



# **FTP Y SSL Linux**

Ivan Santaren



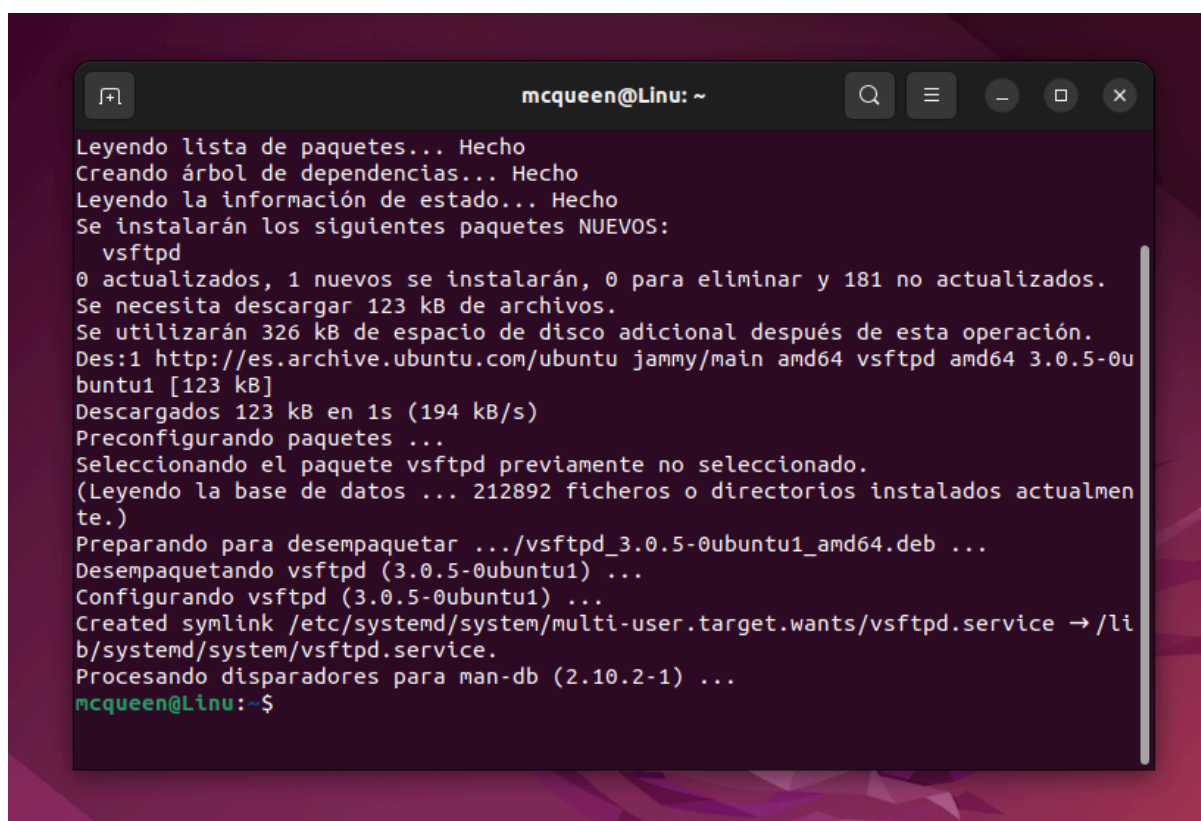
## 1. Explica el ataque FTP-Bounce Attack con tus palabras.

Es un tipo de ciberataque que aprovecha una vulnerabilidad ftp para realizar protocolos restringidos como transferencias de archivos. A día de hoy estos ataques son extraños ya que están bastante obsoletos.

## 2. Instala y configura un servidor FTP.

Lo primero que tenemos que hacer es asegurarnos de que la maquina está actualizada, lo cual haremos un `sudo apt update` y `sudo apt upgrade`.

Ahora tenemos que instalar el servidor con “`sudo apt install vsftpd`”:



```
mcqueen@Linu: ~  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes NUEVOS:  
  vsftpd  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 181 no actualizados.  
Se necesita descargar 123 kB de archivos.  
Se utilizarán 326 kB de espacio de disco adicional después de esta operación.  
Des:1 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 vsftpd amd64 3.0.5-0u  
buntu1 [123 kB]  
Descargados 123 kB en 1s (194 kB/s)  
Preconfigurando paquetes ...  
Seleccionando el paquete vsftpd previamente no seleccionado.  
(Leyendo la base de datos ... 212892 ficheros o directorios instalados actualmen  
te.)  
Preparando para desempaquetar .../vsftpd_3.0.5-0ubuntu1_amd64.deb ...  
Desempaquetando vsftpd (3.0.5-0ubuntu1) ...  
Configurando vsftpd (3.0.5-0ubuntu1) ...  
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /li  
b/systemd/system/vsftpd.service.  
Procesando disparadores para man-db (2.10.2-1) ...  
mcqueen@Linu:~$
```



```
mcqueen@Linu:~$ sudo apt install vsftpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
vsftpd ya está en su versión más reciente (3.0.5-0ubuntu1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 181 no actualizados.
mcqueen@Linu:~$
```

Ahora tenemos que configurarlo, “sudo nano /etc/vsftpd.conf” y nos tendremos que asegurar de que las opciones respeten los siguientes parámetros:

anonymous\_enable=NO

local\_enable=YES

write\_enable=YES

chroot\_local\_user=YES

```
#
# Uncomment this to allow
local_enable=YES
#
# Uncomment this to enable
write_enable=YES
#
# Default umask for local
# if your users expect
```

^G Ayuda      ^O Guardar  
^X Salir      ^R Leer fi



```
mcqueen@Linu: ~  
GNU nano 6.2 /etc/vsftpd.conf  
# Example config file /etc/vsftpd.conf  
#  
# The default compiled in settings are fairly paranoid. This sample file  
# loosens things up a bit, to make the ftp daemon more usable.  
# Please see vsftpd.conf.5 for all compiled in defaults.  
#  
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.  
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's  
# capabilities.  
#  
#  
# Run standalone? vsftpd can run either from an inetd or as a standalone  
# daemon started from an initscript.  
listen=NO  
#  
# This directive enables listening on IPv6 sockets. By default, listening  
# on the IPv6 "any" address (::) will accept connections from both IPv6  
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6  
# sockets. If you want that (perhaps because you want to listen on specific  
# addresses) then you must run two copies of vsftpd with two configuration  
  
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación  
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar      ^J Justificar ^_ Ir a línea
```

Lo siguiente es reiniciar el servidor para que se hagan efectivos los cambios. Lo haremos con “sudo apt vsftpd restart”. Una vez se reinicie podemos opcionalmente activar el cortafuegos como buena práctica. “sudo ufw allow 21”.

```
Actividades Terminal  
mcqueen@Linu: ~$ sudo ufw allow 21  
[sudo] contraseña para mcqueen:  
Reglas actualizadas  
Reglas actualizadas (v6)  
mcqueen@Linu:~$ S
```

El siguiente paso es crear un directorio para nuestro usuario ftp, lo haremos con los siguientes comandos:



- “sudo mkdir /home/mcqueen/ftp”
- “sudo chown nobody:nogroup /home/mcqueen/ftp”
- “sudo chmod a-w /home/mcqueen/ftp”

```
mcqueen@Linu:~$ sudo mkdir /home/mcqueen/ftp
mcqueen@Linu:~$ sudo chown nobody:nogroup /home/mcqueen/ftp
mcqueen@Linu:~$ sudo chmod a-w /home/mcqueen/ftp
mcqueen@Linu:~$
```

Una vez creado este directorio tenemos que crear los usuarios que lo compongan (haremos el usuario con un nombre normal del siguiente ejercicio primero):

- “sudo useradd -m -d /home/mcqueen/ftp -s /bin/bash mcqueen”
- “sudo passwd mcqueen”

```
mcqueen@Linu:~$ sudo ufw allow 21
[sudo] contraseña para mcqueen:
Reglas actualizadas
Reglas actualizadas (v6)
mcqueen@Linu:~$ sudo mkdir /home/mcqueen/ftp
mcqueen@Linu:~$ sudo chown nobody:nogroup /home/mcqueen/ftp
mcqueen@Linu:~$ sudo chmod a-w /home/mcqueen/ftp
mcqueen@Linu:~$ sudo useradd -m -d /home/mcqueen/ftp -s /bin/bash mcqueen
useradd: el usuario «mcqueen» ya existe
mcqueen@Linu:~$ sudo passwd mcqueen
Nueva contraseña:
```

Un usuario normal se crearía de esta manera, en este caso no se crea porque el usuario ya existía pero podriamos hacerlo con uno nuevo. Tambien podemos cambiar la contraseña de un usuario existente de esta manera.

El servidor, directorio y usuario estan creados y funcionando. Para acceder podriamos utilizar un cliente ftp con filezilla o un programa del estilo usando la ip de la maquina virtual.



### 3. Añade usuarios locales (usuario root, usuario con un nombre y usuario profe).

El usuario root ya existe como superusuario en cualquier maquina virtual de linux, entonces creado ya está pero podemos cambiar la contraseña de éste con “sudo passwd root”.

- Al usuario con un nombre le llamaremos tortuguita:

```
mcqueen@Linu:~$ sudo adduser tortuguitina
[sudo] contraseña para mcqueen:
Añadiendo el usuario `tortuguitina' ...
Añadiendo el nuevo grupo `tortuguitina' (1002) ...
Añadiendo el nuevo usuario `tortuguitina' (1002) con grupo `tortuguitina' ...
Creando el directorio personal `/home/tortuguitina' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para tortuguitina
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []:
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] █
```

- De la misma manera creamos el usuario profe:

```
¿Es correcta la información? [S/n] s
mcqueen@Linu:~$ sudo adduser profe
Añadiendo el usuario `profe' ...
Añadiendo el nuevo grupo `profe' (1003) ...
Añadiendo el nuevo usuario `profe' (1003) con grupo `profe' ...
Creando el directorio personal `/home/profe' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para profe
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []: Evelyn
Número de habitación []: 4
Teléfono del trabajo []: 123456789
Teléfono de casa []: 123456789
Otro []: uwu
¿Es correcta la información? [S/n] s
mcqueen@Linu:~$
```



Como es el usuario de la todopoderosa Evelyn le metemos un “sudo usermod -aG profe” para hacer el usuario administrador.

#### 4. Crea cuotas para el usuario con tu nombre y para el usuario profe y explica porque escogiste un límite blando o duro.

Lo primero que tenemos que hacer es asegurarnos de que las cuotas están habilitadas en el sistema de archivos, lo haremos con el comando “sudo nano /etc/fstab” y agregando “usrquota” y “grquota” dentro de las opciones que se abrirán.

```
GNU nano 6.2 /etc/fstab *
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda3 during installation
UUID=cc7d3d41-1b13-4a62-9de5-e88392fcd841 / ext4 errors=remount-ro,usrquota,grpquota 0
# /boot/efi was on /dev/sda2 during installation
UUID=C620-55B4 /boot/efi vfat umask=0077 0 1
/swapfile swap sw 0 0

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea M-E Rehacer
```

Guardamos, salimos y volvemos a montar el sistema de archivos.

```
mcqueen@Linu:~$ sudo mount -o remount /
mcqueen@Linu:~$
```

Ahora tenemos que seguir los siguientes pasos para habilitar las cuotas de cada usuario:



- Habilitar las cuotas en el sistema de archivos con “sudo quotacheck -avug” y “sudo quotaon -avug”.

```
mcqueen@Linu:~$ sudo quotacheck -avug -m
quotacheck: Your kernel probably supports ext4 quota feature but you are using external quota files. Please sw
itch your filesystem to use ext4 quota feature as external quota files on ext4 are deprecated.
quotacheck: Explorando /dev/sda3 [/] echo
quotacheck: Cannot stat old user quota file //aquota.user: No existe el archivo o el directorio. Usage will no
t be subtracted.
quotacheck: Cannot stat old group quota file //aquota.group: No existe el archivo o el directorio. Usage will
not be subtracted.
quotacheck: Cannot stat old user quota file //aquota.user: No existe el archivo o el directorio. Usage will no
t be subtracted.
quotacheck: Cannot stat old group quota file //aquota.group: No existe el archivo o el directorio. Usage will
not be subtracted.
quotacheck: Comprobados 21550 directorios y 211348 archivos.
quotacheck: Archivo antiguo no encontrado.
quotacheck: Archivo antiguo no encontrado.
mcqueen@Linu:~$
```

```
/dev/sda3 [/]: group quotas activadas
/dev/sda3 [/]: user quotas activadas
mcqueen@Linu:~$
```

Ahora que tenemos la cuotas activadas tenemos que configurar las cuotas de tortuguitina, lo haremos con “sudo edquota -u tortuguitina” y las configuraremos con un limite blando de 250mb y uno duro de 300mb (el blando es el limite donde da el aviso y el duro donde el sistema ya no permite más nada y muere).

```
mcqueen@Linu: ~
GNU nano 6.2 /tmp//EdP.aUqoXB8 *
Cuotas de disco para user tortuguitina (uid 1002):
Sist. arch. bloques blando duro inodos blando duro
/dev/sda3 16 250 300 4 250 300

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^/ Ir a línea M-E Rehacer
```





guardamos y salimos.

Ahora toca el de la profe que en este caso usaremos 500mb de blando y 750 de duro.

```
mcqueen@Linu: ~  
GNU nano 6.2 /tmp//EdP.a0VHGkH *  
Cuotas de disco para user profe (uid 1003):  
Sist. arch. bloques blando duro inodos blando duro  
/dev/sda3 16 500 750 4 500 750  
  
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer  
^X Salir ^R Leer fich. ^_ Reemplazar ^U Pegar ^J Justificar ^/ Ir a línea M-E Rehacer
```

## 5. Activa SSL en tu servidor FTP.

Para empezar tenemos que instalar openssl, “sudo apt install openssl”

```
mcqueen@Linu: ~  
mcqueen@Linu:~$ sudo apt install openssl  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se actualizarán los siguientes paquetes:  
  openssl  
1 actualizados, 0 nuevos se instalarán, 0 para eliminar y 180 no actualizados.  
Se necesita descargar 0 B/1.182 kB de archivos.  
Se utilizarán 0 B de espacio de disco adicional después de esta operación.  
(Leyendo la base de datos ... 213011 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../openssl_3.0.2-0ubuntu1.12_amd64.deb ...  
Desempaquetando openssl (3.0.2-0ubuntu1.12) sobre (3.0.2-0ubuntu1.10) ...  
Configurando openssl (3.0.2-0ubuntu1.12) ...  
Procesando disparadores para man-db (2.10.2-1) ...  
mcqueen@Linu:~$
```





- force\_local\_logins\_ssl=YES
- ssl\_tlsv1=YES
- ssl\_sslv2=NO
- ssl\_sslv3=NO
- rsa\_cert\_file=/etc/ssl/private/vsftpd.pem

```
GNU nano 6.2 /etc/vsftpd.conf *
#anon_upload_enable=YES
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
rsa_cert_file=/etc/ssl/private/vsftpd.pem
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
```

^G Ayuda	^O Guardar	^W Buscar	^K Cortar	^T Ejecutar	^C Ubicación	M-U Deshacer	M-A Poner marca
^X Salir	^R Leer fich.	^E Reemplazar	^U Pegar	^J Justificar	^_ Ir a línea	M-E Rehacer	M-6 Copiar

CTRL DEFECTA

Guardamos los cambios, cerramos y el último comando para cerrar sería “sudo service vsftpd restart” para reiniciar el servicio y aplicar las configuraciones.