Merhdaoui Mohamed

TP Serveur et site web

Introduction :

Dans ce TP, nous allons
- Installer un serveur web
- Y déposer un fichier site internet préalablement crée (en première année de SIO)
- Puis sous sécuriserons notre serveur avec un pare-feu (avec iptables)

Sur un ordinateur ayant une machine virtuelle Ubuntu d'installé, nous allons créer un serveur web et y déposer mon site.

Pour installer un serveur web apache, il faut ouvrir un terminal puis saisir les commandes suivantes :
#sudo apt update
#sudo apt install php
#sudo apt install apache2 mysql-server phpmyadmin
#sudo service apache2 start

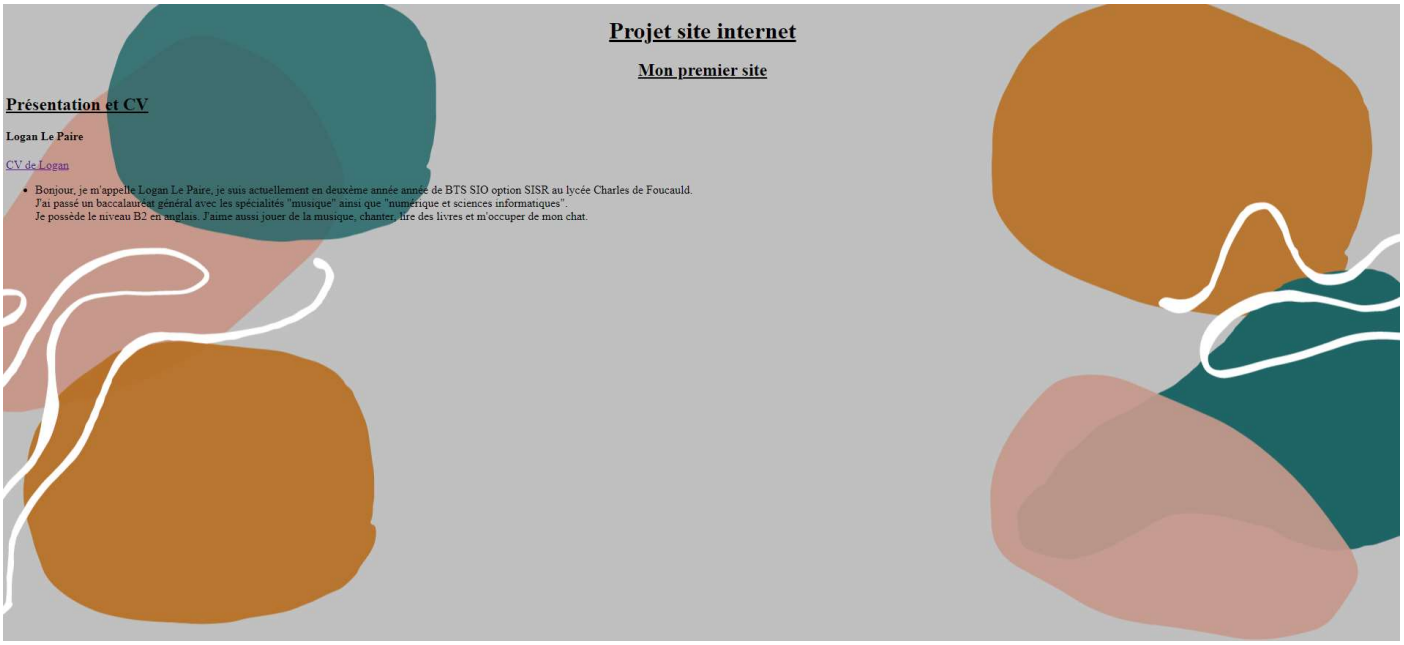
Il faudra ensuite déposer (ou créer) notre fichier index.html dans le répertoire, tel que /var/www/html/index.html

Il faudra redémarrer le service apache pour appliquer les changements :
#sudo service apache2 restart

Nous pourrons retrouver notre site web sur notre navigateur à l'adresse http://127.0.0.1 ou en saisissant notre adresse IP

Comme nous nous trouvons sur machine virtuelle, nous pouvons faire redirection de port pour pouvoir accéder à notre site depuis le navigateur de la machine hôte.
Pour cela, il faut aller dans les paramètres réseau de notre VM et ajouter une règle liant le port invité qui est 80, au port hôte qui peut être n'importe quel port disponible (dans ce cas, 8080).

Ce qui nous affiche cette page sur le navigateur :



Voici donc le code source de ma page web :

```
<style>
  body {
    background-color: #C0C0C0;
    color: black;
    background-image: url('https://cdn.discordapp.com/attachments/874714787051868170/1018486373197561906/fond.png');
    background-repeat: no-repeat;
    background-attachment: fixed;
    background-position: center;
  }

  .table1 {
    width: 285px;
    border: 4px solid;
  }
</style>

<head>
  <title>Travail groupe 4</title>
  <!--  -->
</head>

<body>
  <center>
    <h1><strong><u>Projet site internet</u></strong></h1>
    <h2><strong><u>Mon premier site</u></strong></h2>


  </center>

  <left>
    <h2><u>Présentation et CV</u></h2>
  </left>

  <P>
  <h4>Logan Le Paire</h4>
  </P>
  <a href="cv_logan.pdf">CV de Logan </a>
  <ul>
    <li>Bonjour, je m'appelle Logan Le Paire, je suis actuellement en deuxème année année de BTS SIO option SISR au lycée Charles de
      Foucauld.<br> J'ai passé un baccalauréat général avec les spécialités "musique" ainsi que "numérique et sciences informatiques".<br> Je possède le niveau B2 en anglais. J'aime aussi
      jouer de la musique, chanter, lire des livres et m'occuper de mon chat. </li>
  </ul>



</body>

</html>
```

Partie sécurisation du serveur :

Nous pouvons ensuite sécuriser ce serveur web en y ajoutant des règles de pare-feu.
Nous allons donc bloquer tous les ports et autoriser uniquement ceux que nous utiliserons.

Pour cela, il faut installer iptables qui sera notre firewall :
#apt-get install iptables

Et y ajouter des filtres :

Réinitialise les règles
#sudo iptables -t filter -F
#sudo iptables -t filter -X

Bloque tout le trafic
#sudo iptables -t filter -P INPUT DROP
#sudo iptables -t filter -P FORWARD DROP
#sudo iptables -t filter -P OUTPUT DROP

Autorise les connexions déjà établies et localhost, c'est-à-dire notre ordinateur
#sudo iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
#sudo iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
#sudo iptables -t filter -A INPUT -i lo -j ACCEPT
#sudo iptables -t filter -A OUTPUT -o lo -j ACCEPT

ICMP (Ping)
#sudo iptables -t filter -A INPUT -p icmp -j ACCEPT
#sudo iptables -t filter -A OUTPUT -p icmp -j ACCEPT

SSH (qui nous sers lors de connexions à distance)
#sudo iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT
#sudo iptables -t filter -A OUTPUT -p tcp --dport 22 -j ACCEPT

DNS (pour de la résolution de nom de domaine, donc un accès à internet)
#sudo iptables -t filter -A OUTPUT -p tcp --dport 53 -j ACCEPT
#sudo iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
#sudo iptables -t filter -A INPUT -p tcp --dport 53 -j ACCEPT
#sudo iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

HTTP(C'est la partie la plus importante car c'est un serveur web)
#sudo iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT
#sudo iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT

NTP (horloge du serveur)
#sudo iptables -t filter -A OUTPUT -p udp --dport 123 -j ACCEPT

Nous pouvons également nous prémunir des attaques DOS et du scan de ports avec :
#iptables -A FORWARD -p tcp --syn -m limit --limit 1/second -j ACCEPT
#iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT