

DESPLIEGUE DE APLICACIONES WEB

GUÍA DE RESOLUCIÓN DE LA TAREA 03

Jesús Bono – IES CRISTÓBAL DE MONROY

Contenido

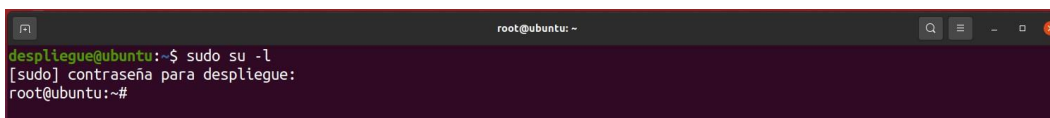
Actividad 1.- Instalación de un servidor FTP.	2
Actividad 2.- Configurar el acceso anónimo para el servidor FTP.....	4
Actividad 3.- Acceso al servicio FTP mediante usuarios virtuales.....	7
Actividad 4.- Configuración del servidor FTP para conexión segura con TLS.....	8
Actividad 5.- Instalación y configuración de un cliente gráfico FTP para conexión segura con TLS.	11
Actividad 5.1.- Instalación de Filezilla FTP Client.	12
Actividad 5.2.- Conexión con usuario anónimo.	12
Actividad 5.3.- Conexión con usuario virtual.	15
Actividad 5.4.- Conexión segura con TLS.....	15
Actividad 6.- Uso de un navegador como cliente FTP.....	17
Actividad 7.- Configuración del servicio FTP en modo activo o pasivo.....	17

Actividad 1.- Instalación de un servidor FTP.

Realiza la instalación del servidor **FTP ProFTPD** en tu servidor Ubuntu/Debian desde el repositorio, comprobando su funcionamiento e indicando cómo se inicia y cómo se para, cómo se comprueba su estado y localiza en el fichero de configuración la línea en la que especifica que se ha instalado en **modo “standalone”**. Documenta el proceso de instalación y comprueba el funcionamiento conectándote desde la consola de comandos con tu usuario de sistema.

- Para instalar PROFTPD abrimos una ventana de terminal y nos identificamos como superusuario (sudo su):

\$ sudo su

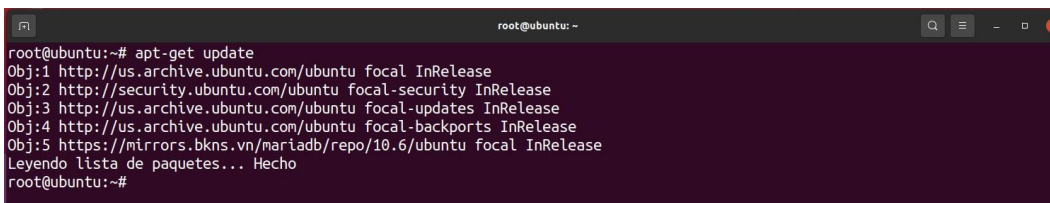


```
despliegue@ubuntu:~$ sudo su -l
[sudo] contraseña para despliegue:
root@ubuntu:~#
```

- Actualizamos nuestro Ubuntu por si hay alguna versión más reciente de las librerías y aplicaciones:

\$ apt-get update

\$ apt-get upgrade



```
root@ubuntu:~# apt-get update
Obj:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Obj:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Obj:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Obj:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Obj:5 https://mirrors.bkns.vn/mariadb/repo/10.6/ubuntu focal InRelease
Leyendo lista de paquetes... Hecho
root@ubuntu:~#
```

- Ahora ya podemos instalar el paquete ProFTPD:

\$ apt-get install proftpd



```
root@ubuntu:~# apt-get install proftpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Nota, seleccionando «proftpd-basic» en lugar de «proftpd»
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libfprint-2-tod1 libllvm10
Utilice «apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libhiredis0.14 libmemcached11 libmemcachedutil2 proftpd-doc
Paquetes sugeridos:
  openssh-inetd | inet-superserver proftpd-mod-ldap proftpd-mod-mysql proftpd-mod-odbc proftpd-mod-pgsql
  proftpd-mod-sqlite proftpd-mod-geoip proftpd-mod-snmp
Se instalarán los siguientes paquetes NUEVOS:
  libhiredis0.14 libmemcached11 libmemcachedutil2 proftpd-basic proftpd-doc
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 3.509 kB de archivos.
Se utilizarán 9.696 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Como hemos podido comprobar, durante la instalación no nos ha preguntado el modo, por lo que tendremos que revisar el fichero `/etc/proftpd/proftpd.conf` para asegurarnos que se ha instalado en modo ‘standalone’ (seguro que sí, porque es el modo por defecto)

\$ sudo nano /etc/proftpd/proftpd.conf

```
root@ubuntu: /etc/proftpd
GNU nano 4.8 proftpd.conf
# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#
# Includes DSO modules
Include /etc/proftpd/modules.conf
# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 on
# If set on you can experience a longer connection delay in many cases.
IdentLookups off
ServerName "Debian"
# Set to inetd only if you would run proftpd by inetd/xinetd.
# Read README.Debian for more information on proper configuration.
ServerType standalone
DeferWelcome off
```

Efectivamente, vemos en que la directiva 'ServerType' tiene el valor 'standalone'.

ara que se inicie con el servidor, ejecutamos el comando:

\$ systemctl enable proftpd

- Si queremos comprobar el estado del servicio tendremos que ejecutar el comando:

\$ systemctl status proftpd

```
root@ubuntu: ~
root@ubuntu:~# systemctl start proftpd
root@ubuntu:~# systemctl enable proftpd
proftpd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable proftpd
root@ubuntu:~# systemctl status proftpd
● proftpd.service - LSB: Starts ProFTPD daemon
   Loaded: loaded (/etc/init.d/proftpd; generated)
   Active: active (running) since Thu 2022-02-24 01:38:08 PST; 2min 4s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 1 (limit: 4588)
   Memory: 2.1M
    CGroup: /system.slice/proftpd.service
            └─2905 proftpd: (accepting connections)

feb 24 01:38:08 ubuntu systemd[1]: Starting LSB: Starts ProFTPD daemon...
feb 24 01:38:08 ubuntu proftpd[2896]: * Starting ftp server proftpd
feb 24 01:38:08 ubuntu proftpd[2904]: 2022-02-24 01:38:08,468 ubuntu proftpd[2904]: processing configuration directory
feb 24 01:38:08 ubuntu proftpd[2896]: ...done.
feb 24 01:38:08 ubuntu systemd[1]: Started LSB: Starts ProFTPD daemon.
root@ubuntu:~#
```

- Ahora ya tenemos disponible nuestro servicio de FTP. Para asegurarnos de poder acceder desde fuera de nuestra máquina, debemos permitir el acceso a través del firewall de Ubuntu (UFW). En este caso habilitaremos el acceso a ftp y ftps:

\$ ufw allow ftp

\$ ufw allow ftps

```
root@ubuntu:~# ufw allow ftp
Regla añadida
Regla añadida (v6)
root@ubuntu:~#
```

```
root@ubuntu:~# ufw allow ftps
Regla añadida
Regla añadida (v6)
root@ubuntu:~#
```

El servicio de FTP permite el acceso de los usuarios de sistema, por lo que podríamos comprobar el funcionamiento usando la cuenta con la que nos “logueamos” en Ubuntu:

```
root@ubuntu:~# ftp
ftp> o
(to) localhost
Connected to localhost.
220 ProFTPD Server (Debian) [::ffff:127.0.0.1]
Name (localhost:despliegue): despliegue
331 Contraseña necesaria para despliegue
Password:
230 Usuario despliegue conectado
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 Comando PORT exitoso
150 Abriendo ASCII modo conexión de datos para file list
drwxr-xr-x  2 despliegue despliegue  4096 Oct 18 09:37 Descargas
drwxr-xr-x  2 despliegue despliegue  4096 Oct 20 07:58 Documentos
drwxr-xr-x  2 despliegue despliegue  4096 Feb  3 08:55 Escritorio
drwxr-xr-x  2 despliegue despliegue  4096 Feb  3 16:09 Imágenes
-rw-rw-r--  1 despliegue despliegue 1018 Dec 15 16:52 Instalación de MariaDB
drwxr-xr-x  2 despliegue despliegue  4096 Oct 18 09:37 Música
drwxr-xr-x  2 despliegue despliegue  4096 Oct 18 09:37 Plantillas
drwxr-xr-x  2 root      root      4096 Oct 26 18:00 public_html
drwxr-xr-x  2 despliegue despliegue  4096 Oct 18 09:37 Público
drwx----- 3 despliegue despliegue  4096 Oct 13 07:23 snap
drwxr-xr-x  2 despliegue despliegue  4096 Oct 18 09:37 Videos
226 Transferencia completada
ftp>
```

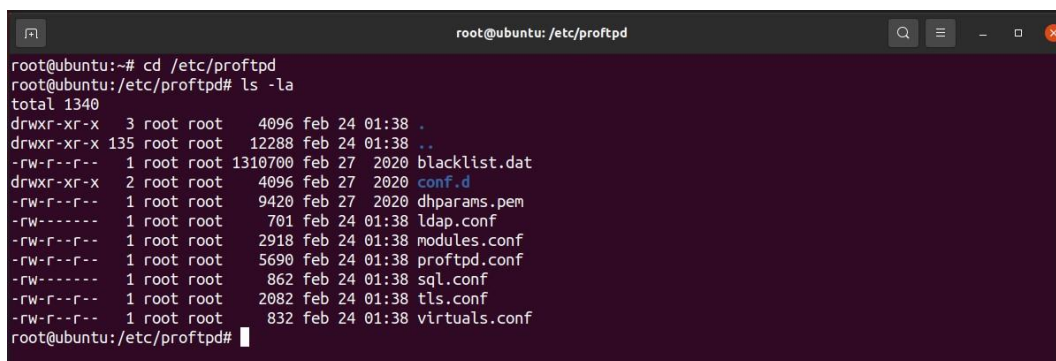
Actividad 2.- Configurar el acceso anónimo para el servidor FTP.

En esta actividad debemos configurar el servidor ProFTPD para que permita el acceso de usuarios anónimos, realizando las siguientes tareas:

- Crea una carpeta con la ruta `/var/ftp/distance` y dentro de ella un fichero de texto cuyo nombre será `anónimo.txt`.
- Configura ProFTPD para que enjaule a los usuarios anónimos en esta carpeta y no les permita escribir ni modificar los archivos, solo descargar.
- Ajusta los parámetros del servidor FTP para que permita 30 conexiones simultáneas de usuarios anónimos.
- Una vez configurado, conéctate con el usuario anónimo y comprueba que tienes acceso al fichero, utilizando el cliente FTP incluido en Linux desde la consola de comandos.

Configura el servidor ProFTPD para que se pueda acceder con usuario anónimo. Crea una carpeta `/var/ftp/distancia` y dentro de ella un fichero de texto cuyo nombre `anónimo.txt`. Recuerda que debes configurar adecuadamente los permisos de la carpeta para que el usuario anónimo solo pueda leer o descargar ficheros en esta carpeta. Ajusta los parámetros del servidor FTP para que solo permita 30 conexiones simultáneas de usuarios anónimos. Una vez realizado lo anterior, conéctate con el usuario anónimo y comprueba que tienes acceso al fichero, utilizando el cliente FTP incluido en Linux desde la consola de comandos y también usando un navegador web.

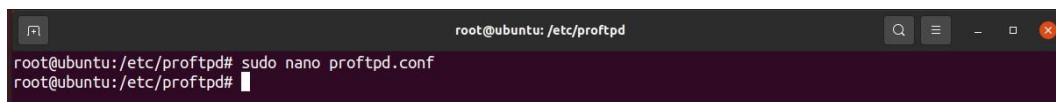
Todas las configuraciones que realizaremos en esta actividad se hacen sobre el fichero de configuración de proftpd, que está en la ruta `/etc/proftpd/proftpd.conf`



```
root@ubuntu:~# cd /etc/proftpd
root@ubuntu:/etc/proftpd# ls -la
total 1340
drwxr-xr-x  3 root root   4096 feb 24 01:38 .
drwxr-xr-x 135 root root 12288 feb 24 01:38 ..
-rw-r--r--  1 root root 1310700 feb 27 2020 blacklist.dat
drwxr-xr-x  2 root root   4096 feb 27 2020 conf.d
-rw-r--r--  1 root root   9420 feb 27 2020 dhparams.pem
-rw-----  1 root root    701 feb 24 01:38 ldap.conf
-rw-r--r--  1 root root   2918 feb 24 01:38 modules.conf
-rw-r--r--  1 root root   5690 feb 24 01:38 proftpd.conf
-rw-----  1 root root    862 feb 24 01:38 sql.conf
-rw-r--r--  1 root root   2082 feb 24 01:38 tls.conf
-rw-r--r--  1 root root    832 feb 24 01:38 virtuals.conf
root@ubuntu:/etc/proftpd#
```

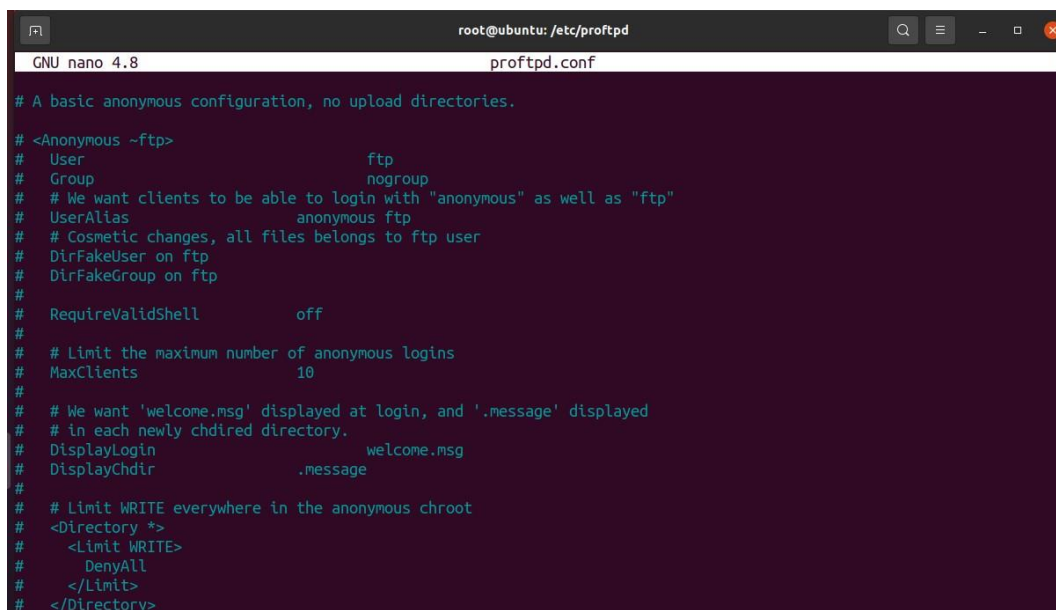
Editamos el fichero `proftpd.conf` con `nano`:

\$ sudo nano proftpd.conf



```
root@ubuntu:/etc/proftpd# sudo nano proftpd.conf
root@ubuntu:/etc/proftpd#
```

Casi al final del fichero nos encontraremos con un bloque comentado como el de la imagen:



```
GNU nano 4.8 proftpd.conf

# A basic anonymous configuration, no upload directories.

# <Anonymous ~ftp>
# User ftp
# Group nogroup
# # We want clients to be able to login with "anonymous" as well as "ftp"
# UserAlias anonymous ftp
# # Cosmetic changes, all files belongs to ftp user
# DirFakeUser on ftp
# DirFakeGroup on ftp
#
# RequireValidShell off
#
# Limit the maximum number of anonymous logins
# MaxClients 10
#
# # We want 'welcome.msg' displayed at login, and '.message' displayed
# # in each newly chdir'd directory.
# DisplayLogin welcome.msg
# DisplayChdir .message
#
# # Limit WRITE everywhere in the anonymous chroot
# <Directory *>
# <Limit WRITE>
# DenyAll
# </Limit>
# </Directory>
```

Tendremos que ir “descomentando” las líneas que vayamos a utilizar y modificar las directivas en función del objetivo de nuestra tarea.

El bloque comienza con la directiva <Anonymous ~ftp>, que deberemos modificar para que use como carpeta la que se nos solicita en el enunciado:

<Anonymous /var/ftp/distancia>

Ahora debemos descomentar la línea donde especifica el User y Group, así como el UserAlias. Activaremos también la línea de RequireValidShell off y MaxClients, cuyo valor lo cambiaremos de 10 a 30 para cumplir con el enunciado.

Un poco más abajo tenemos que activar las líneas donde se aplican restricciones de escritura a las carpetas del usuario ftp anónimo:

<Directory *>

...

</Directory>

Y no nos podemos olvidar de activar la última etiqueta, que es la que cierra el bloque </Anonymous>

```
# # Limit WRITE everywhere in the anonymous chroot
<Directory *>
  <Limit WRITE>
    DenyAll
  </Limit>
</Directory>
#
# # Uncomment this if you're brave.
# # <Directory incoming>
# # # Umask 022 is a good standard umask to prevent new files and dirs
# # # (second parm) from being group and world writable.
# # Umask 022 022
# #
# # <Limit READ WRITE>
# # DenyAll
# # </Limit>
# # <Limit STOR>
# # AllowAll
# # </Limit>
# # </Directory>
#
# /Anonymous>
```

Guardamos y reiniciamos.

Para que funcione adecuadamente debemos crear la carpeta /var/ftp/distancia y poner como propietario de la misma al usuario ftp:

\$ sudo mkdir /var/ftp/

\$ sudo mkdir /var/ftp/distancia

\$ sudo touch /var/ftp/distancia/anonimo.txt

\$ sudo chown ftp -R /var/ftp/distancia

Podemos probar a conectarnos desde la consola de comandos, y comprobar que tenemos acceso al fichero ejecutando un “ls” para que muestre lo que tenemos en el directorio, debiendo ver el fichero anónimo.txt que hemos puesto en la carpeta, y comprobando que no podemos borrarlo ordenando un “delete anonimo.txt”.

Actividad 3.- Acceso al servicio FTP mediante usuarios virtuales.

Configura el servidor ProFTPD para que se pueda acceder mediante usuarios virtuales, teniendo en cuenta lo siguiente:

- Crea un usuario virtual con el nombre 'virtualXX' donde XX son los 2 últimos dígitos de tu DNI.
- El fichero que contiene los usuarios estará en la carpeta /etc/proftpd/distancia/
- La carpeta que se asignará a este usuario al conectarse estará en /var/ftp/virtualXX
- Recuerda comprobar los permisos de esta carpeta para que pueda gestionarla el usuario que ejecuta el servicio FTP.
- Una vez configurado, conéctate con el usuario virtual desde la consola de comandos y comprueba que puedes subir un fichero.

Configura el servidor ProFTPD para que tenga un usuario virtual con el nombre 'virtualXX' donde XX son los 2 últimos dígitos de tu DNI. En mi caso yo trabajaré con virtual12. Comprueba que puedes conectarte desde la terminal de comandos. El fichero que contiene los usuarios estará en /etc/proftpd/distancia/ftp.daw.users. Los archivos y documentos se almacenarán en la carpeta /var/ftp/ftpdaw, por lo que deberemos configurar los permisos de esta carpeta (y del fichero de usuarios) para que los pueda gestionar el usuario ftp (grupo nogroup).

Los usuarios virtuales son aquellos que no son usuarios de sistema, pero sí tienen acceso a algunos recursos a través del servicio FTP. Los crearemos usando el comando **ftpasswd**. Los usuarios y las contraseñas se almacenan en un fichero que vamos a crear en el directorio de proftpd:

```
$ mkdir /etc/proftpd/distancia
```

```
$ touch /etc/proftpd/distancia/ftp.daw.users
```

Según el enunciado debemos crear una carpeta donde se ubicarán los ficheros del usuario virtual:

```
$ mkdir /var/ftp/virtual12
```

```
$ touch /var/ftp/virtual12/usuariovirtual.txt
```

```
$ chown ftp:nogroup -R /var/ftp/virtual12
```

Creamos el usuario:

```
$ sudo ftppasswd --passwd --file=/etc/proftpd/distancia/ftp.daw.users --  
name=virtual12 -uid=3001 --gid=3001 --home=/var/ftp/virtual12 --shell=/bin/false
```

Una vez creado el usuario, debemos realizar algunas modificaciones en el fichero de configuración de proftpd (proftpd.conf) para que configuremos la ruta del fichero de contraseñas

(AuthUserFile) y para que nos permita conectar con usuarios que no tienen Shell (RequiredValidShell).

Ahora guardamos y reiniciamos proftpd. Ya podemos conectar con nuestro usuario virtual:

\$ ftp localhost

Podemos ver el archivo que habíamos creado en ese directorio lanzando un "ls".

Actividad 4.- Configuración del servidor FTP para conexión segura con TLS.

Configura el servidor FTP para que acepte conexiones seguras (TLS), teniendo en cuenta lo siguiente:

- Crea/Instala un certificado en tu servidor Ubuntu/Debian
- Modifica los ficheros de configuración para que utilicen este certificado.
- Configura el servidor para que el usuario creado en la actividad 3 pueda conectarse mediante esta conexión cifrada.
- Debes documentar tanto la creación del certificado como la modificación de los ficheros de configuración.
- Una vez configurado, conéctate con el usuario virtual desde la consola de comandos y comprueba que puedes subir un fichero.

Para activar el acceso al servidor FTP usando una conexión segura debemos instalar un certificado y modificar los ficheros proftpd.conf y tls.conf.

Para crear el certificado tenemos 2 opciones: usar OpenSSL tal y como hicimos en la práctica de Apache Web Server, o usar la utilidad proftpd-gencert. Vamos a probar con esta última:

\$ sudo proftpd-gencert

Completamos la información que nos solicita (te la puedes inventar)


```
root@ubuntu: ~  
root@ubuntu:~# sudo proftpd-gencert  
Generating a RSA private key  
.....+++++  
.....+++++  
writing new private key to '/etc/ssl/private/proftpd.key'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:ES  
State or Province Name (full name) [Some-State]:ALMERÍA  
Locality Name (eg, city) []:AGUADULCE  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES AGUADULCE  
Organizational Unit Name (eg, section) []:FPaD  
Common Name (e.g. server FQDN or YOUR name) []:IESAGUADULCE  
Email Address []:nomail@iesaguadulce.es  
  
Use the following information in your ProFTPD configuration:  
  
TLRSACertificateFile    /etc/ssl/certs/proftpd.crt  
TLRSACertificateKeyFile /etc/ssl/private/proftpd.key  
  
See /etc/proftpd/tls.conf for suggested TLS related configuration  
items and include that file in your /etc/proftpd/proftpd.conf file.  
root@ubuntu:~#
```

Ahora damos permisos a los archivos que acabamos de generar:

\$ sudo chmod 600 /etc/ssl/private/proftpd.key

\$ sudo chmod 644 /etc/ssl/certs/proftpd.crt

```
root@ubuntu: ~  
root@ubuntu:~# sudo chmod 600 /etc/ssl/private/proftpd.key  
root@ubuntu:~# sudo chmod 644 /etc/ssl/certs/proftpd.crt  
root@ubuntu:~#
```

(*) Otra forma de generarlo sería con la utilidad de openssl que usamos para Apache:

**\$ openssl req -x509 -newkey rsa:2048 -keyout
/etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt -nodes -days 365**

Una vez que tenemos el certificado vamos a configurarlo en el fichero tls.conf:

\$ sudo nano /etc/proftpd/tls.conf

Tendremos que configurar las directivas relacionadas con el tipo de certificado que hemos instalado

<IfModule mod_tls.c>

...

*TLS*Engine on

*TLS*Log /var/log/proftpd/tls.log

*TLS*Protocol SSLv23

...

TLRSACertificateFile /etc/ssl/certs/proftpd.crt

TLRSACertificateKeyFile /etc/ssl/private/proftpd.key

...

TLSoptions NoCertRequest EnableDiags NoSessionReuseRequired

...

TLSRequired off

...

</IfModule>

```
root@ubuntu: ~
GNU nano 4.8 /etc/proftpd/tls.conf Mod
#
# Proftpd sample configuration for FTPS connections.
#
# Note that FTPS impose some limitations in NAT traversing.
# See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.html
# for more information.
#
<IfModule mod_tls.c>
  TLSEngine on
  TLSLog /var/log/proftpd/tls.log
  TLSProtocol SSLv23
#
# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey rsa:1024 \
#   -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
#   -nodes -days 365
#
# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.
#
# chmod 0600 /etc/ssl/private/proftpd.key
# chmod 0640 /etc/ssl/private/proftpd.key
#
TLRSACertificateFile /etc/ssl/certs/proftpd.crt
TLRSACertificateKeyFile /etc/ssl/private/proftpd.key
#
```

```
root@ubuntu: ~
GNU nano 4.8 /etc/proftpd/tls.conf Mod
# ...or avoid CA cert and be verbose
#TLSOptions NoCertRequest EnableDiags
# ... or the same with relaxed session use for some clients (e.g. FireFtp)
#TLSOptions NoCertRequest EnableDiags NoSessionReuseRequired
#
#
# Per default drop connection if client tries to start a renegotiate
# This is a fix for CVE-2009-3555 but could break some clients.
#
#TLSOptions AllowClientRenegotiations
#
# Authenticate clients that want to use FTP over TLS?
#
#TLSVerifyClient off
#
# Are clients required to use FTP over TLS when talking to this server?
#
#TLSRequired off
#
# Allow SSL/TLS renegotiations when the client requests them, but
# do not force the renegotiations. Some clients do not support
# SSL/TLS renegotiations; when mod_tls forces a renegotiation, these
# clients will close the data connection, or there will be a timeout
# on an idle data connection.
#
#TLSRenegotiate required off
</IfModule>
```

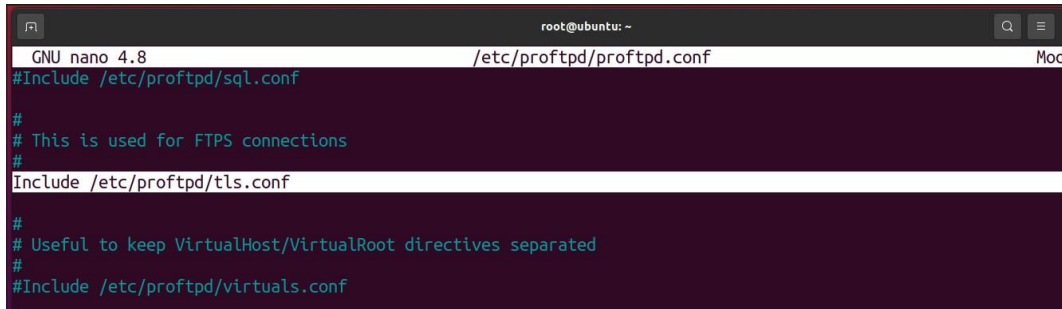
Guardamos y salimos. (Ctrl+X)

Por último, editamos el fichero **/etc/proftpd/proftpd.conf**

\$ sudo nano /etc/proftpd.conf

Descomentamos la línea que permite incluir el fichero tls.conf

#include /etc/proftpd/tls.conf

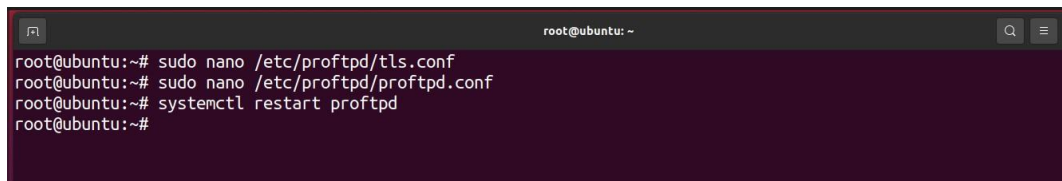


```
GNU nano 4.8 /etc/proftpd/proftpd.conf
#include /etc/proftpd/sql.conf
#
# This is used for FTPS connections
#
#include /etc/proftpd/tls.conf
#
# Useful to keep VirtualHost/VirtualRoot directives separated
#
#include /etc/proftpd/virtuals.conf
```

Guardamos y salimos. (Ctrl+X)

Y reiniciamos el servidor FTP:

\$ sudo systemctl restart proftpd



```
root@ubuntu:~# sudo nano /etc/proftpd/tls.conf
root@ubuntu:~# sudo nano /etc/proftpd/proftpd.conf
root@ubuntu:~# systemctl restart proftpd
root@ubuntu:~#
```

Actividad 5.- Instalación y configuración de un cliente gráfico FTP para conexión segura con TLS.

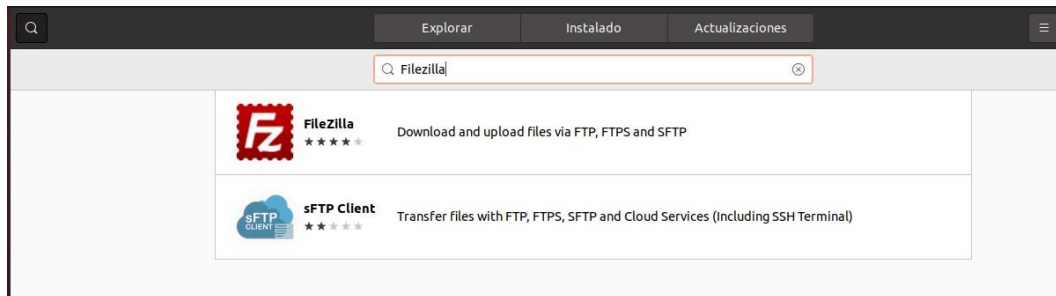
Ahora que ya hemos instalado el servidor FTP vamos a instalar y configurar un cliente gráfico FTP que acceda a los servicios desplegados en el ejercicio anterior. Para ello deberás realizar lo siguiente:

- Instala a través del gestor de paquetes de Ubuntu, el cliente gráfico de **FTP Filezilla**, documentando adecuadamente el proceso.
- Configura un perfil en el gestor de sitios de Filezilla para el **acceso anónimo al servidor FTP** que has configurado en la actividad 2 y comprueba que te puedes conectar, y que no te permite subir ficheros ni borrar el que hay.
- Configura un perfil en el gestor de sitios de Filezilla para el **acceso al servidor FTP mediante el usuario virtual** que has configurado en la actividad 3 y comprueba que te puedes conectar, y que te permite subir ficheros.
- Documenta adecuadamente el proceso.

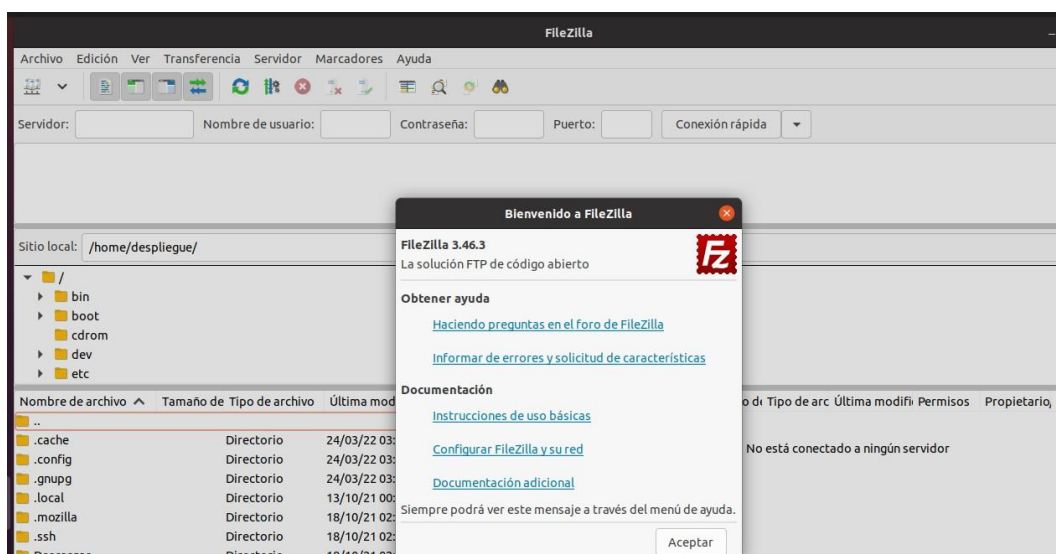
Ahora que ya hemos instalado el servidor FTP vamos a instalar y configurar un cliente gráfico FTP que acceda a los servicios desplegados en el ejercicio anterior. Para ello deberás realizar las siguientes actividades:

Actividad 5.1.- Instalación de Filezilla FTP Client.

Instala a través del gestor de paquetes de Ubuntu, el cliente gráfico de FTP Filezilla, documentando adecuadamente el proceso.



Abrimos el gesto de software de Ubuntu y usamos el buscador para localizar el paquete de Filezilla. Hacemos clic en instalar y a esperar...



Una vez instalado, ya podemos lanzar la aplicación.

Actividad 5.2.- Conexión con usuario anónimo.

Configura un perfil de Filezilla para acceder al servidor FTP con el usuario creado en la actividad 2.3 y conéctate comprobando que tienes acceso a los recursos correspondientes y tienes los permisos adecuados. Documenta adecuadamente el proceso.

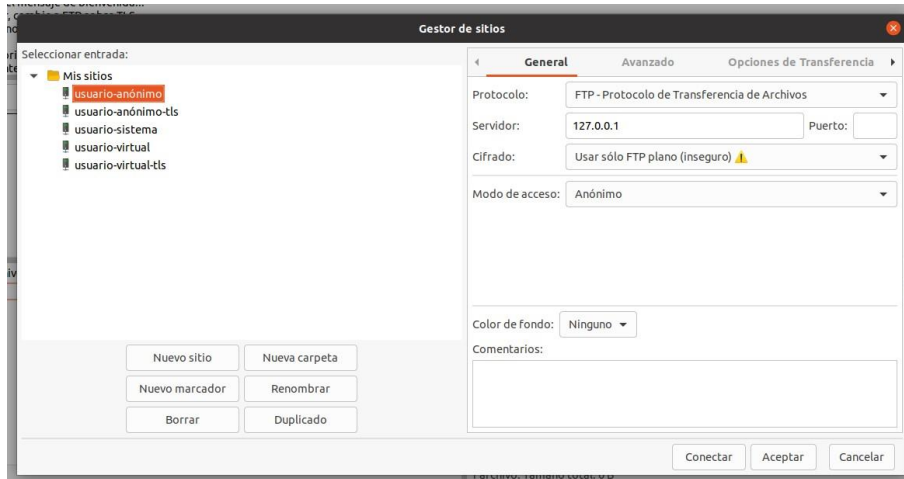
Para crear un perfil abrimos el gestor de sitios de Filezilla y hacemos clic en el botón 'nuevo sitio'.

Nos mostrará varias casillas en las que configuraremos los datos de la conexión:

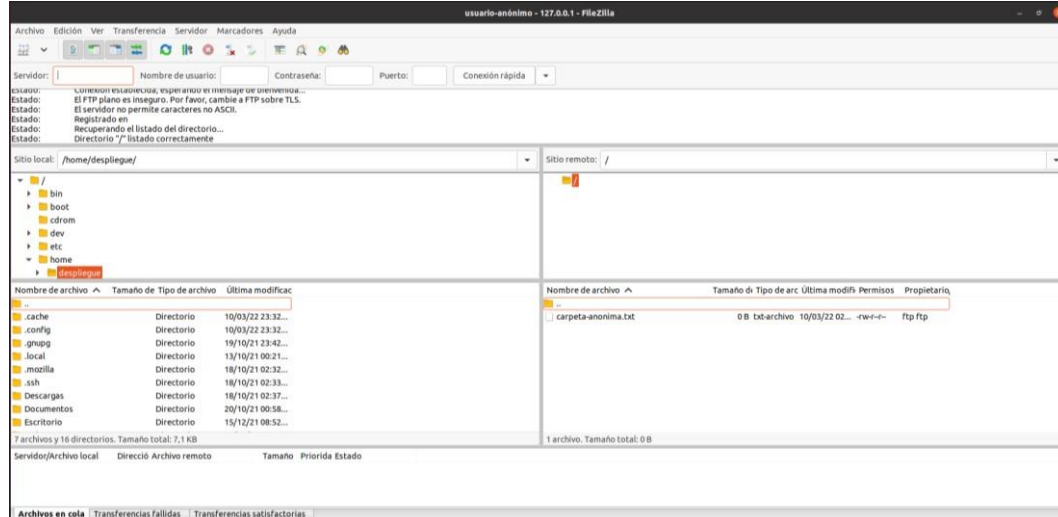
En este caso los valores serán:

- Protocolo FTP
- Cifrado sólo FTP (inseguro)
- Modo de acceso: Anónimo

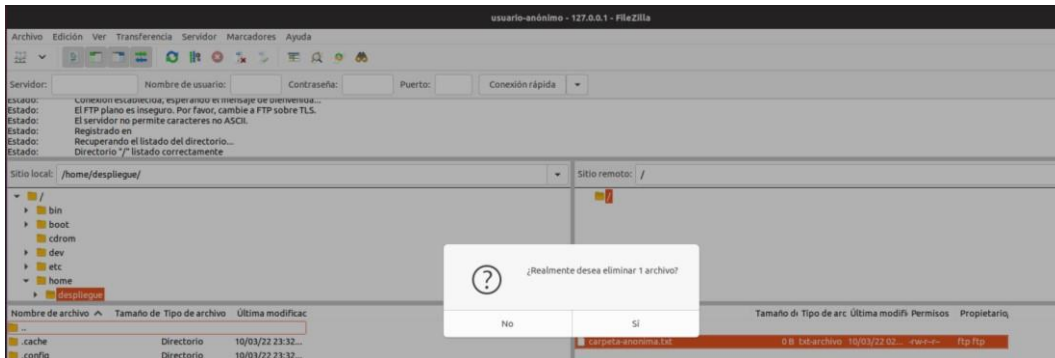
Aceptamos para que guarde la configuración.



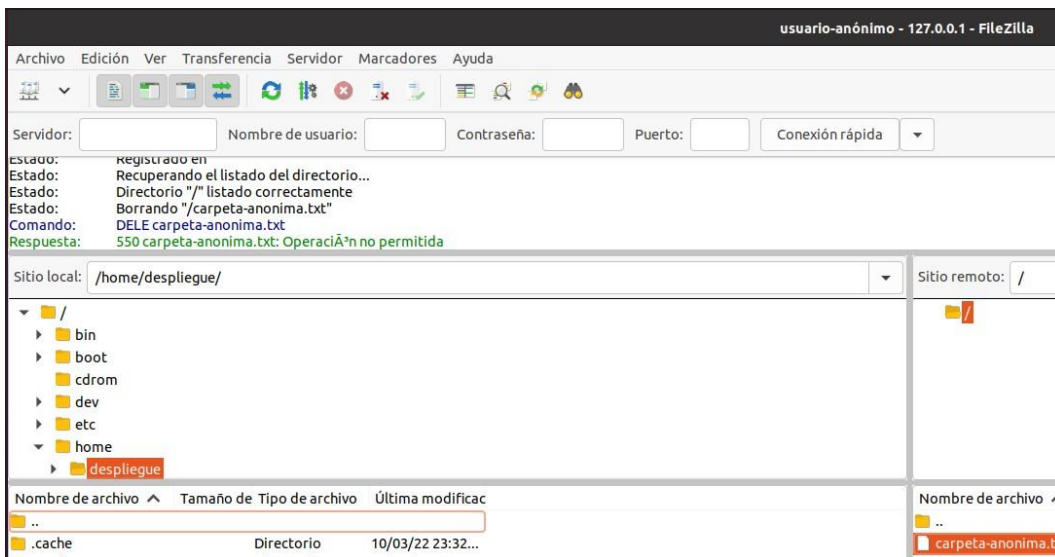
Ahora podemos conectar con el perfil creado:



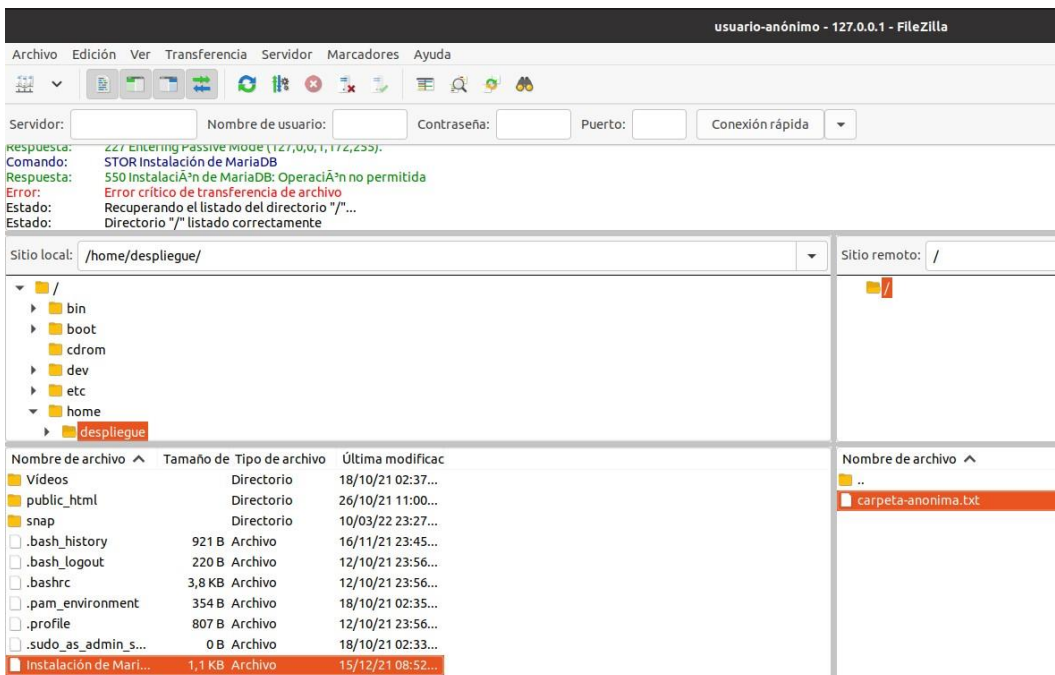
Para comprobar los permisos, podemos por ejemplo intentar borrar el fichero:



Al aceptar nos dará un mensaje de error, ya que no puede borrarlo:



También podemos intentar subir un fichero desde nuestra máquina local al servidor ftp. Tampoco nos dejará:



Actividad 5.3.- Conexión con usuario virtual.

Configura un perfil de Filezilla para acceder al servidor FTP con el usuario creado en la actividad 2.3 y conéctate comprobando que tienes acceso a los recursos correspondientes y tienes los permisos adecuados. Documenta adecuadamente el proceso.

Para crear un perfil abrimos el gestor de sitios de Filezilla y hacemos clic en el botón 'nuevo sitio'.

Nos mostrará varias casillas en las que configuraremos los datos de la conexión:

En este ejemplo los valores serán:

- Protocolo FTP
- Cifrado sólo FTP (inseguro)
- Modo de acceso: Normal
- Usuario: virtual12 (es el usuario virtual)
- Contraseña: usuario12

Aceptamos para que guarde la configuración.



Ahora podemos conectar con el perfil creado,

Y podemos subir un fichero para comprobar que tenemos permisos de escritura.

Actividad 5.4.- Conexión segura con TLS.

Modifica el perfil de Filezilla creado en la actividad anterior (3.3) para que se conecte mediante conexión segura al servidor FTP y haz una prueba de conexión con la configuración que estableciste en el ejercicio 2.4. Documenta adecuadamente el proceso.

Para crear un perfil abrimos el gestor de sitios de Filezilla y hacemos clic en el botón 'nuevo sitio'.

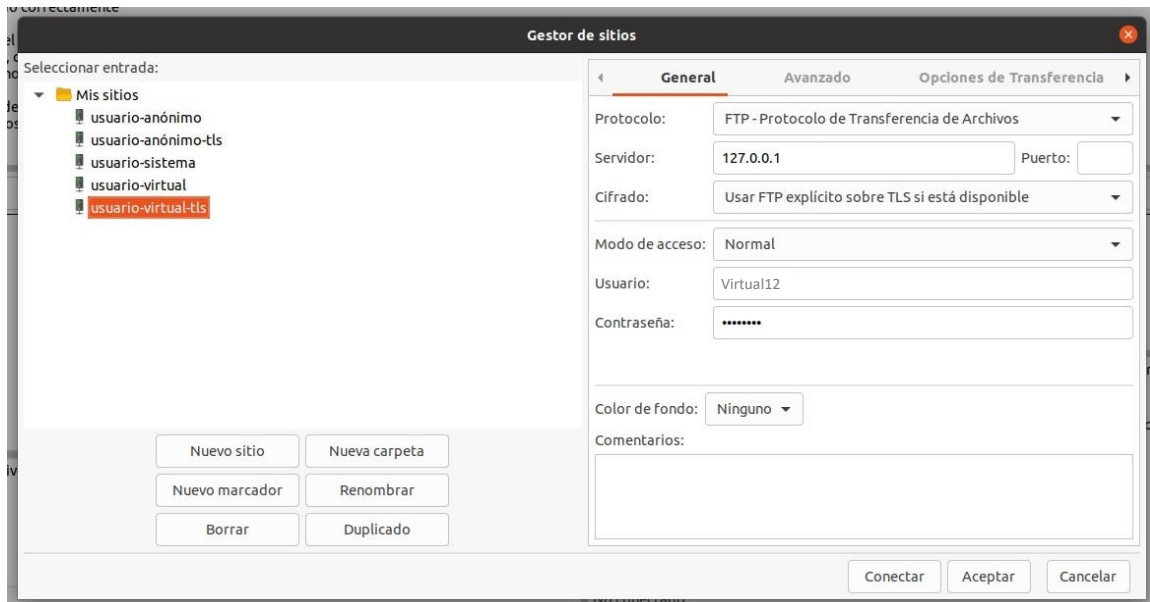
Nos mostrará varias casillas en las que configuraremos los datos de la conexión:

En este caso los valores serán:

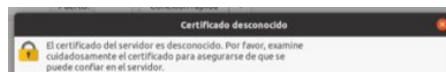
- Protocolo FTP

- Servidor: localhost ó 127.0.0.1 (o la ip del servidor) ? Cifrado: Usar FTP explícito sobre TLS si está disponible.
- Modo de acceso: Normal
- Usuario: virtual12 (es mi usuario virtual)
- Contraseña: usuario1

Aceptamos para que guarde la configuración.



Ahora podemos conectar con el perfil creado. Nos muestra los datos de nuestro certificado:



Continuamos y nos conecta con la carpeta del usuario.

De igual modo podemos hacerlo con la conexión anónima para que se haga con TLS:

En este caso los valores serán:

- Protocolo FTP
- Servidor: localhost ó 127.0.0.1 (o la ip del servidor) ? Cifrado: Usar FTP explícito sobre TLS si está disponible.
- Modo de acceso: Anónimo



Guardamos y nos conectamos y nos muestra nuestra carpeta de usuario anónimo.

Actividad 6.- Uso de un navegador como cliente FTP.

Aunque por motivos de seguridad, la mayoría de los navegadores ya no permiten su uso como clientes FTP, aún es posible hacerlo utilizando navegadores obsoletos o incluso el explorador de archivos de Windows. En esta actividad utilizaremos la primera opción (Si usas una versión 18 de Ubuntu y no has actualizado el navegador Firefox también te puede servir):

- Descarga una versión portable de Mozilla Firefox (70 o anterior). En el foro de la actividad se dejarán instrucciones de cómo descargarla.
- Ahora accede con tu usuario de sistema o con tu usuario virtual.
- Comprueba que tienes acceso a los ficheros y carpetas correspondientes a ese usuario.
- Documenta adecuadamente el proceso.

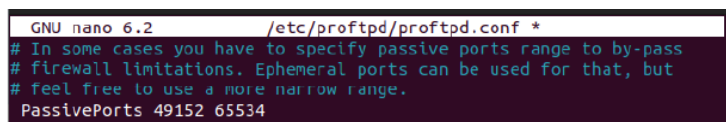
Vais a la dirección <https://ftp.mozilla.org/pub/mozilla.org/firefox/releases/>, os descargáis la versión que necesitéis, abris una terminal y ejecutamos `tar -jxvf nombre_del_fichero_descargado.tar.bz2`. Esto te lo descomprime en una carpeta llamada `firefox`. Entramos a ella desde la terminal y lo echamos a andar ejecutando `./firefox`. Al abrirla, al ser antigua la versión de `firefox` te preguntará si quieres actualizarla, y por supuesto le clicamos en "ahora no" y ya podremos trabajar con ella.

Accedemos al servidor ftp a través de la barra de direcciones usando la IP o el nombre de la maquina: `ftp://localhost`

Actividad 7.- Configuración del servicio FTP en modo activo o pasivo.

Revisa la configuración de tu servidor FTP y comprueba si está configurado en modo activo o pasivo. En caso de que está en modo activo indica qué pasos deberíamos seguir para configurarlo en modo pasivo. ¿Qué modo de funcionamiento es más seguro? Explica tu respuesta.

Por defecto el servidor FTP se encuentra en modo activo. Para configurar el modo pasivo abrimos el archivo de configuración del servidor ProFTPD (`/etc/proftpd/proftpd.conf`), vamos a la línea `PassivePorts` y la habilitamos.



```
GNU nano 6.2 /etc/proftpd/proftpd.conf *
# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
PassivePorts 49152 65534
```

FTP Activo

Es el modo predeterminado para las conexiones FTP. Fue el primero en desarrollarse. En este modo el servidor utilizará el puerto 20 para la transferencia de datos, mientras que transmitirá los comandos utilizando el puerto 21. El cliente en cambio utilizará un puerto aleatorio P superior al 1023 para la transferencia de comandos, y un puerto P+1 para la transferencia de datos.

Inconvenientes de este modo

Históricamente el principal inconveniente de este modo ha radicado en que, si no hay una directiva específica en los firewalls del lado del cliente, la conexión es propensa a ser bloqueada. Esto se debe a que, como hemos visto, existen dos conexiones independientes: una de salida en la que el cliente establece la conexión del canal de control y otra de entrada en la que el servidor hace lo propio con el de datos. Esta última conexión es iniciada por el servidor en el puerto previamente negociado, y en ocasiones es bloqueada por el firewall del cliente al ser identificada como un intento de conexión externa no autorizada.

FTP Pasivo

El modo de FTP pasivo surge como consecuencia de los problemas de conexión del modo activo. Este modo mantiene los dos canales (control y datos) pero en este caso es el cliente el encargado de establecer las dos conexiones.

El servidor sigue manteniendo el puerto 21 como puerto de comandos, el puerto de datos en cambio difiere del modo activo y pasa a ser un rango de puertos Q superior a 1023. Del lado del cliente seguimos manteniendo el puerto P superior a 1023 para control, y el puerto P+1 para datos.

Inconvenientes

El principal inconveniente de habilitar el modo pasivo en un servidor FTP está asociado con el riesgo extra en materia de seguridad que conlleva la apertura de un rango de puertos extra con respecto al modo activo. Notemos que para que el modo pasivo funcione adecuadamente estos puertos deben ser abiertos tanto en el servidor como en el firewall.