Aller au contenu

**AP#2 SISR – Atelier 7: Chiffrement des communications HTTP et FTP avec SSL / TLS**

installation de opensssl sur le serveur : **apt-get install openssl**
Puis créer un dossier pour les certificat : **mkdir /etc/ssl/localcerts**

Création du clé ssl :
**openssl req -x509 -newkey rsa:4096 -nodes -keyout $DIR/m2lkey.key -out $DIR/m2lcert.pem -days 365** Penser a adapter le nom de domaine ici le domaine m2l.org est utilisé

-newkey rsa:4096 Clé RSA de 4096 bits
-keyout : la clef
-out : le certificat
-nodes : pas de phrase de passe lors de l'utilisation pour déverrouiller (no DES)
-days 365 : Correspondant a ma durée de validité du certificat

Pour supprimer les clé aller dans **cd /etc/ssl/localcerts** et supprimer les clées .pem et .key

Dans **nano /etc/apache2/sites-available/default-ssl.conf** mettre les bon chemins pour les clés :

```
SSLCertificateFile /etc/ssl/localcerts/m2l.pem
SSLCertificateKeyFile /etc/ssl/localcerts/m2l.key
```

Refaire les vhost pour chaque site et y ajoute dedans les chemins des clés :
exemple :

```
<VirtualHost *:80>
DocumentRoot /home/htdocs/m2l.org/intranet/
ServerName intranet.m2l.org
ServerAlias intranet

# Autres directives ici
<Directory /home/htdocs/m2l.org/intranet/>
Require all granted
# Déclaration des options de sécurité du répertoire
# Les fichiers d'authentification .htaccess s'ils existent
# remplacent les droits du dossier
AllowOverride All
</Directory>
#Fichier de log
ErrorLog /var/log/apache2/intranet-error.log
CustomLog /var/log/apache2/intranet-access.log combined


ServerAdmin webmaster@m2l.org
</VirtualHost>


<VirtualHost *:443>
DocumentRoot /home/htdocs/m2l.org/intranet/
ServerName intranet.m2l.org
ServerAlias intranet

# Autres directives ici
<Directory /home/htdocs/m2l.org/intranet/>
Require all granted
# Déclaration des options de sécurité du répertoire
# Les fichiers d'authentification .htaccess s'ils existent
# remplacent les droits du dossier
AllowOverride All
</Directory>
#Fichier de log
ErrorLog /var/log/apache2/intranet-error.log
CustomLog /var/log/apache2/intranet-access.log combined
#clé ssl
SSLCertificateFile /etc/ssl/localcerts/m2lcert.pem

```

```
42
43  ServerAdmin webmaster@m2l.org
44  </VirtualHost>
```

**PARTIE B – FTPS**

Création du répertoire pour stocker les clées :
mkdir /etc/proftpd/ssl/

Création du certificat SSL auto-signé et de la clé :
**DIR=/etc/proftpd/ssl/**
**openssl req -x509 -newkey rsa:4096 -nodes -keyout $DIR/mydomainkey.key -out $DIR/mydomaincert.pem -days 365**

-newkey rsa:4096 : Pour une clé RSA de 4096 bits
-keyout : La clef
-out : Le certificat
-nodes : Pas de phrase de passe lors de l'utilisation pour le déverrouiller (no DES)
-days 365 : Correspondant à la durée de validité du certificat

Décommenter la ligne qui est dans **nano /etc/proftpd/proftpd.conf**

```
1  # This is used for FTPS connections
2  #
3  Include /etc/proftpd/tls.conf
```

Pour permettre d'activer TLS pour ftp

Éditer le fichier /etc/proftpd/tls.conf et paramétrer au minimum les directives suivantes :
• TLSEngine (activer/désactiver TLS)
• TLSLog (logguer les connexions chiffrées dans un fichier à part)
• TLSRSACertificateFile (chemin vers le certificat)
• TLSRSACertificateKeyFile (chemin vers la clé)
• TLSOptions (voir http://www.proftpd.org/docs/contrib/mod_tls.html [http://www.proftpd.org/docs/contrib/mod_tls.html])

Faire cette commande dans le répertoire ou se situe la clé :
**Si besoin** Convertir sa clé m2lcert.pem en .crt avec la commande **openssl x509 -outform der -in m2lcert.pem -out m2lcert.crt**

Editer le fichier **nano /etc/proftpd/tls.conf** et décommenter :

```
1  TLSEngine   on     #moteur TLS activer
2  TLSLog      /var/log/proftpd/tls.log #sauvegarde log
3  TLSRSACertificateFile   /etc/proftpd/ssl/m2lcert.pem #location of certificat file
4  TLSRSACertificateKeyFile  /etc/proftpd/ssl/m2lkey.key #location of key file
```

Puis se connecter avec filezilla au serveur en spécifiant le port 21 :

```
Statut :    Connexion à 10.31.112.1:21...
Statut :    Connexion établie, attente du message d'accueil...
Statut :    Initialisation de TLS...
Statut :    Vérification du certificat...
Statut :    Connexion TLS établie.
Statut :    Le serveur ne supporte pas les caractères non-ASCII.
Statut :    Connecté
Statut :    Récupération du contenu du dossier...
Statut :    Contenu du dossier "/" affiché avec succès
```