Servidor FTP multiusuari
amb VSFTPD + PAM + MySQL

Avui instal·larem un servidor FTP convencional però bastant ràpid i segur en un sistema operatiu Ubuntu, basat en Debian GNU/Linux. El servidor requerirà nom i contrasenya per a cada usuari que vulgui accedir, i cada usuari podrà anar adreçat a un directori diferent i modificar-ne el contingut (molt convenient per a un servidor-web compartit). Aquesta guia evita la creació de múltiples usuaris reals al sistema operatiu, i tots els usuaris virtuals actuen amb un mateix compte del sistema.

El servei FTP tradicional consisteix en què els usuaris del sistema operatiu tenen accés al sistema de fitxers amb les seves mateixes credencials i atribucions, i addicionalment hi ha un compte d'usuari anònim per a què públicament es pugui descarregar determinats continguts. La característica especial, doncs, d'aquesta instal·lació és que el cens d'usuaris FTP s'emmagatzema en una base de dades, i passen a ser "usuaris virtuals" en comptes de "usuaris reals" del sistema operatiu; addicionalment s'inhabilita l'accés anònim.

Aquesta guia es basa en el programari servidor de FTP **vsftpd** (vsftpd.beasts.org), però existeixen alternatives tant competents com **ProFTPD** (www.proftpd.org).

Comencem;

Amb el sistema operatiu ja instal·lat, actualitzat i en funcionament, ens hem d'assegurar que tenim el servidor FTP (vsftpd), els mòduls d'autenticació (pam) i el sistema de base de dades (MySQL). Si no és així, ho podem fer amb les instruccions de terminal/consola:

```
sudo apt-get install mysql-server
sudo apt-get install libpam-runtime libpam-modules
sudo apt-get install libpam-mysql
sudo apt-get install vsftpd
```

El MySQL Server en instal·lar-se demanarà que li establim una contrasenya per a l'usuari administrador (root), que necessitarem quan volem fer determinades operacions.

També es poden utilitzar les instruccions d'instal·lació per a saber que els paquets estan instal·lats. Ara es tractarà de configurar-ho tot per a què els diferents programes treballin junts.

Si la teva distribució de GNU/Linux no té el paquet "libpam-mysql" a l'abast, el pots descarregar de la pàgina del projecte *pam-mysql.sourceforge.net* ("Released Files") i instal·lar-lo manualment amb la instrucció:

```
sudo dpkg --install nomdelfitxer.deb
```

- Per a poder restablir la configuració dels fitxers de text que es modifiquen (en cas que alguna cosa falli o volem tornar enrere), és recomanable fer una còpia de cada original. Per exemple: abans d'editar "vsftpd.conf" copiar-lo a "vsftpd.conf.original".
- Si no saps com editar els fitxers de text des d'una consola o terminal, et proposo el programa "nano", que per a utilitzar-la com a superusuari aniria així (exemple):

  ```
  sudo nano /etc/vsftpd.conf
  ```

  (Si el fitxer no existeix, el crea. Per a sortir polsar [Control] + [x])

Configuració de la base de dades

1. Ens connectem a la consola del servidor MySQL (ens demanarà la contrasenya del propi superusuari "root" de MySQL):

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

2. Hi creem una base de dades pels comptes d'usuaris virtuals:

```
CREATE DATABASE vsftpd;
```

3. Creem una taula per a enregistrar els comptes d'accés (fixeu-vos en els noms dels camps):

```
CREATE TABLE vsftpd.usuaris (
nrregistre int AUTO_INCREMENT NOT NULL,
nom varchar(30) binary NOT NULL,
contrasenya varchar(50) binary NOT NULL,
estat varchar(30) binary NOT NULL,
primary key(nrregistre)
);
```

4. Creem una taula per a enregistrar els intents d'accés (fixeu-vos en els noms dels camps):

```
CREATE TABLE vsftpd.bitacola (missatge varchar(255),
usuari varchar(20),
proces int,
servidor char(32),
client char(32),
moment timestamp
);
```

5. Donem permisos a un nou usuari de MySQL per a què el servidor FTP accedeixi a través de PAM només a allò imprescindible:

```
GRANT SELECT ON vsftpd.usuaris TO vsftpd@localhost IDENTIFIED BY 'contrasenya1';
GRANT INSERT ON vsftpd.bitacola TO vsftpd@localhost IDENTIFIED BY 'contrasenya1';
FLUSH PRIVILEGES;
```

(personalitzeu la contrasenya1)

6. Donem permisos a un nou usuari de MySQL diferent per a l'administració d'usuaris:

```
GRANT INSERT,SELECT,DELETE ON vsftpd.usuaris TO ftpadmin@localhost IDENTIFIED BY 'contrasenya2';
GRANT SELECT,DELETE ON vsftpd.bitacola TO ftpadmin@localhost IDENTIFIED BY 'contrasenya2';
FLUSH PRIVILEGES;
```

(personalitzeu la contrasenya2, que sigui diferent)

7. Ens desconnectem de la consola del servidor MySQL:

```
quit
```

Configuració del sistema operatiu

1. Ens hem d'assegurar que al registre de programes de consola/terminal (fitxer **/etc/shells**) hi ha una línia com aquesta:

```
/bin/false
```

Si no hi és, l'afegim al final. Això permet crear els comptes d'usuari dels programes impedint que siguin utilitzats per a accedir a l'ordinador via terminal.

2. Creem un directori per als perfils d'usuari FTP:

```
sudo mkdir /etc/vsftpd
```

3. Creem a dins un altre directori per als usuaris FTP sense perfil encara fet:

```
sudo mkdir /etc/vsftpd/buit
```

4. Fixem el directori buit sense permisos d'escriptura:

```
sudo chmod 555 /etc/vsftpd/buit
```

5. Creem un grup i compte d'usuari per al servidor FTP:

```
sudo groupadd vsftpd
sudo useradd -d /etc/vsftpd -s /bin/false -g nogroup vsftpd
```

6. Creem un grup i compte d'usuari per als clients FTP:

```
sudo groupadd ftp
sudo useradd -d /etc/vsftpd/buit -s /bin/false -g ftp ftp
```

Si ja existia (*user ftp exists*) convé que el modifiquem:

```
sudo usermod -d /etc/vsftpd/buit -s /bin/false -g ftp ftp
```

Configuració de l'autenticador

Pluggable Authentication Modules (PAM) és un sistema múltiple per a què els programes puguin autenticar la identitat d'usuaris i d'altres agents de l'entorn informàtic. L'utilitzem aquí per a què el servidor VSFTPD no hagi de fer aquesta tasca, i simplement consulti a PAM si l'usuari que truca a la porta es correspon al cens de la base de dades.

Revisem els paràmetres del perfil de VSFTPD per al PAM, per tal que es facin les consultes a MySQL. Obrim el fitxer **/etc/pam.d/vsftpd** amb un editor de text i:

1. Per a què no s'exigeixi l'existència dels usuaris al sistema operatiu, desactivem "pam_ftp.so", "common-account", "common-auth" i "pam_shells.so" afegint el símbol "#" a l'inici de cada línia on apareguin:

```
# pam_ftp.so.
#@include common-account
#@include common-auth
#auth    required        pam_shells.so
```

2. Per a especificar les credencials d'accés, taules i camps a consultar a la base de dades MySQL, afegim aquestes dues llaargues línies al final del fitxer:

```
auth  required    pam_mysql.so      verbose=0                  user=vsftpd
passwd=contrasenya1 host=localhost db=vsftpd table=usuaris usercolumn=nom
passwdcolumn=contrasenya      statcolumn=estat      crypt=2      sqllog=true
logtable=bitacola        logmsgcolumn=missatge        logusercolumn=usuari
logpidcolumn=proces loghostcolumn=client logtimecolumn=moment


account     required    pam_mysql.so      verbose=0             user=vsftpd
passwd=contrasenya1 host=localhost db=vsftpd table=usuaris usercolumn=nom
passwdcolumn=contrasenya      statcolumn=estat      crypt=2      sqllog=true
logtable=bitacola        logmsgcolumn=missatge        logusercolumn=usuari
logpidcolumn=proces loghostcolumn=client logtimecolumn=moment
```

(La contrasenya1 de les línies ha de ser la mateixa que hem fixat per a l'usuari "vsftpd" de MySQL)

Configuració del servei FTP

Revisem els paràmetres de la configuració bàsica de VSFTPD, editant el fitxer **/etc/vsftpd.conf** i fixant els què especifiquem de la següent manera (cal buscar-los en el fitxer, i si no hi són afegir-los al final):

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
xferlog_enable=YES
nopriv_user=vsftpd
chroot_local_user=YES
secure_chroot_dir=/etc/vsftpd/buit
pam_service_name=vsftpd
# En octal: 0022 xor 0777 = permisos 755
local_umask=0022
file_open_mode=0777
dirmessage_enable=NO
# Nombre màxim de sessions d'usuarix connectadxs simultàniament
max_clients=50
# Nr. màxim de ss. d'usuarix simultànies per un mateix origen (IP).
max_per_ip=5
# Unificació dels clients com a únicx usuarix del sistema
guest_enable=YES
# Usuarix del sistema amb què actuaran els usuaris FTP
guest_username=ftp
# On trobar les configuracions específiques de cada usuarix
user_config_dir=/etc/vsftpd
# Directori FTP predeterminat. Si no creem un perfil, no toquin res.
local_root=/etc/vsftpd/buit
# Privilegis locals per a escriure, per a usuarixs FTP remotxs.
virtual_use_local_privs=YES
# Emmascarar la informació d'usuarix/grup en directoris com a "ftp"
hide_ids=YES
```

Alguns dels paràmetres no són imprescindibles així, però d'aquesta manera també funciona. El paràmetre "local_umask" és per als permisos que es fixaran als fitxers que pugin els usuaris via FTP; per defecte serien 077, però amb 755 permet que l'usuari propietari dels fitxers i carpetes pugui manipular plenament i en canvi el públic d'una web només pugui llegir.

Posada en marxa

Amb aquesta instrucció reiniciem el servei de VSFTPD per a què apliqui la nova configuració, o també l'iniciem si estava aturat:

```
sudo /etc/init.d/vsftpd restart
```

Com crear un usuari FTP

1. El directori on ha d'accedir l'usuari ha d'estar creat, amb propietari "ftp" i amb permisos per a operar:

```
sudo mkdir /ruta/al/seu/directori
sudo chown -R ftp:ftp /ruta/al/seu/directori
sudo chmod -R 755 /ruta/al/seu/directori
```

2. Amb aquesta instrucció tindrem un nou compte d'usuari a la base de dades:

```
mysql -u ftpadmin --password=contrasenya2 -e "INSERT INTO vsftpd.usuaris
(nom, contrasenya) VALUES ('elnomdusuari', PASSWORD('lacontrasenya'));"
```

Aquests "elnomdusuari" i "lacontrasenya" (així com la localització pública del servidor) són les dades que podrem donar a les persones que volem que es connectin per FTP.

3. Creem un fitxer de text per al perfil d'usuari com a **/etc/vsftpd/elnomdusuari** on hi escriurem la ruta del directori al qual accedirà l'usuari via FTP:

```
local_root=/ruta/al/seu/directori
```

En aquest fitxer podem afegir qualsevol dels paràmetres que són vàlids a **/etc/vsftpd.conf** per tal de personalitzar-los per aquest usuari en concret. També el podem blindar una mica establint permisos:

```
sudo chmod -R 440 /etc/vsftpd/elnomdusuari
```

Com eliminar un usuari FTP

1. Eliminem l'usuari de la base de dades:

```
mysql -u ftpadmin --password=contrasenya2 -e "DELETE FROM vsftpd.usuaris
WHERE nom = 'elnomdusuari';"
```

2. Eliminem el perfil FTP d'usuari:

```
sudo rm /etc/vsftpd/elnomdusuari
```

3. Si volem, podem eliminar el seu directori (es perdrà tot el contingut !):

```
sudo rm -R /ruta/al/seu/directori
```

Problemes comuns, primers auxilis

- **Missatge "500 OOPS: cannot change directory:/etc/vsftpd/buit" del servidor en intentar entrar com a usuari des d'un programa FTP-client:** En crear el compte no has creat el seu perfil (/etc/vsftpd/elnomdusuari), o bé no hi has especificat correctament la ruta del paràmetre "local_root". Revisa també els permisos del directori del qual dóna error.
- **En entrar com a usuari des d'un programa FTP-client es veu un directori buit i no s'hi puc fer res (/etc/vsftpd/buit):** En crear l'usuari no has creat el seu perfil (/etc/vsftpd/elnomdusuari), o bé no hi has especificat correctament la ruta del paràmetre "local_root", o bé el fitxer de perfil té permisos massa restrictius.
- **No aconsegueixo accedir amb un mateix usuari a diferents llocs web:** Si pretens utilitzar el servidor FTP per a mantenir llocs virtuals d'un servidor web, i t'agradaria que es pogués entrar amb un mateix nom d'usuari per a accedir diferenciant el nom de domini o l'adreça IP, et convé fer ús del programari-interfície de xarxa *xinetd* per a fer crides al VSFTPD especificant diferent fitxer de configuració a la línia de la comanda. Més informació a:

  es.wikipedia.org/wiki/Xinetd

  www.xinetd.org
- **Tinc problemes i necessito trobar d'on venen:** Pots consultar diverses bitàcoles per a veure el què passa amb les entrades de clients FTP:
  1. Bitàcola del servidor FTP VSFTPD: fitxer de text **/var/log/vsftpd.log**
  1. Bitàcola de l'autenticador PAM (per a tots els accessos al sistema): fitxer de text **/var/log/auth.log**
  1. Bitàcoles del servidor de bases de dades MySQL: fitxers de text **/var/log/mysql.log** i **/var/log/mysql.err**
  1. Bitàcola entre VSFTPD i PAM (èxits i fracassos en els intents d'entrada normal dels usuaris FTP). Podem veure les anotacions a la base de dades amb la instrucció:

     ```
     mysql -u ftpadmin --password=contrasenya2 -e "SELECT * FROM vsftpd.bitacola;"
     ```

     Posem buidar (eliminar tot l'històric) aquesta bitàcola amb la instrucció:

     ```
     mysql -u ftpadmin --password=contrasenya2 -e "DELETE FROM vsftpd.bitacola;"
     ```
  1. Cens d'usuaris registrats. Podem veure tots els usuaris virtuals amb la instrucció:

     ```
     mysql -u ftpadmin --password=contrasenya2 -e "SELECT * FROM vsftpd.usuaris;"
     ```

     Podem consultar un sol compte d'usuari amb la instrucció:

     ```
     mysql -u ftpadmin --password=contrasenya2 -e "SELECT * FROM vsftpd.usuaris WHERE nom = 'elnomdusuari';"
     ```
  1. Bitàcola de l'instal·lador Debian de programes: fitxer de text **/var/log/installer/status**
- **Necessito controlar la quantitat de dades que puja un usuari (quotes d'espai):** Com podies imaginar, en aquesta guia no trobaràs respostes ni piestes per a tot, doncs a dia d'avui jo tampoc no sé quin és el camí per aplicar aquesta funcionalitat des de VSFTPD amb usuaris virtuals.

Més seguretat, control de la velocitat, comprovacions

Cal tenir en compte que en aquesta guia s'ha donat la manera d'escriure les contrasenyes de forma visible (per a facilitar automatitzacions amb *script*), així que les instruccions escrites queden emmagatzemades tal qual a l'historial de la consola. Per a buidar després aquest historial i també l'historial del MySQL pots utilitzar les següents instruccions:

```
rm $HOME/.bash_history
rm $HOME/.mysql_history
```

(fa efecte si seguidament tanquem la sessió de consola/terminal)

Si no vols deixar escrites les contrasenyes amb les línies d'instruccions en cridar MySQL, pots canviar el seu paràmetre `--password=contrasenya` per `-p` , i demanarà teclejar la contrasenya de forma no visible. Un exemple:

```
mysql -u ftpadmin -p -e "SELECT * FROM vsftpd.usuaris;"
```

Un salt en seguretat és l'autenticació del servidor, és a dir, que un client FTP tingui la certesa de connectar-se a l'autèntic servidor i no a un pescador de contrasenyes. Això, i la comunicació encriptada, s'aconsegueix amb la capacitat SSL del servidor. Però l'objectiu d'aquesta guia és ajudar a posar en marxa un servidor FTP de forma senzilla, doncs consulteu manuals més avançats per a aprendre sobre comunicacions SSL, o barreres adaptatives com *ban2fail*.

El VSFTPD permet una mica de control de l'ample de banda dedicat a les connexions FTP. Es pot establir en *bytes* per segon a **/etc/vsftpd.conf** amb els paràmetres "local_max_rate" i "anon_max_rate". Referiu-vos a la documentació de VSFTPD per a més detalls o novetats.

Aquesta guia publicada en català i castellà el 14 de febrer del 2008 per Narcís Garcia Langa està comprovada amb la Ubuntu GNU/Linux 7.10 server, comptant amb la versió de sèrie 0.6.2 de PAM-MySQL (però pot funcionar amb la majoria de variants de Debian). Referències útils:

- www.ubuntu.com
- doc.ubuntu.com/ubuntu/serverguide/C/
- www.debian.org

No hagués estat possible completar la guia sense:

- Alejandro Ayuso: monocaffe.blogspot.com/2007/09/servidor-virtual-de-ftp-seguro-con.html
- La documentació oficial de vsftpd de Chris Evans: vsftpd.beasts.org
- La documentació de Miles Brennan: www.brennan.id.au/14-FTP_Server.html
- La documentació oficial de PAM-MySQL de Moriyoshi Koizumi:

  pam-mysql.sourceforge.net/Documentation/
- El manual de referència de MySQL: dev.mysql.com/doc/refman/5.0/es/
- El codi font publicat per Gunay Arslan
- o la gran quantitat de preguntes i respostes publicades a Internet per la inquieta comunitat informàtica, lliure. Especial esment mereix el GiLUG (www.gilug.org)