Étape 1 : Installation du service SSH

1. Vérifiez que votre service DHCP est démarré. Si ce n'est pas le cas, démarrez-le.

Le serveur a bien été démarré, grâce à la commande “systemctl status isc-dhcp-server.service” on peut voir son statut.

2. Si le service DNS est installé, vérifiez son état et démarrez-le s'il est inactif.

Le serveur a bien été démarré, grâce à la commande “systemctl status bind9.service” on peut voir son statut.

3. Vous devez installer le paquet logiciel du serveur openssh en vous inspirant du Document 8. (Astuce : trouvez le paquet à installer en effectuant une recherche avec la commande apt et les mots clefs openssh, serveur et shell).

La commande permettant d’installer le service ssh est “sudo apt install openssh-server”.

4. Affichez l'état du service SSH pour vérifier qu'il est bien démarré.

Le serveur a bien été démarré, grâce à la commande “systemctl status ssh” on peut voir son statut.

5. A l'aide de la commande netstat (voir les TPs précédents), recherchez le numéro du port sur lequel le service SSH écoute (inspirez-vous des autres services démarrés).

La commande permettant de visualiser le port du service ssh est “netstat -tulpn | grep -i ssh”.

6. Relevez l'adresse IP de votre serveur sur son interface enp0s3.

L'adresse IP de mon serveur sur son interface enp0s3 est 172.17.100.139/16 .

7. Depuis le terminal de votre poste de travail tapez la commande suivante : ssh sio@IPDuServeur.

“ssh sio@172.17.100.139”.

9, 10. Sur le serveur, tapez la commande suivante : netstat -tun. Analysez le résultat obtenu.

La commande affiche l’IP du serveur et l’ip du server distant

11. Sur le client, déconnectez-vous en tapant exit. Puis refaites les étapes 9 et 10. Que constatez-vous ?

Toutes les données se sont effacées suite à la déconnexion.

Étape 2 : Configuration du service SSH

Sécurisation des accès au service.

2. Connectez vous en SSH au serveur en utilisant le compte root (mot de passe toor). Cela fonctionne-t-il ?

Non, cela ne fonctionne pas.

6. Essayez à nouveau de vous connecter en SSH au serveur en utilisant le compte root (mot de passe toor). Cela fonctionne-t-il ?

Oui la connexion fonctionne.

Étape 3 : Authentification par clefs

4. Vérifiez sur le serveur que le répertoire .ssh existe bien dans le répertoire personnel de sio. Dans le cas contraire, vous devez le créer.

mkdir .ssh

5 . Depuis la machine cliente, copiez votre clé publique (pour moi celle de raoul, pour vous celle de votre compte utilisateur sur le serveur par l'utilitaire scp dans le répertoire .ssh de l'utilisateur sio. Cet utilitaire copie des fichiers entre des machines sur un réseau et utilise SSH pour la transmission cryptée des données.

scp -P 2222 /home/soumare/.ssh/id_rsa.pub
sio@172.17.100.139:~/.ssh/tmp_id_rsa.pub p

10. concaténez (grâce à la commande cat et l'opérateur >>) le contenu du fichier copié dans le fichier authorized_keys
cat /home/sio/.ssh/tmp_id_rsa.pub >> /home/sio/.ssh/authorized_keys

Toujours sur la machine serveur, en mode administrateur, dé-commentez et on modifiez cette fois-ci les directives suivantes du serveur SSH dans le fichier sshd_config.

```
PubkeyAuthentication yes
PasswordAuthentication no
AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
```