

UD 04

SERVIDOR FTP

PRÁCTICA 4.3 SERVICIO SFTP

Emilio Garruta González

Contenido

Instalación de OpenSSH.....	2
Configuración FTP.....	2
Acceso Seguro	2
Enjaular a los usuarios	3
Configuración de /etc/vsftpd.conf.....	5
WireShark.....	6
Instalación	6
Captura de tráfico	8
Conexión ftp.....	8
Conexión sftp.....	9
Comparativa FTP SFTP.....	10

Instalación de OpenSSH

Verifico si está instalado

```
daw-2t@ServidorLinuxegg:~$ sudo systemctl status ssh
[sudo] password for daw-2t:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2025-02-21 16:26:30 UTC; 4min 24s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 743 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 806 (sshd)
      Tasks: 1 (limit: 2224)
     Memory: 3.8M
        CPU: 35ms
    CGroup: /system.slice/ssh.service
            └─806 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

feb 21 16:26:30 ServidorLinuxegg systemd[1]: Starting OpenBSD Secure Shell server...
feb 21 16:26:30 ServidorLinuxegg sshd[806]: Server listening on 0.0.0.0 port 22.
feb 21 16:26:30 ServidorLinuxegg sshd[806]: Server listening on :: port 22.
feb 21 16:26:30 ServidorLinuxegg systemd[1]: Started OpenBSD Secure Shell server.
```

Actualizo todo lo que esté pendiente

```
daw-2t@ServidorLinuxegg:~$ sudo apt update
Obj:1 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Obj:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Ign:5 https://download.webmin.com/download/newkey/repository stable InRelease
Obj:6 https://download.webmin.com/download/newkey/repository stable Release
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Todos los paquetes están actualizados.
daw-2t@ServidorLinuxegg:~$ _
```

Configuración FTP

Acceso Seguro

Necesito configurar las siguientes líneas en el archivo `/etc/ssh/sshd_config`

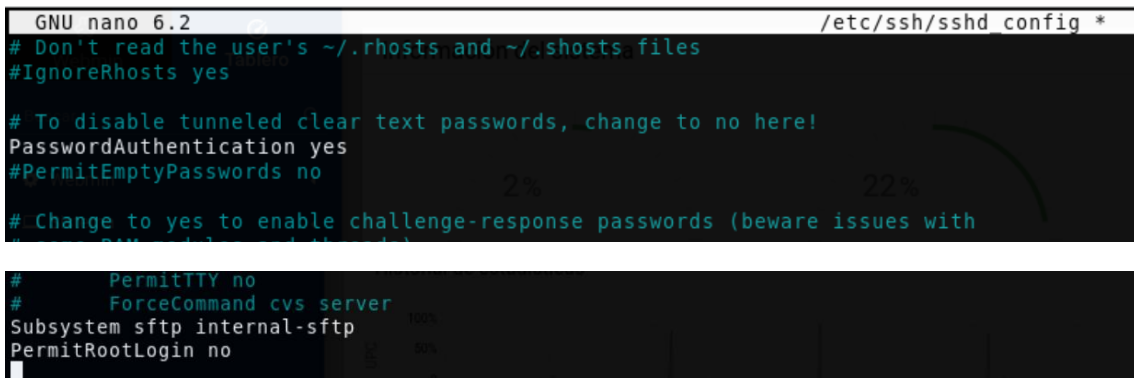
Subsystem sftp internal-sftp

Define el subsistema SFTP en el servidor SSH, utilizando `internal-sftp` en lugar de un binario externo. Esto es útil para restringir el acceso a solo SFTP sin permitir una shell interactiva

PermitRootLogin no

Evita que el usuario root inicie sesión directamente a través de SSH. Esto mejora la seguridad al requerir que los administradores inicien sesión con un usuario normal y luego usen sudo o su para obtener privilegios elevados.

PasswordAuthentication yes



```
GNU nano 6.2 /etc/ssh/sshd_config *
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and systems)

#
#   PermitTTY no
#   ForceCommand cvs server
Subsystem sftp internal-sftp
PermitRootLogin no
```

Enjaular a los usuarios

Necesito agregar las siguientes líneas en el archivo /etc/ssh/sshd_config:

Match User * #Aplica las siguientes reglas a todos los usuarios del sistema.

ChrootDirectory %h # "Enjaula" a cada usuario en su propio directorio home (%h se refiere al home del usuario), evitando que accedan a otros directorios.

ForceCommand internal-sftp # Obliga a los usuarios a usar solo SFTP, incluso si intentan abrir una sesión SSH estándar.

AllowTcpForwarding no # Desactiva el reenvío de puertos, una medida de seguridad adicional para limitar el acceso.



```
Match User *
    ChrootDirectory %h
    ForceCommand internal-sftp
    AllowTcpForwarding no
```

Debo dejar a cada usuario con los permisos correctos

`sudo chown root:root /home/usuariox`

1. El propósito de hacer que el propietario del directorio home de un usuario sea root es reforzar la seguridad, especialmente cuando los usuarios están "enjaulados" usando SFTP.
2. Esto previene que los usuarios puedan modificar los permisos o el contenido de su propio directorio raíz (/home/usuariox), lo que podría permitirles escapar del entorno enjaulado. Aun así, se les da control total sobre subdirectorios específicos, como archivos, donde sí pueden leer, escribir y modificar archivos.
3. Para no tener que hacerlo uno a uno ejecutaré un bash

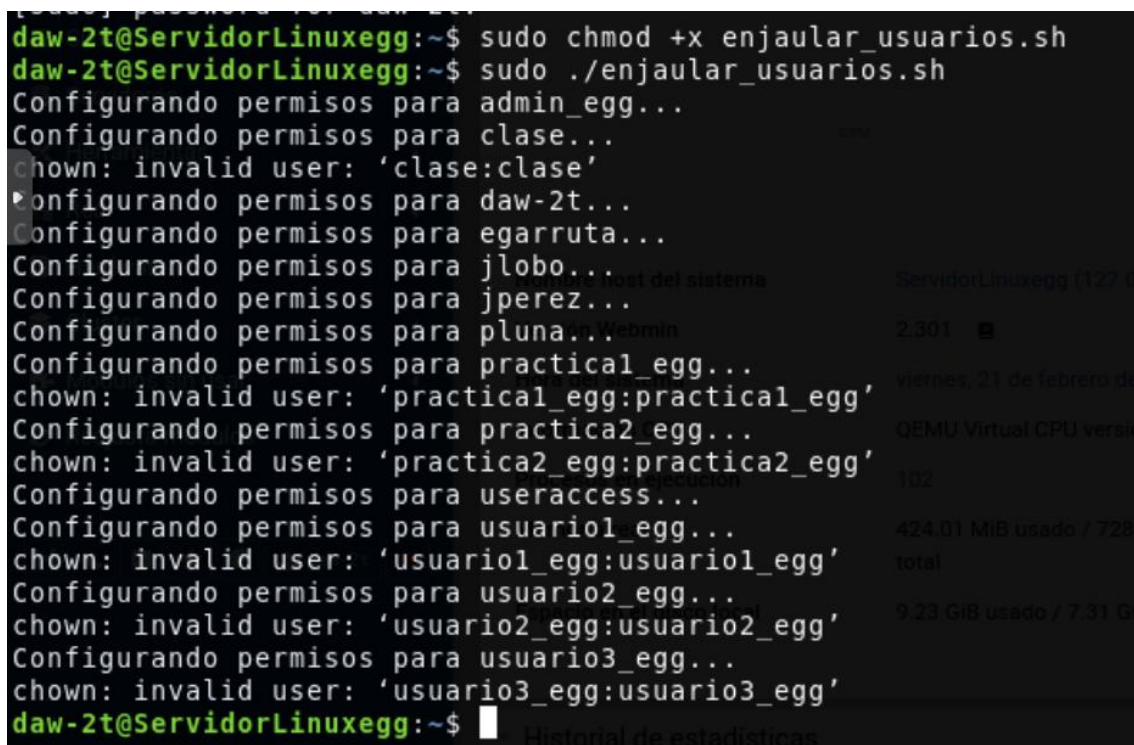


```
GNU nano 6.2 enjaular_usuarios.sh
#!/bin/bash

#permisos para enjaulados

for user in $(ls /home); do
    echo "Configurando permisos para $user..."
    sudo chown root:root /home/$user
    sudo chmod 755 /home/$user
    sudo mkdir -p /home/$user/archivos
    sudo chown $user:$user /home/$user/archivos
done
```

Hago el archivo ejecutable y lo ejecuto



```
daw-2t@ServidorLinuxegg:~$ sudo chmod +x enjaular_usuarios.sh
daw-2t@ServidorLinuxegg:~$ sudo ./enjaular_usuarios.sh
Configurando permisos para admin_egg...
Configurando permisos para clase...
chown: invalid user: 'clase:clase'
Configurando permisos para daw-2t...
Configurando permisos para egarruta...
Configurando permisos para jlobo...
Configurando permisos para jperez...
Configurando permisos para pluna...
Configurando permisos para practical1_egg...
chown: invalid user: 'practical1_egg:practical1_egg'
Configurando permisos para practica2_egg...
chown: invalid user: 'practica2_egg:practica2_egg'
Configurando permisos para useraccess...
Configurando permisos para usuario1_egg...
chown: invalid user: 'usuario1_egg:usuario1_egg'
Configurando permisos para usuario2_egg...
chown: invalid user: 'usuario2_egg:usuario2_egg'
Configurando permisos para usuario3_egg...
chown: invalid user: 'usuario3_egg:usuario3_egg'
daw-2t@ServidorLinuxegg:~$
```

Reinicio el servicio ssh

```
daw-2t@ServidorLinuxegg:~$ sudo systemctl restart ssh
daw-2t@ServidorLinuxegg:~$
```

Configuracion de /etc/vsftpd.conf

Debe contener las siguientes líneas:

local_enable=YES

write_enable=YES

chroot_local_user=YES

allow_writeable_chroot=YES

anonymous_enable=NO

Config File vsftpd.conf

```
23 #
24 # Allow anonymous FTP? (Disabled by default).
25 #anonymous_enable=YES
26 #
27 # Uncomment this to allow local users to log in.
28 local_enable=YES
29 #
30 # Uncomment this to enable any form of FTP write command.
31 write_enable=YES
32 #
33 # Enable this option to allow local users to chroot to their home
34 # directories. Note that the default is not to allow any local
35 # users to chroot, even if the optional --chroot_local_user
36 # option is enabled. If you enable this feature, you may also
37 # want to comment out the following line to enable write
38 # access in local users' home directories. If you want to
39 # disable this feature altogether, uncomment the line below.
```

Config File vsftpd.conf

```
120 # the user does not have write access to the top level directory
121 # chroot)
122 chroot_local_user=YES
123 #chroot_list_enable=YES
124 # (default follows)
125 #chroot_list_file=/etc/vsftpd.chroot_list
126 #
127 # You may activate the "D" option to the built-in ls. This is dis-
```

```

152
153 #
154 # Uncomment this to indicate that vsftpd use a utf8 filesystem.
155 #utf8_filesystem=YES
156 #anon_upload_enable=YES
157 #anon_mkdir_write_enable=YES
158 #anon_other_write_enable=YES
159 #anon_root=/srv/ftp
160 allow_writeable_chroot=YES
161

```

Y reiniciar

```

daw-2t@ServidorLinuxegg:~$ sudo systemctl restart vsftpd.service
[sudo] password for daw-2t:
daw-2t@ServidorLinuxegg:~$

```

WireShark

Instalacion

Me aseguro de que el sistema esté actualizado

```

usuario@usuario-standardpc: ~
usuario@usuario-standardpc:~$ sudo apt update && sudo apt upgrade
[sudo] contraseña para usuario:
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
Des:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Des:3 https://dl.google.com/linux/chrome/deb stable InRelease [1.825 B]
Des:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]

```

Instalo wireshrk

```

usuario@usuario-standardpc: ~
usuario@usuario-standardpc:~$ sudo apt install wireshark -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
libb2-1 libbcg729-0 libcares2 libnghttp3-3 libopencore-amrnb0
libqt6core5compat6 libqt6core6t64 libqt6dbus6t64 libqt6gui6t64
libqt6multimedia6 libqt6network6t64 libqt6opengl6t64
libqt6printsupport6t64 libqt6qml6 libqt6qmlmodels6 libqt6quick6
libqt6svg6 libqt6waylandclient6 libqt6waylandcompositor6
libqt6waylandeglclient6 libqt6waylandintegration6

```


Añado el usuario con el que voy a usar wireshark al grupo y aplico los cambios

```
usuario@usuario-standardpc:~$ sudo usermod -aG wireshark usuario
usuario@usuario-standardpc:~$ newgrp wireshark
usuario@usuario-standardpc:~$ █
```

Ahora está correctamente instalado

```
usuario@usuario-standardpc:~$ wireshark --version
Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1.1build3).

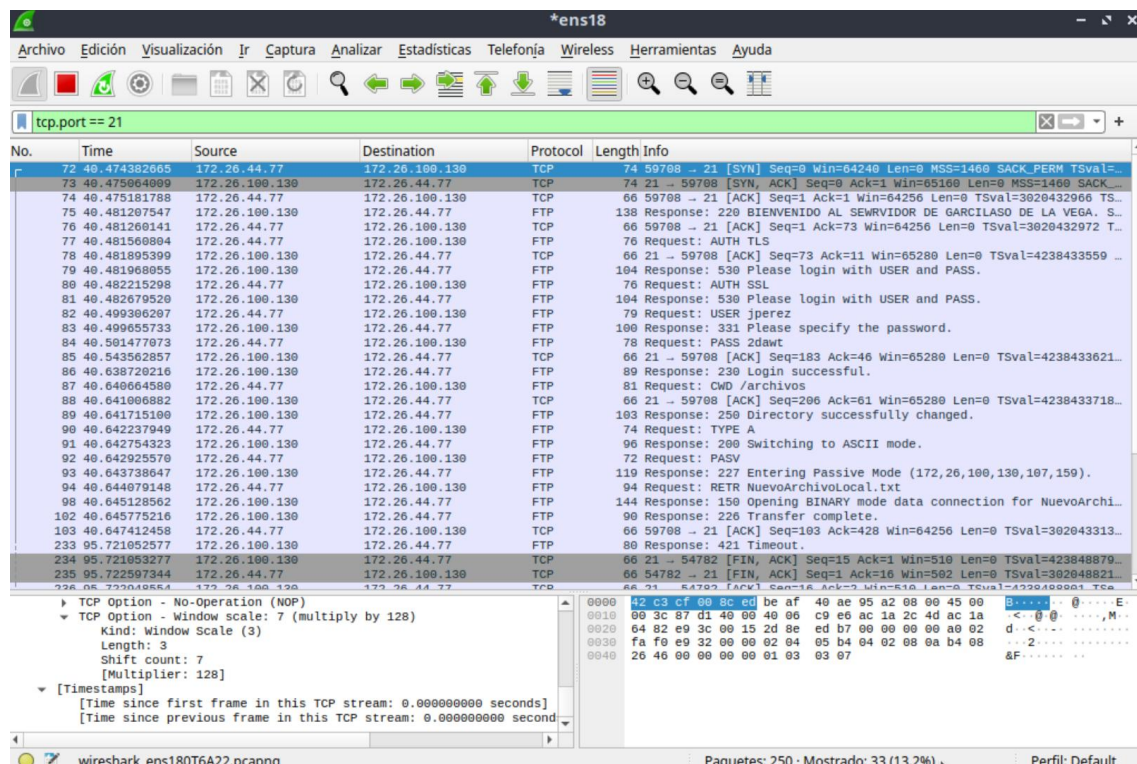
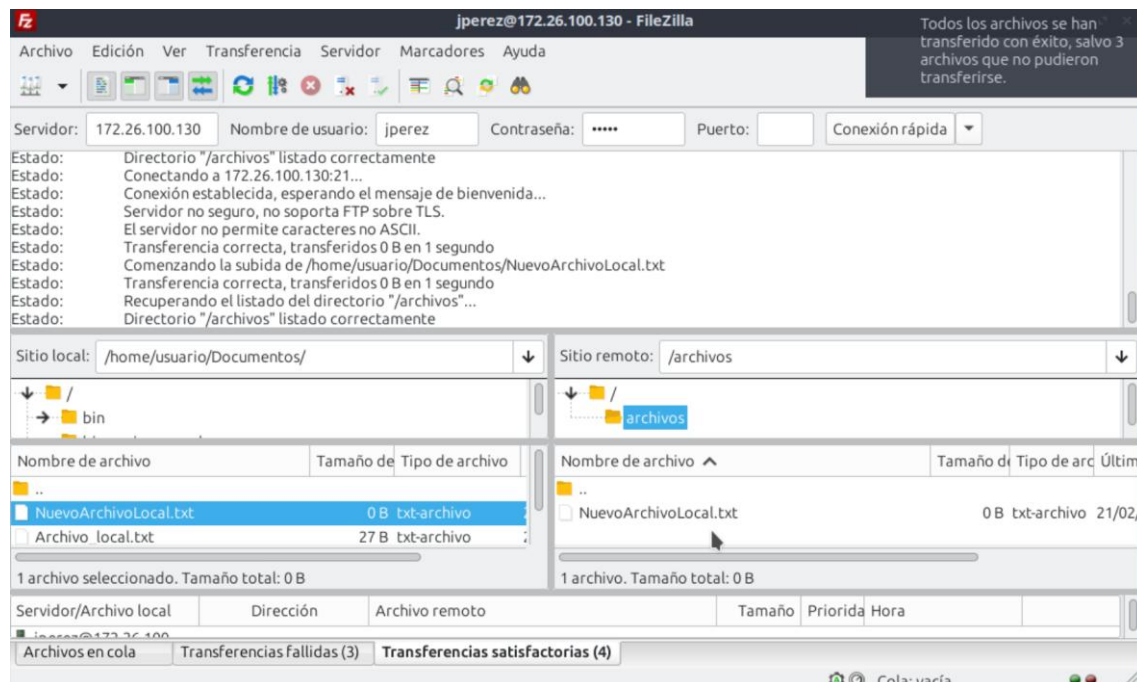
Copyright 1998-2024 Gerald Combs <gerald@wireshark.org> and contributors.
Licensed under the terms of the GNU General Public License (version 2 or later).
This is free software; see the file named COPYING in the distribution. There is
NO WARRANTY; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) using GCC 13.2.0, with GLib 2.80.0, with Qt 6.4.2, with
libpcap, with POSIX capabilities (Linux), with libnl 3, with zlib 1.3, with
PCRE2, with Lua 5.2.4, with GnuTLS 3.8.3 and PKCS #11 support, with Gcrypt
1.10.3, with Kerberos (MIT), with MaxMind, with nghttp2 1.59.0, with nghttp3
0.8.0, with brotli, with LZ4, with Zstandard, with Snappy, with libxml2 2.9.14,
with libsmi 0.4.8, with QtMultimedia, without automatic updates, with Minizip,
with binary plugins.

Running on Linux 6.8.0-52-generic, with QEMU Virtual CPU version 2.5+ (with
SSE4.2), with 1967 MB of physical memory, with GLib 2.80.0, with Qt 6.4.2, with
libpcap 1.10.4 (with TPACKET_V3), with zlib 1.3, with PCRE2 10.42 2022-12-11,
with c-ares 1.27.0, with GnuTLS 3.8.3, with Gcrypt 1.10.3, with nghttp2 1.59.0,
with nghttp3 0.8.0, with brotli 1.1.0, with LZ4 1.9.4, with Zstandard 1.5.5,
with libsmi 0.4.8, with LC_TYPE=es_ES.UTF-8, binary plugins supported.
usuario@usuario-standardpc:~$ █
```


Captura de tráfico

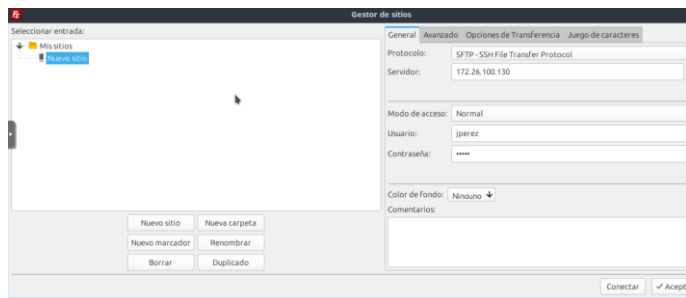
Conexión ftp



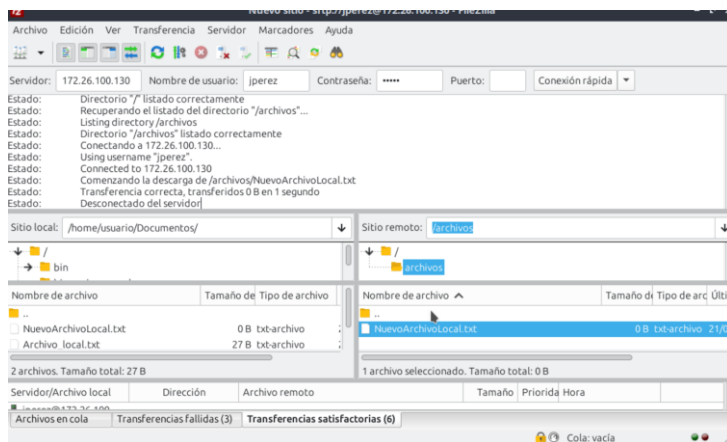
Puede verse que todo se transmite en texto plano, podemos ver el nombre del usuario, la contraseña del usuario y todo.

Conexión sftp

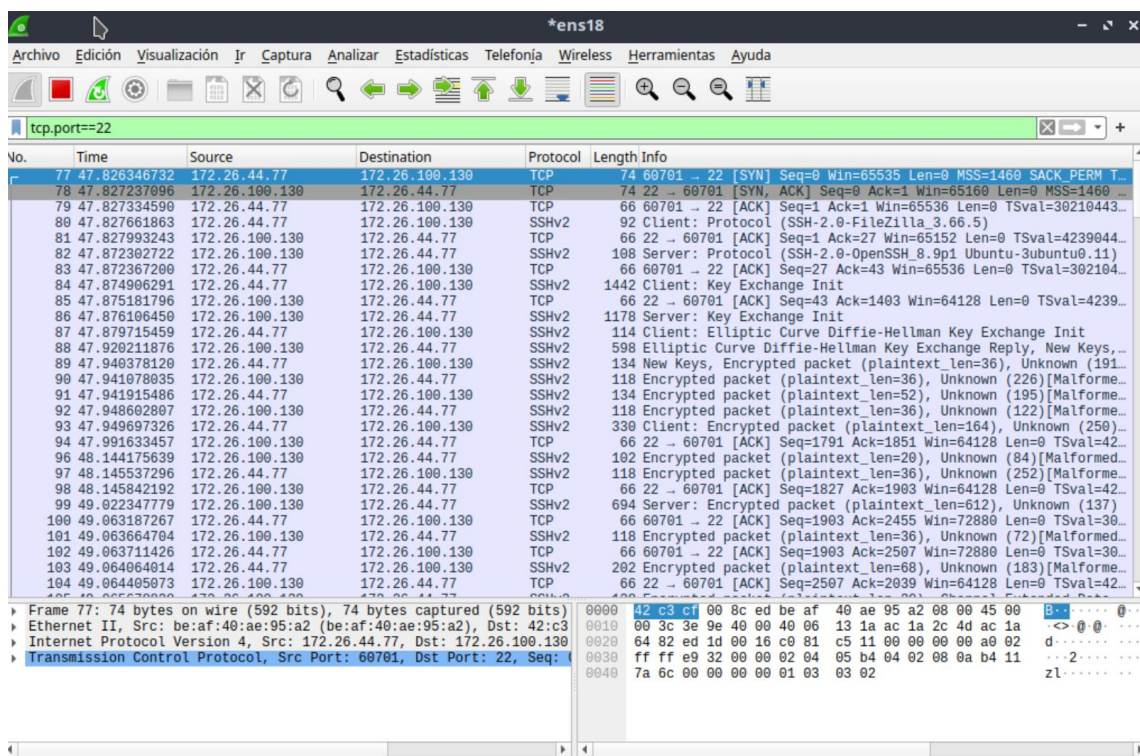
Se configura filezilla para una nueva conexión sftp



Realizamos una descarga



Y ahora todo aparece encriptado



Comparativa FTP SFTP

- FTP es menos seguro porque transmite datos en texto claro.
- SFTP cifra toda la comunicación, protegiendo credenciales y datos.

Tabla con diferencias

Característica	FTP	SFTP
Seguridad	No cifra los datos por defecto; las credenciales y archivos viajan en texto plano.	Cifra tanto los datos como las credenciales mediante SSH.
Autenticación	Basada en nombre de usuario y contraseña.	Utiliza autenticación por clave pública o contraseña.
Puerto por defecto	Usa el puerto 21 (y otros puertos para transferencia de datos en modo activo/pasivo).	Usa el puerto 22, el mismo que SSH.
Protocolo subyacente	TCP/IP estándar.	SSH (Secure Shell).
Compatibilidad	Ampliamente compatible, pero requiere configuraciones adicionales para ser seguro, como tunelizarlo por ssh	Funciona en cualquier servidor SSH, por lo que no requiere configuración adicional de puertos.
Cifrado de datos	No incluye cifrado, salvo que se use FTPS.	Todo el tráfico está cifrado por defecto.
Acceso anónimo	Permite el acceso anónimo si está configurado.	No permite acceso anónimo por defecto.
Enjaulamiento	Requiere configuraciones adicionales para restringir usuarios a sus directorios.	Más sencillo de configurar mediante las opciones de <code>sshd_config</code> .

¿Por qué SFTP es más seguro?

1. Todo el tráfico de datos, contraseñas y comandos se cifra, evitando ataques de tipo *sniffing* o *man-in-the-middle*.
2. Permite el uso de claves SSH, lo que refuerza la seguridad frente a contraseñas débiles.

3. A diferencia de FTP (que requiere múltiples puertos), SFTP solo necesita el puerto 22, facilitando las configuraciones de firewall.
4. Mayor control de permisos: Se integra directamente con los permisos de usuario de Unix/Linux, permitiendo una gestión más detallada.

¿Por qué seguir usando FTP?

- Puede ser más rápido para transferencias locales en redes cerradas.
- Herramientas más antiguas o sistemas heredados pueden no soportar SFTP.
- Puede ser útil en escenarios donde la seguridad no es una prioridad (por ejemplo, transferencia de archivos públicos sin datos sensibles).

Si la prioridad es la seguridad, SFTP es la mejor opción. Aunque FTP puede ser más fácil de implementar en sistemas antiguos, su falta de cifrado lo hace vulnerable en redes no seguras.