FileZilla

Document d'exploitation

VINCIS Christophe BTS SIO SISR

Table des matières

1. Introduction

FTP signifie File Transfer Protocol. Il s'agit d'un protocole qui permet de transférer des fichiers d'un ordinateur à un serveur et vice versa. Vos fichiers trop lourds pour être envoyés par mail peuvent être envoyés par FTP par exemple.

Par défaut, FTP n'est pas sécurisé. Hors, nous avons besoin de sécuriser les transferts de fichiers pour qu'ils ne soient pas interceptés par des personnes malveillantes.

Il y a plusieurs manières de sécuriser FTP. Nous pouvons l'allier à SSH qui est un protocole de communication sécurisé, nous obtiendrons alors un SFTP pour SSH File Transfer Protocol. Nous pouvons également utiliser TLS pour Transport Layer Security qui est le successeur du protocole SSL - Secure Socket Layer. Il s'agit également d'un protocole de communication chiffrée. Le protocole alors obtenu est FTPS - File Transfer Protocol Secure. Il s'agit de la forme implicite. Pour la forme explicite nous avons FTPES - File Transfer Protocol Explicit Protocol.

Dans le cadre du projet pour l'entreprise M2L, nous avons décidé d'utiliser FTPES qui est plus simple à mettre en place que FTPS qui nécessite des configurations sur le pare-feu du poste client mais également sur le routeur fourni par le FAI.

2. Prérequis

Pour utiliser FTP, nous avons besoin de mettre en place un serveur FTP. Dans le cadre de notre projet, nous avons fait le choix d'utiliser un conteneur Debian 11. Un conteneur est un environnement qui ressemble à une Machine Virtuelle mais qui est plus léger, dû au fait qu'il utilise le même noyau que la machine hôte. De plus, il ne possède pas d'interface graphique. Tout se passe en ligne de commande dans un terminal.

Plusieurs choix de serveurs FTP s'offrent à nous, tels que les logiciels ProFTPD et VsFTPD. Nous avons choisi d'utiliser ce dernier.

Le serveur FTP passe son temps à attendre les requêtes de connexion des clients FTP, et les acceptent ou non en fonction des configurations mises en place.

Nous avons donc également besoin de télécharger un client FTP qui sera ici, le logiciel FileZilla.

3. Installation

Une fois le conteneur Debian créé, nous devons télécharger les mises à jour disponibles pour le système d'exploitation préalablement installé ainsi que les programmes déjà contenus par celui-ci.

Pour se faire, si vous êtes sur une machine virtuelle, ouvrez un terminal en utilisant les touches CTRL + ALT + T en même temps. Si vous êtes dans un conteneur, vous n'avez pas d'interface graphique et êtes donc directement sur le terminal.

Entrez la commande suivante pour mettre à jour les fichiers disponibles dans les dépôts APT présent dans le fichier de configuration /etc/apt/sources.list. Il est recommandé de les exécuter régulièrement pour tenir à jour la liste des paquets disponibles.

```
root@Grp1-Debian-FTPS:~# apt update
```

Ensuite tapez :

```
root@Zabbix : ~ #   apt   upgrade
```

Cela met à jour les paquets déjà installés sans en supprimer et installe de nouveaux paquets si nécessaire.

Ensuite nous installons VsFTPD :

```
root@Grp-1-Debian-Ftps:~#  apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
```

Puis OpenSSL qui nous permettra de sécuriser FTP :

```
root@Grp-1-Debian-Ftps:~# apt-get install openssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Nous nous déplaçons dans le dossier /etc/

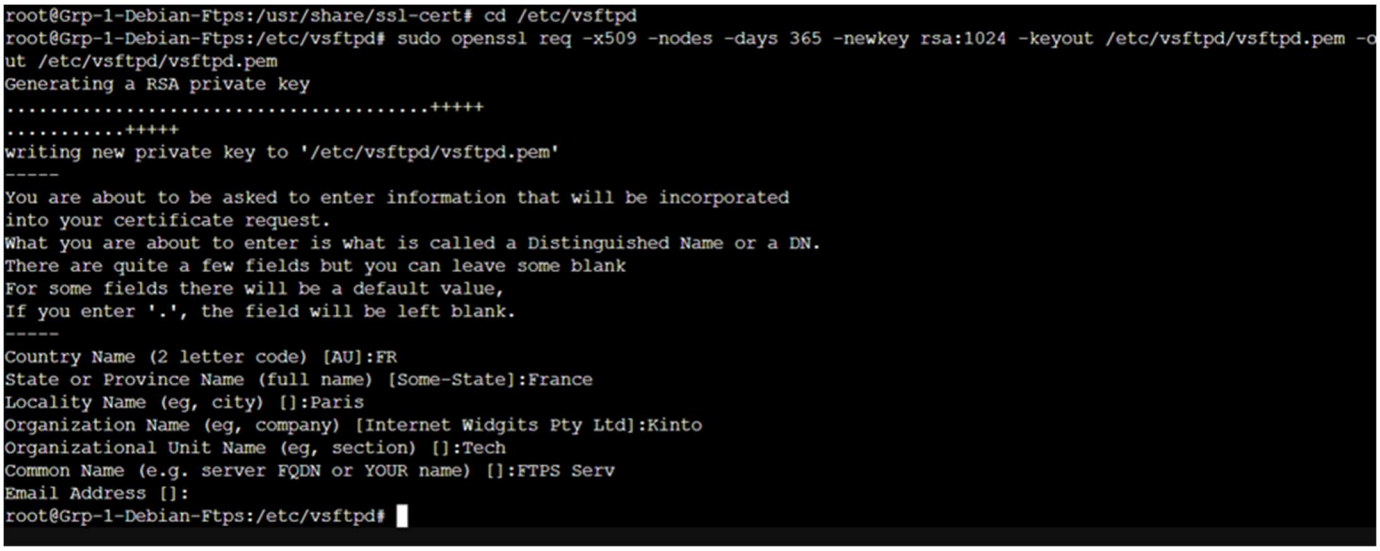
```
root@Grp1-Debian-FTPS:~# cd /etc/
```

Nous créons un dossier “vsftpd” qui accueillera les clés de certificats d’openssl :

```
root@Grp-1-Debian-Ftps:/etc# mkdir vsftpd
```

Déplaçons-nous dans le fichier nouvellement créé. Nous devons générer le fichier de certificat SSL et le fichier de la clé RSA. Ceux-ci vont nous permettre de chiffrer la communication entre l’ordinateur et le serveur, ainsi que les données lors de celles-ci. Cela rend donc la communication sécurisée.

La commande “***/usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout vsftpd.pem -out vsftpd.pem***” demande à openssl de générer le certificat ssl de la norme x509, valable pendant une durée de 365 jours, ainsi que la clé rsa d’une longueur de 1024 bits et de les placer dans /etc/vsftpd/ dans le fichier vsftpd.pem.



4. Configuration

Maintenant que nous avons installé vsftpd, openssl, généré le certificat SSL et la clé RSA, nous pouvons passer à la configuration du serveur.

Retournons dans /etc/

```
root@Grp1-Debian-FTPS:~# cd /etc/
```

Puis nous ouvrons le fichier vsftpd.conf pour accéder à sa configuration

```
root@Grp-1-Debian-Ftps:/etc# nano vsftpd.conf
```

Nous modifions les paramètres suivants, si ceux-ci sont commentés avec un “#” le désactivant, enlevez-le :

Autorisons l’écoute des adresses IPv4 :

```
# daemon started from an initscript.
listen=YES
```

Et nous désactivons celle des adresses en IPv6 :

```
listen_ipv6=NO
```

Nous empêchons ensuite les connexions FTP de personnes anonymes et autorisons les comptes locaux créés sur le serveur de se connecter ainsi que de leur permettre d’écrire dedans.

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

Nous indiquons ensuite au serveur où trouver le certificat et clé RSA. Et nous activons et forçons la communication en ssl. Nous autorisons

également les trois versions de ssl ainsi que la première de TLS. Et pour finir nous activons une sécurité élevée grâce à la suite de cryptographie qui combine les algorithmes de chiffrement par bloc, d'échange de clé, d'authentification ainsi que la génération du code d'authentification de message (mac).

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_sslv2=YES
ssl_sslv3=YES
ssl_tlsv1=YES
ssl_ciphers=HIGH
```

Ensuite, nous devons restreindre les accès de l'utilisateur FTP pour éviter qu'il n'accède à des dossiers qui ne lui sont pas autorisés. Le but étant de l'empêcher de faire des modifications sur des fichiers systèmes par inadvertance ou encore d'accéder à des données qui ne lui sont pas destinées. Cela empêchera également tout attaquant ayant piraté le compte de l'utilisateur FTP d'en faire de même.

Nous allons donc cantonner l'utilisateur local à un dossier spécifique c'est-à-dire dans le dossier /home/$USER/FTP :

```
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
user_sub_token=$USER
local_root=/home/$USER/FTP
```

Nous ajoutons ensuite le userlist_enable. Celui-ci permettra d'activer la liste des utilisateurs autorisés à se connecter au serveur par le biais de FTP.

Nous ajoutons également userlist_file et userlist_deny. Le premier définit où se trouve la liste des utilisateurs autorisés à se connecter. Le second, lorsqu'il est définie sur "NO" autorise les utilisateurs indiqués dans la liste, à l'inverse, s'il est définie sur "YES", les utilisateurs inscrits sont refusés.

```
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

Nous activons par la suite le suivi des téléchargements dans le fichier de logs. Un fichier de log est un fichier qui relate tous les évènements qui se sont déroulés. Cela permet d'avoir une trace et de savoir donc ici qui à fait des téléchargements, du serveur à l'ordinateur et vice versa.

```
# Activate logging of uploads/downloads.
xferlog_enable=YES
```

Indiquons ensuite au serveur dans quel fichier enregistrer les logs

```
# below.
xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
```

Maintenant que nous avons terminé, nous enregistrons les modifications en faisant CTRL + O, puis quittons le fichier en faisant CTRL + X.

Nous devons redémarrer vsftpd suite aux modifications dans sa configuration :

```
root@Grp-1-Debian-Ftps:~# service vsftpd restart
```

Vérifions ensuite l'état du service grâce à systemctl. Il s'agit de l'outil de gestion essentiel pour contrôler le système, pour modifier le statut des services, comme démarrer, arrêter ou redémarrer des services ou encore modifier la configuration d'un service.

Si nous n'avons pas fait d'erreur le service devrait être noté comme activé.

```
root@Grp1-Debian-FTPS:/etc# systemctl status vsftpd.service
* vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset:>
     Active: active (running) since Wed 2022-02-02 11:20:24 UTC; 5s ago
    Process: 23520 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited>
   Main PID: 23521 (vsftpd)
      Tasks: 1 (limit: 43320)
     Memory: 876.0K
        CPU: 9ms
     CGroup: /system.slice/vsftpd.service
             `-23521 /usr/sbin/vsftpd /etc/vsftpd.conf

Feb 02 11:20:24 Grp1-Debian-FTPS systemd[1]: Starting vsftpd FTP server...
Feb 02 11:20:24 Grp1-Debian-FTPS systemd[1]: Started vsftpd FTP server.
```

Or, notre service était indiqué comme failed, avec comme indication code=exited, status 2.

Cela peut correspondre à plusieurs problèmes. Après maintes recherches et un petit passage dans le fichier /usr/sbin/ dans lequel nous avons lancé le fichier vsftpd avec la commande :

```
root@Grp1-Debian-FTPS:~# cd /usr/sbin/
root@Grp1-Debian-FTPS:/usr/sbin# ./vsftpd
```

qui nous a indiqué une erreur dans le fichier de configuration. Nous nous sommes aperçus que dans le fichier en question, un des paramètres apparaissait à deux reprises, ce que le serveur ne sait pas gérer. Nous avons donc supprimé une fois le paramètre mais le service ne démarrait toujours pas.

Finalement, après régénération du certificat ssl et de la clé rsa, le serveur apparaissait comme activé.

Le serveur FTP est presque fonctionnel. Nous avons besoin de créer un utilisateur qui sera le seul à pouvoir utiliser FTP.

Nous allons donc créer un utilisateur avec la commande suivante.

```
root@Grp1-Debian-FTPS:~# adduser user
```

Il faut maintenant définir son mot de passe :

```
root@Grp1-Debian-FTPS:~# passwd user
```

Créons maintenant le dossier FTP auquel le compte user sera cantonné :

```
root@Grp1-Debian-FTPS:/# mkdir /home/user/FTP
```

Définissons le propriétaire du fichier :

```
root@Grp1-Debian-FTPS:/# chown user:sftp_user /home/user/FTP
```

Et ajoutons le compte user dans la liste d'autorisation de connexion :

```
root@Grp1-Debian-FTPS:/etc# echo "user" | tee -a /etc/vsftpd.userlist
user
```

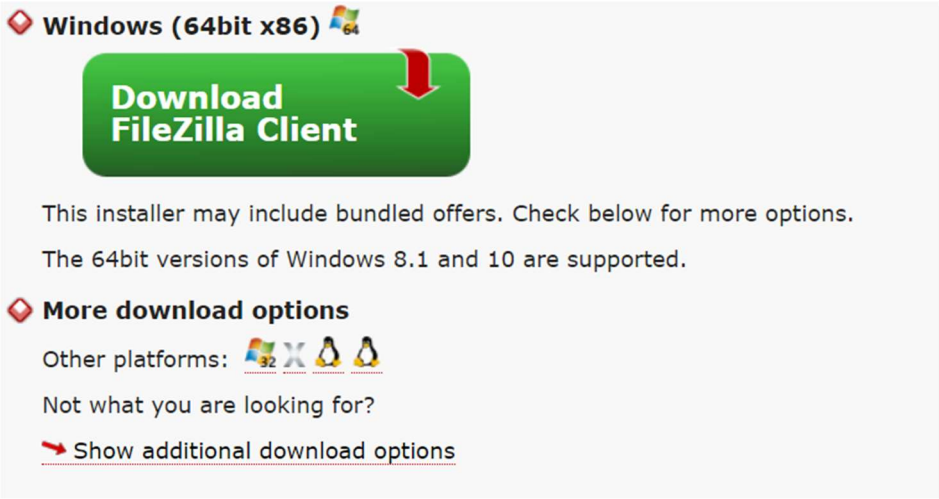
Redémarrons à nouveau le service vsftpd puis vérifions à nouveau son état mais comme nous n'avons rien modifié dans le fichier de configuration, le service doit bien être activé.

5. FileZilla

FileZilla est un client FTP. Ce logiciel permet de se connecter à un serveur distant et de télécharger des fichiers à partir et sur ce serveur. Celui-ci est gratuit.

Nous nous sommes rendus sur le site https://filezilla-project.org/. Deux choix s'offraient à nous, FileZilla Client et FileZilla Serveur. Nous avons sélectionnés FileZilla Client :

Puis avons choisi la version qui correspondait à notre système d'exploitation, c'est-à-dire celle étant compatible avec Windows 10.



Maintenant que FileZilla est installé, lançons le puis configurons le pour pouvoir se connecter au serveur.

Dans Hôte, indiquons l'adresse ip du serveur précédé de l'indicatif "ftpes".

Puis nous entrons le nom du compte local autorisé à se connecter au serveur, son mot de passe et le numéro de port.

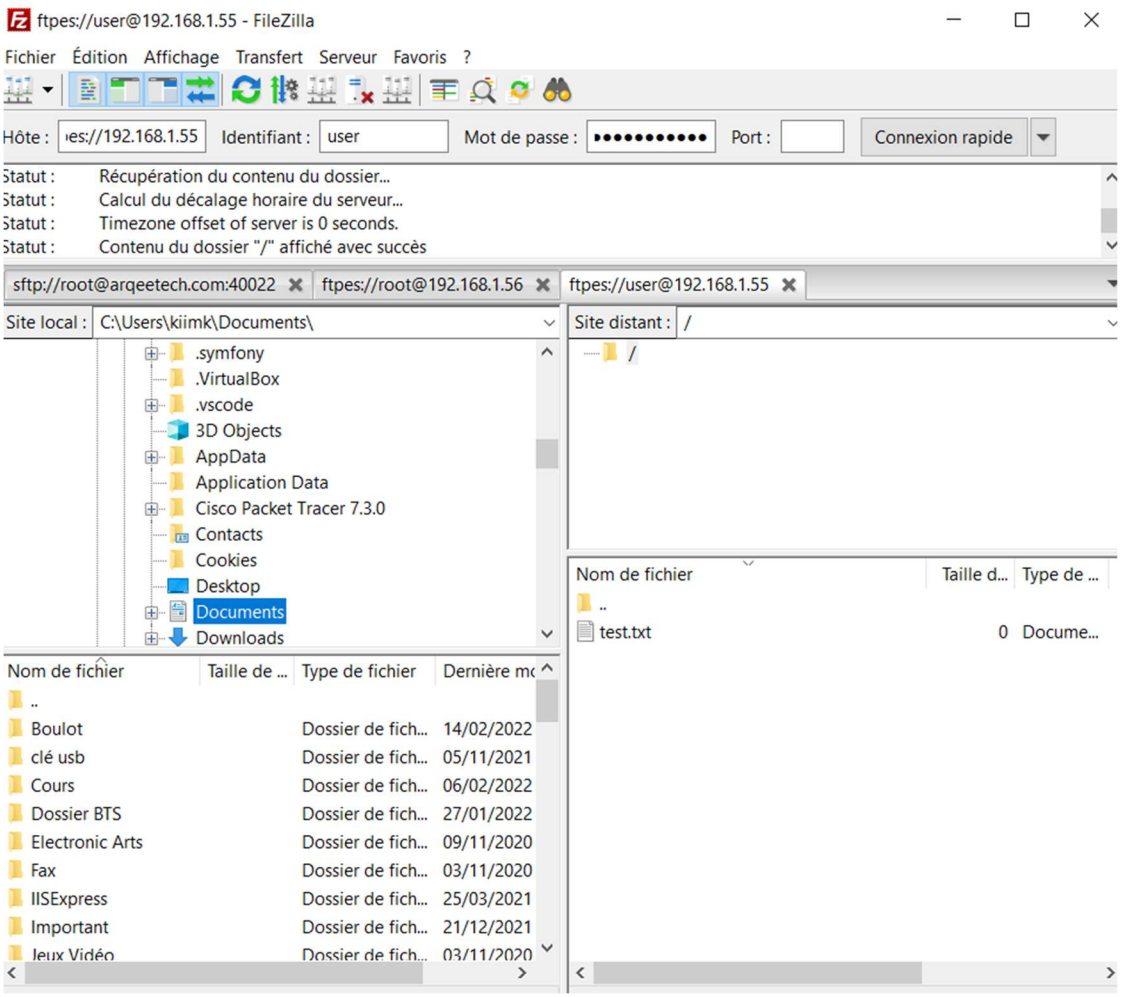
Par défaut, FTP se connecte sur le port 20, FTPS les ports 989 et 990 FTPES sur le port 21 et SFTP sur le port 22.

Une fois la connexion lancée, une demande de vérification du certificat apparaît :

Une fois validé, la connexion se termine, et nous pouvons créer des dossiers et importer des fichiers.

Le site local correspond à l'arborescence des documents contenus sur le disque de l'ordinateur, tandis que le site distant correspond à l'arborescence des documents du serveur FTP.

L'utilisateur étant restreint au dossier FTP, il n'en voit que le contenu. Le nom n'apparaît pas, on ne voit que le "/" qui signifie qu'il est à la racine du dossier.



Le serveur et le client FTP sont désormais en place et prêt à l'emploi.