



Centro de Enseñanza Técnica Industrial

Desarrollo de Software

Instalación del servidor FTP + SSL

Jesús Alberto Aréchiga Carrillo

22310439 5N

Profesor

José Francisco Pérez Reyes

Diciembre 2024

Guadalajara, Jalisco

Introducción

El protocolo FTP es una herramienta estándar utilizada para la transferencia de archivos entre sistemas cliente y servidor. Sin embargo, en su forma básica, FTP transmite datos sin cifrar, lo que puede ser un riesgo de seguridad en redes públicas o no confiables.

Para mitigar este problema, se puede utilizar FTPS (FTP Secure), una versión de FTP que agrega una capa de seguridad mediante el protocolo SSL/TLS. El servidor vsftpd, conocido por su seguridad y eficiencia, soporta el uso de certificados SSL/TLS para habilitar conexiones FTPS, asegurando que las comunicaciones entre el cliente y el servidor estén cifradas.

Desarrollo

El objetivo principal de este proyecto es habilitar conexiones FTPS en un servidor vsftpd mediante la instalación y configuración de un certificado SSL/TLS. Esto garantizará que todas las transferencias de archivos y credenciales sean seguras, protegiendo la integridad y confidencialidad de los datos. Se va a utilizar una VM con el servidor ya instalado previamente, en este caso la VM tiene una IP 10.0.0.8.

Para instalar el certificado se utiliza el comando “openssl req -x509 -nodes -days 1825 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/ssl/certs/vsftpd.crt”

La consola va a mostrar los campos del certificado que hay que ingresar para poder generarlo:

Country Name (2 letter code) [GB]: MX

State or Province Name (full name) [Berkshire]: Jalisco

Locality Name (eg, city) [Newbury]: Guadalajara

Organization Name (eg, company) [My Company Ltd]: Empresa, S.A. de C.V.

Organizational Unit Name (eg, section) []: Departamento de TI

Common Name (eg your name or your server's hostname) []: *.dominio.org

Email Address []: webmaster@dominio.org

Se le dan los permisos al certificado y a la clave privada con “chmod 400 /etc/ssl/certs/vsftpd.crt /etc/ssl/private/vsftpd.key”

Ahora se agregan las configuraciones al archivo vsftpd.cfg

```
# Habilita el soporte de TLS/SSL
ssl_enable=YES
# Deshabilita o habilita utilizar TLS/SSL con usuarios anónimos
allow_anon_ssl=NO
# Obliga a utilizar TLS/SSL para todas las operaciones,
# es decir, transferencia de datos y
# autenticación de usuarios locales. Establecer el valor NO,
# hace que sea opcional utilizar TLS/SSL.
force_local_data_ssl=YES
force_local_logins_ssl=YES
# Se prefiere TLSv1 sobre SSLv2 y SSLv3
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
# Rutas del certificado y firma digital
rsa_cert_file=/etc/ssl/certs/vsftpd.crt
rsa_private_key_file=/etc/ssl/private/vsftpd.key
# Los desarrolladores de FileZilla decidieron con la versión 3.5.3 que
# eliminarían el soporte para
# el algoritmo de cifrado 3DES-CBC-SHA, con el argumento de que este
# algoritmo es una de los más
# lentos. Sin embargo con ésto rompieron compatibilidad con miles de
# servidores FTP que utilizan
# FTPES. La solución temporal, mientras los desarrolladores de FileZilla
# razonan lo absurdo de su
# decisión, es utilizar la siguiente opción:
ssl_ciphers=HIGH
# Filezilla además requiere desactivar la siguiente opción que puede
# romper compatibilidad con otros
# clientes. Cabe señalar que Filezilla se ha convertido en un desarrollo
# políticamente incorrecto
# por dejar de respetar los estándares.
require_ssl_reuse=NO
```

Se reinicia el servicio y se prueba.

Evidencias

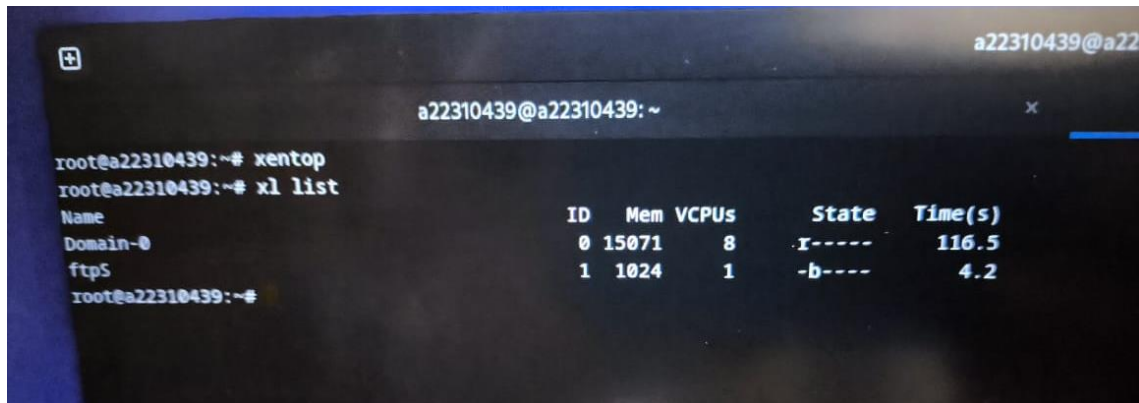
Consola mostrando la dirección IP de la máquina virtual con la que está trabajando en ese momento

```
a22310439@a22310439:~  
[ OK ] Started dbus.service - D-Bus System Message Bus.  
[ 3.288812] cryptd: max_cpu_qlen set to 1000  
[ OK ] Started systemd-logind.service - User Login Management.  
root@ftp5:~# ip a s  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:16:3e:a5:94:b7 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.0.8/24 brd 10.0.0.255 scope global enX0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::216:3eff:fea5:94b7/64 scope link  
        valid_lft forever preferred_lft forever  
root@ftp5:~#
```

Consola mostrando los procesos que se están ejecutando en la máquina virtual y visualizando correctamente el proceso vsftpd

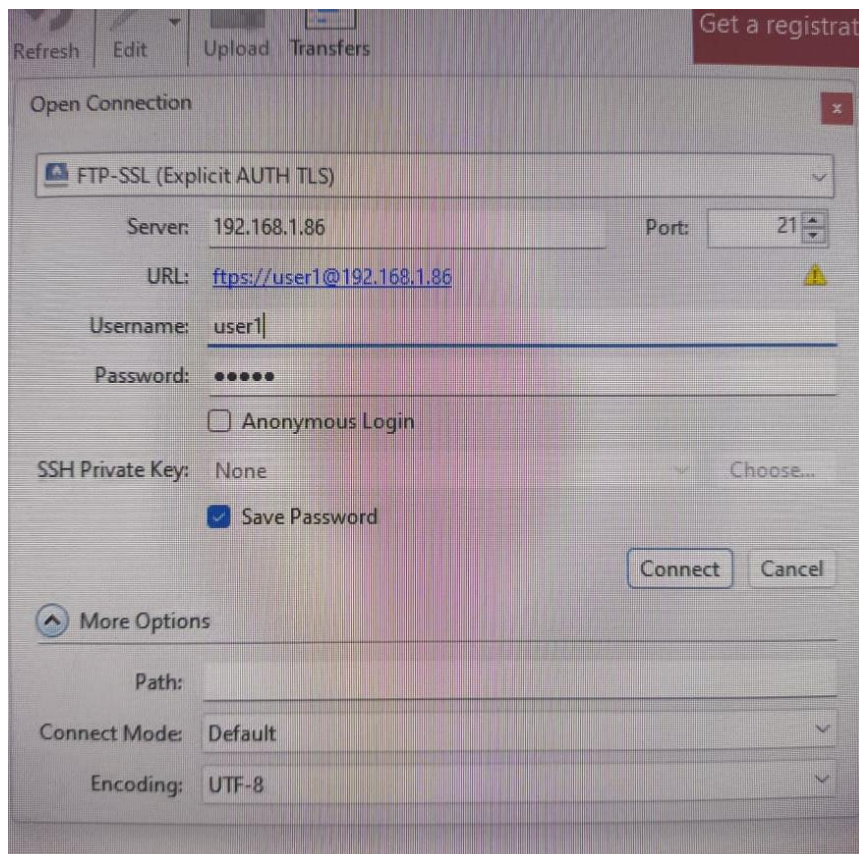
```
a22310439@a22310439:~  
50 ?      00:00:00 mld  
51 ?      00:00:00 ipv6_addrconf  
56 ?      00:00:00 kstrp  
61 ?      00:00:00 zswap-shrink  
62 ?      00:00:00 kworker/u3:0  
135 ?     00:00:00 jbd2/xvda2-8  
136 ?     00:00:00 ext4-rsv-conver  
173 ?     00:00:00 systemd-journal  
177 ?     00:00:00 kworker/u2:3-events_unbound  
200 ?     00:00:00 systemd-udev  
225 ?     00:00:00 cron  
226 ?     00:00:00 dbus-daemon  
228 ?     00:00:00 systemd-logind  
229 ?     00:00:00 cryptd  
291 ?     00:00:00 kworker/0:4-cgwb_release  
354 ?     00:00:00 vsftpd  
355 tty1   00:00:00 agetty  
356 hvc0   00:00:00 login  
357 ?     00:00:00 sshd  
364 ?     00:00:00 systemd  
365 ?     00:00:00 (sd-pam)  
371 hvc0   00:00:00 bash  
381 hvc0   00:00:00 ps  
root@ftp5:~#
```

Consola del Dom0 mostrando la información de la ejecución de tu máquina virtual que está ejecutando el servidor de FTP

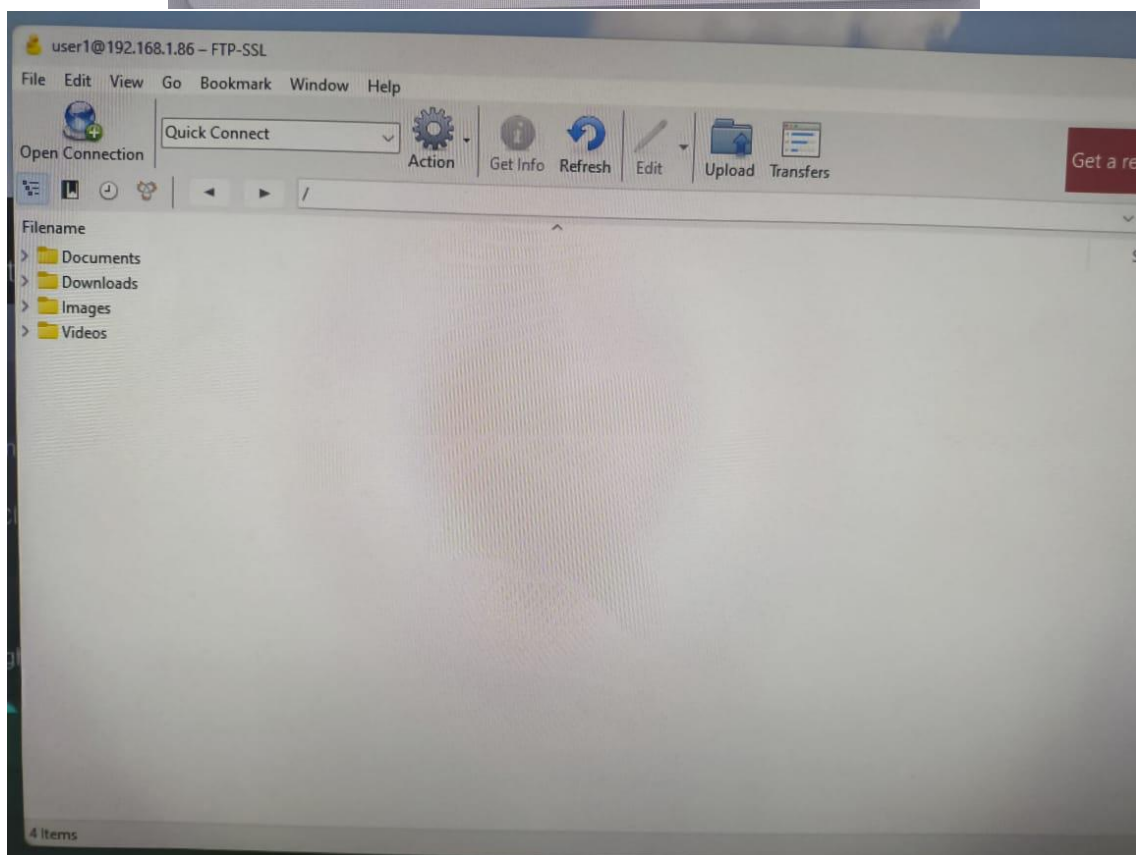
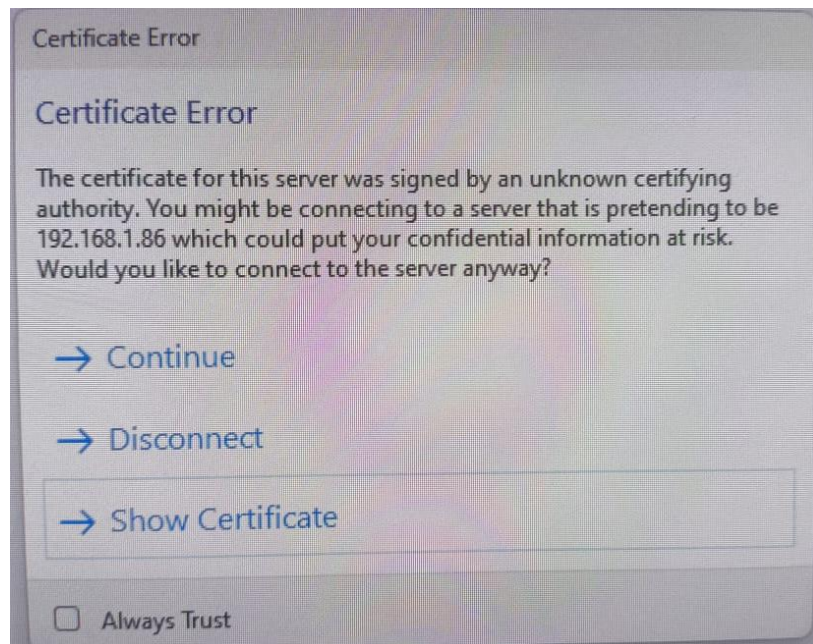


```
root@a22310439:~# xentop
root@a22310439:~# xl list
Name                               ID   Mem VCPUs   State   Time(s)
Domain-0                           0  15071    8   r----- 116.5
ftpS                                1   1024    1   -b----- 4.2
root@a22310439:~#
```

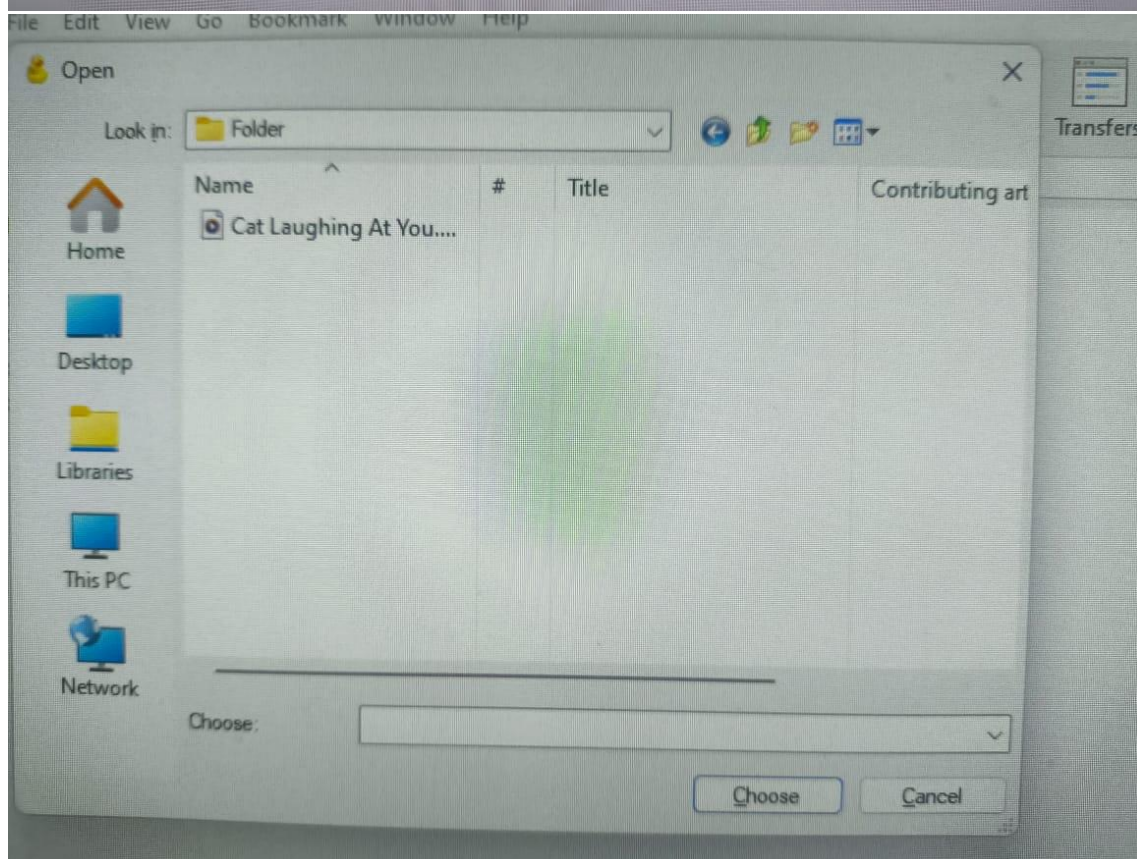
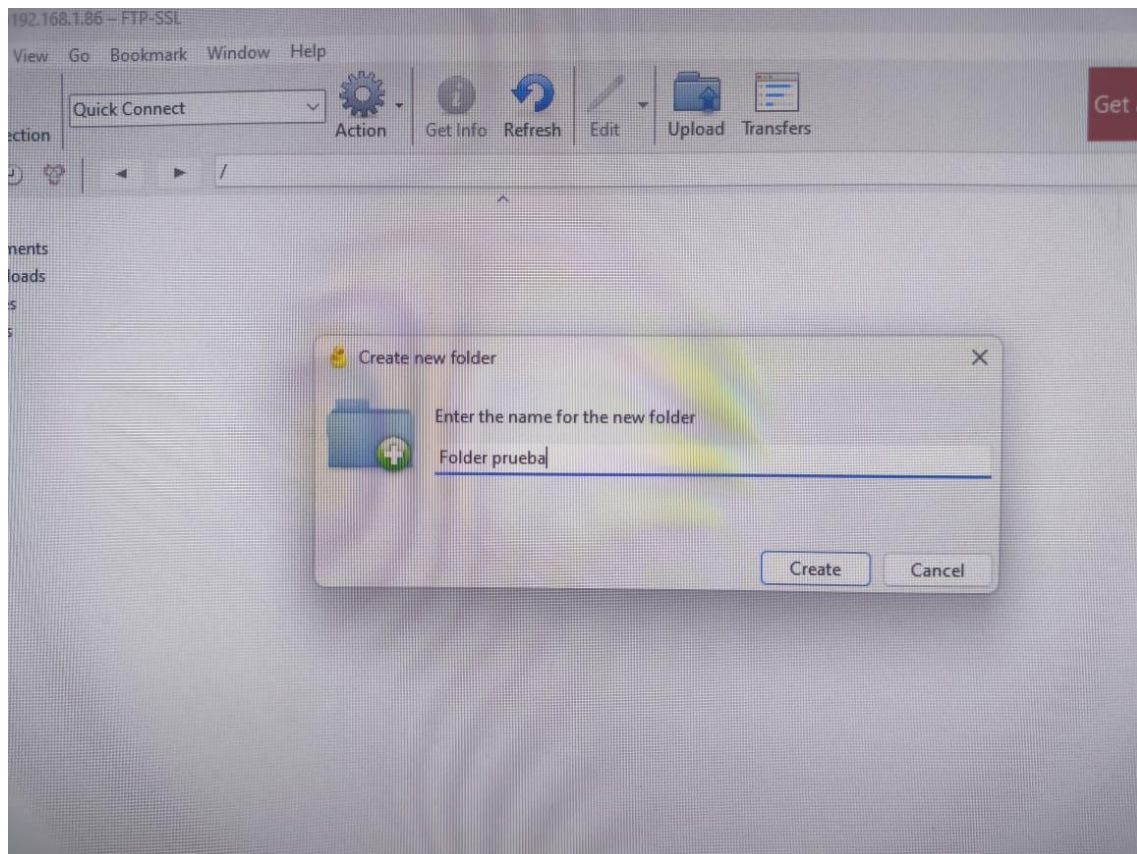
Ventana del cliente FTP para establecer la conexión (antes de establecer conexión) con toda la información y configuración requerida

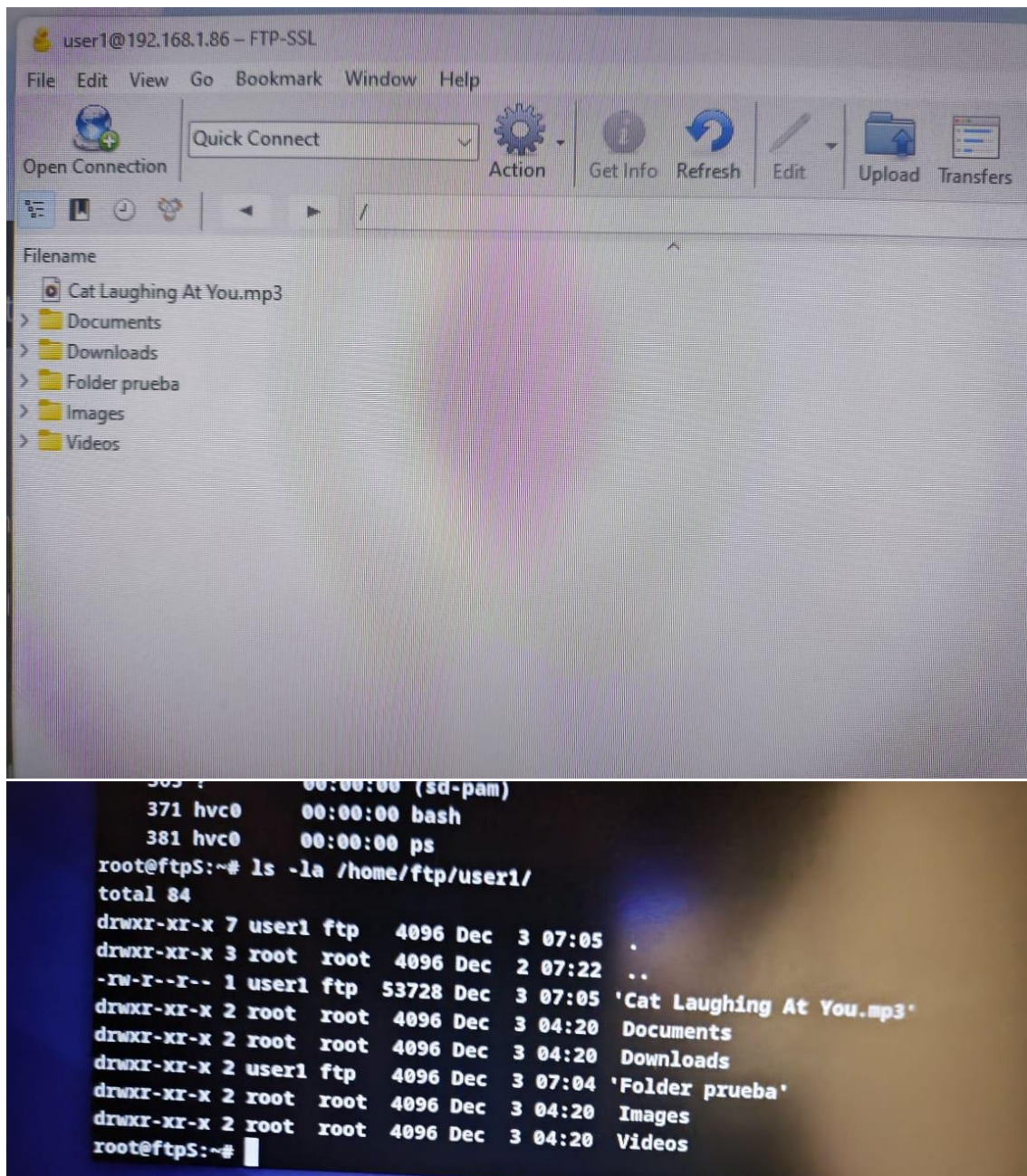


Ventana del cliente FTP mostrando la conexión realizada y mostrando las carpetas que tienes en tu servidor FTP.



Consola de la máquina virtual mostrando el detalle de la carpeta y archivo (comando: ls -la) que subiste desde el cliente FTP





Conclusiones

La implementación de un certificado SSL en el servidor vsftpd para habilitar conexiones FTPS constituye un avance significativo hacia la protección de la información en entornos de transferencia de archivos.

La transición de FTP a FTPS responde a la creciente necesidad de mitigar riesgos asociados con la interceptación de datos sensibles, particularmente en redes públicas. Al incorporar un certificado SSL, se garantiza una comunicación segura y verificable, protegiendo tanto las credenciales como los archivos intercambiados.