Prince BALOUKOULA
Dehn BATONDA

Introduction

SSH, ou Secure Shell

Définition dans un terme simple:

SSH, qui signifie Secure Shell, est un protocole de communication sécurisé utilisé pour l'accès à distance à des systèmes informatiques via un réseau. Il fournit un moyen sécurisé de se connecter à des machines distantes et d'exécuter des commandes de manière sécurisée. SSH utilise une architecture client-serveur et chiffre les données transitant entre le client et le serveur, ce qui rend difficile leur interception par des tiers non autorisés.

L'hôte ciblé (celui dont on veut prendre le contrôle) est un serveur SSH il y a une version serveur de SSH installée dessus il gère les requêtes de connexion ssh. L'hôte souhaitant prendre le contrôle de la cible est un client SSH il y a une version ssh client installée capable d'émettre des requêtes de connexion ssh vers un serveur ssh .

OpenSSH : est un logiciel sous l'infrastructure client-serveur, c'est le logiciel le plus utilisé dans les cas de connexion à des systèmes d'information distants en toute sécurité utilisant le protocole ssh .

Connexion SSH Windows/Linux (Ubuntu)

Première étape : installation d'Openssh sur Ubuntu.

Avant de commencer, je recommande de faire la mise à jour de votre système Linux. Voici quelques étapes pour vous aider :

Debian et Ubuntu (apt):

Mettez à jour la liste des packages disponibles dans les référentiels:

```
sudo apt update
```

Mettez à jour les paquets installés packages installés sur le système vers les versions les plus récentes disponibles:

```
sudo apt upgrade
```

Redémarrez votre machine si nécessaire: Certaines mises à jour peuvent nécessiter un redémarrage.

Sur les versions les plus récentes d'Ubuntu, OpenSSH est préinstallé. Au cas où OpenSSH n'est pas installé, tapez la commande :

```
sudo apt install openssh-server
```

Ceci va installer une infrastructure serveur/client OpenSSH, qui permettra une connexion distante vers cet hôte.

Côté Windows, nous allons nous connecter vers notre hôte Ubuntu.
Pour ce faire, notre machine Windows a besoin d'un client SSH.

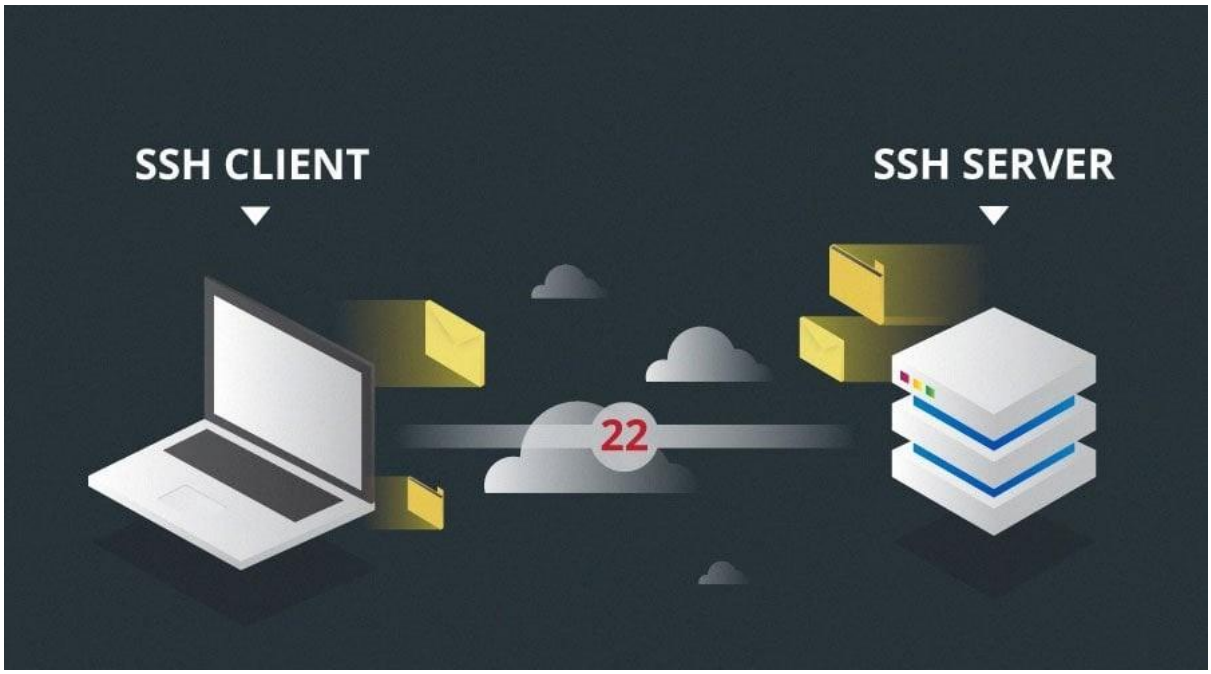
Par défaut, Windows a un client SSH préinstallé. Au cas où vous n'en avez pas installée, utilisez la commande suivante en lançant PowerShell en mode administrateur :

```
Add-WindowsCapability -Online -Name OpenSSH.Client
```

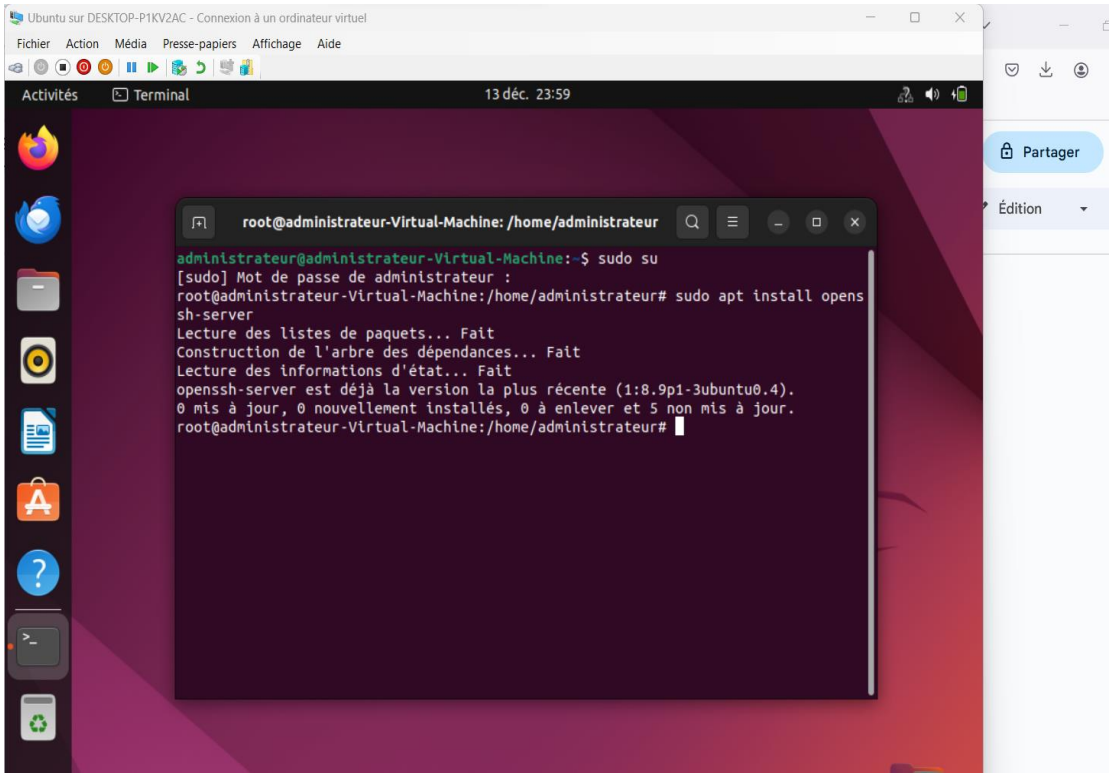
```
PS C:\WINDOWS\system32> Add-WindowsCapability -Online -Name OpenSSH.Client

Path          :
Online        : True
RestartNeeded : False
```

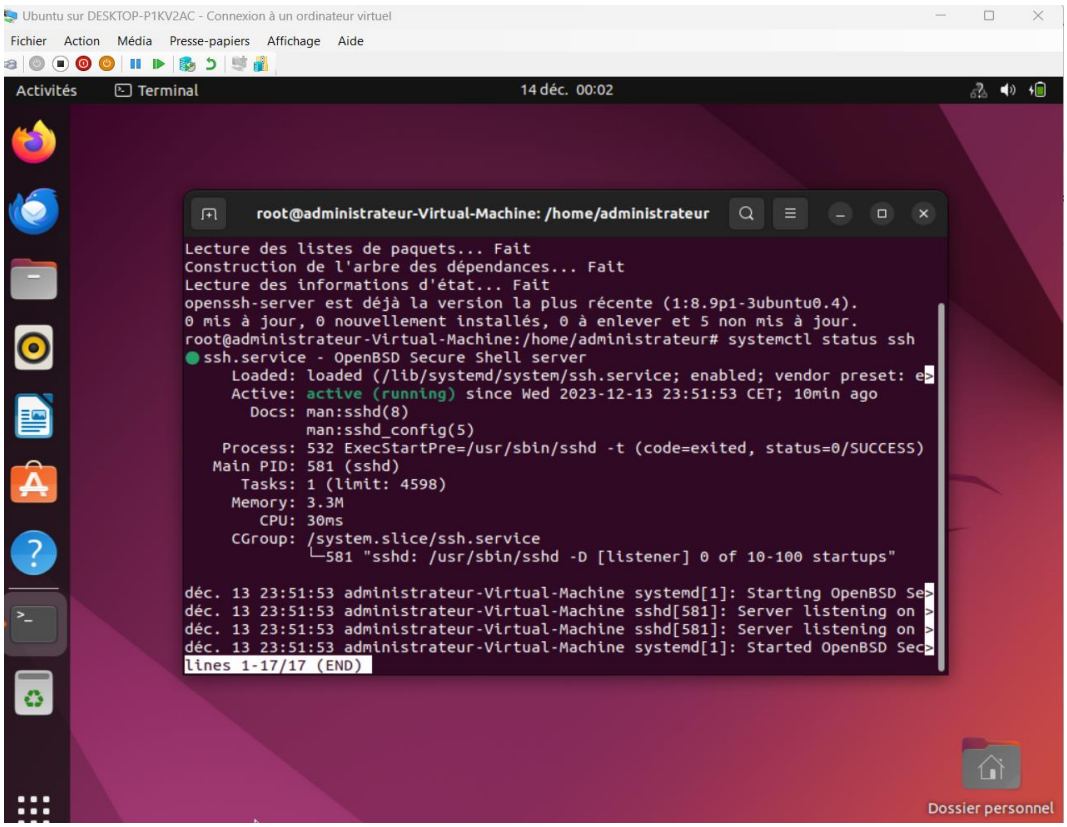
Démonstration



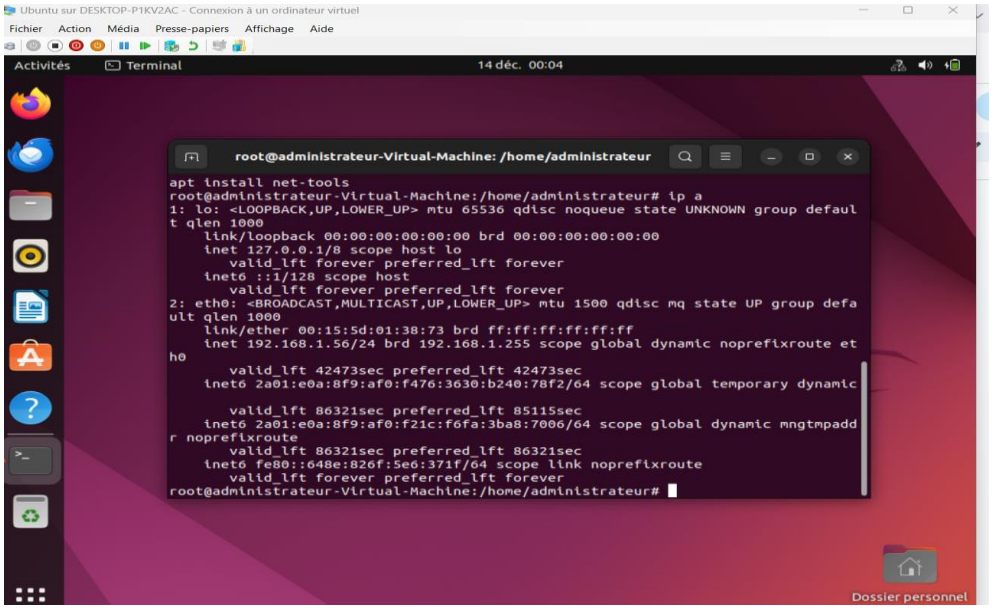
Sur ma machine Ubuntu, j'ai accédé en tant que superutilisateur (root) et ensuite j'ai installé le serveur OpenSSH.



La commande `**systemctl status ssh**` permet de vérifier si le service SSH est correctement installé sur votre système.



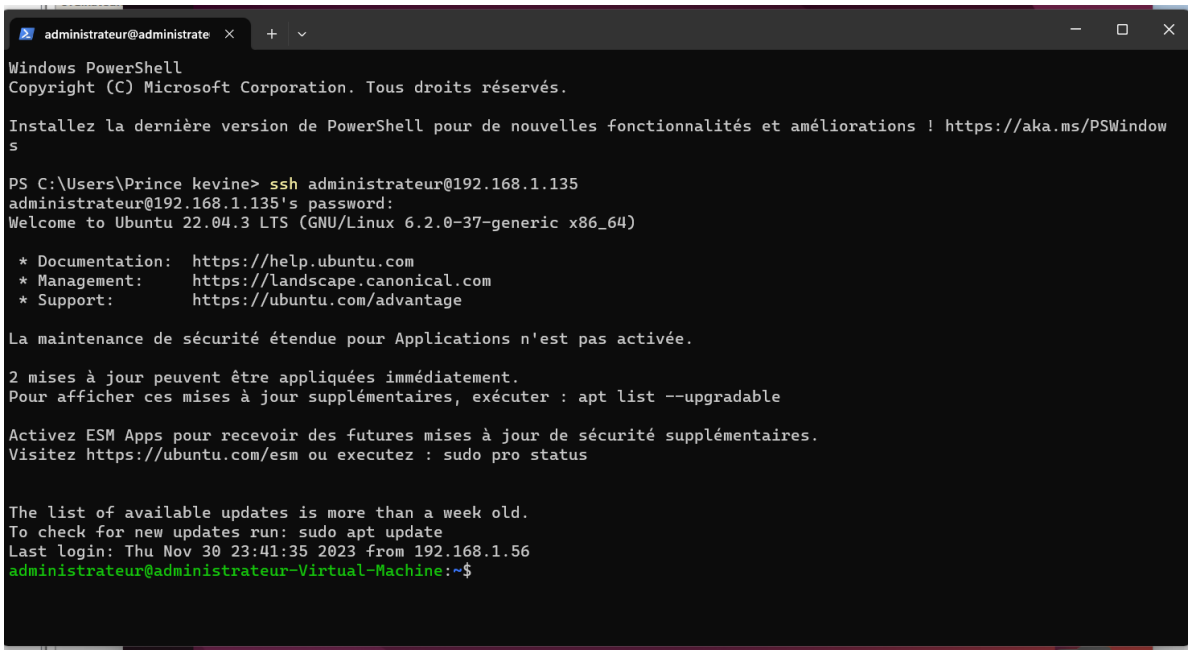
Afin de connecter la machine Ubuntu à un serveur Windows via SSH, il est nécessaire d'obtenir l'adresse IP de la machine hôte (Ubuntu) pour établir la connectivité. Pour trouver cette adresse IP sur une machine Windows, utilisez la commande suivante :
ipconfig ou ip –a



Pour établir la connexion, de Windows vers notre hôte cible, (Ubuntu) en utilisant soit, PuTTY , WinSCP , Termius et Windows Terminale apparue depuis la version Windows 10 version 1903, sur notre Windows terminale on exécute la commande suivante soit

ssh (nom_utilisateur_machine_Ubuntu_ou_Debian)@(adresse_IP_de_la_machine)

Une fois cela fait, on vous demandera le mot de passe de l'utilisateur auquel vous avez souhaité vous connecter sur la machine Ubuntu ou Debian.



Pour la partie 2 nous verrons la connexion SSh sans mot passe grâce au paire de clé/public