Chiffrement des Communications HTTP et FTP avec SSL/TLS

PARTIE A – HTTPS : Création et utilisation d'un certificat auto-signé

1. Installation d'OpenSSL et création du répertoire pour les certificats

- **Installation d'OpenSSL**

La première étape consiste à installer OpenSSL pour générer les clés et certificats nécessaires.

```
  <code bash>
  apt-get install openssl
  </code>
```

- **Création du répertoire pour stocker les certificats**

Créez un répertoire dans `/etc/ssl/` pour stocker vos certificats SSL.

```
  <code bash>
  mkdir /etc/ssl/localcerts
  </code>
```

2. Création du certificat SSL

- **Génération du certificat SSL auto-signé**

Utilisez la commande suivante pour générer un certificat SSL auto-signé et sa clé privée.

```
  <code bash>
  DIR=/etc/ssl/localcerts
  openssl req -x509 -newkey rsa:4096 -nodes -keyout $DIR/mydomainkey.key -
out $DIR/mydomaincert.pem -days 365
  </code>
```

- **Explications des paramètres** :
  1. `-newkey rsa:4096` : Crée une clé RSA de 4096 bits.
  2. `-keyout` : Fichier de sortie pour la clé privée.
  3. `-out` : Fichier de sortie pour le certificat.
  4. `-nodes` : Ne pas utiliser de phrase de passe pour la clé (pour simplification).
  5. `-days 365` : Durée de validité du certificat de 365 jours.

3. Activation du VirtualHost SSL pour Apache

- **Activer le site SSL par défaut pour Apache**

Utilisez la commande suivante pour activer le site SSL par défaut dans Apache :

```
<code bash>
a2ensite default-ssl
</code>
```

- **Activer le module SSL pour Apache**

Activez le module SSL pour permettre à Apache de gérer les connexions sécurisées :

```
<code bash>
a2enmod ssl
</code>
```

- **Modification de la configuration du VirtualHost SSL**

Éditez le fichier `/etc/apache2/sites-available/default-ssl.conf` et assurez-vous que les directives `SSLCertificateFile` et `SSLCertificateKeyFile` pointent vers les bons fichiers de certificat et de clé.

4. Redémarrage d'Apache et vérification

- **Redémarrer Apache**

Après avoir effectué les modifications, redémarrez Apache pour que les changements prennent effet.

```
<code bash>
systemctl restart apache2
</code>
```

- **Vérification des ports ouverts**

Vérifiez que le port 443 (HTTPS) est bien ouvert et en écoute.

```
<code bash>
netstat -tuln | grep 443
</code>
```

5. Test de la connexion HTTPS

- **Test via un navigateur**

Accédez à l'URL suivante dans votre navigateur pour tester la connexion HTTPS :

```
```
https://www.mycompany.org
```
```

```
  ```
```

- **Gestion des erreurs liées au certificat auto-signé**

Vous recevrez probablement un avertissement concernant le certificat auto-signé. Vous pouvez accepter l'avertissement en toute sécurité, car le certificat a été généré par vous-même.

### 6. Documentation des étapes

```
1. **Toutes les étapes de création du certificat avec les explications**
  - Installation d'OpenSSL
  - Création du répertoire pour les certificats
  - Génération du certificat SSL
  - Configuration d'Apache pour SSL
  - Vérification des ports et redémarrage d'Apache
  - Test avec un navigateur et gestion des erreurs
```

```
2. **Modifications apportées aux fichiers de configuration d'Apache**
  - Activation du site SSL par défaut avec `a2ensite default-ssl`
  - Activation du module SSL avec `a2enmod ssl`
  - Modification du fichier `/etc/apache2/sites-available/default-ssl.conf`
pour spécifier le certificat et la clé.
```

```
3. **Certificat généré**
   - Certificat : `/etc/ssl/localcerts/mydomaincert.pem`
   - Clé privée : `/etc/ssl/localcerts/mydomainkey.key`
```

```
4. **Résultats**
   - Apache fonctionne maintenant avec HTTPS, et le certificat SSL est
appliqué.

5. **Erreurs rencontrées et leur résolution**
   - Erreur : Le certificat est auto-signé, donc une alerte de sécurité
apparaît dans le navigateur.
   - Solution : Accepter l'alerte en toute sécurité, car vous avez généré le
certificat.
```

PARTIE B – FTPS :

1. Création du certificat pour ProFTPd

- **Création du répertoire pour stocker le certificat et la clé**

Créez un répertoire pour stocker les fichiers SSL pour ProFTPd.

```
  <code bash>
  mkdir /etc/proftpd/ssl/
```
```

```
  </code>
```

- **Génération du certificat SSL pour ProFTPd**

Utilisez la commande suivante pour générer un certificat SSL pour FTPS :

```
  <code bash>
  DIR=/etc/proftpd/ssl/
  openssl req -x509 -newkey rsa:4096 -nodes -keyout $DIR/mydomainkey.key -
out $DIR/mydomaincert.pem -days 365
  </code>
```

2. Configuration de FTPS

- **Édition du fichier de configuration de ProFTPd**

Modifiez le fichier `/etc/proftpd/proftpd.conf` pour activer FTPS en incluant la ligne suivante :

```
  ```
  Include /etc/proftpd/tls.conf
  ```
```

- **Configuration du fichier `/etc/proftpd/tls.conf`**

Ajoutez ou modifiez les directives suivantes dans `tls.conf` :

```
  ```
  TLSEngine on
  TLSLog /var/log/proftpd/tls.log
  TLSRSACertificateFile /etc/proftpd/ssl/mydomaincert.pem
  TLSRSACertificateKeyFile /etc/proftpd/ssl/mydomainkey.key
  TLSOptions NoCertRequest
  ```
```

3. Test de la connexion FTPS

- **Test via un client FTP**

Utilisez un client FTP comme FileZilla pour tester la connexion FTPS. Configurez-le pour utiliser TLS.

- **Résolution des erreurs**

Si vous rencontrez des erreurs, vérifiez les logs pour identifier les problèmes :

```
  <code bash>
  tail -f /var/log/proftpd/tls.log
  </code>
```

- **Vérification des permissions des fichiers**

Assurez-vous que les fichiers de certificat et de clé ont les bonnes permissions.

```
<code bash>
chmod 600 /etc/proftpd/ssl/*
</code>
```