Serveur FTP : Very secure FTP daemon

I Présentation

VsFTPd est un serveur conçu avec la problématique d'une sécurité maximale. Contrairement aux autres serveurs (ProFTPd, PureFTPd, etc.), aucune faille majeure de sécurité n'a jamais été décelée dans VsFTPd.

Néanmoins deux failles permettent un DoS avaient été détectées, la première était due à une faille d'un vieux noyau linux (avant 2.6.35), et la deuxième à été très vite corrigée.

Ce serveur est notamment utilisé à grande échelle par des entreprises telles que Red Hat.

La configuration *par défaut* de VsFTPd est très restrictive :

1. Seul le compte anonyme est autorisé à se connecter au serveur ;
2. En lecture seule ;
3. Les utilisateurs ne peuvent pas accéder à leurs répertoires.

Remarque :

Aussi sécurisé que soit un serveur ftp, le protocole ftp en lui même **n'est pas sûr** ! En effet l'échange du nom d'utilisateur et du mot de passe transite en clair sur le réseau. Si vous utilisez ce serveur sur votre réseau, pas de souci, mais attention si vous comptez utiliser le serveur ftp depuis internet, il peut être piraté. De fait n'utilisez pas un compte qui a les droits sudo via ftp (en fait n'utilisez de l'extérieur ce compte QUE via ssh ou tout autre protocole sécurisé, POPs, etc.).

II Installation et configuration de base

Installez le paquet vsftpd en ligne de commande :

```
root@debian1:~# apt-get install vsftpd
```

Il est parfois nécessaire de créer un compte ftp, l'absence de l'option *system* crée une faille de sécurité et bloque la désinstallation du paquet.

```
root@debian1:~# useradd --system ftp
```

La configuration de VsFTPd est centralisée dans un seul et même fichier « **/etc/vsftpd.conf** ». Choisissez votre éditeur de texte favori (en mode super utilisateur) et appliquez les modifications en fonction du mode de fonctionnement de VsFTPd.

Remarque : tout ce qui commence par '#' sera considéré comme commentaire et ne sera pas appliqué.

Vous pouvez personnaliser le texte de connexion au serveur en modifiant la ligne « ftpd_banner » dans le fichier « **/etc/vsftpd.conf** ».

Exemple :

```
ftpd_banner=Bienvenue sur le serveur ftp de LUCAS
```

Attention : Il ne faut pas oublier de redémarrer le service lorsque l'on modifie le fichier de configuration pour que les nouveaux paramètres puissent être mis en place :

```
root@debian1:~# systemctl restart vsftpd
```

Il faut ensuite vérifier qu'aucune erreur n'a été détectée :

```
root@debian1:~# systemctl status vsftpd
```

III Configuration de l'accès en anonyme

Vous pouvez permettre aux utilisateurs anonymes (login anonymous) de se connecter au serveur en **lecture seule** en modifiant ou ajoutant les lignes suivantes dans le fichier de configuration « **/etc/vsftpd.conf** » :

```
anonymous_enable=YES
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
```

```
anon_world_readable_only=YES
anon_root=/var/public
```

Ces lignes précisent :

- ✗ **anonymous_enable=YES** permet d'accepter les connexions anonymes.
- ✗ **anon_upload_enable=NO** indique que les upload sont interdits.
- ✗ **anon_mkdir_write_enable=NO** définit que les créations de répertoire sont interdites
- ✗ **anon_other_write_enable=NO** définit que les créations, suppressions, renommages de répertoire … sont interdits.
- ✗ **anon_world_readable_only=YES** définit qu'un utilisateur virtuel pourra télécharger un fichier même s'il n'est pas world readable
- ✗ **anon_root=/var/public** précise que le répertoire /var/public est celui sur lequel le compte anonymous pourra lire des fichiers.

Pour cela, il faut le créer si ce n'est pas le cas et la configuration du répertoire peut être la suivante :

- ✗ Propriétaire et groupe propriétaire : root
- ✗ Droits d'accès 755 (rwxr-xr-x).

Exemple :

```
root@debian1:~# mkdir /var/public
root@debian1:~# chown -R root /var/public
root@debian1:~# chmod 755 /var/public
```

Remarque : Si vous voulez que le mot de passe ne soit pas demandé, vous devez ajouter la ligne suivante :

```
no_anon_password=YES
```

IV Test du compte anonymous

Pour vérifier votre serveur FTP, vous devez le tester grâce à la commande ftp ou à un logiciel client ftp comme FileZilla à partir d'un poste distant.

1. Par exemple, il faut copier des fichiers dans le répertoire indiqué dans la ligne « anon_root ». Vous pouvez copier des fichiers sous Linux en étant root ou bien à distance en utilisant la commande pscp.
2. Il faut lancer ftp et donner comme nom anonymous et sans mot de passe puis vérifier qu'il est possible de lister les fichiers présents et de copier en local un fichier.

Exemple : connexion en anonymous sans mot de passe : la lecture (get) est autorisée mais pas l'écriture (put)

```
C:\Users\Barbara>ftp 192.168.0.112
Connecté à 192.168.0.112.
220 (vsFTPd 3.0.2)
Utilisateur (192.168.0.112:(none)) : anonymous
331 Please specify the password.
Mot de passe :
230 Login successful.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 111      0              28 Oct 06 13:18 essaiFTP.txt
226 Directory send OK.
ftp : 70 octets reçus en 0,00 secondes à 70000,00 Ko/s.
ftp> get essaiFTP.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for essaiFTP.txt (28 bytes).
226 Transfer complete.
ftp : 28 octets reçus en 0,03 secondes à 0,90 Ko/s.
```

```
ftp> put essaiFTP.txt
200 PORT command successful. Consider using PASV.
550 Permission denied.
ftp> quit
221 Goodbye.
```

Remarque : vous n'avez pas le droit d'écrire sur le serveur FTP si vous êtes connecté en tant qu'anonyme.

V Configuration des comptes utilisateur

Vous pouvez permettre à vos utilisateurs locaux (ceux qui ont un compte sur la machine) de se connecter au serveur. Il faut bien sûr créer les utilisateurs grâce à la commande useradd et si nécessaire le groupe grâce à la commande groupadd.

Exemple : création du compte « bmaheux » appartenant au groupe professeurs avec création du répertoire « /home/bmaheux » et utilisation du shell « /bin/bash »

```
root@debian1:~# groupadd professeurs
root@debian1:~# useradd  -g professeurs -m  -s  /bin/bash  bmaheux
```

Pour permettre aux utilisateurs autre que anonymous d'accéder au serveur FTP, il faut ajouter les lignes suivantes dans le fichier de configuration « **/etc/vsftpd.conf** » :

```
local_enable=YES
write_enable=YES
local_umask=022
```

La ligne local_enable=YES indique que les utilisateurs locaux sont autorisés. write_enable=YES indique que les écritures sont autorisées et local_umask= 022 indique que les fichiers créés le seront avec les droits 644, c'est-à-dire lecture/écriture pour le propriétaire, lecture seule pour le groupe et les autres.

Vous pouvez « emprisonner » certains utilisateurs dans leur dossier personnel afin qu'il ne puissent pas naviguer dans le système de fichier, il faut :

1. Créer un répertoire dédié à la configuration de vsftpd :

```
root@debian1:~# mkdir /etc/vsftpd
```

2. Mettre dans ce répertoire le fichier liste « chroot.list » qui renseigne les identifiants des utilisateurs concernés dans « **/etc/vsftpd/chroot.list** » sous la forme d'une simple liste:

```
root@debian1:~# nano /etc/vsftpd/chroot.list

utilisateur_1
utilisateur_2
…
```

Exemple : contenu du fichier chroot.list

```
bmaheux
mmadani
```

3. Modifier la configuration générale (**/etc/vsftpd.conf**) en ajoutant ou modifiant ces lignes :

```
chroot_local_user=NO
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot.list
user_config_dir=/etc/vsftpd/users/
allow_writeable_chroot=YES
```

La ligne local_root définit le chemin pour tous les utilisateurs autres que ceux définis.

4. Créer le répertoire « **/etc/vsftpd/users/** »
5. Créer dans ce répertoire, un fichier par utilisateur ayant pour nom celui de l'utilisateur et contenant le chemin du répertoire.

Exemple : contenu du fichier /etc/vsftp/users/bmaheux

```
local_root=/home/bmaheux
```

VI Test du serveur FTP

Pour vérifier votre serveur FTP, vous devez le tester grâce à la commande ftp ou à un logiciel client ftp comme FileZilla à partir d'un poste distant.

Dans ce cas, il faut entrer le login et le mot de passe du compte.

Attention : le port doit être égal à **21** !

Vous devez pouvoir lister les fichiers, lire ou écrire des fichiers dans le répertoire de l'utilisateur du compte d'une part et ne pas aller dans d'autres répertoires.

Exemple :