par Mario M. Knopf
<netzmeister/at/neo5k/dot/org>

L´auteur:

Mario s'occupe volontiers, avec Linux, des réseaux et ce qui touche à la sécurité. Pendant son temps libre, il maintient les sites neo5k.org et linuxwallpapers.de.

vsftpd – une introduction au Very Secure FTP Daemon.

Résumé:

Cet article donne une petite introduction au "Very Secure FTP Daemon". Je commence par une introduction générale du protocole FTP puis de vsftpd. Ensuite nous regarderons l'installation, la configuration et les options de démarrage du démon vsftpd. Nous terminerons avec un petit essai.

Traduit en Français par:
Marc Remy
<mremy(at)gmx(punkt)ch>

Introduction

Le File Transfer Protocol (FTP) sert à l'échange de données sur internet, indépendamment de la plate−forme et il est basé sur une architecture client−serveur. La RFC 959 [1] décrit que le protocole FTP est séparé en deux canaux, l'un pour les données (TCP−Port 20) et l'autre sert pour l'administration (TCP−Port 21). Le canal de commande sert à l'échange des commandes entre les deux cotés (Serveur et Client), qui préparent les transferts des données.
Une session FTP se déroule en quatre étapes:

- Authentification de l'utilisateur
- Etablissement du canal de contrôle
- Etablissement du canal de données
- Fermeture de la connexion

FTP utilise TCP (Transmission Control Protocol), qui est orienté connexion comme protocole de transport garantissant l'acheminement des données jusqu'au destinataire. Ainsi, FTP n'a pas à se préoccuper d'une possible perte de paquet ou de contrôle d'erreur lors du transfert. Simplement dit, TCP s'assure que chaque paquet de données arrive une et une seule fois, sans erreur et dans le bon ordre.

Il existe trois modes de transmission des données. La fin de la transmission est indiquée par un End−of−File EOF en mode stream, par un End−of−Record (EOR) pour les deux autres.

- Stream
- Block
- Compressed

En plus, il y a deux modes de transfert différents:

- ASCII
- Binary

Le mode ASCII est utilisé pour le transfert de fichiers texte, tandis que le mode binary l'est pour le transfert de programmes ou de données similaires. L'utilisateur n'a pas besoin de choisir entre ces deux modes car, aujourd'hui, tous les clients FTP reconnaissent le type de fichier à transférer et choisissent le mode adéquat.

Puisque le transfert du nom d'utilisateur et du mot de passe pour l'authentification n'est pas sécurisé, il est très important d'attirer l'attention sur ce risque potentiel pour la sécurité. C'est pour cette raison qu'il y a eu beaucoup de réflexion sur la sécurité de FTP. En octobre 1997 a été publiée la RFC 2228[2], qui définit des ajouts spécifiques au File Transfer Protocol.

vsftpd

vsftpd est un serveur FTP pour les systèmes d'exploitation de type UNIX et il fonctionne sur des plates−formes telles que Linux, *BSD, Solaris, HP−UX et IRIX. Il possède de nombreuses caractéristiques qui manquent sur les autres serveurs FTP, comme:

- très haut niveau de sécurité
- limitation de la bande passante
- bonne ajustabilité
- possibilité de définir des utilisateurs virtuels
- support IPnG
- performance meilleure que la moyenne
- possibilité d'attribuer des adresses IP virtuelles
- haute vitesse

L'acronyme vsftpd signifie "Very Secure FTP Daemon", qui était le souci du développeur, Chris Evans. Depuis le début de la conception et du développement du serveur FTP, la haute sécurité a été une de ses principales exigences.

Par exemple, on peut citer le fait que vsftpd fonctionne en mode chroot. Cela signifie que le programme (ici vsftpd) s'exécute dans un nouveau répertoire racine (/) et ne peut donc pas accéder aux autres programmes et fichiers en dehors de ce répertoire. Il est en quelque sorte « emprisonné » dans cet environnement. Si un attaquant potentiel compromettait le serveur FTP, il serait isolé du reste du système et limiterait les risques de dégâts. On trouve plus d'informations sur l'environnement chroot dans l'article [3]. L'article [4] est à recommander à ceux qui s'intéressent à la conception et aux mécanismes de sécurité de vsftpd.

Avec toutes ses capacités − parmi lesquelles le besoin de sécurité est la plus haute priorité − vsftpd se positionne nettement au dessus des autres serveurs FTP. WU−FTP[5] peut être cité comme exemple négatif, car il a présenté de nombreuses failles de sécurité ses dernières années.

Installation

L'installation du démon vsftpd est très simple, puisque la plupart des grandes distributions proposent un paquet RPM pour l'installer. Il l'est d'ailleurs déjà dans la plupart des cas. Sinon, il est possible de télécharger le code source ici [6] et l'installer manuellement.

Une fois le code source téléchargé, décompressez le fichier tar, allez dans le répertoire, créez et tapez la commande make. Voici un exemple des commandes nécessaires:

```
neo5k@phobos> tar xzvf vsftpd−x.x.x.tar.gz
neo5k@phobos> cd vsftpd−x.x.x
neo5k@phobos> make
```

Avant cela, il faut s'assurer que l'utilisateur « nobody » et que le répertoire « /usr/share/empty » existent et les créer si besoin. Pour prévoir un accès aux utilisateurs anonymes, il faut créer un utilisateur « ftp », avec pour répertoire racine « /var/ftp ». Cela se fait à l'aide des deux commandes suivantes:

```
neo5k@phobos> mkdir /var/ftp
neo5k@phobos> useradd −d /var/ftp ftp
```

Pour des raisons de sécurité, le répertoire « /var/ftp » ne doit pas appartenir à l'utilisateur « ftp » et il ne doit pas non plus avoir le droit d'écriture dedans. Lorsque l'utilisateur existe, on peut changer le propriétaire et les droits d'accès avec les deux commandes suivantes:

```
neo5k@phobos> chown root.root /var/ftp
neo5k@phobos> chmod og−w /var/ftp
```

Lorsque les pré−requis sont satisfaits, on peut installer le démon vsftpd:

```
neo5k@phobos> make install
```

Il faut normalement copier maintenant les pages de manuels et le programme au bon endroit. Dans le cas de problèmes, on peut le faire à la main.

```
neo5k@phobos> cp vsftpd /usr/sbin/vsftpd
neo5k@phobos> cp vsftpd.conf.5 /usr/share/man/man5
neo5k@phobos> cp vsftpd.8 /usr/share/man/man8
```

Le fichier de configuration d'exemple n'a pas encore été copié à ce stade − il facilite l'introduction − il faut encore taper:

```
neo5k@phobos> cp vsftpd.conf /etc
```

Configuration

Le fichier de configuration de vsftpd est « /etc/vsftpd.conf ». Comme dans la plupart des fichiers de configuration, les lignes commençant par un dièse sont des commentaires

```
# Ligne de commentaire
```

Une configuration d'exemple pourrait ressembler à ça:

```
# Autoriser le FTP anonyme? YES/NO
anonymous_enable=NO

# Autoriser l'upload anonyme? YES/NO
anon_upload_enable=NO

# Autoriser les utilisateur anonymes à créer des répertoires? YES/NO
anon_mkdir_write_enable=NO

# Autoriser les autres opérations d'écriture, comme renommer ou effacer, aux utilisateurs anonymes? YES/NO
anon_other_write_enable=NO

# Autoriser les utilisateurs locaux à se connecter? YES/NO
local_enable=YES

# Les utilisateurs locaux doivent−ils être bloqués dans leur répertoires racine? YES/NO
chroot_local_user=YES

# Taux de transfert maximum autorisé aux utilisateurs locaux en bytes/seconde. Par défaut = 0 (illimité)
local_max_rate=7200

# Autoriser le droit d'écriture principal? YES/NO
write_enable=YES

# Montrer le message lors du changement de répertoire? YES/NO
dirmessage_enable=YES

# Bannière de connexion.
ftpd_banner="Bienvenu sur le service FTP de neo5k."

# Activer le fichier de log? YES/NO
xferlog_enable=YES

# Collecter toutes les activités du serveur dans le fichier de log? YES/NO
# Attention! Cela génère un gros volume de données.
log_ftp_protocol=NO

# Confirmer que les connexions se font seulement sur le port 20 (ftp−data). YES/NO
connect_from_port_20=YES

# Déconnexion en cas d'inactivité (time out) après (idle sessions)
idle_session_timeout=600

# Durée, après laquelle la connexion est interrompue.
data_connection_timeout=120

# Accès gérés avec Pluggable Authentication Modules (PAM).
pam_service_name=vsftpd
```

 # Utilisation en ligne de commande? YES/NO – dépendant de l'utilisation (inetd, xinetd, Standalone)
 # Le serveur FTP de l'auteur est géré par xinetd, donc NO.
listen=NO

Démarrage du service FTP

vsftpd peut être utilisé de trois manières différentes. Soit avec inetd ou xinetd, soit en mode autonome.

inetd

Si le service FTP est géré par inetd, il faut ouvrir le fichier de configuration "/etc/inetd.conf" avec un éditeur:

neo5k@phobos> vi /etc/inetd.conf

Ensuite, chercher la ligne concernant le service FTP et supprimer le signe de commentaire en début de ligne. S'il n'y a pas déjà une ligne, il suffit de l'insérer manuellement. Puis, redémarrer inetd. L'entrée doit ressembler à ça:

```
# ftp   stream   tcp   nowait   root   /usr/sbin/tcpd   in.ftpd
ftp   stream   tcp   nowait   root   /usr/sbin/tcpd   vsftpd
```

xinetd

Il est recommandé de démarrer le démon vsftpd avec xinetd, qui apporte beaucoup d'améliorations par rapport à inetd. Quelques une d'entre elles sont, par exemple, l'enregistrement des requêtes, le contrôle des accès, l'association du service à une interface réseau particulière, etc... Une très bonne introduction à xinetd se trouve là [7]. Après avoir modifié le fichier, il est nécessaire de redémarrer xinetd. La configuration peut ressembler à ça:

```
# vsftp daemon.
service ftp
{
    disable = no
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/vsftpd
    per_source = 5
    instances = 200
    no_access = 192.168.1.3
    banner_fail = /etc/vsftpd.busy_banner
    log_on_success += PID HOST DURATION
    log_on_failure += HOST
    nice = 10
}
```

Utilisation autonome

Il est également possible d'utiliser le démon vsftpd en mode autonome. Pour cela, il faut de nouveau éditer le fichier de configuration « /etc/vsftpd.conf » et de changer la ligne suivante:

 # Le démon vsftp doit−il tourner en mode Standalone? YES/NO
listen=YES

Ensuite, le démon est démarré de la manière suivante

neo5k@phobos> /usr/sbin/vsftpd &

Si le chemin de recherche est correctement renseigné, cette commande suffit

neo5k@phobos> vsftpd &

L'entrée suivante permet de voir si le chemin de recherche est correctement initialisé:

neo5k@phobos> echo $PATH
/usr/sbin:/bin:/usr/bin:/sbin:/usr/X11R6/bin

Naturellement, en mode autonome, il faut faire attention que le démon vsftpd n'est démarré ni par inetd, ni par xinetd.

Essai

Après avoir installé et configuré avec succès, nous pouvons nous connecter une première fois à notre serveur FTP.

```
neo5k@phobos> ftp phobos
Connected to phobos
220 "Welcome to neo5k's FTP service."
Name (phobos:neo5k): testuser
331 Please specify the password.
Password:
230 Login successful
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode
150 Here comes the directory listing
drwxr-xr-x      11  500      100         400  May 07 16:22  docs
drwxr-xr-x        9  500       100         464  Feb   01 23:05  hlds
drwxr-xr-x      39  500      100       4168  May 10 09:15  projects
226 Directory send OK.
ftp>
```

Conclusion

Comme nous l'avons vu, le démon vsftpd n'est pas difficile à installer, ni à configurer. Malgré tout, il offre de nombreuses possibilités de configuration et un très bon niveau de sécurité.

Il est évident que cette introduction ne donne qu'un petit aperçu des multiples possibilités de configuration offertes par vsftpd. Ceux d'entre vous qui veulent en apprendre plus sur vsftpd doivent se rendre sur la page du projet [6] et lire la volumineuse documentation.

Liens

[1] ftp://ftp.rfc−editor.org/in−notes/rfc959.txt [RFC 959 − File Transfer Protocol]
[2] ftp://ftp.rfc−editor.org/in−notes/rfc2228.txt [RFC 2228 − FTP Security Extensions]
[3] article 225, Janvier 2002 [chroot]
[4] http://vsftpd.beasts.org/DESIGN [Mécanisme de sécurité de vsftpd]
[5] http://www.wu−ftpd.org/ [WU−FTPD]
[6] http://www.vsftpd.beasts.org/ [Home of vsftpd]
[7] article 175, Novembre 2000 [xinetd]

Translation information:
de −−> −− : Mario M. Knopf <netzmeister/at/neo5k/dot/org>
de −−> fr: Marc Remy <mremy(at)gmx(punkt)ch>

2005−01−22, generated by lfparser_pdf version 2.51