXINIT" (Key Exchange Initialization) et "KEXDH_INIT" (Key Exchange Diffie-Hellman Initialization) dans le cas de l'algorithme de clé Diffie-Hellman.

Échange des clés Diffie-Hellman

6. **Diffie-Hellman Key Exchange (Échange de clés Diffie-Hellman)** : C'est une étape de l'échange de clés qui utilise l'algorithme Diffie-Hellman pour générer une clé de session commune entre le client et le serveur, tout en évitant de divulguer les clés secrètes réelles.
7. **New Keys (Nouvelles clés)** : Une fois l'échange de clés Diffie-Hellman terminé, de nouvelles clés de session sont utilisées pour chiffrer les données échangées entre le client et le serveur, assurant ainsi une communication sécurisée.

Chapitre 3 : Réalisation et mise en oeuvre

Pour cette mise en œuvre nous avons utilisé les machines virtuelles mises en place lors d'un précédent TP, soit, 2 machines Ubuntu présentes sur un même réseau local.
Nous avons souhaité mettre en place une simple connexion ssh d'un hôte vers un autre, pour ce faire nous avons tout d'abord démarré le daemon sshd sur chaque machine, puis avons exécuté la commande afin de se connecter sur la seconde machine.



Capture d'écran du statut du serveur SSH et de la connexion à un autre serveur

Nous voyons ici que la connexion à été réalisé avec succès cependant en faisant ceci, nous n'utilisons qu'une fraction des possibilités mises à disposition par le protocole ssh. En effet, il est notamment possible de créer des clés d'authentification en ayant la possibilité de choisir l'algorithme chiffrement, ici nous avons choisi de créer une clé en utilisant l'algorithme RSA.

```
lab1@ubuntu:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/lab1/.ssh/id_rsa):
Created directory '/home/lab1/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lab1/.ssh/id_rsa
Your public key has been saved in /home/lab1/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:MTiDAHCypLgcttc9K/3sUcm3BQ/l/D5OskRSLFLYYSg lab1@ubuntu
The key's randomart image is:
+---[RSA 3072]----+
|=oo       ++.   . |
|++ . . E oo.. +   |
|+o  . + +. . = o |
|o.o . .o oo + + .|
|.o . . oS  = o o.|
|  .    . o . + o. |
|     . o .    + o.|
|      . o . . = .|
|        .+    . . |
+----[SHA256]-----+
```

Capture d'écran de la génération d'une paire de clés RSA

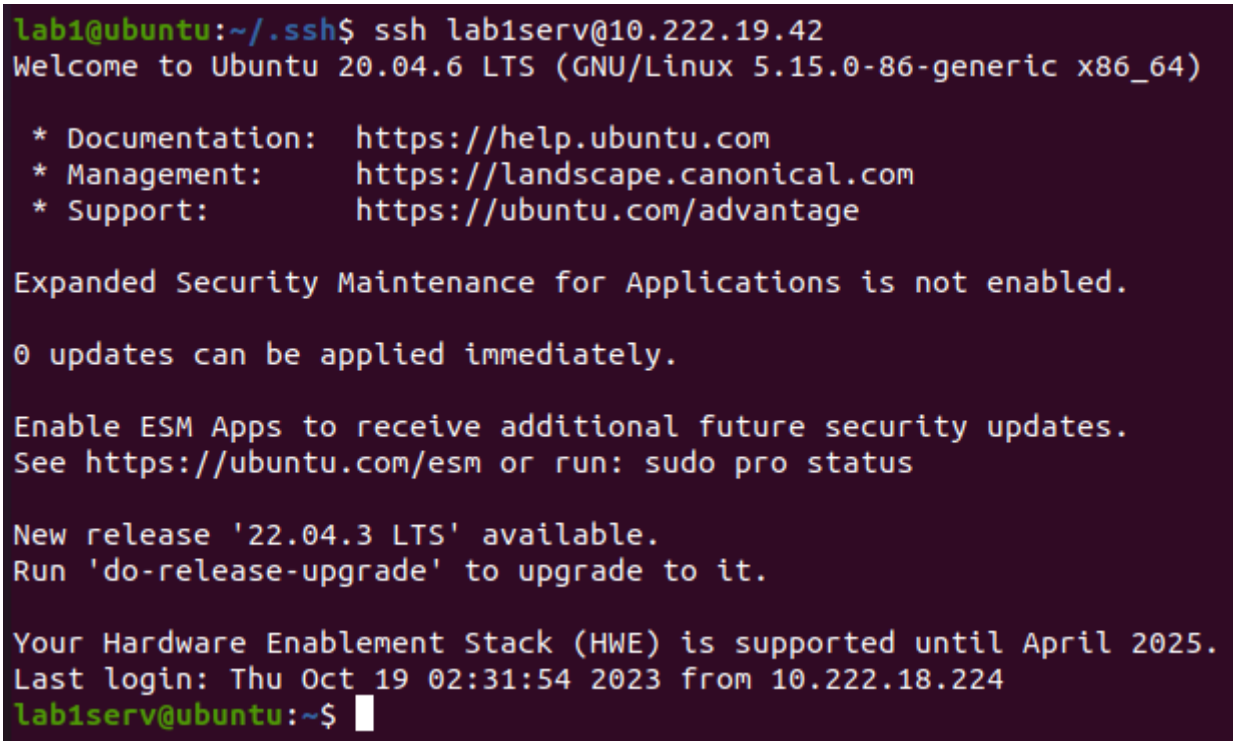
Une fois cette paire de clés créées, nous devons envoyer l'une des clés dans le répertoire authorized_keys de l'hôte cible afin de pouvoir l'utiliser par la suite.

```
lab1@ubuntu:~/.ssh$ ssh-copy-id -i id_rsa lab1serv@10.222.19.42
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "id_rsa.pub"
The authenticity of host '10.222.19.42 (10.222.19.42)' can't be established.
ECDSA key fingerprint is SHA256:IlKiYrX3mrKX5TPVCCmnD844jlzLOh7WOz6NK8wQU1w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
 already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
install the new keys
lab1serv@10.222.19.42's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'lab1serv@10.222.19.42'"
and check to make sure that only the key(s) you wanted were added.
```

Capture d'écran de l'envoi de la clé publique vers le serveur auquel on souhaite se connecter par la suite

Ci-dessous on voit que pour faire la copie de la clé, un mot de passe est requis, en effet on doit se connecter à l'hôte cible avant de pouvoir copier la clé dans son répertoire.

Ensuite nous pouvons essayer de nous connecter en ssh sur la machine de destination et nous n'aurons plus à entrer de mot de passe, la clé faisant office de ce dernier.



Capture d'écran de la connexion au serveur après lui avoir envoyé la clé publique

Conclusion générale

En conclusion, ce projet nous a permis de plonger dans le protocole SSH et d'explorer en profondeur son rôle essentiel dans la sécurité des communications. Nous avons appris les principes fondamentaux de chiffrement symétrique et asymétrique, ainsi que le fonctionnement du protocole, y compris le TCP 3-Way Handshake et l'échange de clés Diffie-Hellman.

La mise en pratique de nos connaissances avec la configuration d'un serveur SSH et l'utilisation de paires de clés RSA a démontré la puissance de ce protocole pour assurer la sécurité des communications.

En envisageant des perspectives d'approfondissement, nous pourrions explorer davantage l'analyse des trames SSH pour mieux comprendre le processus de chiffrement et d'intégrité des données. Ce projet nous a fourni une base solide pour comprendre et utiliser efficacement SSH dans des environnements Linux, renforçant ainsi nos compétences en sécurité informatique.

Références :

Cours AP4 : Linux
Cours licence CNAM : UTC 505
https://www.cnam.fr/
Manuel commandes SSH