TP: Sécurisation d'un serveur de fichier (FTPS)

N.B: ***Ce Tp a été testé sous ubuntu 14.04 LTS***

I. Outils utilisés:
- Machine ubuntu 14.04 LTS qui va jouer le rôle du client et du serveur.
- Installerz le serveur vsftpd, Filezilla, l'analyseur de trafic wireshark et l'outil de chiffrement openssl. **# sudo apt-get install vsftpd ssl filezilla wireshark**

II. Travail à faire

1) configuration du serveur vsftpd

La configuration se fait à travers le fichier /etc/vsftpd.conf

==> Configuration du service de téléchargement (Download).

- Pour autoriser la connexion par le compte anonymous : **anonymous_enable=YES**
- Pour autoriser la connexion par les utilisateurs non privilégiés du système et ne les autoriser que de travailler dans leur répertoire sous /home

local_enable=YES

chroot_local_user=YES

==> Configuration du service de dépôt (Upload) anonyme.

- Pour autoriser l'écriture dans les répertoires par défaut : **write_enable=YES**
- Pour autoriser le dépôt (Upload) par l'utilisateur anonymous : **anon_upload_enable=YES**
- Créer un répertoire sous /var/ftp réservé pour le Upload
- Lui assigner les permissions nécessaires pour qu'il soit accessible pour l'utilisateur anonymous
- A chaque modification des paramètres du service relancer vsftpd :

1) Test du serveur vsftpd non sécurisé

a. Lancer le serveur vsftpd: **# sudo service vsftpd start**
b. Créer un utilisateur "user1" et lui assigner le mot de passe "user1password" et le répertoire de connexion /home/user1 (commande adduser ou useradd).
c. Lancer wireshark et commencer la capture sur l'interface loopback
d. Se connecter au serveur vsftpd en utilisant la commande "ftp" (**#ftp localhost**). Analyser le trafic capturé par wireshark et localiser le login et le mot de passe.

2) FTPS (FTP Secure): mise en place de vsftpd sécurisé

L'objectif de cette activité est de sécuriser le trafic entre client Filezilla et le serveur vsftpd par le biais du protocole TLS (postérieur à SSLv3). On utilisera l'outil openssl pour générer essentiellement le certificat garantissant, auprès du client, l'authenticité de la clé publique du serveur.

Créer un certificat et une clé privée pour le serveur

sudo openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout /etc/ssl/private/ssl-cert-snakeoil.key -out /etc/ssl/certs/ssl-cert-snakeoil.pem

Ajouter sur vsftpd.conf

location of the RSA certificate to use for SSL encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

location of the RSA key to use for SSL encrypted connections.
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key

force SSL. This will restrict clients that can't deal with TLS
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES

configure the server to use TLS (more secure than SSL)

#explicitly allowing TLS and denying the use of SSL

ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

#If set to yes, all SSL data connections are required to exhibit SSL session reuse (which proves that they know the same master secret as the control channel). Although this is a secure default, it may break many FTP clients, so you may want to disable it
require_ssl_reuse=NO

#select which SSL ciphers vsftpd will allow for encrypted SSL connections
ssl_ciphers=HIGH

allow writeable chroot if **chroot_local_user** was set to **YES**
allow_writeable_chroot=YES

Lancer wireshark et commencer la capture sur l'interface loopback. Puis, à partir de filezilla, se connecter au serveur vsftpd sécurisé.
Analyser le trafic en identifiant :
- La Phase de connexion (Three way handshake)
- Les étapes d'établissement d'un tunnel TLS
- les algorithmes de chiffrement, signature et hashage utilisés
- Chiffrement des données.