SelfLinux-0.13.0

Very Secure FTP Daemon

Autor: Mario M. Knopf (*netzmeister@neo5k.org*)
Autor: Florian Frank (*florian.frank@pingos.org*)
Formatierung: Florian Frank (*florian.frank@pingos.org*)

Dieser Artikel soll eine grundlegende Einführung zum **Very Secure FTP Daemon** darstellen. Beginnen möchte ich mit einer allgemeinen Beschreibung von **FTP** und `vsftpd`. Danach sehen wir uns die Installation, Konfiguration und Startmöglichkeiten des `vsftp`-Daemons genauer an. Abschließend wird noch ein kurzer Funktionstest durchgeführt werden.

Inhaltsverzeichnis

1 Einleitung

Das File Transfer Protocol (FTP) dient zur plattformunabhängigen Dateiübertragung im Internet und basiert auf einer Server-Client-Architektur. RFC 959 schreibt vor, dass FTP in zwei unterschiedliche Kanäle getrennt wird, wobei ein Kanal für die Daten (TCP-Port 20) und der andere zur Steuerung (TCP-Port 21) dient. Über den Steuerkanal tauschen die beiden Seiten (Server und Client) Kommandos aus, welche dann den Datentransfer einleiten. Eine FTP-Verbindung verläuft in vier Schritten:

1. Benutzerauthentifizierung
2. Aufbau des Steuerungskanals
3. Aufbau des Datenkanals
4. Beenden der Verbindung

FTP benutzt als Transportprotokoll das verbindungsorientierte TCP (Transmission Control Protocol), welches sicherstellt, dass die Daten auch wirklich beim Empfänger ankommen. Somit braucht sich FTP nicht um einen möglichen Paketverlust bzw. eine Fehlerkontrolle bei der Dateiübertragung kümmern. Grob formuliert sorgt TCP also dafür, dass jedes einzelne Datenpaket nur einmal ankommt - fehlerfrei bei der Übertragung und in der richtigen Reihenfolge.

Bei der Dateiübertragung unterscheidet man drei Transferarten, wobei der Abschluß des Transfers im Stream-Modus durch ein End-of-File (EOF), bei den beiden anderen Übertragungsarten durch ein End-of-Record (EOR) gekennzeichnet wird.

* Stream
* Block
* Compressed

Des Weiteren gibt es zwei verschiedene Transfermodi:

* ASCII
* Binary

Der ASCII-Modus dient zur Übertragung von Textdateien, wohingegen der Binary-Modus beispielsweise zum Transfer von Programmen oder dergleichen dient. Der Benutzer muß den Transfermodus für gewöhnlich nicht explizit auswählen, da mittlerweile alle FTP-Clients die zu übertragende Datei erkennen und automatisch umschalten.

Da die Übermittlung der Benutzerkennung und des Passwortes zur Authentifizierung nicht verschlüsselt wird, ist es sehr wichtig, ausdrücklich auf dieses potentielle Sicherheitsrisiko hinzuweisen. Aus diesem Grund machte man sich Gedanken über die Sicherheit von FTP. Im Oktober 1997 wurde schließlich das RFC 2228 veröffentlicht, welches sicherheitsspezifische Erweiterungen für das File Transfer Protocol definiert.

2 vsftpd

vsftpd stellt einen FTP-Server für unixoide Betriebssysteme dar und läuft somit auf Plattformen wie Linux, *BSD, Solaris, HP-UX und IRIX. Dabei unterstützt vsftpd viele Merkmale, die man bei anderen FTP-Servern unter Umständen schmerzlich vermisst. Einige davon sind beispielsweise:

* sehr hohe Sicherheitsansprüche
* Bandbreitenbegrenzung
* gute Skalierbarkeit
* Möglichkeit, virtuelle User zu erstellen
* IPnG-Unterstützung
* überdurchschnittliche Performance
* Möglichkeit, virtuelle IPs zu vergeben
* hohe Geschwindigkeit

Der Name vsftpd steht für **Very Secure FTP Daemon**, welcher auch gleich eines der Hauptanliegen des Entwicklers *Chris Evans* wiederspiegelt. Bei der Entwicklung und dem Design des FTP-Servers wurde von Anfang an sehr viel Wert auf Sicherheit gelegt.

Als Beispiel hierfür kann die Tatsache genannt werden, dass vsftpd im chroot-Modus betrieben wird. chroot bedeutet, dass einem Programm (in diesem Fall vsftpd) ein neues Wurzelverzeichnis (/) zugewiesen wird und es somit nicht mehr auf Programme oder Dateien außerhalb dieses Verzeichnisses zugreifen darf - es wird sozusagen in einem Gefängnis eingesperrt. Sollte nun ein potentieller Angreifer den FTP-Server kompromittieren, ist er vom übrigen System abgeschottet und kann dadurch keinen größeren Schaden anrichten. Wer sich jedoch besonders für die Implementierung und das Design der diversen Sicherheitsmechanismen von vsftpd interessiert, dem sei http://vsftpd.beasts.org/DESIGN empfohlen.

Durch diese umfangreichen Merkmale - wobei der Anspruch an die Sicherheit des FTP-Dienstes höchste Priorität genießen sollte - hebt sich vsftpd deutlich von anderen FTP-Servern ab. Als Negativbeispiel sei hier der WU-FTPD genannt, welcher in den vergangenen Jahren ständig durch diverse Sicherheitslücken auffiel.

3 Installation

Die Installation des vsftp-Daemons verläuft recht einfach, da jede größere Distribution fertige RPM-Pakete zu vsftpd bereitstellt, welche in den meisten Fällen sogar schon installiert sind. Alternativ besorgt man sich von http://www.vsftpd.beasts.org/ die Quellen und übersetzt das Programm manuell.

Hat man sich die Quellen beschafft, entpackt man den Tarball, wechselt in das soeben enstandene Verzeichnis und führt make aus. Nachfolgend werden die dazu benötigten Befehle demonstriert:

```
root@linux / # tar xzvf vsftpd-x.x.x.tar.gz
root@linux / # cd vsftpd-x.x.x
root@linux / # make
```

Zuvor sollte man jedoch überprüfen, ob der Benutzer **nobody** und das Verzeichnis /usr/share/empty existiert und gegebenenfalls neu anlegen. Plant man Zugriffsmöglichkeiten für anonyme Benutzer, muss der User **ftp** mitsamt Homeverzeichnis /var/ftp angelegt werden. Letzteres erreicht man durch die Eingabe der folgenden beiden Befehle:

```
root@linux / # mkdir /var/ftp
root@linux / # useradd -d /var/ftp ftp
```

Aus Sicherheitsgründen sollte das Verzeichnis /var/ftp dem Benutzer **ftp** weder gehören, noch sollte dieser darin Schreibrechte besitzen. Wenn der Benutzer bereits existiert, genügen die nächsten beiden Kommandos, um den Besitzer zu ändern und anderen Benutzern die Schreibrechte zu entziehen:

```
root@linux / # chown root.root /var/ftp
root@linux / # chmod og-w /var/ftp
```

Sofern alle Voraussetzungen erfüllt sind, kann man den vsftp-Daemon installieren:

```
root@linux / # make install
```

Jetzt werden normalerweise die Manpages und das Programm an den richtigen Ort im Dateisystem kopiert. Wenn es wider Erwarten zu Komplikationen kommt, hilft jedoch auch ein manuelles Kopieren der Dateien.

```
root@linux / # cp vsftpd /usr/sbin/vsftpd
root@linux / # cp vsftpd.conf.5 /usr/share/man/man5
root@linux / # cp vsftpd.8 /usr/share/man/man8
```

Da die Beispiel-Konfigurationsdatei nicht mit kopiert wird, diese aber den Einstieg erleichtert, muss man auch hier noch einmal Hand anlegen:

```
root@linux / # cp vsftpd.conf /etc
```

4 Konfiguration

Die Konfigurationsdatei zu `vsftpd` lässt sich unter /etc/vsftpd.conf finden. Wie bei den meisten Konfigurationsdateien werden auch bei `vsftpd` Kommentare mit einer einleitenden Raute gekennzeichnet.

```
# Kommentarzeile
Eine beispielhafte Konfiguration könnte so aussehen:

# Anonymen FTP-Zugriff erlauben? YES/NO
anonymous_enable=NO

# Anonymen Upload erlauben? YES/NO
anon_upload_enable=NO

# Dürfen anonyme User Verzeichnisse erstellen? YES/NO
anon_mkdir_write_enable=NO

# Dürfen anonyme User andere Schreiboperationen wie Umbenennen oder Löschen durchführen?
YES/NO
anon_other_write_enable=NO

# Anmeldung von lokalen Usern erlauben? YES/NO
local_enable=YES

# Sollen lokale Benutzer in ihrem Homeverzeichnis eingesperrt werden? YES/NO
chroot_local_user=YES

# Die maximal erlaubte Datentransferrate in Bytes/Sekunde für lokal angemeldete User.
Vorgabe = 0 (unbegrenzt)
local_max_rate=7200

# Schreibrechte prinzipiell erlauben? YES/NO
write_enable=YES

# Nachrichten bei Verzeichniswechsel anzeigen? YES/NO
dirmessage_enable=YES

# Bannermeldung, welche der sich anmeldende User sieht.
ftpd_banner="Welcome to neo5k's FTP service."

# Protokollierung aktivieren? YES/NO
xferlog_enable=YES

# Sämtliche FTP-Aktivitäten protokollieren? YES/NO
# Achtung! Durch diesen Eintrag können sehr große Datenmengen entstehen.
log_ftp_protocol=NO

# Versichern, daß Verbindungen nur an Port 20 (ftp-data) zustande kommen. YES/NO
connect_from_port_20=YES

# Unterbrechung (time out) bei Leerlaufzeiten (idle sessions)
idle_session_timeout=600

# Zeit, nach der eine Datenverbindung unterbrochen wird.
data_connection_timeout=120

# Zugriff wird über Pluggable Authentication Modules (PAM) geregelt.
pam_service_name=vsftpd

# Standalone-Betrieb? YES/NO - abhängig vom Betriebsmodus (inetd, xinetd, Standalone)
# Des Autors FTP-Dienst wird per xinetd gestartet, deswegen lautet der Wert hier NO.
listen=NO
```

5 Starten des FTP-Dienstes

vsftpd läßt sich auf drei verschiedene Arten betreiben. Zum einen über inetd oder xinetd, zum anderen im Standalone-Betrieb.

5.1 inetd

Soll der FTP-Dienst via inetd betrieben werden, öffnet man die Konfigurationsdatei /etc/inetd.conf mit einem Editor:

```
root@linux / # vi /etc/inetd.conf
```

Dann sucht man sich die entsprechenden Zeilen zu den FTP-Diensten und entfernt nur noch das Kommentarzeichen vor dem vsftpd-Eintrag. Sollte kein entsprechender Eintrag vorhanden sein, kann man ihn auch manuell erstellen. Dabei ist zu beachten, dass nach den durchgeführten Änderungen der inetd zwingend neu gestartet werden muss. Der Eintrag sollte dann so aussehen:

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

5.2 xinetd

Empfehlenswert ist es jedoch, den vsftp-Daemon per xinetd starten zu lassen, da dieser zahlreiche Erweiterungen gegenüber inetd besitzt. Einige davon sind bspw. Protokollierung von Anfragen, Zugriffssteuerung, Bindung des Dienstes an bestimmte Netzwerkschnittstellen, et cetera. Eine sehr gute Einführung zum Thema xinetd findet man in diesem Kapitel. Auch hier ist nach erfolgter Modifikation ein Neustart des xinetd nötig. Die Konfiguration des xinetd könnte folgendermassen aussehen:

```
# 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
}
```

5.3 Standalone-Betrieb

Zusätzlich besteht die Möglichkeit, den vsftp-Daemon im Standalone-Modus zu betreiben. Dazu öffnet man wieder die Datei /etc/vsftpd.conf und führt die folgende Änderung durch:

```
# Soll der vsftp-Daemon im Standalone-Betrieb laufen? YES/NO
listen=YES
```

Nach erfolgtem Eintrag kann man den Daemon dann durch die nachfolgend genannte Eingabe starten.

```
root@linux / # /usr/sbin/vsftpd &
```

Sofern die Einstiegspfade richtig gesetzt sind, genügt zum Starten auch ein schlichtes

```
root@linux / # vsftpd &
```

Durch die nächste Eingabe kann geprüft werden, ob die Einstiegspfade richtig gesetzt wurden:

```
root@linux / # echo $PATH

/usr/sbin:/bin:/usr/bin:/sbin:/usr/X11R6/bin
```

Natürlich sollte man beim Betrieb im Standalone-Modus darauf achten, dass der `vsftp`-Daemon weder per `inetd` noch xinetd gestartet wird.

6 Funktionstest

Hat man die Installation und Konfiguration erfolgreich hinter sich gelassen, kann man das erste Mal auf seinen FTP-Server zugreifen.

```
root@linux / # 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.
```

7 Fazit

Wie man sehen konnte, ist der vsftp-Daemon weder schwer aufzusetzen noch schwierig zu konfigurieren. Trotzdem bietet er zahlreiche Funktionsmerkmale und ein hohes Maß an Sicherheit.

Es versteht sich von selbst, dass diese Einführung nur einen kleinen Ausschnitt aus der Welt von vsftpd bieten kann, da der FTP-Server äußerst umfangreiche Konfigurationsmöglichkeiten zur Verfügung stellt. Wer sich nach diesem Artikel eingehender mit vsftpd beschäftigen möchte, sollte die Projektseite unter http://www.vsftpd.beasts.org/ besuchen und sich dort die umfangreiche Dokumentation zu Gemüte führen.