Securisation SSL d'un Serveur Web

Mise en place de SSL avec certificats auto-signés sur un serveur Apache2

ANATOLE BILLET

09 novembre 2015
Version 1.00

Securisation SSL d'un Serveur Web

Mise en place de SSL avec certificats auto-signés sur un serveur Apache2

Avant de commencer…

Objectif :

L'objectif principal du TP est la création d'une autorité de certification et création de certificats SSL. Le certificat SSL sera ensuite déployé sur un serveur Web Apache.

Prérequis :

-Debian 8.1

Code couleur :

-Bleu pour les commandes Debian

-Vert pour les noms des fichiers de configurations

-Italic pour les descriptions et anecdotes.

Table des matières

1. Installation et configuration de openSSL

Pour installer openSSL : **apt-get install openSSL** mais il également inclut dans le paquet d'apache2 que nous utiliserons pour ce tutoriel.

2. Générer le certificat

Dans le dossier **/etc/ssl** on créé un dossier pour notre domaine :

domaine=gsb.local

cd /etc/ssl

mkdir $domaine

cd $domaine

On crée la clé privée avec l'algorithme RSA 2048 bits.

openssl genrsa -out $domaine.key 2048

Ensuite il faut générer un fichier de « demande de signature de certificat », en anglais CSR

openssl req -new -key $domaine.key -out $domaine.csr

On répond à un certain nombre de questions.
Il faut bien mettre le nom (ou l'ip) du serveur tel qu'il est appelé de l'extérieur dans le champ « Common Name » (CN).

Ensuite, on génère le certificat signé au format x509 (ici pour 365jours auto-signé):

openssl x509 -req -days 365 -in $domaine.csr -signkey $domaine.key -out $domaine.crt

Ce certificat n'est authentifié par aucune autorité, vous aurez donc un message d'avertissement quand vous vous connectez au serveur.
C'est le fichier **gsb.local.crt** qu'on ajoute au besoin dans les navigateurs internet pour ne pas accepter le certificat à chaque fois.

Ou au lieu d'auto-signer le certificat on peut envoyer le fichier CSR à une autorité de certification reconnue.

3. Éditer le "virtualhost" SSL dans apache

Exemple ici sur Gentoo, mais le fichier de configuration peut se trouver dans un autre fichier, comme **/etc/httpd/conf.d/ssl.conf** pour CentOS :

Code BASH :

nano /etc/apache2/vhosts.d/00_default_ssl_vhost.conf

Éditer les lignes :

ServerName linuxtricks.fr

SSLCertificateFile /etc/ssl/linuxtricks.fr/linuxtricks.fr.crt

SSLCertificateKeyFile /etc/ssl/linuxtricks.fr/linuxtricks.fr.key