

Shockware Gaming S.A. | Crédito de Síntesi 2014

VSFTPD

Servidor FTP para la transmisión y compartición de archivos.



•¿Qué es un “FTP”?

Significados

“... El acrónimo de **FTP** es “**protocolo de transferencia de ficheros**” (*File Transfer Protocol*), es un software basado en la arquitectura **cliente-servidor** que permite a usuarios transferir ficheros entre ordenadores en una red TCP/IP. ...”

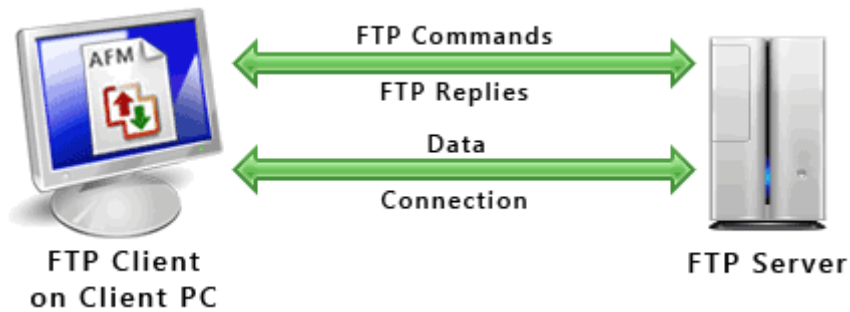
“... FTP es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Ficheros) y es el ideal para transferir grandes bloques de datos por la red ...”

“... El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red **20** y el **21** ...”

“... Un problema básico de FTP es que está pensado para ofrecer la máxima **velocidad en la conexión**, pero no la máxima **seguridad** ...”

“... Para solucionar este problema son de gran utilidad aplicaciones como **scp** y **sftp**, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico. ..”

El FTP es muy usado en el **mantenimiento** de una página, ya que sirve para transferir archivos fácilmente, sin utilizar los malos servicios por web. Se puede manejar los archivos como si se tratase del Explorador de Windows.



•¿Cómo funciona?

El funcionamiento es sencillo. Una persona desde su ordenador invoca un programa cliente FTP para conectar con otro ordenador, que a su vez tiene instalado el programa servidor FTP. Una vez establecida la conexión y debidamente autenticado el usuario con su contraseña, se pueden empezar a intercambiar archivos de todo tipo.

Primero debemos conseguir un programa que maneje el FTP para facilitarnos las tareas. Por ejemplo los programas más populares son el FileZilla, CuteFTP, WS_FTP; los cuales son realmente buenos.

Los requisitos para conectarnos a un servidor FTP son los siguientes:

1.La dirección del servidor: primero se debe introducir una dirección que normalmente encontraremos en una página web. Esta dirección puede introducirse de dos maneras, en forma de dirección IP o con un nombre similar a las páginas web. Por ejemplo un FTP en dirección IP puede ser 200.38.49.198, pero también lo podemos encontrar como "ftp://ftp.alegsa.com.ar". Una vez introducido este dato, pasaremos al siguiente paso.

2.Nombre y contraseña: Ahora se debemos saber el nombre y la contraseña con que se puede ingresar al FTP. Si es un servidor de acceso público encontrarás la información fácilmente, pero hay casos en donde se requiere un previo registro.

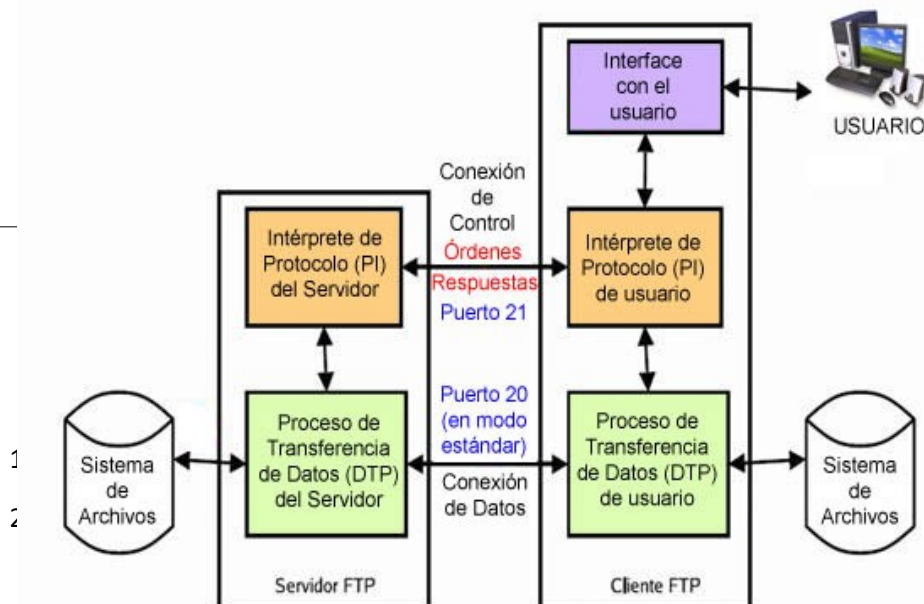
3.Puerto: El puerto tradicional del FTP es el 21, éste está como predeterminado en todos los programas FTP; aunque a veces el puerto no es 21, encontrará el número en la página web donde obtuvo la dirección. Normalmente encontraremos la opción para cambiar el

puerto en las propiedades del programa.

Pero si todo marcha bien, verás en forma de explorador los archivos del servidor. Ya ahí podrás entrar o salir de un directorio (carpeta) y podremos bajar archivos con solo hacer seleccionar el archivo y hacer un clic en un botón.

Fi

Finalmente debemos aclararles que el servicio de FTP no está exento de archivos infectados, por esto debe ser cauteloso al ejecutar ciertos archivos bajados de la Red.



mo y sus op-
:n su home, es

Empezaremos habilitando el usuario anónimos, descomentando esta línea:

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
..
```

Habilitaremos también la opción de “escribir” en el servidor.

```
# Uncomment this to enable any form of FTP write command.
write_enable=YES|
```

```
# Uncomment this to enable any form of FTP write command.  
write_enable=NO  
#
```

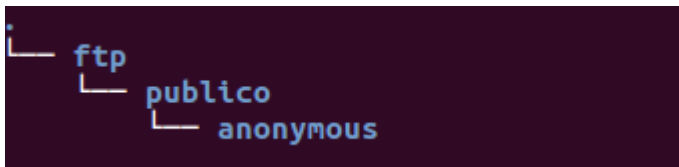
Descomentaremos también la opción que le permite al usuario anónimo cargar o subir archivos al servidor y añadiremos una segunda línea, para especificar cuál será la carpeta de arranque del usuario anónimo.

```
anon_upload_enable=YES  
anon_root=/srv/ftp/publico  
#
```

Habilitaremos también la opción de que el usuario anónimo pueda crear nuevos directorios.

```
# Uncomment this if you want the anonymous FTP user to be able to create  
# new directories.  
anon_mkdir_write_enable=YES
```

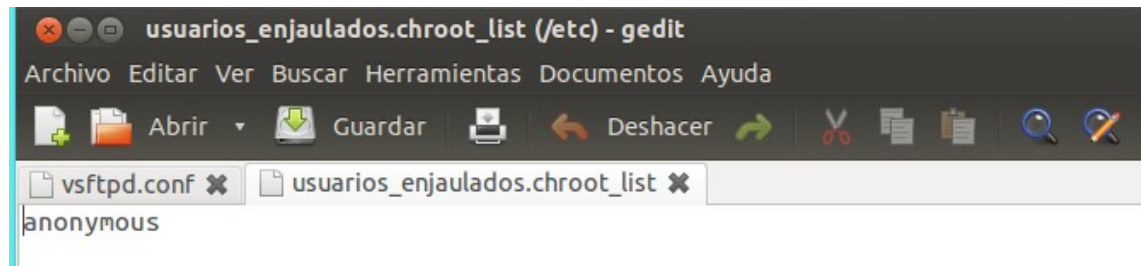
- Una vez habilitado las opciones del usuario anónimo, procederemos a crear las carpetas en las que se accederá de forma anónima. Nos vamos a la ruta /srv dentro de esta carpeta encontraremos la carpeta /ftp le asignaremos los permisos correspondientes de lectura y ejecución para todos, "chmod 555 ftp/", seguidamente dentro de esta carpeta crearemos la carpeta publico/ a la que le asignaremos los mismos permisos de ejecución y lectura para todos chmod 555 publico/ dentro de la carpeta publico crearemos la carpeta anonymous/ y le asignaremos los permisos 775, es decir chmod 775 anonymous, todos los permisos a los usuarios y grupos y a otros usuarios solo lectura y escritura.



- En la siguiente opción enjaularemos al usuario anonymous en su home, para ellos descomentaremos y habilitaremos las siguientes líneas en el archivo vsftpd.conf

```
chroot_local_user=NO  
chroot_list_enable=YES  
# (default follows)  
chroot_list_file=/etc/usuarios_enjaulados.chroot_list  
..
```

- Seguidamente nos vamos a la carpeta /etc y creamos el archivo que hemos indicado para enjaular usuarios "gedit usuarios_enjaulados.chroot_list" y dentro de este archivo escribimos el nombre de los usuarios, en este caso escribimos anonymous y aquí podemos añadir futuros usuarios que queremos que estén enjaulados en su home.



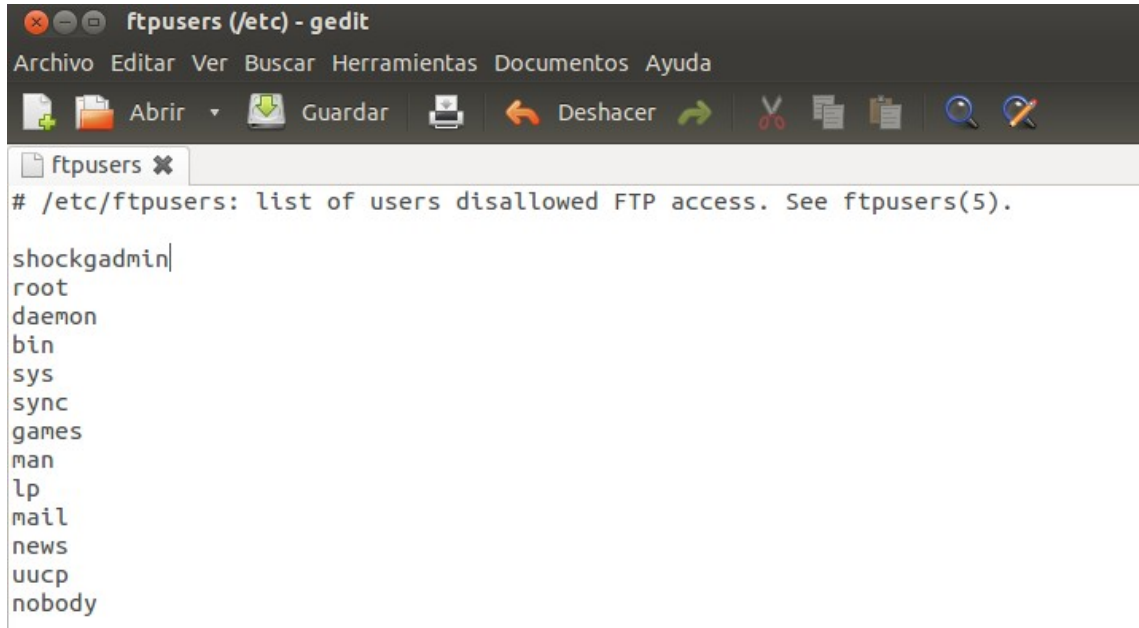
- Para finalizar especificaremos nuestro mensaje de bienvenida al servidor FTP para ellos nos vamos de nuevo al archivo vsftpd.conf y descomentamos la siguiente línea y especificamos nuestro mensaje personalizado, reiniciamos el servicio.

```
# You may fully customise the login banner string:  
ftpd_banner=Bienvenidos al Servidor FTP de shockwaregaming / Welcome to Server FTP of Shockwaregaming  
#
```

- Comprobamos la conexión desde un cliente y no especificamos un usuario ni contraseña, para acceder de forma anónima y vemos que nos conectamos correctamente.

```
Estado: Conexión establecida, esperando el mensaje de bienvenida...  
Respuesta: 220 Bienvenidos al Servidor FTP de shockwaregaming / Welcome to Server FTP of Shockwaregaming  
Comando: USER anonymous  
Respuesta: 331 Please specify the password.  
Comando: PASS *****
```

- Denegaremos el acceso al usuario shockgadmin, que es el usuario local del propio servidor, para ello nos vamos a la ruta /etc y editamos el archivo ftpusers con el comando gedit /etc/ftpusers, en este archivo se encuentran todos los usuarios que no tendrán acceso al ftp, agregamos el usuario shockgadmin:



```
ftpusers (/etc) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
ftpusers x
# /etc/ftpusers: list of users disallowed FTP access. See ftpusers(5).

shockgadmin|
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
nobody
```

Reiniciamos el servicio y comprobamos el acceso con el usuario shockgadmin

```
Respuesta: 220 Bienvenidos al Servidor FTP de shockwaregaming / Welcome to Server FTP of Shockwaregaming
Comando: USER shockgadmin
Respuesta: 530 This FTP server is anonymous only.
Error: No se pudo conectar al servidor
Estado: Esperando para reintentar...
Estado: Conectando a 192.168.1.110:21...
Estado: Conexión establecida, esperando el mensaje de bienvenida...
Respuesta: 220 Bienvenidos al Servidor FTP de shockwaregaming / Welcome to Server FTP of Shockwaregaming
Comando: USER shockgadmin
Respuesta: 530 This FTP server is anonymous only.
Error: No se pudo conectar al servidor
```

Denegamos el acceso la escritura en la raíz debido a la inseguridad que se genera permitiendo ver los archivos de la raíz y crear carpetas documentos en ella, además de que el usuario anonymous lo usara cualquiera al que se le facilite nuestra dirección IP.

Version final FTP

Como alternativa para enjaular los usuarios en su homes, hemos utilizado la siguiente configuración en el archivo vsftpd.conf, hemos especificado solo los parámetros necesarios, además de añadir en el archivo vsftpd.chroot_list los usuarios que solo tendrán acceso a su propio home.

Esta es la configuración del archivo vsftpd.conf:

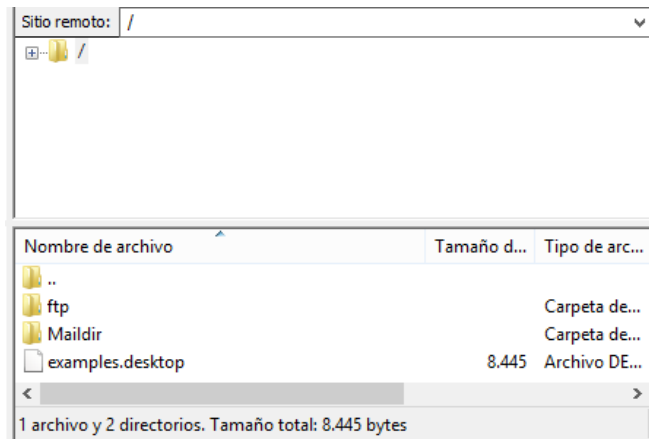
```
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
ftpd_banner=Bienvenido al FTP de Shockware Gaming
chroot_local_user=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/private/vsftpd.pem
chroot_local_user=NO
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
```

En el archivo vsftpd.chroot_list hemos especificado los usuarios que están tendrán acceso solo a su home y dentro de su home hay una carpeta llamada ftp, donde se almacenaran todos los archivos que el usuario desee compartir a través de su ftp.

Este es el archivo vsftpd.chroot_list:

```
admin
adm01
adm02
alm01
alm02
cal01
cal02
com01
com02
fin01
fin02
public
rel01
rel02
rhh01
rhh02
```

Los usuarios pueden ver su carpeta personal, pero solo podrán crear carpeta dentro de la carpeta ftp que se almacena en su home.



Los permisos son los siguientes, en la home del usuario es solo de acceso 2555 y dentro de cada \$HOME tendrá una carpeta que se llama ftp donde dentro tendrá los permisos 755 y que solamente podrá escribir por FTP. Ya que utilizamos los perfiles de SAMBA para el modo de acceso con el SERVIDOR.

```
drwxrwsr-x 12 root ShockwareGaming 4096 may  9 16:47 ../
dr-xr-xr-x  4 com01 Comercial        4096 may 26 19:33 com01/
dr-xr-xr-x  4 com02 Comercial        4096 may 26 19:34 com02/
```