NGINX configuration et sécurisation

Cette fiche de procédure contient les étapes importantes pour la configuration du service apache et de la sécurisation sous Debian 11

Explication de NGINX

Nginx est un serveur web léger et performant, ainsi qu'un serveur proxy inverse. Il sert à héberger des sites web et à acheminer les requêtes des clients vers les serveurs appropriés. Il peut être utilisé comme un serveur web autonome pour héberger des sites statiques ou dynamiques, ou en combinaison avec d'autres serveurs web pour répartir la charge entre plusieurs serveurs.

Installation d'NGINX

Vérifier les dépôts Debian avant l'installation en mode root :

```
apt update

apt upgrade -y

apt install nginx

systemctl status nginx.service (vérifie si le service est en cour d'exécution)
```

Configuration de NGINX

Pour vérifier que le service est bien activé saisir sur un navigateur : Affichant une page lie à apache

```
http://localhost
```

Le répertoire courant ou se trouve « index.html » se trouve dans :

```
cd /var/www/html
```

Le fichier de configuration principale d'apache contenant les directives pour le fonctionnement se trouve dans :

```
cd /etc/nginx/nginx.conf
```

Et dans ce fichier on peut ajouter l'emplacement du site web

```
http {
   # Configurer les paramètres du serveur
   server {
      listen 80 default_server;
      listen [::]:80 default_server;
      root /var/www/html; « Indique le répertoire racine du serveur web »
      index index.html index.htm; « Définit les noms de fichiers d'index que Nginx doit chercher »
      server_name _;
      location / {
         try_files $uri $uri/ =404;
« Définit comment Nginx doit répondre aux requêtes pour des fichiers qui ne sont pas trouvés »
      }
   }
```

Sécurisation d'Apache

Pour supprimer la visibilité de la version d'apache faut ajouter dans le fichier :

```
cd /etc/nginx/nginx.conf
```

Et mettre :

```
http {
   # Désactiver le serveur signature
   server_tokens off;

   # Activer la protection contre l'injection de contenu
   add_header X-Content-Type-Options nosniff;

   # Activer la protection contre la divulgation de l'origine
   add_header Referrer-Policy "same-origin";

   # Activer la protection contre le détournement de clics
   add_header X-Frame-Options SAMEORIGIN;

   # Activer la protection contre les attaques XSS
   add_header X-XSS-Protection "1; mode=block";
```

Autoriser que le trafic nécessaire pour communiquer avec le serveur web « Apache » avec iptables :

```
apt install iptables
```

Règles de filtrage :

iptables -P INPUT DROP «politique par défaut »

iptables -P OUTPUT ACCEPT «politique par défaut »

iptables -A INPUT -p tcp --dport http -j ACCEPT « Cette règle autorise le trafic HTTP entrant. »

iptables -A INPUT -p tcp --dport https -j ACCEPT « Cette règle autorise le trafic HTTPS entrant. »

iptables -A OUTPUT -p udp --dport 53 -j ACCEPT « Cette règle autorise le trafic DNS sortant UDP »

iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT « Cette règle autorise le trafic DNS sortant TCP »

iptables -A INPUT -j DROP

« Cette règle bloque tous les autres paquets entrants qui n'ont pas été autorisés par les règles précédentes. »