Administration Linux - FTP

Sommaire

*Un compte-rendu au format texte (**UTF-8**) devra être rédigé et envoyé à l'adresse*
tvaira@free.fr
La convention de nommage pour les compte-rendus est la suivante :
admin-linux-ftp-nom.txt

Mise en situation

Vous devez disposer d'un PC possédant un système d'exploitation Linux ou Windows et du logiciel de virtualisation *VirtualBox*. Le système invité sera une installation du **serveur Ubuntu 12.10**.

FTP (*File Transfer Protocol*)

Le protocole de transfert de fichiers FTP (*File Transfer Protocol*) permet l'échange informatique de fichiers sur un réseau TCP/IP : déposer des fichiers et/ou en récupérer.

FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. Par convention, deux ports sont attribués (*well known ports*) pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données.

Le protocole FTP est un des premiers protocoles de l'Internet : il est issu de la RFC 1142 créée le 16 avril 1971. Cette spécification fut remplacée par la RFC 7653 en juin 1980. Elle fut elle-même rendue obsolète par la RFC 9594 en octobre 1985, version finale de la spécification. Il a servi à diffuser des fichiers avant même l'invention du Web (la RFC 1945 décrivant le protocole HTTP/1.0 date de 1996 mais le protocole existait depuis 1990).

De nombreux serveurs FTP sont disponibles sous Linux (`ftpd`, `proftpd`, `wu-ftpd`, `pure-ftpd`, ...).

vsFTPd

Introduction

`vsFTPd` (*Very Secure FTP Daemon*), créé en 2000, est un serveur FTP qui mise beaucoup sur la sécurité, ce qui n'a rien d'étonnant puisqu'il est développé par Chris Evans chargé de la sécurité de *Google Chrome*. Il est distribué selon les termes de la licence Licence publique générale GNU.

Site officiel : https ://security.appspot.com/vsftpd.html

Installation

Il suffit d'installer le paquet `vsftpd` :

```
# apt-get install vsftpd
...

# service vsftpd status
vsftpd start/running, process 1805

// Recherche du fichier de configuration de vsftpd
# find /etc -name "vsftpd.conf"
/etc/vsftpd.conf
/etc/init/vsftpd.conf
```

L'installation du paquet entraîne la création d'un utilisateur système `ftp`. Ce compte est systématiquement employé pour gérer les connexions FTP anonymes, et son répertoire personnel (`/srv/ftp/`) est la racine de l'arborescence mise à disposition des utilisateurs se connectant sur le service.


```
# cat /etc/passwd | grep ftp
ftp:x:107:115:ftp daemon,,,:/srv/ftp:/bin/false

# cat /etc/group | grep ftp
ftp:x:115:

# ls -l /srv/ | grep ftp
drwxr-xr-x 2 root ftp 4096 mars 25 07:47 ftp/
```

Configuration

La configuration de vsFTPd est réalisée à partir du fichier "vsftpd.conf".

```
// Recherche du fichier de configuration de vsftpd

# find /etc -name "vsftpd.conf"
/etc/vsftpd.conf
/etc/init/vsftpd.conf
```

Le fichier vsftpd.conf propose un grand nombre d'options dont les plus importantes sont :

- listen : permet de définir si le démon est en *standalone* (YES) ou dirigé par (x)inetd (NO)
- anonymous_enable : permet d'accepter les connexions anonymes
- local_enable : oblige les personnes à s'identifier avec un compte utilisateur
- write_enable : donne la permission d'écriture
- xferlog_file : écriture d'un log des fichiers
- ftpd_banner : bannière d'affichage à la connexion FTP
- chroot_local_user : permet de "chrooter" la connexion de l'utilisateur

La documentation en ligne : https ://security.appspot.com/vsftpd/vsftpd_conf.html

chroot (*change root*) est une commande UNIX/Linux permettant de changer le répertoire racine d'un processus de la machine hôte. Cette commande permet d'isoler l'exécution d'un programme et d'éviter ainsi la compromission complète d'un système lors de l'exploitation d'une faille. Si un pirate utilise une faille présente sur l'application chrootée, il n'aura accès qu'à l'environnement isolé et non pas à l'ensemble du système d'exploitation. Cela permet donc de limiter les dégâts qu'il pourrait causer.

La configuration par défaut de vsFTPd est très restrictive :
- Le compte anonyme n'est pas autorisé à se connecter au serveur (anonymous_enable=NO)
- Les utilisateurs ne peuvent accéder qu'à leur compte, et en lecture seule (local_enable=YES)

```
# cat /etc/vsftpd.conf | grep -e "^\(listen\|anonymous\|local\|write\|chroot\)"
listen=YES
anonymous_enable=NO
local_enable=YES
```

Tests

On peut utiliser le client `ftp` en ligne de commande :

```
# ftp 192.168.52.9
Connected to 192.168.52.9.
220 (vsFTPd 2.3.5)
Name (192.168.52.9:tv): tv
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated. Commands are:
...
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
...
ftp> bye
221 Goodbye.
```

On peut aussi utiliser un client graphique comme FileZilla :

```
Statut :      Connexion à 192.168.52.9:21...
Statut :      Connexion établie, attente du message d'accueil...
Réponse :     220 (vsFTPd 2.3.5)
Commande :    USER tv
Réponse :     331 Please specify the password.
Commande :    PASS ********
Réponse :     230 Login successful.
Commande :    SYST
Réponse :     215 UNIX Type: L8
Commande :    FEAT
Réponse :     211-Features:
Réponse :      EPRT
Réponse :      EPSV
Réponse :      MDTM
Réponse :      PASV
Réponse :      REST STREAM
Réponse :      SIZE
Réponse :      TVFS
Réponse :      UTF8
Réponse :     211 End
Commande :    OPTS UTF8 ON
Réponse :     200 Always in UTF8 mode.
Statut :      Connecté
Statut :      Récupération du contenu du dossier...
Commande :    PWD
Réponse :     257 "/home/tv"
Commande :    TYPE I
Réponse :     200 Switching to Binary mode.
Commande :    PASV
Réponse :     227 Entering Passive Mode (192,168,52,9,207,159).
Commande :    LIST
Réponse :     150 Here comes the directory listing.
Réponse :     226 Directory send OK.
...
```

On peut alors vérifier les restrictions d'accès :


```
// Envoi d'un fichier
Commande :    STOR test.txt
Réponse :     550 Permission denied.

// Création d'un répertoire
Commande :    MKD /home/tv/test
Réponse :     550 Permission denied.

// Renommage d'un fichier
Commande :    RNFR fichier.txt
Réponse :     550 Permission denied
```

Liste des commandes `ftp` : wikipedia.fr

Manipulations

Séquence 1 : serveur ftp anonyme et sécurisé

Question 1. Configurer le serveur `vsFTPd` (en mode *standalone*) afin qu'il n'accepte que les connexions anonymes chrootées et en lecture seule. Il vous faudra l'indiquer dans la bannière d'accueil. On journalisera l'activité du serveur dans le fichier `/var/log/vsftpd.log`.

Question 2. Créer un fichier de test téléchargeable anonymement (compte ftp) puis placez-le à la racine de votre serveur ftp.

Question 3. Tester.

On vérifie que les utilisateurs ne peuvent se connecter au serveur :

```
Commande :    USER tv
Réponse :     530 This FTP server is anonymous only.
```

On teste une connexion anonyme :

```
Statut :      Connexion à 192.168.52.9:21...
Statut :      Connexion établie, attente du message d'accueil...
Réponse :     220 Bienvenue sur le serveur FTP anonyme.
Commande :    USER anonymous
Réponse :     331 Please specify the password.
Commande :    PASS ********
Réponse :     230 Login successful.
Commande :    OPTS UTF8 ON
Réponse :     200 Always in UTF8 mode.
Statut :      Connecté
```

On télécharge (*download*) un fichier :

```
Statut :      Démarrage du téléchargement de /test.txt
Commande :    CWD /
Réponse :     250 Directory successfully changed.
Commande :    TYPE A
Réponse :     200 Switching to ASCII mode.
Commande :    PASV
Réponse :     227 Entering Passive Mode (192,168,52,9,46,37).
Commande :    RETR test.txt
Réponse :     150 Opening BINARY mode data connection for test.txt (0 bytes).
Réponse :     226 Transfer complete.
```


On tente l'envoi d'un fichier (*upload*) :

```
Statut :      Démarrage de l'envoi de /home/tv/Téléchargements/essai.txt
Commande :    CWD /
Réponse :     250 Directory successfully changed.
Commande :    TYPE A
Réponse :     200 Switching to ASCII mode.
Commande :    PASV
Réponse :     227 Entering Passive Mode (192,168,52,9,219,97).
Commande :    STOR essai.txt
Réponse :     550 Permission denied.
```

On consulte le journal (*log*) :

```
# cat /var/log/vsftpd.log
```

Séquence 2 : serveur ftp utilisateurs

La version 2.3.5 livrée en standard avec Ubuntu est boguée. L'utilisation du mode chrooté provoque une erreur : `500 OOPS: vsftpd: refusing to run with writable root inside chroot()`. L'utilisateur ne peut pas accéder à son répertoire personnel. Pour contourner ce bug, quelqu'un a réalisé un *backport* de l'option `allow_writeable_chroot` depuis vsftpd 3 en attendant que celle-ci soit présente dans les dépôts.

```
// vérification de la version installée

# vsftpd -v
vsftpd: version 2.3.5

# wget http://ppa.launchpad.net/thefrontiergroup/vsftpd/ubuntu/pool/main/v/vsftpd/vsftpd_2.3.5-1
    ubuntu2ppa1_amd64.deb

# dpkg --install vsftpd_2.3.5-1ubuntu2ppa1_amd64.deb
... Y
```

Maintenant, l'option `allow_writeable_chroot=YES` est utilisable dans `vsftpd.conf`.

Question 4. Configurer le serveur `vsFTPd` (en mode *standalone*) afin qu'il n'accepte que les connexions d'utilisateurs authentifiés (chrootées) et en lecture/écriture. Il vous faudra l'indiquer dans la bannière d'accueil. On journalisera toujours l'activité du serveur dans le fichier `/var/log/vsftpd.log`.

Question 5. Réaliser les différents tests pour valider la configuration du serveur.

