INSTALACIÓN DEL SERVIDOR PROFTPD

1 Proftpd+Mysql+Quotas

El servidor elegido es Proftpd, uno de los más utilizados en la web. La instalación se hizo sobre una distribución Debian 3.11

Lo primero es instalar los paquetes... en Debian existe un paquete específico para el servidor proftpd con apoyo de myql:

```
apt-get install proftpd-mysql mysql-server
```

El instalador nos preguntará si queremos arrancar el ftp como servicio de red (inetd) o como 'standalone' (independent); elegiremos 'independent'.

Si lo vamos a hacer des el código fuente deberemos desempaquetar el programa y configurarlo:

```
tar xvfz proftpd-1.2.8p.tar.gz
```

```
cd proftpd-1.2.8p
```

```
.(./configure –with-modules=mod_sql: mod_sql_mysql: mod_quotatab:
mod_quotatab_sql --with-includes=/usr/include/mysql)
```

```
make
```

```
make install
```

Una vez instalado miramos si Proftpd tiene los módulos necesarios para seguir con la configuración. Para ver los módulos

```
 proftpd -l
```

Lo segundo es crear un usuario y grupo específico para el ftp que seran los propietarios de los archivos que se transfieran. Ya que los usuarios del ftp no son usuarios reales.

```
groupadd -g 2001 ftpgroup
useradd -u 2001 -s /bin/false -d /bin/null -c "usuario proftpd " -g ftpgroup
ftpuser
```

A continuación cambiamos la clave del root del mysql y creamos la base de datos y un usuario específico para esa base de datos:

```
 mysqladmin -u root password contraseña
```

Entramos en el MysSQL

```
 mysql -u root -p
```

Creamos la base de datos ftp y le damos los permisos al usuario proftpd

```
mysql > create database ftp;
mysql > GRANT SELECT, INSERT, UPDATE, DELETE ON ftp.* TO
'proftpd'@'localhost' IDENTIFIED BY 'password';
mysql > GRANT SELECT, INSERT, UPDATE, DELETE ON ftp.* TO
'proftpd'@'localhost.localdomain' IDENTIFIED BY 'password';
mysql > FLUSH PRIVILEGES;
```

recuerda cambiar password por la contraseña que tu elijas

Una vez creada la tabla procedemos a crear las tablas de la base de datos que contendrán la información de los usuarios que podrán acceder al ftp:

```
mysql > USE ftp;
mysql > CREATE TABLE ftpgroup (
groupname varchar(16) NOT NULL default '',
gid smallint(6) NOT NULL default '5500',
members varchar(16) NOT NULL default '',
KEY groupname (groupname)
) TYPE=MyISAM COMMENT='ProFTP group table';
```

```
mysql > CREATE TABLE ftpquotalimits (
name varchar(30) default NULL,
quota_type enum('user','group','class','all') NOT NULL default 'user',
per_session enum('false','true') NOT NULL default 'false',
limit_type enum('soft','hard') NOT NULL default 'soft',
bytes_in_avail int(10) unsigned NOT NULL default '0',
bytes_out_avail int(10) unsigned NOT NULL default '0',
bytes_xfer_avail int(10) unsigned NOT NULL default '0',
files_in_avail int(10) unsigned NOT NULL default '0',
files_out_avail int(10) unsigned NOT NULL default '0',
files_xfer_avail int(10) unsigned NOT NULL default '0'
) TYPE=MyISAM;
```

```
mysql > CREATE TABLE ftpquotatallies (
name varchar(30) NOT NULL default '',
quota_type enum('user','group','class','all') NOT NULL default 'user',
bytes_in_used int(10) unsigned NOT NULL default '0',
bytes_out_used int(10) unsigned NOT NULL default '0',
bytes_xfer_used int(10) unsigned NOT NULL default '0',
files_in_used int(10) unsigned NOT NULL default '0',
files_out_used int(10) unsigned NOT NULL default '0',
files_xfer_used int(10) unsigned NOT NULL default '0'
) TYPE=MyISAM;
```

```
mysql > CREATE TABLE ftpuser (
id int(10) unsigned NOT NULL auto_increment,
userid varchar(32) NOT NULL default '',
```

```
passwd varchar(32) NOT NULL default '',
uid smallint(6) NOT NULL default '5500',
gid smallint(6) NOT NULL default '5500',
homedir varchar(255) NOT NULL default '',
shell varchar(16) NOT NULL default '/sbin/nologin',
count int(11) NOT NULL default '0',
accessed datetime NOT NULL default '0000-00-00 00:00:00',
modified datetime NOT NULL default '0000-00-00 00:00:00',
PRIMARY KEY (id),
UNIQUE KEY userid (userid)
) TYPE=MyISAM COMMENT='ProFTP user table';
```

```
mysql > quit;
```

Algunas aclaraciones al respecto. La tabla ftpgroup lista los usuarios de cada grupo, como solo habrá un grupo (inicialmente) no necesita más registros para comenzar a usar el servicio. La tabla ftuser guarda los usuarios, estadísticas y es la usada por Proftpd para comparar los datos de autentificación. Usando la directiva 'asdfasf' haremos que Proftpd cree el directorio raíz del usuario si este no existe. La tabla ftpquotalimits define los límites de cuota en disco y ftpquotatalities va guardando los datos de cada usuario para totalizar y comprobar que el límite no sobrepasa lo acordado en ftpquotalimits. Si el valor de algún campo de límite es '0' automáticamente se definirá como ilimitado.

Ahora configuraremos el proftp: Abre el fichero /etc/proftpd.conf

```
vi /etc/proftpd/proftpd.conf
```

Sitúate al final y añade todas estas líneas y sálvalo:

```
 DefaultRoot ~


# The passwords in MySQL are encrypted using CRYPT
SQLAuthTypes            Plaintext Crypt
SQLAuthenticate         users* groups*


# used to connect to the database
# databasename@host database_user user_password
SQLConnectInfo  ftp@localhost proftpd password


# Here we tell ProFTPd the names of the database columns in the "usertable"
# we want it to interact with. Match the names with those in the db
SQLUserInfo     ftpuser userid passwd uid gid homedir shell

# Here we tell ProFTPd the names of the database columns in the "grouptable"
# we want it to interact with. Again the names match with those in the db
SQLGroupInfo    ftpgroup groupname gid members

# set min UID and GID - otherwise these are 999 each
SQLMinID        500
```

```
# create a user's home directory on demand if it doesn't exist
SQLHomedirOnDemand on

# Update count every time user logs in
SQLLog PASS updatecount
SQLNamedQuery updatecount UPDATE "count=count+1, accessed=now() WHERE
userid='%u'" ftpuser

# Update modified everytime user uploads or deletes a file
SQLLog  STOR,DELE modified
SQLNamedQuery modified UPDATE "modified=now() WHERE userid='%u'" ftpuser

# User quotas
# ===========
QuotaEngine on
QuotaDirectoryTally on
QuotaDisplayUnits Mb
QuotaShowQuotas on

SQLNamedQuery get-quota-limit SELECT "name, quota_type, per_session,
limit_type, bytes_in_avail, bytes_out_avail, bytes_xfer_avail,
files_in_avail, files_out_avail, files_xfer_avail FROM ftpquotalimits WHERE
name = '%{0}' AND quota_type = '%{1}'"

SQLNamedQuery get-quota-tally SELECT "name, quota_type, bytes_in_used,
bytes_out_used, bytes_xfer_used, files_in_used, files_out_used,
files_xfer_used FROM ftpquotatallies WHERE name = '%{0}' AND quota_type =
'%{1}'"

SQLNamedQuery update-quota-tally UPDATE "bytes_in_used = bytes_in_used +
%{0}, bytes_out_used = bytes_out_used + %{1}, bytes_xfer_used =
bytes_xfer_used + %{2}, files_in_used = files_in_used + %{3}, files_out_used
= files_out_used + %{4}, files_xfer_used = files_xfer_used + %{5} WHERE name
= '%{6}' AND quota_type = '%{7}'" ftpquotatallies

SQLNamedQuery insert-quota-tally INSERT "%{0}, %{1}, %{2}, %{3}, %{4}, %{5},
%{6}, %{7}" ftpquotatallies

QuotaLimitTable sql:/get-quota-limit
QuotaTallyTable sql:/get-quota-tally/update-quota-tally/insert-quota-tally

RootLogin off
RequireValidShell off
```

Reinicia el servidor ftp:

```
 /etc/init.d/proftpd restart
```

Si queremos poner un mensaje con el espacio disponible/usado por cada usuario añadir las siguientes líneas en el proftpd. (enviadas por Martin Mrajca)

```
SQLNamedQuery gettally  SELECT "ROUND((bytes_in_used/1048576),2) FROM
ftpquotatallies WHERE name='%u'"

SQLNamedQuery getlimit  SELECT "ROUND((bytes_in_avail/1048576),2) FROM
ftpquotalimits WHERE name='%u'"

SQLNamedQuery getfree   SELECT "ROUND(((ftpquotalimits.bytes_in_avail-
ftpquotatallies.bytes_in_used)/1048576),2) FROM
ftpquotalimits,ftpquotatallies WHERE ftpquotalimits.name = '%u' AND
ftpquotatallies.name = '%u'"

SQLShowInfo   LIST    "226" "Used %{gettally}MB from %{getlimit}MB. You have
%{getfree}MB available space."
```

Reiniciar el servidor porftpd de nuevo

```
 /etc/init.d/proftpd restart
```

Ahora vamos a crear un usuario de prueba:

```
$: mysql -u root -p
mysql > USE ftp;

INSERT INTO `ftpgroup` (`groupname`, `gid`, `members`) VALUES ('ftpgroup',
2001, 'ftpuser');

INSERT INTO `ftpquotalimits` (`name`, `quota_type`, `per_session`,
`limit_type`, `bytes_in_avail`, `bytes_out_avail`, `bytes_xfer_avail`,
`files_in_avail`, `files_out_avail`, `files_xfer_avail`) VALUES
('exampleuser', 'user', 'true', 'hard', 15728640, 0, 0, 0, 0, 0);

INSERT INTO `ftpuser` (`id`, `userid`, `passwd`, `uid`, `gid`, `homedir`,
`shell`, `count`, `accessed`, `modified`) VALUES (1, 'exampleuser',
'secret', 2001, 2001, '/home/www.example.com', '/sbin/nologin', 0, '', '');
quit;
```

Ahora vamos a crear un usuario de prueba:

Hemos creado un usuario exampleuser para probar el servicio. Agreguemos ahora una cuota para ese usuario de 15Mb:

Si queremos cambiarle la cuota tenemos que entrar a la base de datos y ejecutar :

```
update ftpquotalimits set bytes_in_avail=0 where name like 'ftpottn'
```

Hemos creado un usuario llamado ‘exampleuser’, con contraseña ’secret’, al que previamente le hemos asignado una cuota de disco y capacidad para subir y bajar archivos. Esto luego lo podremos hacer con cualquier gestor de base de datos como phpmyadmin, mysqladmin o mysql administrator

Si estamos actualizando desde una versión anterior hay que cambiar la directiva

SQLHomedirOnDemand on hay que cambiarla por **CreateHome on**

http://www.cyberciti.biz/tips/linux-installing-configuring-proftpd-ftp-server.html

proftpd + ssl/tls

Para poder configurar el soporte de transferencia encriptada de datos y autenticación en un servidor ftp, en este caso proftpd, es necesario compilar proftpd con el modulo mod_tls o en su defecto si utilizas una version superior a la 1.2.8, el soporte ya viene compilado y listo para utilizar, basta activar el soporte en el archivo de configuración (/etc/proftpd.conf).

Estos son los pasos para habilitar este servicio de manera de que soporte:

- encriptación de datos de control y datos en si.
- acepte sólo clientes con soporte ssl/tls

Lo primero, generar los certificados con el comando (ingresar los datos que se solicitan): openssl req -new -x509 -nodes -out ftpd-rsa.pem -keyout ftpd-rsa-key.pem

<Note>Al generar el certificado una de las preguntas es Common name: Hay que poner el nombre del equipo, por ejemplo, webserver.midominio.net o en su defecto localhost</note>

Esto genera dos archivos ftpd-rsa.pem , ftpd-rsa-key.pem que copiamos en /etc/ssl/certs.

Ahora, modificaremos el archivo de configuración /etc/proftpd.conf para habilitar el soporte y agregaremo las siguientes lineas:

```
# soporte TLS
# habilitar el modulo TLS
TLSEngine on
# logs
TLSLog /var/log/ftpd/tls.log
# Versión del protocolo a autilizar.
TLSProtocol SSLv23
# Si sólo permitimos el acceso con SSL
TLSRequired on
# Dónde se encuentran los certificados.
TLSRSACertificateFile /etc/ssl/certs/ftpd-rsa.pem
TLSRSACertificateKeyFile /etc/ssl/certs/ftpd-rsa-key.pem
# certificados de los usuarios
TLSVerifyClient off
# Si solicitamos el certificado del cliente.
TLSOptions NoCertRequest
```

Reiniciamos el servicio y probamos conectandonos con ftp-ssl o el filezilla

Para ver como van pasando los datos podemos usar tcpdump de la siguiente manera: tcpdump dst portrange 20-21 -qX

Podemos hacer esta prueba conectandonos desde clientes con/sin soporte ssl/tls y ver como pasan

los datos e identificar algunos textos como USER..

Otra forma es la siguiente:

```
openssl genrsa 1024 >host.key
openssl req -new -x509 -nodes -sha1 -days 365 -key host.key >host.cert
cat host.cert host.key > host.pem
chmod 0400 host.key host.pem
```

Y modificar el fichero /etc/proftpd.conf

```
TLSEngine on
TLSLog /var/log/proftpd/proftpd_ssl.log
TLSProtocol TLSv1
# Are clients required to use FTP over TLS when talking to this server?
TLSRequired off
# Server's certificate
TLSRSACertificateFile /etc/proftpd/host.cert
# Key to the server certificate
TLSRSACertificateKeyFile /etc/proftpd/host.key
# CA the server trusts
TLSCACertificateFile /etc/proftpd/host.pem
# Authenticate clients that want to use FTP over TLS?
TLSVerifyClient off
```

Debido a las últimas actualizaciones del servidor proftpd algunos de los comandos han sido sustituidos por otrs nuevos y por tanto hay que hacer los siguientes cambios para que todo funcione correctamente: añadir la línea siguiente al inicio del proftpd.conf

```
include /etc/proftpd/modules.conf
comentar la línea SQLAutenthicate users* groups*
añadir AuthOrder mod_sql.c
```

El archivo de configuracion resultante de todo es el siguiente:

```
#
# /etc/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes reload proftpd after modifications.
#
include /etc/proftpd/modules.conf

ServerName                      "SERVIDOR FTP"
ServerType                      standalone
DeferWelcome                    off
UseIPV6                         off

MultilineRFC2228                on
DefaultServer                   on
ShowSymlinks                    on

TimeoutNoTransfer               600
```

```
TimeoutStalled                  600
TimeoutIdle                     1200

DisplayLogin                    welcome.msg
DisplayFirstChdir               .message
ListOptions                     "-l"

DenyFilter                      \*.*/



# Port 21 is the standard FTP port.
Port                            21

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances                    30

# Set the user and group that the server normally runs at.
User                            nobody
Group                           nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask                           022  022
# Normally, we want files to be overwriteable.
AllowOverwrite                  on

# Delay engine reduces impact of the so-called Timing Attack described in
# http://security.lss.hr/index.php?page=details&ID=LSS-2004-10-02
# It is on by default.
#DelayEngine                    off

# Enjaulamos a los usuarios
DefaultRoot ~

# Usar SSL para encriptar las comunicaciones
TLSEngine on

    # logs
   TLSLog /var/log/ftpd/tls.log

    # Versión del protocolo a autilizar.
    TLSProtocol SSLv23

    # Si sólo permitimos el acceso con SSL
    TLSRequired off
```

```
# Server's certificate
TLSRSACertificateFile /etc/ssl/certs/ftpd-rsa.pem
TLSRSACertificateKeyFile /etc/ssl/certs/ftpd-rsa-key.pem

    #si le pedimos certificados a los usuarios
    TLSVerifyClient off

    # Si solicitamos el certificado del cliente.
    TLSOptions NoCertRequest

AuthOrder mod_sql.c
# The passwords in MySQL are encrypted using CRYPT
SQLAuthTypes            Plaintext Crypt
#SQLAuthenticate         users* groups*


# used to connect to the database
# databasename@host database_user user_password
SQLConnectInfo  ftp@localhost proftpd password


# Here we tell ProFTPd the names of the database columns in the "usertable"
# we want it to interact with. Match the names with those in the db
SQLUserInfo     ftpuser userid passwd uid gid homedir shell

# Here we tell ProFTPd the names of the database columns in the "grouptable"
# we want it to interact with. Again the names match with those in the db
SQLGroupInfo    ftpgroup groupname gid members

# set min UID and GID - otherwise these are 999 each
SQLMinID        500

# create a user's home directory on demand if it doesn't exist
SQLHomedirOnDemand on

# Update count every time user logs in
SQLLog PASS updatecount
SQLNamedQuery updatecount UPDATE "count=count+1, accessed=now() WHERE
userid='%u'" ftpuser

# Update modified everytime user uploads or deletes a file
SQLLog  STOR,DELE modified
SQLNamedQuery modified UPDATE "modified=now() WHERE userid='%u'" ftpuser

# User quotas
# ===========
QuotaEngine on
QuotaDirectoryTally on
QuotaDisplayUnits Mb
QuotaShowQuotas on
```

```
SQLNamedQuery get-quota-limit SELECT "name, quota_type, per_session,
limit_type, bytes_in_avail, bytes_out_avail, bytes_xfer_avail,
files_in_avail, files_ou$

SQLNamedQuery get-quota-tally SELECT "name, quota_type, bytes_in_used,
bytes_out_used, bytes_xfer_used, files_in_used, files_out_used,
files_xfer_used FROM $

SQLNamedQuery update-quota-tally UPDATE "bytes_in_used = bytes_in_used +
%{0}, bytes_out_used = bytes_out_used + %{1}, bytes_xfer_used =
bytes_xfer_used + %$

SQLNamedQuery insert-quota-tally INSERT "%{0}, %{1}, %{2}, %{3}, %{4}, %{5},
%{6}, %{7}" ftpquotatallies

QuotaLimitTable sql:/get-quota-limit
QuotaTallyTable sql:/get-quota-tally/update-quota-tally/insert-quota-tally

RootLogin off
RequireValidShell off
```

Configuración FTP privado

Si hemos decidio esta opcion deberemos de crear las cuentas de usuario antes. Las cuentas se crean como un usuario cualquiera de linux, es decir:

```
# su
# adduser <usuario>         #ej: adduser pepito
# passwd <usuario>          #ej: passwd pepito => pepitopassword
```

Acontinuacion deberemos de editar el archivo /etc/passwd y modificar la linea que hace referente al usuario pepito:

```
 vim /etc/passwd
```

Al editar el fichero, en el final de este nos aparecera una linea como esta(siguiendo el ejemplo anterior):

```
pepito:x:1007:100::/home/pepito:/bin/bash
```

Deberemos de modificarlo para que quede de asi:

```
pepito:x:1007:100::/home/ftp:/bin/false
```

Es decir, le decimos que su carpeta personal es donde tenemos el ftp, y su shell es una shell falsa(/bin/false). El password como os fijais aparece con un x, esto quiere decir que el password esta en el archivo /etc/shadow con una encriptacion MD5(mucho mas seguro que si ponemos el pasword en texto plano).

Asi lo haremos con todos los usuarios que queramos añadir.

Una vez listo los usuarios, continuaremos por donde nos hemos quedado con la edicion del archivo proftpd.conf:

```
<Directory /home/ftp/>        #Le decimos que el directorio del ftp es
/home/ftp y                  #acontinucacion le damos unas características
Umask 077 077
AllowOverwrite off
</Directory>
```

Si ademas queremos tener nuestra carpeta de subida deberemos de añadir, debajo de </Directory> lo siguiente:

```
<Directory /home/ftp/subir>  #nuestro directorio de subida se encontrara en
/home/ftp/subir
Umask 077 077
AllowOverwrite on
<Limit READ WRITE STOR>  #El directorio tendra acceso de lectura, escritura
y grabacion para todos(Allow All), en estos caso es muy recomendable
AllowAll #usar dentro del limit el order, denny y allow para que solo
ciertos usuarios pueden tener este privilegio, igual que cuando aceptavamos
o denegabamos permisos a ciertas ip's
</Limit>
</Directory>
```

Verificar sintaxis

```
proftpd -t6
```