**INTRODUCTION**

Ce document est la documentation du projet réalisé au sein de l'école La Plateforme, qui consiste en l'installation et la configuration des serveurs DHCP, FTP, SSH et DNS sur deux machines virtuelles fonctionnant sous Debian 12. Ce projet a été mené en équipe. Les membres de cette équipe sont Aymen Sadaoui, Mugire Can et Mehmet Yildiz. Le projet a duré une semaine au total et a été finalement défendu devant l'équipe pédagogique par le biais d'une présentation.

**CONSIGNES**

Tout d'abord, deux machines virtuelles utilisant le système d'exploitation Debian ont été créées. Ces machines ont été configurées pour ne pas utiliser d'interface graphique. De plus, l'activation automatique du DHCP sur le réseau où ces machines fonctionnent a été désactivée.

Dans une deuxième étape, les mises à jour du système ont été effectuées en entrant les commandes nécessaires afin que Debian puisse fonctionner correctement.

Troisièmement, un serveur DHCP a été installé sur la première machine virtuelle, puis configuré et activé.

Quatrièmement, une fois le serveur DHCP activé, la deuxième machine virtuelle a été créée et, après l'installation, nous avons vérifié si le serveur DHCP distribuait correctement les adresses IP. Une fois cette étape validée avec succès, les serveurs FTP et SSH ont été installés et configurés sur cette deuxième machine virtuelle conformément aux exigences. Les connexions au serveur FTP ont été sécurisées via SFTP en utilisant le serveur SSH.

Cinquièmement, nous sommes revenus sur la première machine virtuelle pour installer et configurer le serveur DNS. Ce serveur a été configuré de manière à ce que la connexion utilise le domaine “dns.ftp.com” et qu'il pointe vers l'adresse IP de la première machine virtuelle où le serveur FTP est installé.

Dans la sixième étape, la connexion au serveur SFTP a été réalisée en utilisant les identifiants fournis. L'adresse “dns.ftp.com” a été utilisée pour établir cette connexion.

Enfin, lors de la septième et dernière étape, des réglages supplémentaires ont été effectués afin de sécuriser le serveur SFTP. Ces mesures incluent :

-L'accès au serveur uniquement via des identifiants.

-L'utilisation du port 6500 pour le serveur.

-Le blocage de toute connexion anonyme ou d'invité.

**DOCUMENTATIONS**

**1 – Première Étape**

Avant d’installer nos machines virtuelles, il était nécessaire de configurer le réseau sur lequel elles allaient fonctionner. Tout d’abord, comme nous allions installer notre propre serveur DHCP, nous avons désactivé l’option DHCP dans les paramètres du mode NAT. Ensuite, comme nous voulions que le réseau fonctionne avec une adresse **IP de classe B**, les configurations nécessaires ont été effectuées.

À ce stade, nous avons rencontré des difficultés pour accéder à Internet, car nous ne savions pas encore qu’il existe des adresses **IP publiques et privées** dans cette classe. En effet, certaines adresses IP publiques sont déjà attribuées à des institutions et organisations, ce qui rend leur utilisation pour l’accès à Internet impossible. Après nos recherches, nous avons découvert que nous pouvions nous connecter à Internet en utilisant une adresse IP privée comme **172.16.0.0**.

Nous avons donc configuré notre réseau en définissant l’adresse IP et la passerelle par défaut en conséquence. Une fois cette configuration effectuée, nous avons terminé l’installation de notre première machine virtuelle et lui avons attribué une adresse IP statique en modifiant le fichier /etc/network/interfaces. Enfin, nous avons vérifié l’accès à Internet en envoyant une requête ping.

**2 - Deuxième Étape**

Dans cette deuxième étape, nous devions effectuer les mises à jour nécessaires pour que le système et nos serveurs puissent être installés et mis à jour correctement. Cependant, après avoir entré les commandes requises pour la mise à jour, nous avons constaté que le processus échouait.

Après quelques recherches, nous avons découvert que le fichier **/etc/apt/source.list** était vide et qu’il était nécessaire d’y ajouter les liens permettant de récupérer les mises à jour. Une fois ces liens ajoutés, nous avons relancé les commandes de mise à jour. Cette fois, nous n’avons pas reçu de message d’erreur, mais les mises à jour ne pouvaient toujours pas être effectuées car l’accès au site debian.org était impossible.

Grâce à nos recherches, nous avons compris que le fichier resolv.conf était absent, ce qui nous empêchait d’obtenir une réponse des sites web. Nous avons donc créé ce fichier et y avons ajouté les adresses DNS de Google. Après cette configuration, nous avons enfin pu effectuer les mises à jour du système et avons pu passer à l’installation des serveurs.

**3 - Troisième Étape**

À cette étape, comme nous avions désactivé l’option DHCP dans les paramètres NAT avant l’installation, il nous a été demandé d’installer un serveur DHCP sur notre première machine virtuelle.

Tout d’abord, nous avons installé le serveur DHCP en entrant la commande correspondante. Ensuite, nous avons commencé la configuration du serveur en ajoutant l’interface réseau utilisée par notre réseau. Nous avons identifié que l’interface réseau utilisée sur notre machine était **"ens33"** grâce à la commande **"ip a"**, puis nous avons intégré cette configuration dans le fichier de configuration situé à **/etc/default/isc-dhcp-server**.

Après cette configuration, nous avons modifié le fichier **/etc/dhcp/dhcpd.conf** afin de définir les paramètres nécessaires au bon fonctionnement de notre serveur, tels que le **subnet, netmask, plage d’adresses IP, nom de domaine, passerelle par défaut**, etc. Grâce à ces réglages, notre serveur attribuera une adresse IP de classe B à toutes les machines qui s’y connectent.

Une fois la configuration terminée, nous avons redémarré le serveur à l’aide de la commande **"sudo systemctl restart isc-dhcp-server"**. Ensuite, nous avons vérifié son bon fonctionnement avec la commande **"sudo systemctl status isc-dhcp-server"** afin de nous assurer qu’il était bien actif.

**4 – Quatrième Étape**

Après l’installation du serveur DHCP, nous avons installé notre deuxième machine et lancé le système. Tout d’abord, nous avons vérifié que le serveur DHCP effectuait correctement les configurations nécessaires en consultant le fichier /etc/network/interfaces.

Ensuite, nous avons installé ProFTPd, un serveur FTP fonctionnant sous Linux, ainsi que OpenSSH, un serveur SSH également sous Linux.

Après l’installation, conformément aux exigences du projet, nous avons limité le serveur FTP à une seule session en modifiant le fichier /etc/proftpd/proftpd.conf et en y ajoutant la ligne "**MaxClients 1**".

Une fois cette configuration terminée, nous avons créé un utilisateur nommé "**laplateforme**" à l’aide de la commande appropriée. Puis, nous avons défini son mot de passe avec la commande suivante :

**echo "laplateforme:Marseille!" | sudo chpasswd**

Après avoir finalisé les configurations du serveur FTP, nous avons vérifié s’il était bien actif. Une fois la vérification réussie, nous avons poursuivi avec l’installation du serveur SSH.

Nous avons choisi OpenSSH comme serveur SSH et avons complété son installation. Comme ProFTPd possède déjà son propre module SFTP, nous avons modifié le fichier proftpd.conf pour y ajouter les configurations suivantes :

**<ifModule mod\_sftp.c>**

**SFTPEngine on**

**Port 2222 (pour éviter les conflits avec le port SSH)**

**SFTPL /var/log/proftpd/sftp.log**

**SFTPHostKey /etc/ssh/ssh\_host\_rsa\_key**

**SFTPHostKey /etc/ssh/ssh\_host\_ecdsa\_key**

**SFTPHostKey /etc/ssh/ssh\_host\_ed25519\_key**

**</ifModule>**

Au départ, nous ne savions pas que le serveur ProFTPd possédait déjà ce module, nous avions donc initialement réalisé la connexion SFTP via le client lftp. Cependant, après avoir effectué ces configurations, nous avons pu établir la connexion avec la commande suivante :

**sftp -P 2222 laplateforme@dns.ftp.com**

**5 – Cinquième Étape**

À cette étape, conformément aux exigences du projet, nous avons installé BIND9, un serveur DNS, sur notre première machine virtuelle. Nous avons configuré ce serveur de manière à ce qu’il pointe vers l’adresse IP de notre deuxième machine virtuelle, où est installé le serveur FTP. De plus, nous avons défini la connexion pour qu’elle se fasse via "dns.ftp.com".

**6 – Sixième Étape**

Une fois toutes les configurations terminées, nous nous sommes connectés au serveur SFTP situé sur notre deuxième machine virtuelle en utilisant l’utilisateur "laplateforme", que nous avions créé précédemment. Cette connexion a été réalisée via l’adresse "dns.ftp.com".

Par ailleurs, nous avons testé si une deuxième session pouvait être ouverte en tentant de nous connecter avec un autre utilisateur alors que "laplateforme" était déjà connecté. Ce test nous a renvoyé le message "too many connections", confirmant ainsi que la configuration avait été correctement appliquée.

**7 – Septième Étape**

Dans cette dernière étape, nous avons effectué quelques configurations supplémentaires afin d’augmenter la sécurité des connexions sur le serveur SFTP.

Tout d’abord, pour restreindre l’authentification des utilisateurs sur le serveur SFTP, nous avons modifié le fichier proftpd.conf en y ajoutant les lignes suivantes :

**SFTPAuthorizedUserKeys /etc/proftpd/authorized\_keys/%u**

**SFTPAuthMethods publikey password**

Ensuite, nous avons créé les répertoires destinés à stocker les clés autorisées pour les utilisateurs avec les commandes suivantes :

**sudo mkdir -p /etc/proftpd/authorized\_keys**

**sudo chmod 700 /etc/proftpd/authorized\_keys**

Après cela, nous avons généré une clé SSH pour notre utilisateur et l’avons enregistrée dans le fichier suivant :

**sudo nano /etc/proftpd/authorized\_keys/laplateforme**

Puis, nous avons appliqué les permissions nécessaires :

**sudo chmod 700 /etc/proftpd/authorized\_keys/laplateforme**

**sudo chown laplateforme:laplateforme /etc/proftpd/authorized\_keys/laplateforme**

Une fois cette configuration terminée, nous avons redémarré le serveur ProFTPd, et désormais, seules les connexions effectuées par des utilisateurs autorisés sont acceptées.

Ensuite, nous avons modifié le fichier proftpd.conf pour changer le port utilisé par le serveur en le remplaçant par port 6500, garantissant ainsi que notre serveur FTP fonctionne désormais sur ce port.

Enfin, pour empêcher les connexions anonymes et les connexions invitées sur le serveur FTP, nous avons ajouté la configuration suivante dans proftpd.conf :

**<Anonymous ~ftp>**

**User ftp**

**Group nogroup**

**RequireValidShell off**

**UserAlias anonymous ftp**

**</Anonymous>**

Grâce à ces modifications, nous avons renforcé la sécurité du serveur SFTP, limitant l’accès uniquement aux utilisateurs autorisés et empêchant toute connexion anonyme.

**CONCLUSION**

En résumé, ce projet a permis d’installer et de configurer plusieurs serveurs essentiels sur deux machines virtuelles sous Debian 12, en respectant les exigences définies. Nous avons mis en place un serveur **DHCP**, un serveur **FTP sécurisé par SFTP**, un serveur **SSH**, ainsi qu’un serveur **DNS** pour faciliter la connexion via un nom de domaine. Chaque étape a nécessité des ajustements spécifiques, comme la modification des fichiers de configuration et la sécurisation des accès.

Cependant, nous avons rencontré plusieurs difficultés tout au long du projet. L’une des premières problématiques était liée à la configuration réseau et à l’attribution des adresses IP, ce qui a initialement empêché l’accès à Internet. De plus, la mise à jour du système a nécessité une correction des fichiers de sources **APT** et du fichier **resolv.conf**. La gestion des connexions **FTP et SFTP** a aussi demandé des ajustements pour garantir que seules les connexions autorisées soient acceptées et qu’aucune connexion anonyme ne soit possible. Malgré ces défis, nous avons su trouver des solutions adaptées en effectuant des recherches approfondies et en appliquant les bonnes pratiques en matière d’administration système. Ce projet nous a ainsi permis d’acquérir une expérience concrète dans la gestion et la sécurisation de serveurs sous Linux.