Mise en place d'un serveur web sécurisé (Apache2, HTTPS et DNSSEC)

Mise en place d’un serveur web sécurisé (Apache2, HTTPS et DNSSEC)

1. Installation et configuration d’Apache2

Installation d’Apache2

```
sudo apt update
sudo apt install apache2 -y
```

Création et configuration d’un hôte virtuel

- Créer un fichier de configuration pour le site :

```
sudo nano /etc/apache2/sites-available/monsite.conf
```

Ajouter :

```
<VirtualHost *:80>
  ServerName monsite.cyber
  DocumentRoot /var/www/monsite
  <Directory /var/www/monsite>
    Options -Indexes
    AllowOverride All
  </Directory>
</VirtualHost>
```

- Activer le site :

```
sudo a2ensite monsite.conf
sudo systemctl restart apache2
```

- Vérifier le fonctionnement en accédant à http://monsite.cyber

2. Activation de HTTPS

Installation du module SSL

```
sudo a2enmod ssl
sudo systemctl restart apache2
```

Ouverture du port 443

Vérifier que le fichier /etc/apache2/ports.conf contient :

```
Listen 443
<IfModule ssl_module>
   Listen 443
</IfModule>
```

Génération d'un certificat SSL auto-signé

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
-keyout /etc/ssl/private/monsite.key \
-out /etc/ssl/certs/monsite.crt
```

Configuration d'Apache pour HTTPS

Modifier le fichier de configuration /etc/apache2/sites-available/monsite.conf :

```
<VirtualHost *:443>
   ServerName monsite.cyber
   DocumentRoot /var/www/monsite
   SSLEngine on
   SSLCertificateFile /etc/ssl/certs/monsite.crt
   SSLCertificateKeyFile /etc/ssl/private/monsite.key
</VirtualHost>
```

Activer le site HTTPS et redémarrer Apache :

```
sudo a2ensite monsite.conf
sudo systemctl restart apache2
```

- Tester en accédant à https://monsite.cyber

3. Sécurisation d'Apache

Désactivation des informations serveur

Modifier /etc/apache2/conf-enabled/security.conf :

```
ServerTokens Prod
ServerSignature Off
Redémarrer Apache :
sudo systemctl restart apache2
```

Redirection HTTP vers HTTPS

Ajouter cette configuration dans le fichier /etc/apache2/sites-available/monsite.conf :

```
<VirtualHost *:80>
  ServerName monsite.cyber
  Redirect / https://monsite.cyber/
</VirtualHost>
```

Appliquer et redémarrer :

```
sudo systemctl restart apache2
```

4. Mise en place de DNSSEC

Vérification du service DNS (BIND9)

```
systemctl status bind9
Vérification avec :
host -l monsite.cyber
```

Configuration de la zone DNS

Éditer /etc/bind/named.conf.local :

```
zone "monsite.cyber" {
   type master;
   file "/etc/bind/db.monsite";
};
```

Créer /etc/bind/db.monsite :

```
$TTL 86400
@   IN  SOA  ns1.monsite.cyber. admin.monsite.cyber. (
         2024031901 ; Serial
         3600      ; Refresh
         1800      ; Retry
         604800    ; Expire
         86400 )   ; Minimum TTL
@   IN  NS  ns1.monsite.cyber.
ns1 IN  A   192.168.1.1
```

Redémarrer BIND9 :

```
sudo systemctl restart bind9
```

Activation de DNSSEC

- Génération des clés :

```
sudo dnssec-keygen -a NSEC3RSASHA1 -b 2048 -3 monsite.cyber
sudo dnssec-keygen -a NSEC3RSASHA1 -b 4096 -3 -f KSK monsite.cyber
```

- Configurer le fichier /etc/bind/named.conf.options :

```
options {
   dnssec-validation auto;
   allow-recursion { any; };
};
```

- Appliquer les signatures :

```
sudo systemctl restart bind9
```

- Tester DNSSEC :

```
dig +dnssec monsite.cyber
```

Conclusion

La mise en place de **HTTPS** et **DNSSEC** sur un serveur Apache2 permet de garantir la sécurité et l'authenticité des communications. Une fois les configurations appliquées et testées, le serveur est prêt à fonctionner en toute sécurité.