LinuxFocus article number 341
http://linuxfocus.org

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

Over de auteur:

Mario houdt zich graag bezig met Linux, netwerken en andere onderwerpen die betrekking hebben op beveiliging. In z'n vrije tijd onderhoudt hij twee webstekken: neo5k.org en linuxwallpapers.de.

Vertaald naar het Nederlands door:
Hendrik-Jan Heins
<hjh/at/NOSPAM/dot/passys/dot/nl>

vsftpd - Een introductie in de Very Secure FTP Daemon

Kort:

Dit artikel is een introductie in de "Very Secure FTP Daemon". Ik zal beginnen met een algemene beschrijving van FTP en vsftpd. Daarna gaan we kijken naar de installatie, configuratie en de opstart-opties van de of vsftp daemon. We beëindigen het artikel met een korte test van de functies.

Inleiding

Het doel van het File Transfer Protocol is platform-onafhankelijke gegevensoverdracht over internet, en het is gebaseerd op een server/client architectuur. RFC 959[1] stelt vast dat FTP opgesplitst dient te zijn in twee verschillende kanalen, een die de gegevens verstuurt (TCP-poort 20) en de andere voor de controle hierop (TCP-poort 21). De twee partijen (server en client) wisselen de commando's voor de initiatie van de gegevensoverdracht uit over het controle-kanaal
Een FTP verbinding bestaat uit vier stappen:

- Gebruikersautorisatie
- Het instellen van het controle-kanaal
- Het instellen van het gegevenskanaal
- Het beëindigen van de verbinding

FTP gebruikt het verbindings-controlerende protocol TCP (Transmission Control Protocol) als verbindingsprotocol, om aankomst van de gegevens bij de ontvanger te verzekeren. Daarom hoef je je bij FTP geen zorgen te maken over pakketverlies of foutcontrole tijdens de gegevensoverdracht. Anders gezegd zorgt TCP ervoor dat alle data pakketten slechts één maal aankomen - zonder fouten en in de juiste volgorde.

Gegevensoverdracht bestaat uit drie verschillende typen overdracht waarbij de completering van de streaming modus wordt gemarkeerd door een "end-of-file" (EOF) en in de andere twee overdrachtsmodi met een "end-of-record" (EOR) marker.

- Stream
- Blok
- Gecomprimeerd

Daarnaast zijn er nog twee verschillende overdrachtsmodi:

- ASCII
- Binair

De ASCII-modus wordt gebruikt voor de overdracht van tekstbestanden, en de binaire modus wordt gebruikt voor de overdracht van programma’s en soortgelijke gegevens.De gebruiker hoeft de overdrachtsmodus niet zelf te selecteren, aangezien tegenwoordig alle FTP programma’s wisselen naar het type dat voor het te verzenden bestand het beste is.

Aangezien de gebruikersherkenning en het wachtwoord van de autorisatie niet gecodeerd zijn, is het van belang dat ik hierbij aangeef dat dit een potentieel veiligheidslek is. Dit is de reden dat er nagedacht wordt over beveiliging van FTP. In oktober 1997 werd de RFC 2228[2] eindelijk gepubliceerd; hiermee werden belangrijke aanvullingen aan het File Transfer Protocol toegevoegd.

vsftpd

vsftpd is een server voor unix-achtige besturingssystemen, het draait op platformen als Linux, xxxBSD, Solaris, HP-UX en IRIX. Het ondersteunt veel mogelijkheden die niet aanwezig zijn bij andere FTP-servers. Enkelen hiervan zijn:

- Zeer hoge beveiligingseisen
- Bandbreedte limitering
- Goede schaalbaarheid
- De mogelijkheid virtuele gebruikers aan te maken
- IPnG ondersteuning
- Beter dan doorsnee performance
- De mogelijkheid virtuele IP-adressen toe te wijzen
- hoge snelheden

De naam *vsftpd* staat voor "very secure FTP daemon", en dat is een van de belangrijkste punten voor

ontwikkelaar Chris Evans. Vanaf het begin van de ontwikkeling en het ontwerp van de FTP server was zeer hoge beveiliging een van de hoofdpunten.

Een voorbeeld hiervan is het feit dat *vsftpd* kan worden gedraaid in *chroot* modus, wat zoveel betekent dat een programma (in dit geval *vsftpd*) wordt weggezet in een eigen root map(l), en dat het geen programma's buiten die map meer kan benaderen - het programma zit zogezegd "opgesloten". Mocht er op een FTP-server worden ingebroken dan zit de potentiele aanvalle opgesloten in een hokje dat niet in verbinding staat met de rest van het systeem en kan hij dus relatief maar weinig schade aanrichten. Meer informatie over *chroot* is te vinden in het artikel onder [3]. Artikel [4] wordt aangeraden voor diegenen die geïnteresseerd zijn in de specifieke beveiligingsmechanismen van *vsftpd*

Met deze vele mogelijkheden - waarvan de eisen aan de beveiliging van de FTP-service de hoogste prioriteit hebben - verheft *vsftpd* zich boven de andere FTP-servers. Hierbij kan WU-FTPD[5] worden genoemd als een negatief voorbeeld vanwegde de vele beveiligingslekken die in de laatste paar jaar in het programma gevonden zijn.

Installatie

De installatie van de *vsftpd* daemon is vrij eenvoudig aangezien er complete RPM pakketten van *vsftpd* te vinden zijn in iedere grote distributie, in veel gevallen is hij zelfs al geinstalleerd. Maar anders kan de broncode worden gevonden onder [6] en handmatig worden geïnstalleerd.

Na het ophalen van de broncode, pak je de tarball uit, ga je naar de map die net is aangemaakt, en voer je het *make*-commando uit. Hier een voorbeeld van de noodzakelijke commando's:

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

Voordat we dit doen, moeten we wel gecontroleerd hebben of de gebruiker *"nobody"* en de map *"/usr/share/empty"* bestaat en moeten we ze zonodig aanmaken. Wanneer je van plan bent toegang voor anonieme gebruikers vrij te geven, moet je een gebruiker *"ftp"* met als persoonlijke map *"/var/ftp"* aanmaken. Dit doe je via de volgende twee commando's:

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

Vanwege veligheidsredenen zou de map *"/var/ftp"* geen eigendom moeten zijn van de gebruiker *"ftp"*, deze gebruiker zou ook geen schrijfrechten moeten hebben in die map. Met de volgende twee commando's kunnen we de eigenaar wijzigen en de schrijfrechten van andere gebruikers afnemen mocht de gebruiker al bestaan:

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

Na alle voorzorgen genomen te hebben, kunnen we nu de *vsftp*-daemon installeren:

neo5k@phobos> make install

De manpagina's en het programma moeten nu gecopieerd worden naar de juiste plek in het gegevenssysteem. Mochten er onverwachte complicaties optreden, dan kan je de bestanden ook handmatig copieren.

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

Aangezien het voorbeeld van ons configuratiebestand op dit moment nog niet gecopieerd is - wat de inleiding makkelijker zou maken - moeten we handmatig het volgende nog aanmaken:

neo5k@phobos> cp vsftpd.conf /etc

Configuratie

Het configuratiebestand kan worden gevonden op de volgende plek: *"/etc/vsftpd.conf"*. Zoals met de meeste configuratiebestanden, worden commentaren gemarkeerd met een initiele hash marker.

Commentaarregel

Een voorbeeldconfiguratiebestand zou er zo uit kunnen zien:

 # Anonymous FTP-access permitted? YES/NO
anonymous_enable=NO

 # Permit anonymus upload? YES/NO
anon_upload_enable=NO

 # Permission for anonymus users to make new directories? YES/NO
anon_mkdir_write_enable=NO

 # Permission for anonymus users to do other write operations - like renaming or deleting? YES/NO
anon_other_write_enable=NO

 # Log on by local users permitted? YES/NO
local_enable=YES

 # Shall local users be locked into their home directory? YES/NO
chroot_local_user=YES

 # Highest permitted data transfer rate in bytes per second for local logged on users. Default = 0 (unlimited)
local_max_rate=7200

 # General write permission? YES/NO
write_enable=YES

 # Enable messages when changing directories? YES/NO
dirmessage_enable=YES

 # Welcome banner at users logon.
ftpd_banner="Welcome to neo5k's FTP service."

 # Activate logging? YES/NO
xferlog_enable=YES

 # Logging of all FTP activities? YES/NO
 # Careful! This can generate large quantities of data.
log_ftp_protocol=NO

 # Confirm connections are established on port 20 (ftp data) only. YES/NO
connect_from_port_20=YES

 # Timeout during idle sessions
idle_session_timeout=600

 # Data connection timeout
data_connection_timeout=120

 # Access through Pluggable Authentication Modules (PAM)
pam_service_name=vsftpd

 # Standalone operation? YES/NO - depending on operation mode (inetd, xinetd, Standalone)
 # The author's FTP service is being startet with xinetd, therefore the value here is NO.
listen=NO

De FTP-Service starten

vsftpd kan op drie verschillende manieren werken. Een is via *inetd*, twee via *xinetd*, en de derde is een losstaande service.

inetd

Wanneer de FTP service wordt gedraaid via *inetd* openen we het configuratiebestand *"/etc/inetd.conf"* met een editor:

neo5k@phobos> vi /etc/inetd.conf

We zoeken naar de regels die betrekking hebben op de FTP service en verwijderen het

commentaarsymbool voor de regel over*vsftpd*. Wanneer er nog niet zo'n regel is, dan kan deze toegevoegd worden. Daarna moeten we *inetd* herstarten. De regel zou er als volgt uit moeten zien:

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

xinetd

Het wordt aangeraden de *vsftp* daemon te starten met *xinetd* aangezien deze meer up-to-date is dan *inetd*. Enkele verbeteringen zijn bijvoorbeeld het logging van aanvragen, toegangscontrole, het binden van een service aan een specifieke netwerkinterface enzovoort. Een zeer goede introducte in *xinetd* staat onder [7]. Na de wijziging, moet *xinetd* opnieuw gestart worden. De configuratie van *xinetd* zou er ongeveer zo uit moeten zien:

```
# 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
}
```

Losstaande service

Het is ook mogelijk de *vsftp* daemon op zichzelf te draaien. Hiervoor openen we opnieuw het bestand *"/etc/vsftpd.conf"* en veranderen het volgende:

 # Shall the vsftp daemon run in standalone operation? YES/NO
listen=YES

Hierna kan de daemon worden gestart met het volgende commando:

neo5k@phobos> /usr/sbin/vsftpd &

Wanneer het pad correct gedefinieerd is, zal het programma nu starten.

neo5k@phobos> vsftpd &

Met het volgende commando kunnen we controleren of het pad correct gedefinieerd is:

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

In losstaande modus moeten we natuurlijk opletten dat de *vsftp* daemon niet ook nog eens wordt gestart met *inetd* of *xinetd*.

Operationele Test

Na de succesvolle installatie en configuratie kunnen we onze FTP server voor het eerst benaderen.

```
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>
```

Conclusie

Zoals we al zeiden is het niet moeilijk de *vsftp* daemon te installeren of te configureren. De daemon biedt vele mogelijkheden en een goede beveiliging.

Natuurlijk geeft deze introductie slechts een klein kijkje in de omgeving die *vsftpd* biedt, aangezien de FTP server zeer veel configuratiemogelijkheden biedt. Voor degenen die *vsftpd* meer in diepte willen onderzoeken, is er de project pagina[6] waar uitgebreide documentatie te vinden is.

Links

[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] linuxfocus.org: artikel225, januari2002 [chroot]
[4] http://vsftpd.beasts.org/DESIGN [Security vsftpd]
[5] http://www.wu-ftpd.org/ [WU-FTPD]

[6] http://www.vsftpd.beasts.org/ [Thuisbasis van vsftpd]
[7] linuxfocus.org: artikel 175, November2000 [xinetd]

Vertaling info:
de --> -- : Mario M. Knopf <netzmeister/at/neo5k/dot/org>
de --> en: Jürgen Pohl <sept.sapins/at/verizon.net>
en --> nl: Hendrik-Jan Heins <hjh/at/NOSPAM/dot/passys/dot/nl>

2005-01-14, generated by lfparser_pdf version 2.51