Technicien Supérieur Gestionnaire
Exploitant de Ressources Informatiques
et Réseaux

How to get "Epic faill"

Not Very secure FTP

Unfollow this guide

O RLY?

Marchal Ludovic

Table des matières

VSFTP

Very Secure FTP

1. Presentation

Le FTP est un protocole de la couche application du modèle OSI

2. Installation

username@machine:~$sudo apt-get update

username@machine:~$sudo apt-get install vsftpd

```
username@SRV-ubuntu:~$ sudo apt-get install vsftpd
[sudo] password for xtbushido:
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés : vsftpd
0 mis à jour, 1 nouvellement installés, 0 à enlever et 6 non mis à
jour.
Il est nécessaire de prendre 111 ko dans les archives.
Après cette opération, 361 ko d'espace disque supplémentaires
seront utilisés.
Réception de : 1 http://fr.archive.ubuntu.com/ubuntu/ trusty-
updates/main vsftpd amd64 3.0.2-1ubuntu2.14.04.1 [111 kB]
111 ko réceptionnés en 0s (8 406 ko/s)
Préconfiguration des paquets...
Sélection du paquet vsftpd précédemment désélectionné.
(Lecture de la base de données... 86191 fichiers et répertoires
déjà installés.)
Préparation du décompactage de .../vsftpd_3.0.2-
1ubuntu2.14.04.1_amd64.deb ...
Décompactage de vsftpd (3.0.2-1ubuntu2.14.04.1) ...
Traitement déclenché pour  man-db (2.6.7.1-1ubuntu1) ...
Traitement déclenché pour  ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Paramétrage de vsftpd (3.0.2-1ubuntu2.14.04.1) ...
vsftpd start/running, process 2101
Traitement déclenché pour  ureadahead (0.100.0-16) …
```

3. configuration

Activer le partage de fichiers de manière anonyme ; en modifiant précisément la ligne 23, et en indiquant YES

Modifier le fichier /etc/vsftpd.conf

user@machine:~$ sudo vi /etc/vsftpd.conf

Allow anonymous FTP? (Disabled by default)

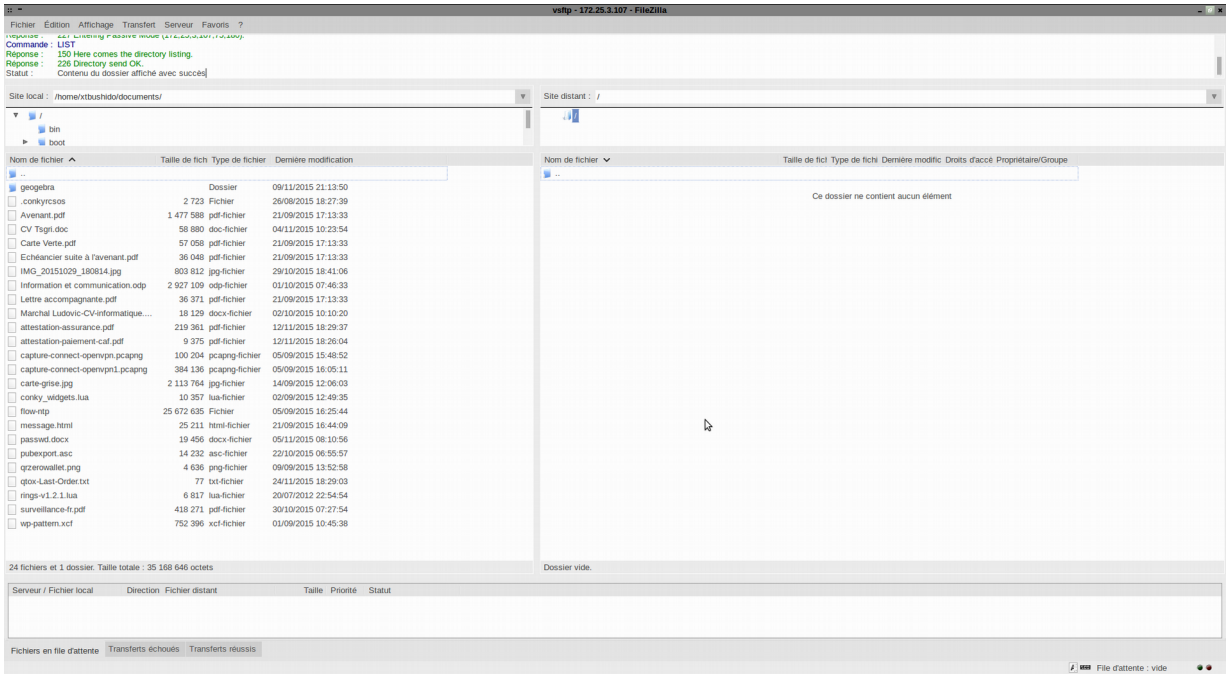
anonymous_enable=YES

Enregistrer puis relancer le service :

sudo service vsftpd restart

3.1. Test

On se connecte en anonymous sur le FTP avec FileZilla



3.2.Observation avec wireshark

Le protocole FTP fonctionne en mode « connecté », le client va donc contacter le serveur FTP pour initier une connexion.

J'ai constaté un dialogue de 14 échanges entre le client et le serveur, dont 3 pour :

TCP

2 0.692219000 172.25.3.23 172.25.3.107 TCP 74 58126→21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1914264 TSecr=0 WS=128

3 0.692378000 172.25.3.107 172.25.3.23 TCP 74 21→58126 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2959270 TSecr=1914264 WS=128

4 0.692402000 172.25.3.23 172.25.3.107 TCP 66 58126→21 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1914264 TSecr=2959270

Puis l'échange FTP commence avec une réponse du serveur,et nous allons nous concentrer dessus.

5 0.693854000 172.25.3.107 172.25.3.23 FTP 86 Response: 220 (vsFTPd 3.0.2).

7 0.733367000 172.25.3.23 172.25.3.107 FTP 82 Request: USER anonymous

9 0.733830000 172.25.3.107 172.25.3.23 FTP 100 Response: 331 Please

specify the password.

11	0.734166000	172.25.3.23	172.25.3.107	FTP	87	Request: PASS anon@localhost
12	0.740053000	172.25.3.107	172.25.3.23	FTP	89	Response: 230 Login successful.
13	0.740188000	172.25.3.23	172.25.3.107	FTP	80	Request: OPTS UTF8 ON
14	0.740406000	172.25.3.107	172.25.3.23	FTP	92	Response: 200 Always in UTF8 mode.
15	0.740871000	172.25.3.23	172.25.3.107	FTP	71	Request: PWD
16	0.741033000	172.25.3.107	172.25.3.23	FTP	75	Response: 257 "/"
17	0.779624000	172.25.3.23	172.25.3.107	TCP	66	58126→21 [ACK] Seq=57 Ack=113 Win=29312 Len=0 TSval=1914286 TSecr=2959282

3.3.Utilisateur local

Modifier à nouveau le fichier /etc/vsftp.conf:

sudo vi /etc/vstfpd.conf

```
# Allow anonymous FTP? (Disabled by default)                    Ligne 23
anonymous_enable=NO

# Uncomment this to allow local users to log in.                Ligne 26
local_enable=YES

# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
```

On enregistre puis on redémarre le service

```
username@SRV-ubuntu:~$ sudo service vsftpd restart
vsftpd stop/waiting
vsftpd start/running, process 2457
```

Avec cette configuration le couple ID-MdP est demandé, toutefois l'utilisateur à la possibilité de naviguer dans toute l'arborescence.

On constate qu'un loggin est demandé ; mais le mot-de-passe transite en clair.

Pour des raisons de sécurité, c'est 2 points ne sont pas souhaitable.

10	6.352057000	172.25.3.35	172.25.3.107	FTP	82	Request: USER username
12	6.352466000	172.25.3.107	172.25.3.35	FTP	100	Response: 331 Please specify the password.
13	6.354551000	172.25.3.35	172.25.3.107	FTP	83	Request: MdP-en-clair
17	6.368420000	172.25.3.35	172.25.3.107	FTP	71	Request: PWD
18	6.368559000	172.25.3.107	172.25.3.35	FTP	89	Response: 257 "/home/username"

a) Interdire l'écriture dans un autre user

Modifiez les paramètres suivant :

```
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
```

Ligne 120 à 123

```
# You may fully customise the login banner string:
ftpd_banner=Welcome to Read The Fucking Manual.
```

Ligne 100

```
## Local user ?
local_root=/home
```

Puis créer le fichier /etc/vsftpd.chroot_list

Et y ajouter les utilisateurs.

Sudo vi /etc/vsftpd.chroot_list

b) Utilisateur virtuel

Ajoutez et apportez les modifications nécessaire

```
guest-enable=YES
guest_username=ftpd
nopriv_user=ftp
virtual_use_local_privs=YES
user_sub_token=$USER
local_root=/ftp/$USER
hide_ids=YES
nopriv_user=ftpd
```

c) Ajouter l'utilisateur système

```
sudo useradd --home /ftp --shell /bin/false ftpd
```

d) Login utilisateur virtuel

Créer un fichier :

/etc/vsftpd_loggin.txt

Et y placer les « user »- « MdP »

Création des répertoires

sudo mkdir /srv/ftp/toto /srv/ftp/titi /srv/ftp/tata /srv/ftp/tete

Y mettre un fichier

sudo cp README.test /srv/ftp/tata

e) Base de données

Installation db

```
sudo apt-get install libdb4.8
```

Creation fichier user

```
sudo mkdir -p /etc/vsftpd/vsftpd_user_conf
```

Sauvegarde

```
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.default.bak
sudo cp /etc/pam.d/vsftpd /etc/pam.d/vsftpd.default.bak
```

Création du fichier PAM : Il faut effacer le contenu du fichier /etc/pam.d/vsftpd et le remplacer par :

```
auth required /lib/security/pam_userdb.so db=/etc/vsftpd/login
account required /lib/security/pam_userdb.so db=/etc/vsftpd/login
```

f) Connexion chiffrée

Avec le module éponyme : SSL , activez SSL avec :

```
ssl_enable=yes
```

g) surveiller le serveur

```
-$ ps -aef | grep vsftpd
```

```
root      739     1  0 21:09 ?        00:00:00 /usr/sbin/vsftpd
xtbushi+  1401  1289  0 21:49 pts/0    00:00:00 grep --color=auto vsftpd
```

```
sudo tail -f /var/log/vsftpd.log
```

```
Sun Dec  6 21:27:05 2015 [pid 1350] CONNECT: Client "192.168.8.100"
Sun Dec  6 21:27:19 2015 [pid 1349] [xtbushido] FAIL LOGIN: Client "192.168.8.100"
Sun Dec  6 21:27:35 2015 [pid 1352] CONNECT: Client "192.168.8.100"
Sun Dec  6 21:27:45 2015 [pid 1351] [xtbushido] OK LOGIN: Client "192.168.8.100"
Sun Dec  6 21:42:33 2015 [pid 1358] CONNECT: Client "192.168.8.100"
Sun Dec  6 21:42:33 2015 [pid 1357] [xtbushido] OK LOGIN: Client "192.168.8.100"
Sun Dec  6 21:43:04 2015 [pid 1362] CONNECT: Client "192.168.8.100"
Sun Dec  6 21:43:04 2015 [pid 1363] CONNECT: Client "192.168.8.100"
Sun Dec  6 21:43:04 2015 [pid 1361] [xtbushido] OK LOGIN: Client "192.168.8.100"
Sun Dec  6 21:43:04 2015 [pid 1360] [xtbushido] OK LOGIN: Client "192.168.8.100"
```

3.4. References

Security.appspot

Ubuntu.com

Digitalocean

Debian.org

Et beaucoup d'autres...