UNIVERSITÉ DE CARTHAGE
INSTITUT NATIONAL DES SCIENCES APPLIQUÉES ET DE TECHNOLOGIE

AU : 2019-2020
Section : GL4

Protocoles de sécurité

Date : ***Janvier 2020*** ***Openssl(3)*** **Responsable du cours : Yousfi Souheib**

Introduction

Ce TP a pour objectif d'instaurer une PKI. Cette Public Key Infrastructure est une organisation centralisée, gérant les certificats x509 afin d'instaurer la confiance dans les échanges de données et des clefs publiques et l'identification des différents participants. Commençons par interroger un site sécurisé qui s'appuie sur une couche SSL/TLS et vérifions son certificat :

— Afin de se connecter un serveur, nous devons avoir son hostname et son port, par exemple : "`www.laposte.tn:443`".

— Utiliser cette ligne de commande "`openssl s_client -connect www.laposte.tn:443`" pour avoir le certificat du site de laposte.tn.

— Copier le certificat qui est limité par –BEGIN CERTIFICATE– et –End CERTIFICATE– dans un fichier, puis essayer de le lire dans un format texte lisible par la commande openssl X509 vu dans le TP précédent. Donner l'autorité AC qui a signé le certificat de ce serveur, ainsi que toutes les autres informations.

— Le format pem est un type de format pour les certificats, c'est un certificat codé en ASCII (en Base 64). Il en existe trois principaux formats : DER, PKCS7 et PKCS12. Convertir le certificat .pem au format DER "`openssl x509 -outform der -in certificat.pem -out certificat.der`". Puis, lisez ce format en utilisant "`openssl x509 -in certificat.der -inform der -text`".

Après avoir fait le tour sur les différents formats des certificats, commençons par instaurer notre PKI.

1. Étape1 : Création du certificat de l'autorité de certification AC :

   (a) Générer la paire de clef de l'autorité : "`CLEF_AC`" (protéger toutes vos clefs par un pwd)

   (b) Á partir de "`CLEF_AC`", créer un certificat x509 pour une durée de validité de 10 ans : "`AC_cert`".

   (c) Le résultat obtenu est le certificat de l'autorité de certification qui va permettre de signer les certificats crées.

2. Étape2 : Création du certificat du serveur (dans notre cas de figure apache2)

(a) Générer la clef privée "`CLEF_apache`". Tâchez à donner un pwd à votre clef pour une éventuelle vérification de l'exactitude de votre manipulation lors du redémarrage du serveur.

(b) Générer une demande de signature de certificat (CSR Certificate Signing Request) de votre serveur. Vous pouvez identifier votre institut (INSAT) comme serveur.

(c) AC signe la demande de certificat du serveur, on obtient "`Apache_cert`".

3. Étape3 : Création du certificat du client

(a) Générer la clef privée "`CLEF_client`".

(b) Générer une demande de signature de certificat de votre client. Vous pouvez identifié votre filière GL4. Le common Name de cette demande est gl4.tn.

(c) AC signe la demande de certificat du client, on obtient "`client_cert`".

(d) Générer votre enveloppe pkcs12 de votre client "`client_pfx`". Donner un pwd différent de celui de la clef pour mieux comprendre les différentes étapes.

Le but de ce TP est de sécuriser l'accès à notre site www.gl4.tn.

1. Configuration de Apache :

(a) Installation de apache2 : apt-get install apache2

(b) Tester votre localhost

(c) En ajoutant à votre hosts, le Domain Name Server www.gl4.tn, tester votre site.

(d) Sous sites-available, éditer le fichier de configuration du port 80. Avec le ServerName est www.gl4.tn

(e) Activer SSL et default-ssl /*a2enmod et a2ensite*/

(f) Sur la configuration du port 443, modifier le chemin de la clef du serveur, le certificat du serveur ainsi que celui de l'autorité : SSLCertificateFile, SSLCertificatekeyFile et SSLCertificateChainFile.

(g) Redémarrer le service apache, vous serez amené à donner le pwd de votre serveur.

(h) Authentification ssl mutuelle :

i. Ajouter le certificat de l'AC : SSLCACertificateFile

ii. Décommenter SSLVerifyClient require et SSLVerifyDepth 1

2. Test d'accès :

   (a) Accéder à votre site en http et en https (apachectl pourrait être utilisé pour viser une éventuelle erreur)

3. Redirection :

   (a) Sur le fichier de configuration du port 80, on oblige le passage par le port 443.

   (b) RedirectMatch permanent ∧(.*)$ https ://www.gl4.tn$1

   (c) ou bien :
   RewriteEngine On

   RewriteCond %{SERVER_PORT} !∧443$

   RewriteRule ∧/(.*) https ://%{SERVER_NAME}/$1

   (d) Ou bien tout simplement :

   Redirect permanent / https ://www.gl4.tn

♣ S.Y. ♣
Bon travail