Etablissement : ENP d'Oran
Département : Génie des Systèmes
Module : Sécurité des systèmes d'information

TP_03 : Configuration SSL/TLS sous Lunix

Objectif de TP :

L'Objectif de TP est de configurer SSL/TLS pour une communication sécurisée client-serveur.

Pour réaliser le TP il suffit de suivre les étapes ci-dessous :

1. Générer une clé privée RSA : **openssl genrsa -out key.pem 2048** .
2. Créer une demande de signature de certificat (CSR) : **openssl req -new -key key.pem -out csr.pem**
3. Générer un certificat auto-signé : **openssl x509 -req -days 365 -in csr.pem -signkey key.pem -out cert.pem**
4. Copier la clé privée et le certificat auto-signé dans l'emplacement approprié sur votre serveur (par exemple, /etc/ssl/private/ et /etc/ssl/certs/) :
   sudo cp key.pem /etc/ssl/private/
   sudo cp cert.pem /etc/ssl/certs/
5. Installer un serveur web selon votre choix, pour Apache
   Installer le module SSL :
   sudo apt-get install apache2 openssl
   sudo a2enmod ssl
6. Configurer Apache pour utiliser SSL **:**
   sudo nano /etc/apache2/sites-available/default-ssl.conf
   Ajouter les lignes suivantes :
   SSLEngine on
   SSLCertificateFile /etc/ssl/certs/cert.pem
   SSLCertificateKeyFile /etc/ssl/private/key.pem
7. Activer la configuration SSL :
   sudo a2ensite default-ssl.conf
8. Redémarrer Apache pour appliquer les modifications : **sudo systemctl restart apache2**
9. Tester le fonctionnement de HTTPS par la connexion en localhost : **curl -Ik https://localhost -k**

F.Kabli