DDWS

JOB 1.1 : Installation d’une machine virtuelle (Debian) avec interface graphique.

Définition d’une machine virtuelle :

En informatique, une machine virtuelle (VM) est une illusion d’un appareil informatique créée par un logiciel d’émulation ou instanciée sur un hyperviseur.
Le logiciel d’émulation simule la présence de ressources matérielles et logicielles.

Installation de la machine virtuelle Debian :

Voici les différentes étapes afin de réaliser l'installation de Debian sur une VM :

- Téléchargement et installation d’une VM tel que VMware Worksation Player 17.5.0 : VMware Workstation Player - VMware Customer Connect
- Téléchargement de Debian en sélectionnant l’image ISO appropriée pour son système : Debian -- Obtenir Debian
- Lancement de VMware Workstation et création d’une nouvelle machine virtuelle en appuyant sur “**Ctrl + N**” ou en cliquant sur l'option “**Create a New Virtual Machine**”.
- Sélection du type de configuration parmi les options disponibles (recommandée ou avancée).
- Sélection du fichier ISO téléchargé.
- Installation de l’image disque.
- Spécification de la taille du disque.
- Vérification des paramètres.
- Lancement de la VM créée.
- Sélection du type d’installation, dans notre cas : Installation graphique.
- Sélection du langage.
- Sélection du fuseau horaire.
- Spécification du nom d’hôte.
- Spécification du nom de domaine.
- Spécification du mot de passe.
- Configuration d’un nouvel utilisateur.
- Configuration de l’horloge en fonction du pays.
- Choix du disque et du schéma de partition.
- Choix de différents logiciels à installer.
- Fin de l’installation.

Configuration SSH :

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé.
Le protocole de connexion impose un échange de clés de chiffrement en début de connexion.
Ensuite tous les segments TCP (Transmission Control Protocol) sont authentifiés et chiffrés.
Il devient donc impossible d'utiliser un *sniffer* (analyseur de paquets) pour voir ce que l'utilisateur fait.

Voici les différentes étapes afin de configurer SSH sur Debian :

- Installer le paquet OpenSSH via la commande : sudo apt-get install openssh-server
- Le fichier de configuration SSH est situé à l'emplacement suivant : /etc/ssh/sshd_config.
- Créer un utilisateur SSH et lui attribuer un mot de passe via les commande : sudo adduser sshuser et sudo passwd sshuser
- Configurer le pare-feu pour autoriser le trafic SSH via la commande sudo ufw allow 22/tcp
- Activer le pare-feu via la commande sudo ufw enable

JOB 2 : Installation d’un serveur web (Apache2).

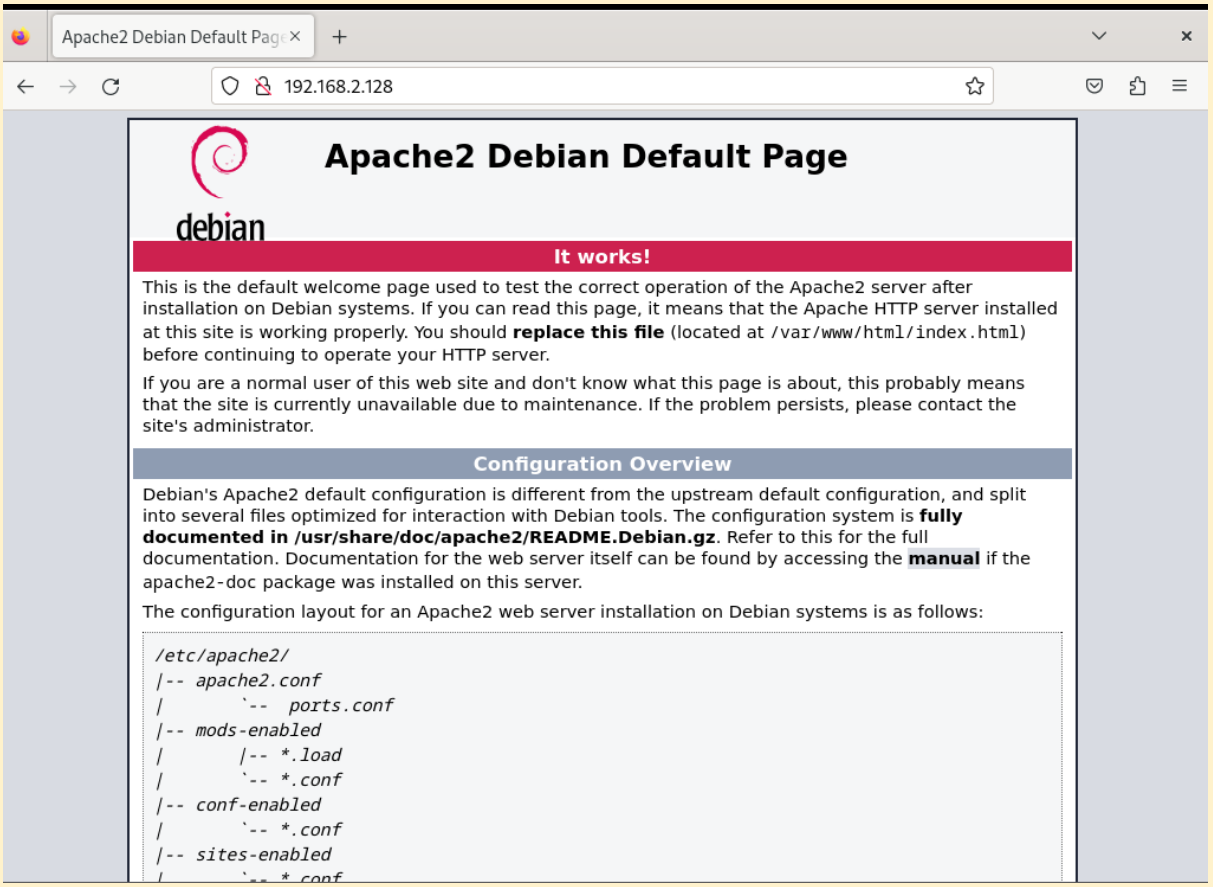
Installation d’Apache2 :

Voici les étape de l’installation d’Apache2 :

- Mise à jour : sudo apt update && sudo apt -y upgrade
- Installation d’Apache2 : sudo apt-get install apache2
- Activation d’Apache2 : sudo systemctl enable apache2
- Aperçu des fichiers :

```
root@web01:/etc/apache2# ls
apache2.conf    conf-enabled  magic           mods-enabled  sites-available
conf-available  envvars       mods-available  ports.conf    sites-enabled
```

- Test du serveur web : Pour ce faire nous devons connaître l’adresse IP : ip address
- Ouvrir le navigateur et taper l’adresse IP dans la barre de recherche.



JOB 3 : Les différents serveurs Web existants.

Définition d'un serveur web :

Un serveur web est soit un logiciel de service de ressources web (serveur HTTP), soit un serveur informatique (ordinateur) qui répond à des requêtes du Wolrd Wide Web sur un réseau public (internet) ou privé (intranet), en utilisant principalement le protocole HTTP.

Les différents serveurs web, leurs avantages et inconvénients :

Il existe 4 types d'hébergement web pour les sites internet :

- L'hébergement sur un serveur mutualisé.
- L'hébergement sur un serveur dédié.
- L'hébergement VPS (Serveur Privé Virtuel).
- L'hébergement Cloud.

Serveur mutualisé :

L'hébergement mutualisé consiste à se partager à plusieurs un seul et même serveur.
Il à pour avantages d'être le plus économique de tous, d'être facile à configurer, utiliser et monitorer grâce au cPanel et aux nombreux outils mis à disposition par les hébergeurs.
En revanche, les inconvénients principaux étant que l'on partage un même serveur avec plusieurs autres sites internet pouvant affecter les performances de nôtre site internet, il n'est donc pas adapté aux sites à fort trafic. Les utilisateurs avancés ne peuvent pas personnaliser la configuration de leur serveur web.

Il sera principalement utilisé pour les sites vitrines attirant peu de visites par mois (en dessous de 50 000), les blogs attirant peu de visiteurs et les petites boutiques en ligne ayant un faible trafic et peu de produits.

Serveur dédié :

L'hébergement dédié consiste à louer auprès d'un hébergeur web un serveur complet qu'il est ensuite possible de configurer selon ses besoins (choix du système d'exploitation, choix de la configuration et des applications).
Il à pour avantages d'être adapté à tous les sites dont ceux à fort trafic, de permettre la personnalisation intégrale de la configuration du serveur, d'améliorer les performances de son site web, et de mieux sécuriser son site et les données associées.

Il est en revanche plus coûteux pour une entreprise, la configuration et la gestion du serveur dédié nécessite de bonnes connaissances en administration système, et les interventions techniques sont à la responsabilité et à la charge du client.

Il sera principalement utilisé pour les sites à fort trafic et gourmands en ressources commes les boutiques en ligne avec plusieurs milliers de produits et plusieurs dizaines de milliers de visiteurs.

Serveur privé virtuel (VPS) :

L'hébergement VPS est un système hybride à mi-chemin entre l' hébergement mutualisé et l'hébergement dédié.
Il consiste à créer plusieurs serveurs virtuels sur un même serveur réel, via des technologies logicielles de virtualisation, pouvant être redémarrées indépendamment et évoluer sur des systèmes d'exploitation distincts.
Cette solution permet à l'utilisateur de choisir précisément les paramètres de son serveur que lui seul utilisera.
Il offre un bon rapport prix-performance, permet d'adapter son serveur virtuel en fonction de réels besoins et peut être redémarré, arrêté ou configuré à chaque fois que le besoin s'en fait ressentir.
Il nécessite cependant de bonnes connaissances en administration système.
Il est particulièrement adapté pour les utilisateurs avancés souhaitant profiter de bonnes performances sans avoir à opter pour un serveur dédié.
Il conviendra pour les boutiques en ligne de taille moyenne, aux sites communautaires avec de nombreux utilisateurs ou encore aux sites vitrines et blog à fort trafic.

Serveur Cloud :

L'hébergement cloud ne repose pas sur un serveur mais sur une multitude de serveurs et le client paye pour ce qu'il utilise vraiment, ce qui permet une flexibilité accrue.
Il permet aux sites de supporter de fortes variations de besoins en bande passante.
Il implique en revanche que les données soient hébergées hors de l'entreprise et demande de s'assurer que le fournisseur met tout en place en termes de sécurité des données.
Il est particulièrement adapté aux entreprises envisageant de croître rapidement et souhaitant obtenir une solution d'hébergement flexible.

JOB 4 : Mise en place d'un DNS sur le serveur Linux.

Etapes pour la mise en place d'un DNS sur le serveur Linux :

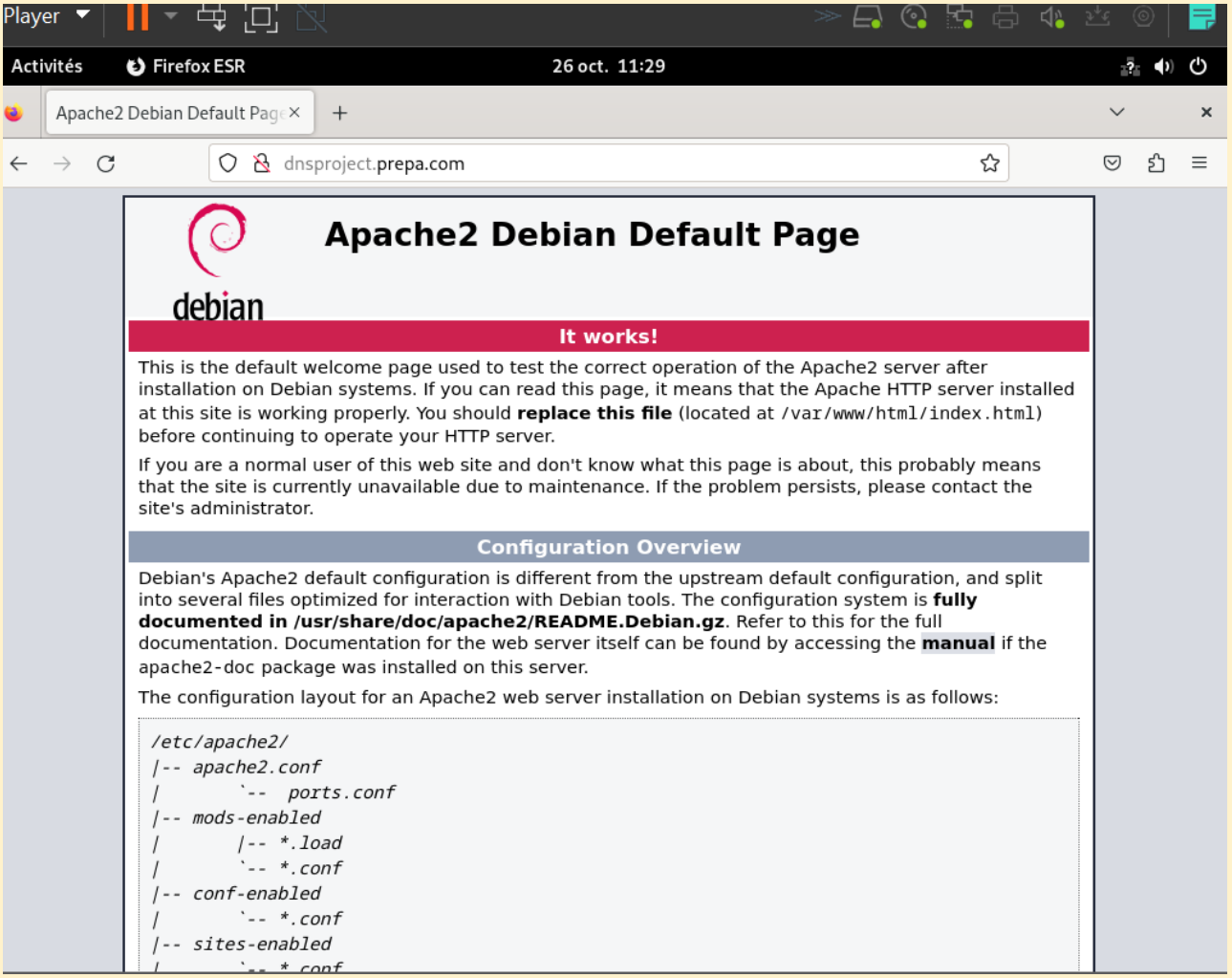
- Installer Bind9, serveur DNS le plus utilisé sous Linux via la commande : sudo apt-get install bind9 dnsutils
- Configurer le système pour utiliser le serveur DNS local en modifiant le fichier /etc/resolv.conf et en ajoutant la ligne **nameserver 192.168.2.128**
- Créer un fichier zone pour le nom de domaine /etc/bind/dnsproject.prepa.com et ajouter les informations suivantes

```
;
; BIND data file for dnsproject.prepa.com
;
$TTL 604800
@       IN      SOA     dnsproject.prepa.com amdin.dnsproject.prepa.com (
              2023102501 ; Serial
              604800 ; Refresh
              86400 ; Retry
              2419200 ; Expire
              604800 ) ; Negative Cache TTL
;
@       IN      NS      dnsproject.prepa.com.
@       IN      A       192.168.2.128
```

- Déclarer la zone dans le fichier /etc/bind/named.conf.local en ajoutant ces lignes :

```
zone "dnsproject.prepa.com" {
 type master;
 file "/etc/bind/dnsproject.prepa.com";
};
```

- Redémarrer le service bind9 via la commande : sudo service bind9 restart
- Tester le serveur DNS via la commande : ping dnsproject.prepa.com


Player
Activités
Firefox ESR
26 oct. 11:29
Apache2 Debian Default Page
dnsproject.prepa.com
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled

JOB 5 : Les noms de domaine.

Définition d'un nom de domaine :

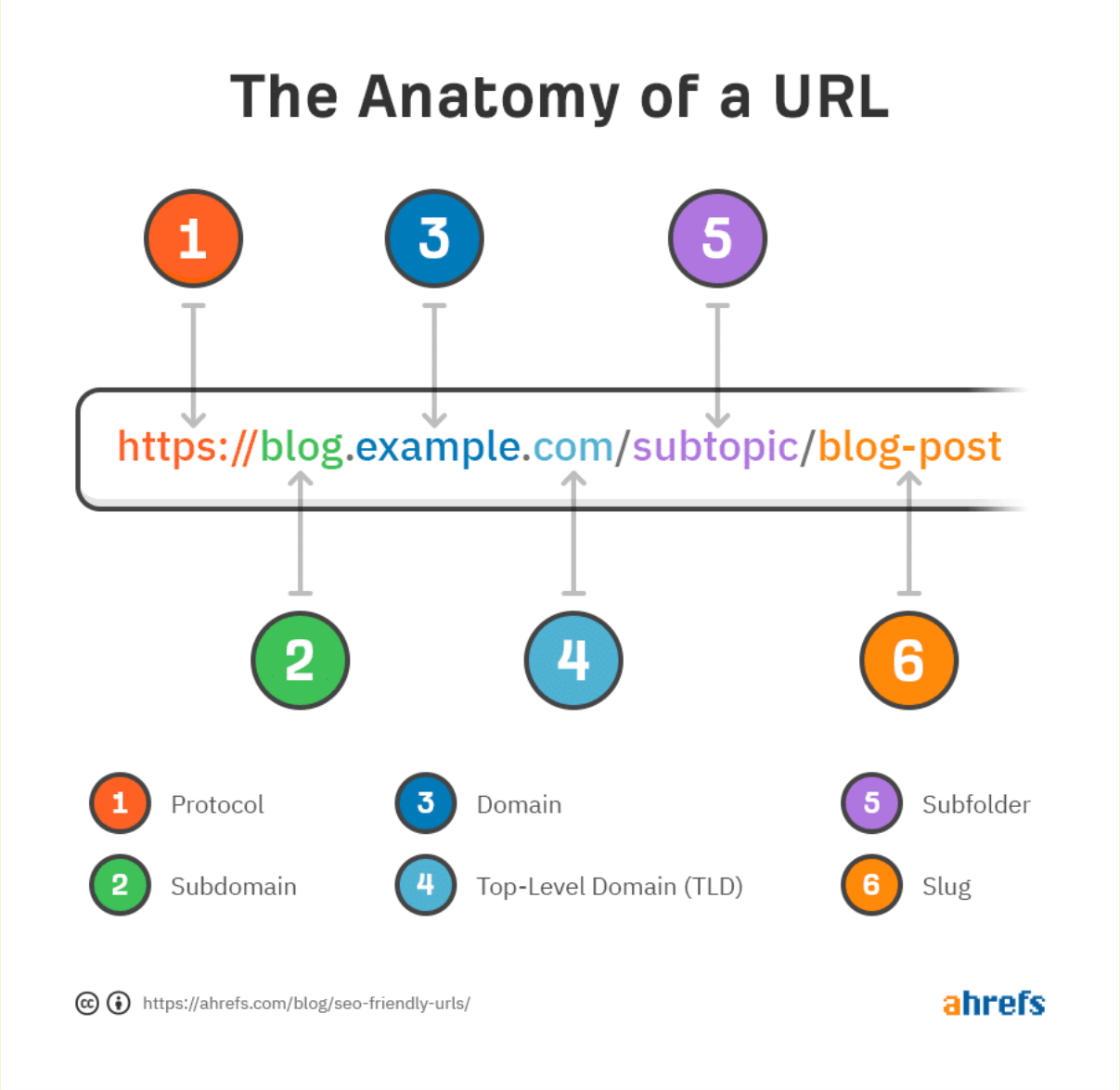
Un DNS (Domain Name System) permet d'associer une adresse IP à un nom de domaine. C'est un service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements.
C'est un composant essentiel du développement du réseau informatique.

Obtention d'un nom de domaine public :

Par définition, un serveur DNS public est accessible à tous et ne requiert aucune authentification. Il est donc ouvert à l'Internet public et n'utilise pas de pare-feu pour limiter les accès.
Il est possible d'en trouver en faisant des recherches sur un navigateur Web ou via des applications listant les différents DNS publics accessibles en les classant par rapidité et sécurité..

Spécificités de certaines extensions de nom de domaine :

La plupart des sites web auxquels on accède se terminent par **.com**, **.org**, **.edu** ...
Ces lettres à la fin d'une adresse web sont appelées extension de domaine, et il existe environ 1500 possibilités dont certaines sont réservées à des organisations ou des personnes spécifiques.
Un autre terme pour une extension de domaine est un domaine de premier niveau car on peut considérer les parties d'un nom de domaine comme des niveaux de classification.
Au sommet nous avons les extensions de domaine et à ce niveau, les domaines sont divisés en grandes catégories.
Par exemple l'extension **.de** place le domaine dans la catégorie "Allemand", l'extension **.gov** place le domaine dans la catégorie "Organisation gouvernementale américaine".
Le niveau inférieur suivant est le domaine. C'est la partie située juste avant l'extension. Elle désigne le site web auquel appartient l'URL.
Il existe parfois un autre niveau appelé sous-domaine qui organise un site web en parties distinctes.



Il existe trois types d'extensions de domaines :

- Les TLD génériques
- Les TLD sponsorisés
- Les TLS avec code pays

TLD génériques :

Les domaines de premier niveau génériques (gTLD), aussi connus comme internationaux, ne sont pas assignés à un pays en particulier mais se réfèrent à l'industrie du demandeur (entreprise, institution, etc...), ou au site Web associé, ou à une zone géographique.

Examples of Top-Level Domains

Traditional gTLDs	New gTLDs	ccTLDs
.com	.guru	.ca
.net	.plumbing	.tw
.org	.realtor	.uk
.gov	.space	.fr
.edu	.design	.de
.info	.cloud	.in
.biz	.ninja	.br
…	…	…

TLD sponsorisés :

Il s'agit d'extensions utilisées par une entité spécifique pouvant être une entreprise, une branche gouvernementale ou un autre type de groupe.
Par exemple, certains sTLD les plus courants sont :

.gov
.edu
.mil
.jobs
...

TLD de code pays :

Ces extensions représentent un pays spécifique, chaque extension de domaine de code pays possède ses propres règles et certaines sont réservées aux organisations du pays, tandis que d'autres sont accessibles à tous.

.ru
.fr
.cn
.de
.ca
...

JOB 6 : Connection de l’hôte au nom de domaine local du serveur.

Afin de configurer le connexion de l’hôte au nom de domaine local du serveur il vas falloir suivre la procédure suivante :
Accéder aux paramètres réseau et internet, paramètres avancés, wi-fi, autres options d’adaptateur, propriété IPv4 et entrer l’adresse IP préféré correspondante à l’IP du serveur : **192.168.2.128**

JOB 7 : Mise en place d’un pare-feu en utilisant ufw.

Pour mettre en place un pare-feu en utilisant ufw sur votre serveur principal de manière que votre hôte puisse accéder à la page apache par défaut, mais qu’il ne puisse plus ping votre serveur, vous pouvez suivre les
étapes suivantes :

- Installez ufw si ce n’est pas déjà fait avec la commande sudo apt-get install ufw.
- Définissez la politique par défaut de ufw pour refuser toutes les connexions entrantes et autoriser toutes les connexions sortantes avec les commandes sudo ufw default deny incoming et sudo ufw default allow outgoing.
- Autorisez le port 80 (HTTP) pour que votre hôte puisse accéder à la page apache par défaut avec la commande sudo ufw allow 80.
- Bloquez le protocole ICMP (ping) pour que votre hôte ne puisse plus pinguer votre serveur avec la commande sudo ufw deny icmp. Vous devrez peut-être éditer le fichier /etc/ufw/before.rules et commenter la ligne qui contient -A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT.
- Activez ufw avec la commande sudo ufw enable.
- Vérifiez le statut de ufw et les règles en vigueur avec la commande sudo ufw status.
-

JOB 8 : Mise en place d'un dossier partagé avec les membres du réseau.

Pour créer un dossier partagé avec les membres du réseau Apache2, il faut d'abord configurer le serveur web Apache pour qu'il reconnaisse le dossier comme un répertoire virtuel. Ensuite, il faut donner les permissions nécessaires aux utilisateurs ou aux groupes qui peuvent accéder au dossier. Voici les étapes à suivre :

- Créez un dossier sur votre ordinateur, à l'emplacement de votre choix. Donnez-lui un nom facilement identifiable par les autres utilisateurs du réseau.
- Ouvrez le fichier de configuration Apache, généralement situé dans /etc/apache2/apache2.conf ou /etc/httpd/httpd.conf, selon votre distribution Linux.
- Ajoutez les lignes suivantes à la fin du fichier, en remplaçant les valeurs entre crochets par celles qui correspondent à votre situation :

```
Alias /monlien "/chemin/vers/mon/dossier"
<Directory "/chemin/vers/mon/dossier">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

- Sauvegardez le fichier et redémarrez le service Apache avec la commande sudo systemctl restart apache2 ou sudo systemctl restart httpd, selon votre distribution Linux.
- Pour partager le dossier avec d'autres utilisateurs ou groupes, vous pouvez utiliser le protocole Samba, qui permet de créer des partages compatibles avec Windows. Pour cela, vous devez installer le paquet samba avec la commande sudo apt install samba ou sudo yum install samba, selon votre distribution Linux.
- Ouvrez le fichier de configuration Samba avec la commande sudo nano /etc/samba/smb.conf et ajoutez les lignes suivantes à la fin du fichier, en remplaçant les valeurs entre crochets par celles qui correspondent à votre situation :

```
[monlien]
    path = /chemin/vers/mon/dossier
    browseable = yes
    read only = no
    valid users = @mon_groupe
```

- Sauvegardez le fichier et redémarrez le service Samba avec la commande sudo systemctl restart smbd ou sudo systemctl restart smb, selon votre distribution Linux.
- Il est maintenant possible d'accéder au dossier partagé depuis un navigateur web en tapant l'adresse http://mon_serveur/monlien ou depuis un explorateur de fichiers en tapant l'adresse \\mon_serveur\monlien.

Pour aller plus loin : Installation d'un certificat pour le serveur web via openSSL.

Définition et utilités d'un certificat ;

Les certificats numériques fonctionnent comme des mots de passe permettant de protéger des données et des communications, souvent entre des sites web et des navigateurs.

Installation du certificat :

Pour installer un certificat pour le serveur web Apache 2 via OpenSSL, vous devez suivre les étapes suivantes :

- Générer une clé privée et une requête de signature de certificat (CSR) avec la commande openssl genrsa et openssl req.
- Obtenir un certificat signé par une autorité de certification (CA) à partir de la CSR. Vous pouvez utiliser un service gratuit comme Let's Encrypt, openSSL ou acheter un certificat auprès d'un fournisseur comme VeriSign, GoDaddy, Namecheap, etc.
- Copier le certificat et la clé privée dans un dossier sécurisé sur votre serveur, par exemple /etc/apache2/ssl.
- Modifier le fichier de configuration Apache pour activer le module SSL et spécifier le chemin vers le certificat et la clé privée. Vous pouvez utiliser la directive SSLEngine on et les directives SSLCertificateFile et SSLCertificateKeyFile.
- Redémarrer le service Apache pour appliquer les changements.

Différence entre les certificats SSL donnés par des organismes extérieurs et le certificat auto-signé généré pour le projet :

Techniquement, tout propriétaire de site web peut créer son propre certificat SSL. De tels certificats sont appelés certificats auto-signés. Cependant, les navigateurs ne considèrent pas les certificats auto-signés comme étant aussi fiables que les certificats SSL émis par une **autorité de certification**.

Pourquoi le certificat apparaît comme non sécurisé sur le navigateur ?

Les utilisateurs peuvent parfois se trouver bloqués avant d'avoir atteint un site web par un message « Votre connexion n'est pas privée ».
Cette erreur signifie que la connexion entre le client (l'appareil de l'utilisateur, tel qu'un ordinateur portable ou une tablette) et le serveur (l'hôte du site web) n'est pas chiffrée, même si l'appareil client s'attendait à ce qu'elle soit chiffrée.
Par conséquent, les personnes malveillantes peuvent voir ce que l'utilisateur fait sur le site web : les messages entre le client et le serveur sont envoyés en texte brut, au lieu d'être brouillés par chiffrement.
En outre, le client n'est pas en mesure de vérifier qu'il est connecté au serveur approprié.
C'est la raison pour laquelle le navigateur indique « Votre connexion n'est pas privée » ou « Votre connexion n'est pas sécurisée » : il ne peut pas vérifier le serveur web, et il ne peut pas chiffrer les messages pour empêcher les attaquants de les lire.
Cette erreur est causée par un problème avec le certificat SSL du site web (il est manquant, ou il a expiré, ou il n'a pas été émis par une autorité de certification légitime, ou le client ne peut pas y accéder pour une autre raison). Les certificats SSL sont nécessaires pour servir les sites web via des connexions sécurisées en HTTPS.

Pour aller encore plus loin : Installation d'un DHCP en dehors de VMWare.

Définition d'un DHCP :

Dynamic Host Configuration Protocol (DHCP, protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.
DHCP peut aussi configurer l'adresse de la passerelle par défaut et configurer des serveurs de noms de domaine comme DNS ou NBNS.

Installation et configuration du DHCP :

D'abord, pour avoir un serveur DHCP, il faut installer le service :

```
apt install isc-dhcp-server
```

Ne pas lancer tout de suite le service DHCP !

Configuration du serveur DHCP

Sur Debian, il y a une petite spécificité, il faut indiquer dans **/etc/default/isc-dhcp-server** sur quelles interfaces va écouter le service DHCP.

```
vi /etc/default/isc-dhcp-server
```

On dé-commente :

```
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
```

Et un peu plus bas, on spécifie les interfaces d'écoute.

```
INTERFACESv4="enp23s0" .
INTERFACESv6="enp23s0"
```

Récupérer le nom avec la commande :

```
ip addr
```

Lancement et configuration du service

Une fois la config terminée, on lance notre DHCP:

```
systemctl start isc-dhcp-server
```

Et on ajoute le service au démarrage :

```
systemctl enable isc-dhcp-server
```