**TP SSL/TLS**

Voici les étapes pour configurer un serveur web avec SSL/TLS pour offrir une connexion HTTPS sécurisée en utilisant des outils de chiffrement comme OpenSSL et en mettant en place des politiques de chiffrement appropriées :

**Installation d'un serveur web :**

Choisissez un serveur web comme Apache HTTP Server, Nginx ou Microsoft IIS.

Installez le serveur web sur votre système d'exploitation Linux.

**Activation du module SSL/TLS :**

Activez le module SSL/TLS dans la configuration du serveur web.

Pour Apache, vous pouvez activer le module SSL en utilisant la commande :

sudo a2enmod ssl

**Génération de clés privées et publiques :**

Utilisez OpenSSL pour générer une paire de clés privées et publiques.

Exécutez la commande suivante pour générer une clé privée :

*openssl genpkey -algorithm RSA -out server.key*

Puis, générez une demande de signature de certificat (CSR) avec la commande :

*openssl req -new -key server.key -out server.csr*

**Auto-signature d'un certificat (pour une utilisation interne) :**

Si vous n'utilisez pas de certificat signé par une autorité de certification (CA), vous pouvez auto-signer votre certificat.

Utilisez la commande suivante pour auto-signer le certificat :

*openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt*

**Configuration du serveur web :**

Configurez le serveur web pour utiliser le certificat SSL/TLS généré.

Pour Apache, vous pouvez ajouter les directives suivantes dans le fichier de configuration du site virtuel (par exemple /etc/apache2/sites-available/default-ssl.conf) :

*SSLEngine on*

*SSLCertificateFile /chemin/vers/server.crt*

*SSLCertificateKeyFile /chemin/vers/server.key*

**Mise en place de politiques de chiffrement :**

Définissez des politiques de chiffrement dans la configuration du serveur web pour garantir l'utilisation d'algorithmes sécurisés et de paramètres de sécurité appropriés.

Consultez les recommandations de sécurité et les bonnes pratiques pour choisir les meilleurs paramètres de chiffrement pour votre environnement.

**Redémarrage du serveur web :**

Une fois la configuration terminée, redémarrez le serveur web pour appliquer les changements :

*sudo systemctl restart apache2 # Pour Apache*