Modo activo

Modo activo.

En modo Activo, el servidor siempre crea el canal de datos en su puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024. Para ello, el cliente manda un comando PORT al servidor por el canal de control indicándole ese número de puerto, de manera que el servidor pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados, en el puerto especificado.

Lo anterior tiene un grave problema de seguridad, y es que la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1024, con los problemas que ello implica si tenemos el equipo conectado a una red insegura como Internet. De hecho, los cortafuegos que se instalen en el equipo para evitar ataques seguramente rechazarán esas conexiones aleatorias. Para solucionar esto se desarrolló el modo *pasivo*.

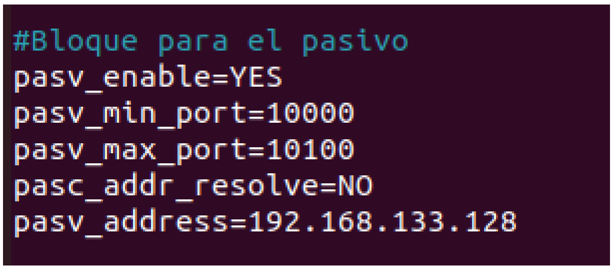
Modo pasivo

Modo pasivo.

Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control, el puerto (mayor a 1023 del servidor.) al que debe conectarse el cliente. El cliente inicia una conexión desde el puerto siguiente al puerto de control hacia el puerto del servidor especificado anteriormente.

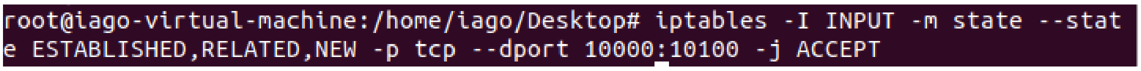
Antes de cada nueva transferencia tanto en el modo Activo como en el Pasivo, el cliente debe enviar otra vez un comando de control (PORT o PASV, según el modo en el que haya conectado), y el servidor recibirá esa conexión de datos en un nuevo puerto aleatorio (si está en modo pasivo) o por el puerto 20 (si está en modo activo). En el protocolo FTP existen 5 tipos de transferencia en ASCII y en binarios.

Configuramos el archivo de configuración y le añadimos las siguientes líneas



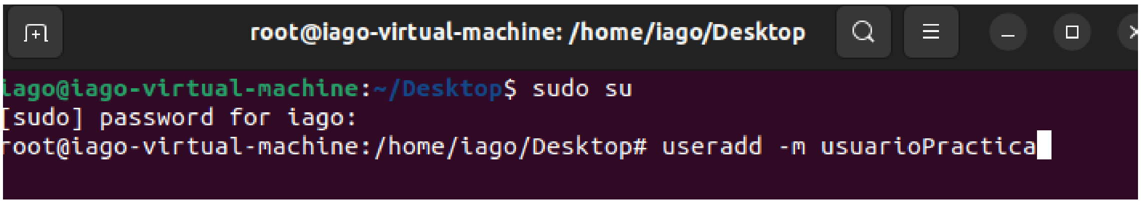
```
#Bloque para el pasivo
pasv_enable=YES
pasv_min_port=10000
pasv_max_port=10100
pasc_addr_resolve=NO
pasv_address=192.168.133.128
```

Modificamos los puertos

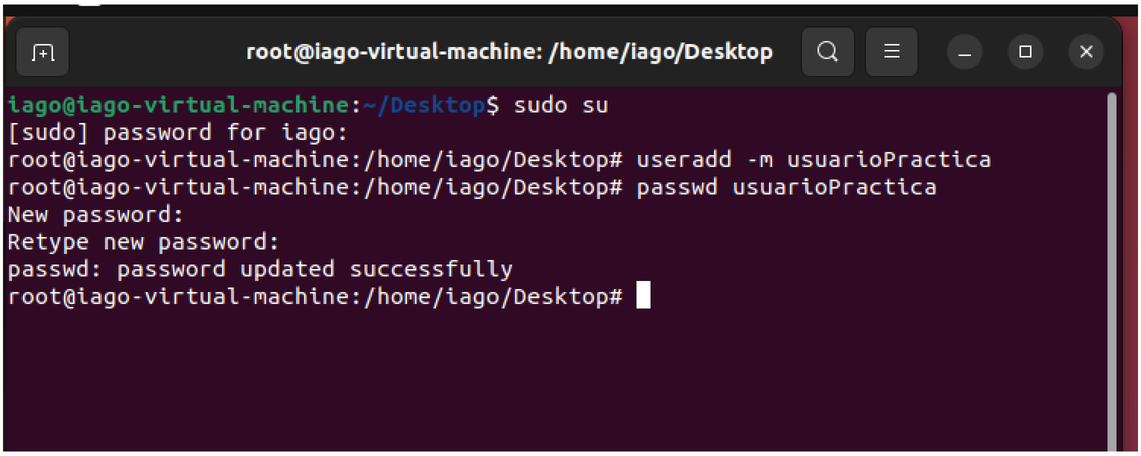


```
root@iago-virtual-machine:/home/iago/Desktop# iptables -I INPUT -m state --stat
e ESTABLISHED,RELATED,NEW -p tcp --dport 10000:10100 -j ACCEPT
```

Creamos el nuevo usuario y le añadimos contraseña:

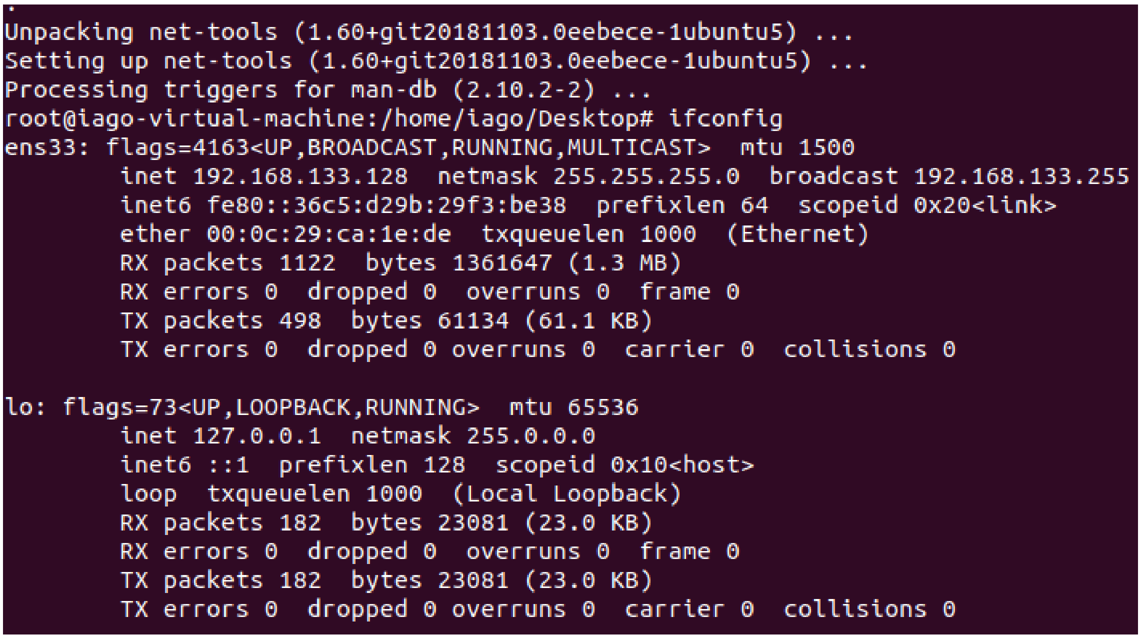


```
iago@iago-virtual-machine:~/Desktop$ sudo su
[sudo] password for iago:
root@iago-virtual-machine:/home/iago/Desktop# useradd -m usuarioPractica
```

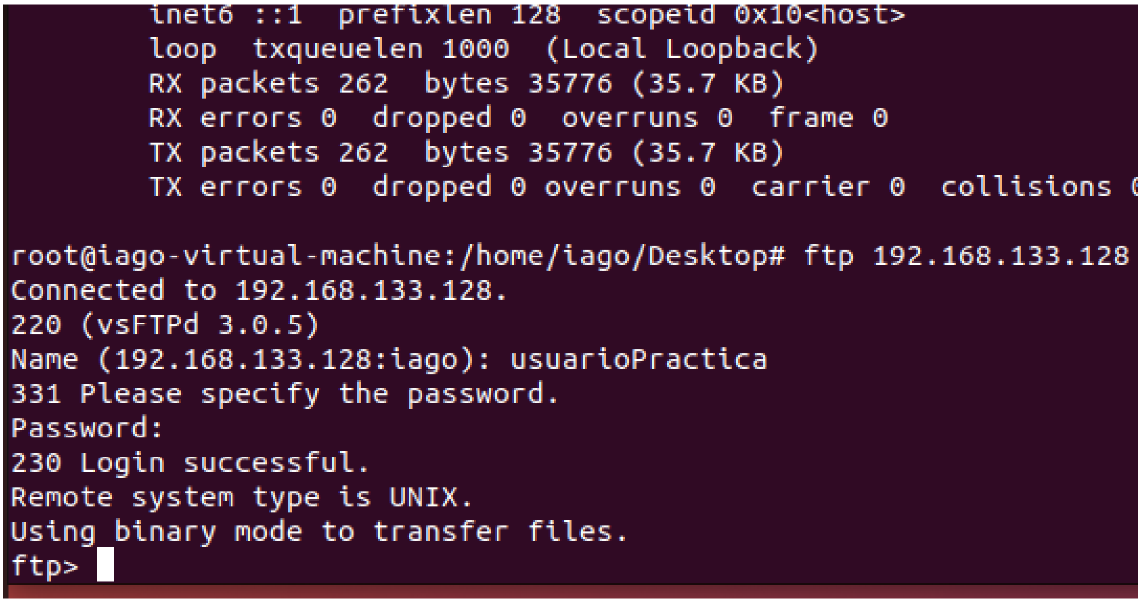


```
iago@iago-virtual-machine:~/Desktop$ sudo su
[sudo] password for iago:
root@iago-virtual-machine:/home/iago/Desktop# useradd -m usuarioPractica
root@iago-virtual-machine:/home/iago/Desktop# passwd usuarioPractica
New password:
Retype new password:
passwd: password updated successfully
root@iago-virtual-machine:/home/iago/Desktop# 
```

Checkeamos la IP y entramos al FTP

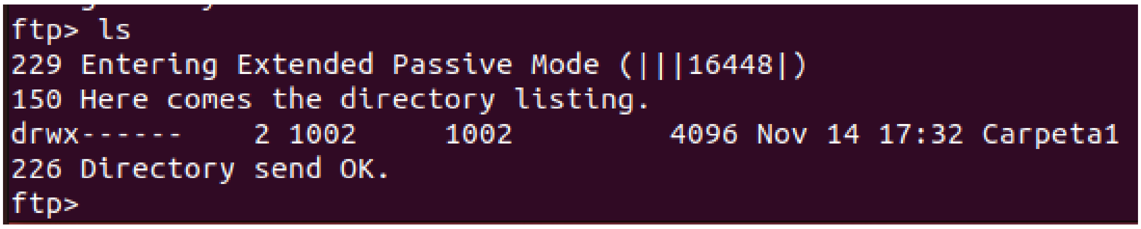


```
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Processing triggers for man-db (2.10.2-2) ...
root@iago-virtual-machine:/home/iago/Desktop# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.133.128  netmask 255.255.255.0  broadcast 192.168.133.255
        inet6 fe80::36c5:d29b:29f3:be38  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ca:1e:de  txqueuelen 1000  (Ethernet)
        RX packets 1122  bytes 1361647 (1.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 498  bytes 61134 (61.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 182  bytes 23081 (23.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 182  bytes 23081 (23.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



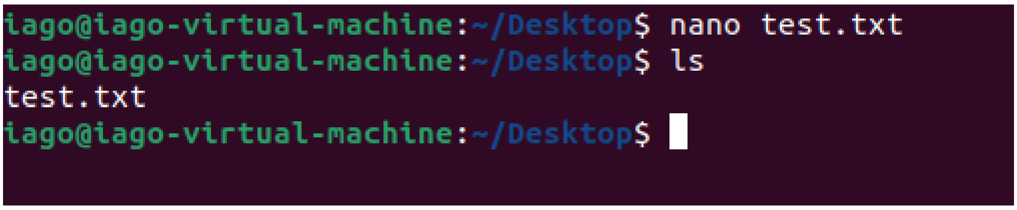
```
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 262  bytes 35776 (35.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 262  bytes 35776 (35.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

root@iago-virtual-machine:/home/iago/Desktop# ftp 192.168.133.128
Connected to 192.168.133.128.
220 (vsFTPd 3.0.5)
Name (192.168.133.128:iago): usuarioPractica
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

No he puesto el comando para crear la carpeta porque soy tonto pero es MKDIR CARPETA1

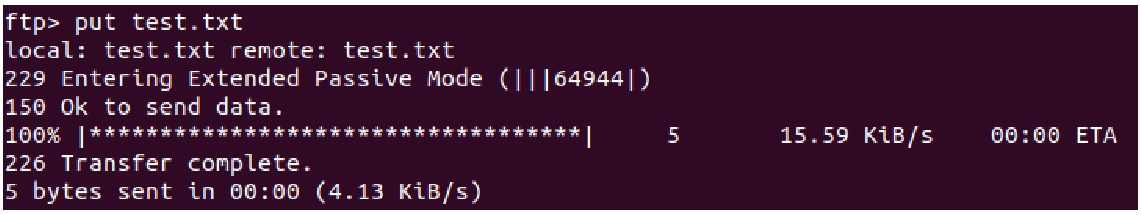


```
ftp> ls
229 Entering Extended Passive Mode (|||16448|)
150 Here comes the directory listing.
drwx------    2 1002     1002         4096 Nov 14 17:32 Carpeta1
226 Directory send OK.
ftp>
```

Creamos localmente un archivo y lo subimos en FTP usando PUT

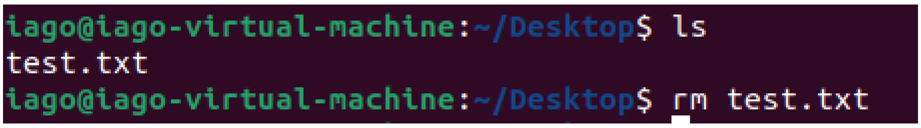


```
iago@iago-virtual-machine:~/Desktop$ nano test.txt
iago@iago-virtual-machine:~/Desktop$ ls
test.txt
iago@iago-virtual-machine:~/Desktop$ 
```

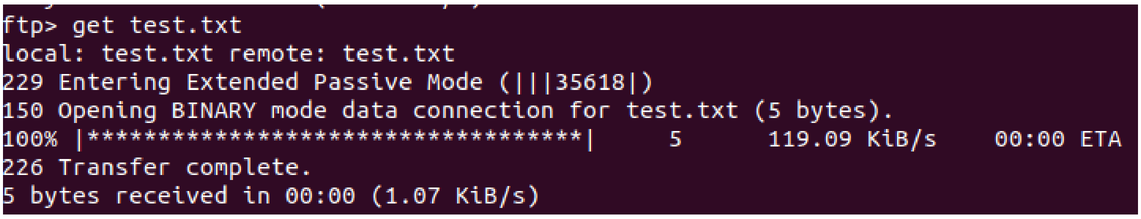


```
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||64944|)
150 Ok to send data.
100% |***********************************|     5       15.59 KiB/s    00:00 ETA
226 Transfer complete.
5 bytes sent in 00:00 (4.13 KiB/s)
```

Borramos el archivo local y lo descargamos de nuevo desde el FTP usando GET

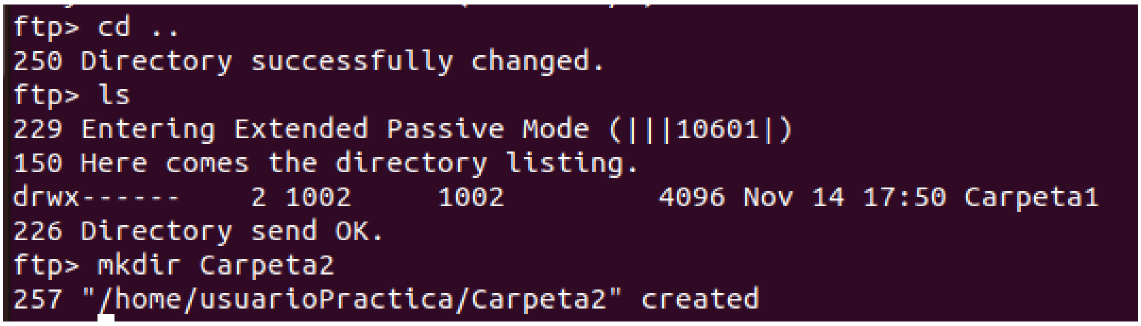


```
iago@iago-virtual-machine:~/Desktop$ ls
test.txt
iago@iago-virtual-machine:~/Desktop$ rm test.txt
```



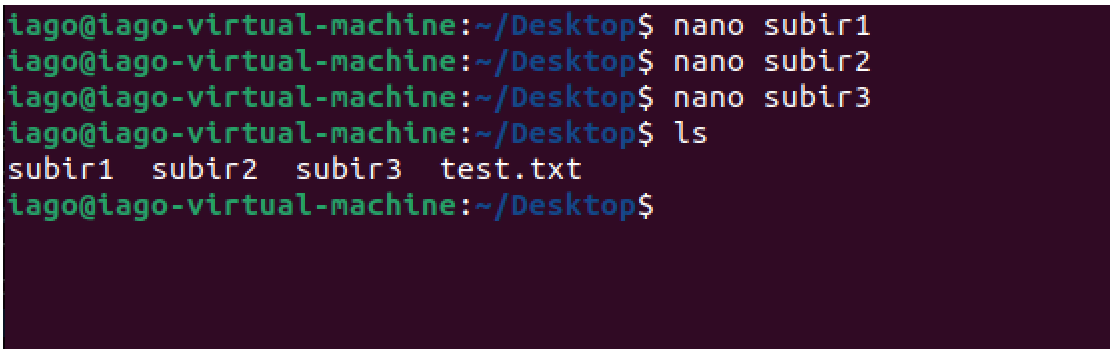
```
ftp> get test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||35618|)
150 Opening BINARY mode data connection for test.txt (5 bytes).
100% |***********************************|     5      119.09 KiB/s    00:00 ETA
226 Transfer complete.
5 bytes received in 00:00 (1.07 KiB/s)
```

Salimos al directorio anterior y creamos otra carpeta con mput*

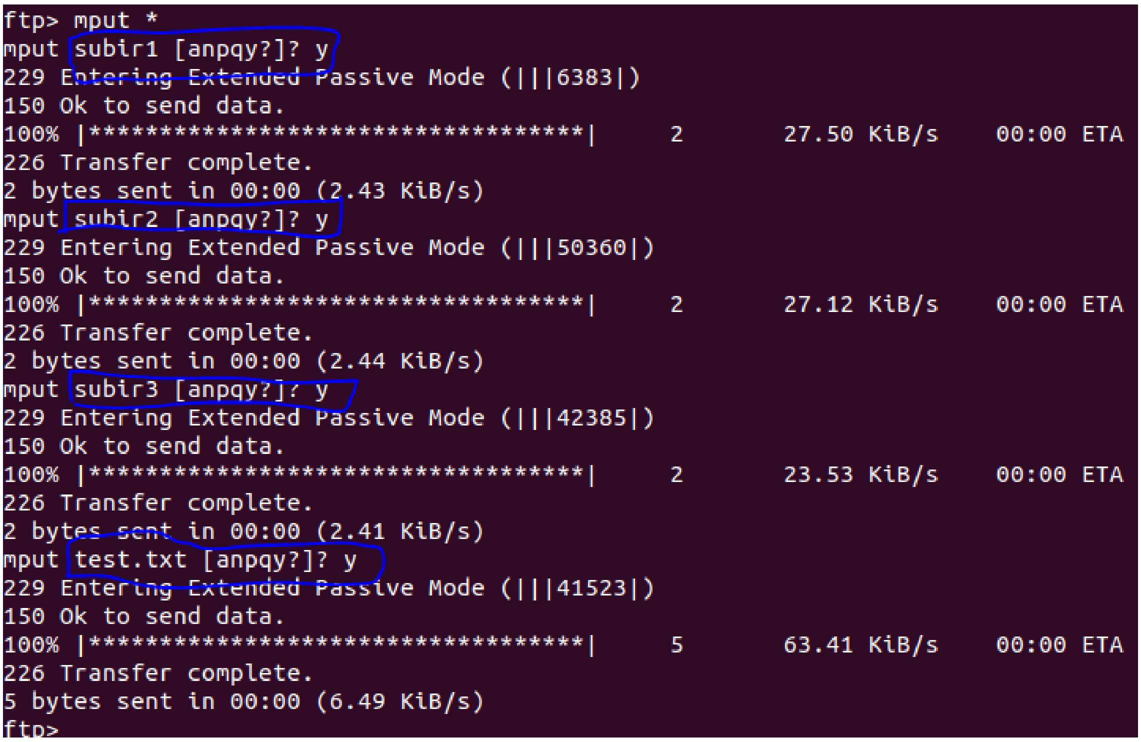


```
ftp> cd ..
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||10601|)
150 Here comes the directory listing.
drwx------    2 1002     1002         4096 Nov 14 17:50 Carpeta1
226 Directory send OK.
ftp> mkdir Carpeta2
257 "/home/usuarioPractica/Carpeta2" created
```

Creamos varios archivos y los subimos en Carpeta2

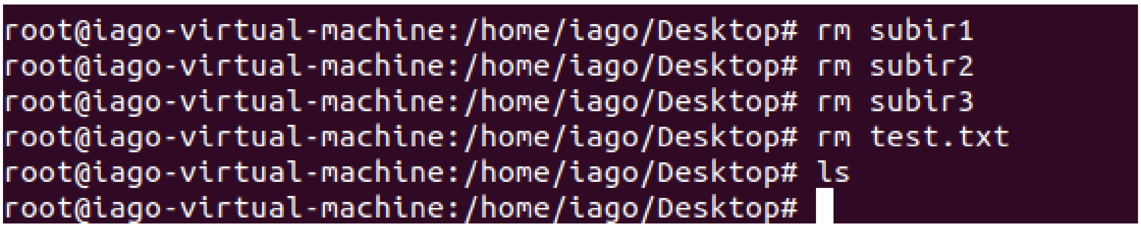


```
iago@iago-virtual-machine:~/Desktop$ nano subir1
iago@iago-virtual-machine:~/Desktop$ nano subir2
iago@iago-virtual-machine:~/Desktop$ nano subir3
iago@iago-virtual-machine:~/Desktop$ ls
subir1  subir2  subir3  test.txt
iago@iago-virtual-machine:~/Desktop$
```

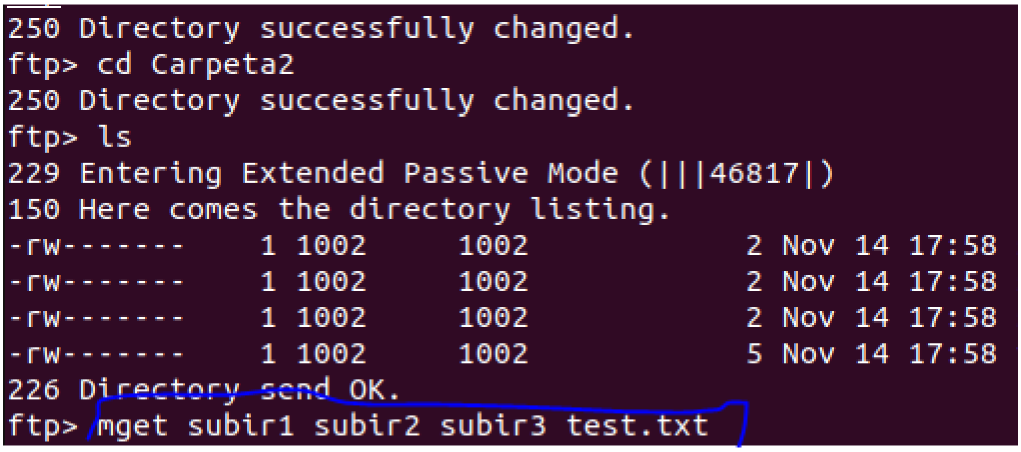


```
ftp> mput *
mput subir1 [anpqy?]? y
229 Entering Extended Passive Mode (|||6383|)
150 Ok to send data.
100% |***********************************|     2       27.50 KiB/s    00:00 ETA
226 Transfer complete.
2 bytes sent in 00:00 (2.43 KiB/s)
mput subir2 [anpqy?]? y
229 Entering Extended Passive Mode (|||50360|)
150 Ok to send data.
100% |***********************************|     2       27.12 KiB/s    00:00 ETA
226 Transfer complete.
2 bytes sent in 00:00 (2.44 KiB/s)
mput subir3 [anpqy?]? y
229 Entering Extended Passive Mode (|||42385|)
150 Ok to send data.
100% |***********************************|     2       23.53 KiB/s    00:00 ETA
226 Transfer complete.
2 bytes sent in 00:00 (2.41 KiB/s)
mput test.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||41523|)
150 Ok to send data.
100% |***********************************|     5       63.41 KiB/s    00:00 ETA
226 Transfer complete.
5 bytes sent in 00:00 (6.49 KiB/s)
ftp>
```

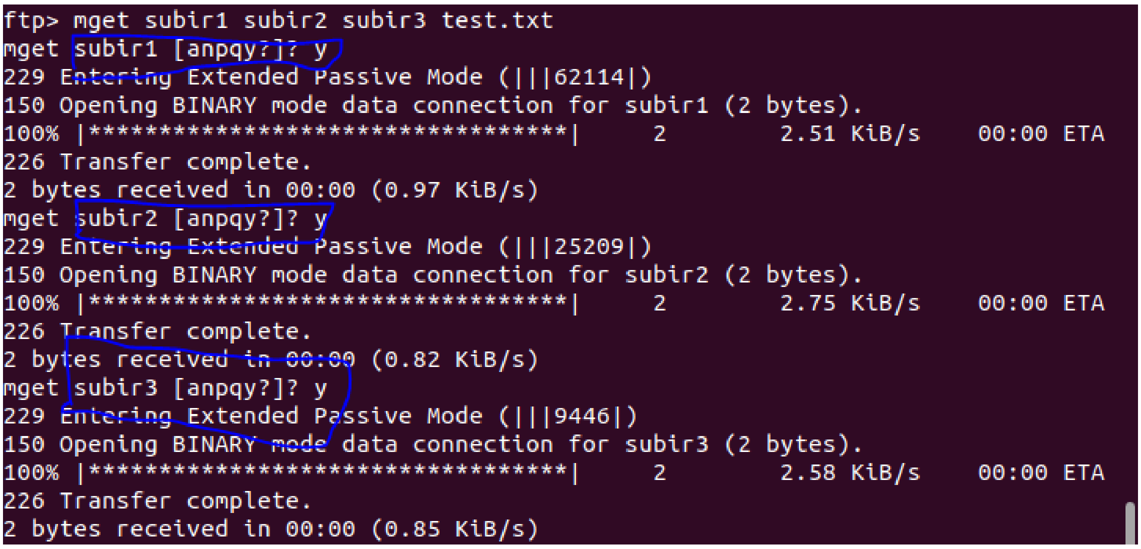
Borramos todos los archivos y los volvemos a descargar a la vez usando mget



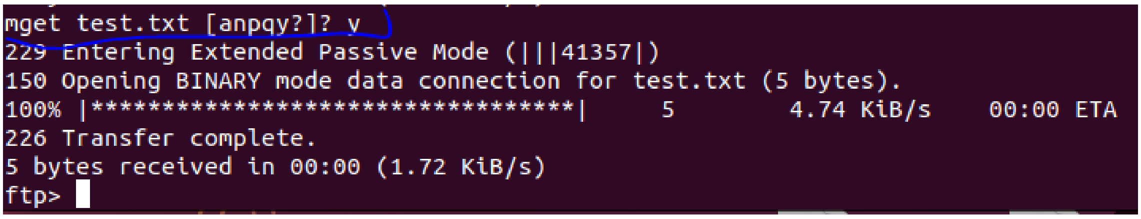
```
root@iago-virtual-machine:/home/iago/Desktop# rm subir1
root@iago-virtual-machine:/home/iago/Desktop# rm subir2
root@iago-virtual-machine:/home/iago/Desktop# rm subir3
root@iago-virtual-machine:/home/iago/Desktop# rm test.txt
root@iago-virtual-machine:/home/iago/Desktop# ls
root@iago-virtual-machine:/home/iago/Desktop#
```



```
250 Directory successfully changed.
ftp> cd Carpeta2
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||46817|)
150 Here comes the directory listing.
-rw-------     1 1002      1002               2 Nov 14 17:58
-rw-------     1 1002      1002               2 Nov 14 17:58
-rw-------     1 1002      1002               2 Nov 14 17:58
-rw-------     1 1002      1002               5 Nov 14 17:58
226 Directory send OK.
ftp> mget subir1 subir2 subir3 test.txt
```

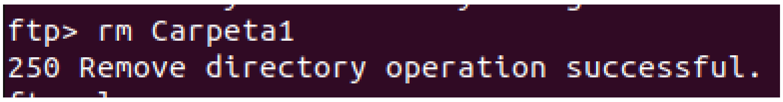


```
ftp> mget subir1 subir2 subir3 test.txt
mget subir1 [anpqy?]? y
229 Entering Extended Passive Mode (|||62114|)
150 Opening BINARY mode data connection for subir1 (2 bytes).
100% |***********************************|     2        2.51 KiB/s    00:00 ETA
226 Transfer complete.
2 bytes received in 00:00 (0.97 KiB/s)
mget subir2 [anpqy?]? y
229 Entering Extended Passive Mode (|||25209|)
150 Opening BINARY mode data connection for subir2 (2 bytes).
100% |***********************************|     2        2.75 KiB/s    00:00 ETA
226 Transfer complete.
2 bytes received in 00:00 (0.82 KiB/s)
mget subir3 [anpqy?]? y
229 Entering Extended Passive Mode (|||9446|)
150 Opening BINARY mode data connection for subir3 (2 bytes).
100% |***********************************|     2        2.58 KiB/s    00:00 ETA
226 Transfer complete.
2 bytes received in 00:00 (0.85 KiB/s)
```

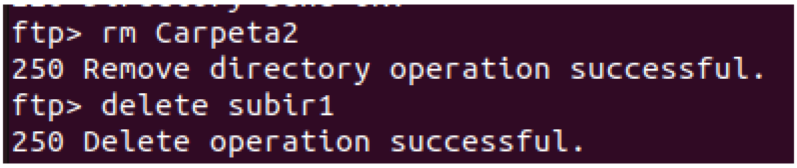


```
mget test.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||41357|)
150 Opening BINARY mode data connection for test.txt (5 bytes).
100% |***********************************|     5        4.74 KiB/s    00:00 ETA
226 Transfer complete.
5 bytes received in 00:00 (1.72 KiB/s)
ftp> 
```

Borramos todos los directorios

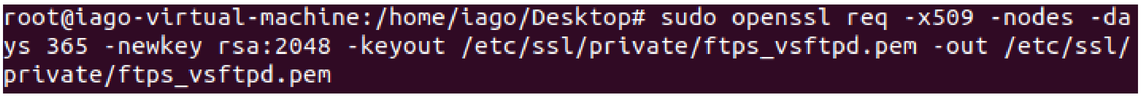


```
ftp> rm Carpeta1
250 Remove directory operation successful.
```

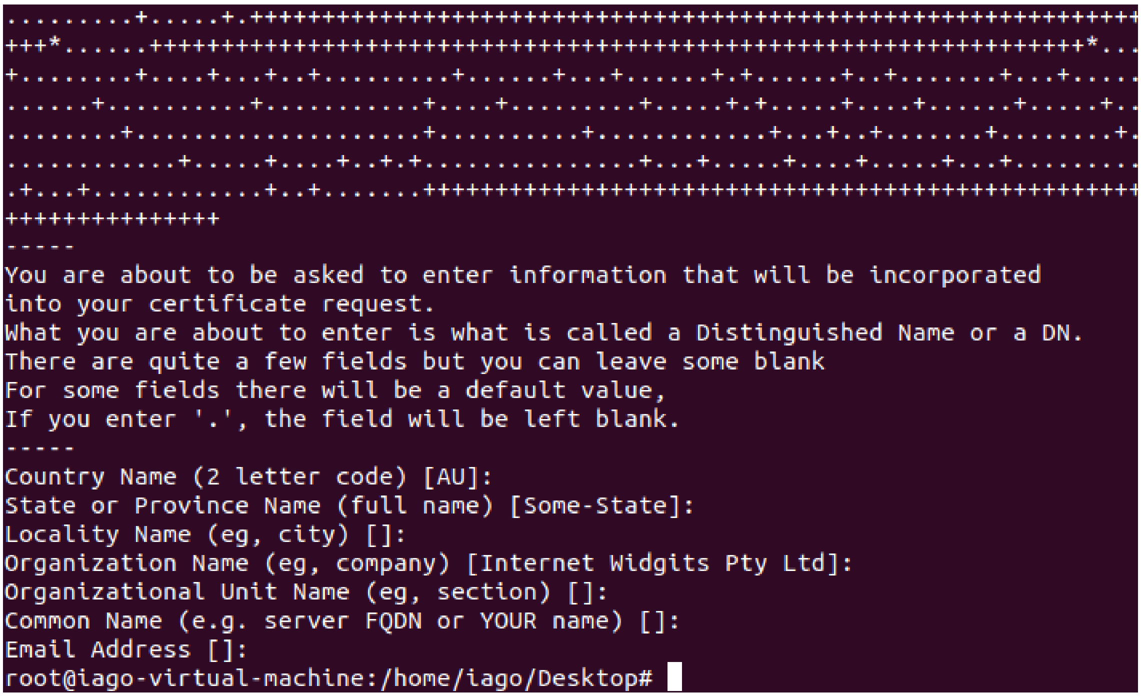


```
ftp> rm Carpeta2
250 Remove directory operation successful.
ftp> delete subir1
250 Delete operation successful.
```

Configuramos el servidor en FTPS de la siguiente forma

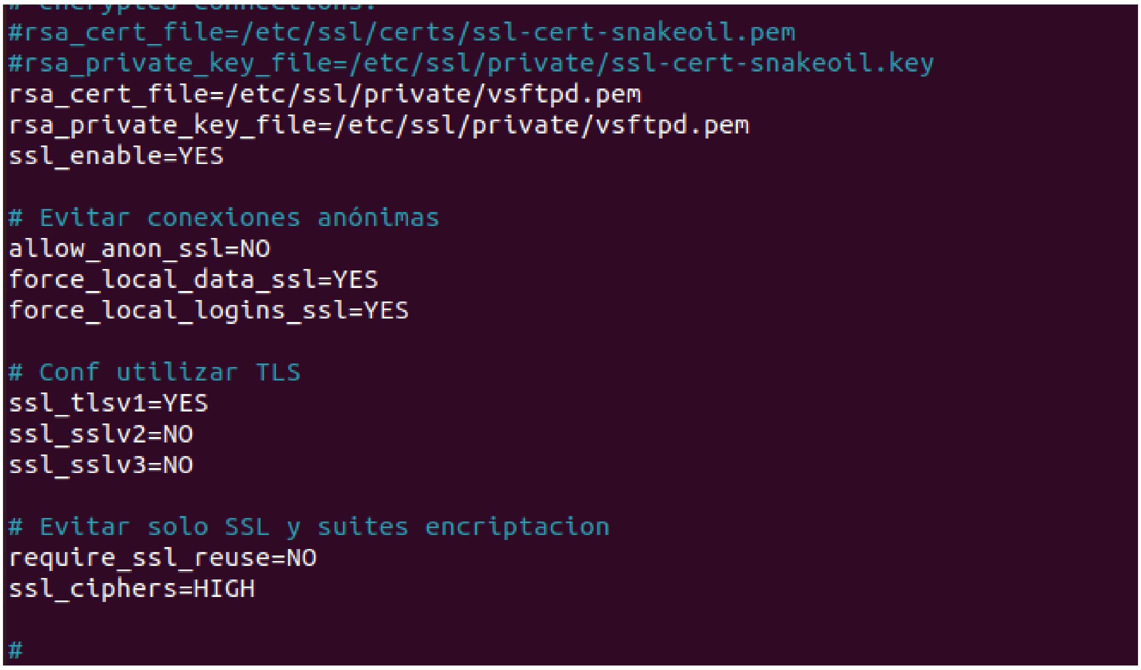


```
root@iago-virtual-machine:/home/iago/Desktop# sudo openssl req -x509 -nodes -da
ys 365 -newkey rsa:2048 -keyout /etc/ssl/private/ftps_vsftpd.pem -out /etc/ssl/
private/ftps_vsftpd.pem
```

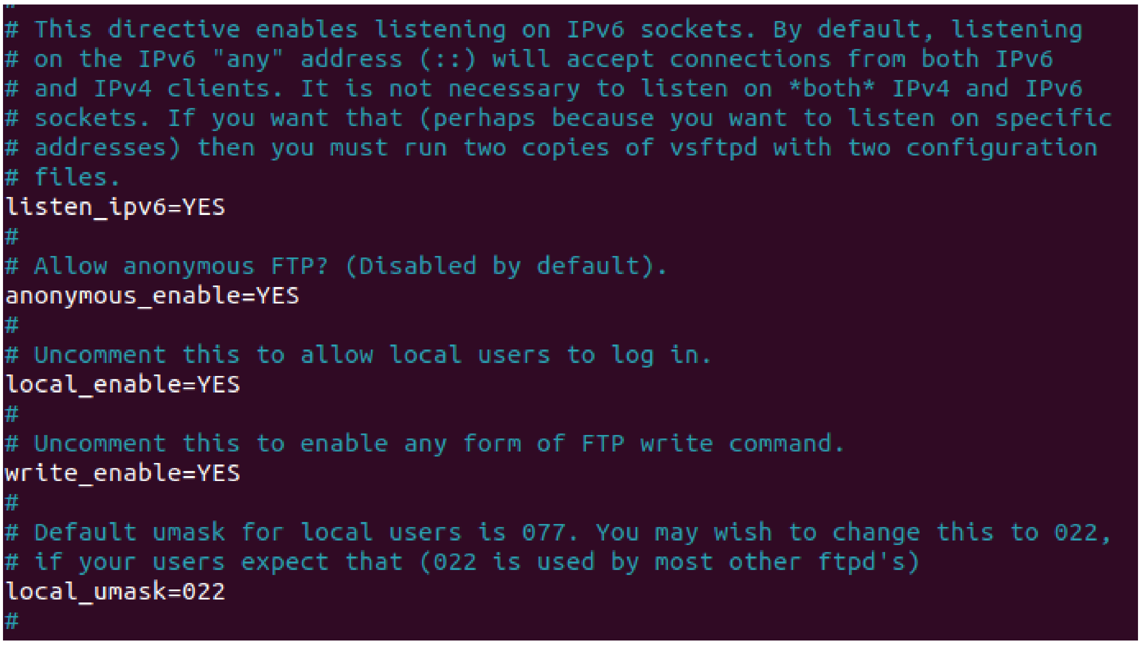


```
.........+.....+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++*......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...
+........+....+...+..+.........+......+...+......+.+......+..+.......+...+......
......+..........+...........+....+.........+.....+.+.....+....+......+.....+..
........+...................+..........+...........+...+..+.......+........+.
............+.....+....+..+.+..............+...+.....+....+.....+...+.........
.+...+...........+..+.......++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++
-----
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]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
root@iago-virtual-machine:/home/iago/Desktop# 
```

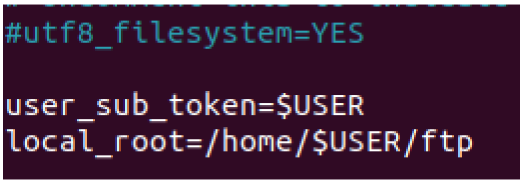
Configuramos el archivo vsftpd de la siguiente forma:



```
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES

# Evitar conexiones anónimas
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES

# Conf utilizar TLS
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

# Evitar solo SSL y suites encriptacion
require_ssl_reuse=NO
ssl_ciphers=HIGH

#
```

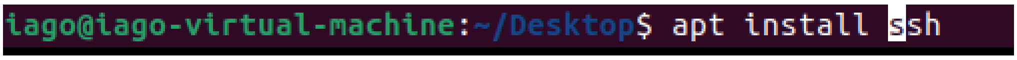


```
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
```

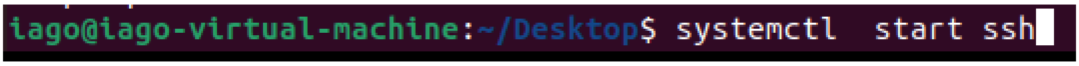


```
#utf8_filesystem=YES

user_sub_token=$USER
local_root=/home/$USER/ftp
```

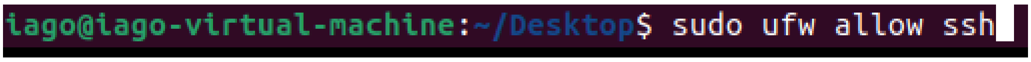
Instalamos SSH y lo configuramos



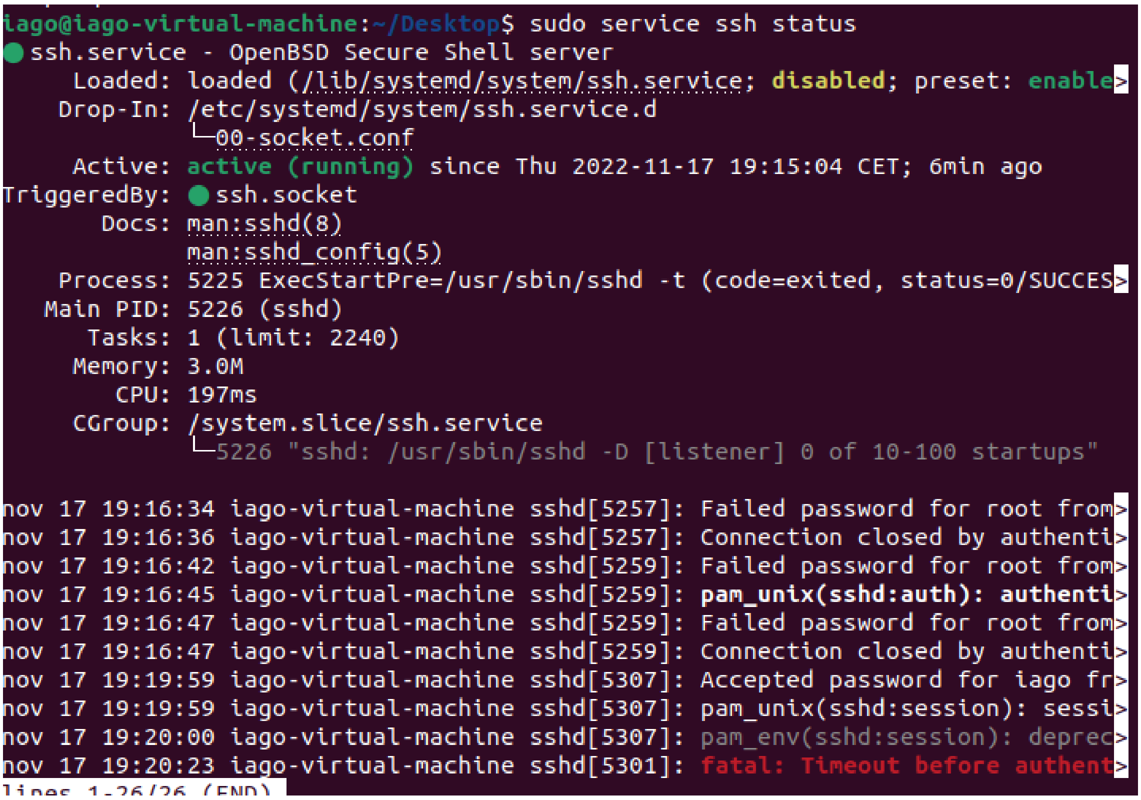
```
iago@iago-virtual-machine:~/Desktop$ apt install ssh
```



```
iago@iago-virtual-machine:~/Desktop$ systemctl  start ssh
```

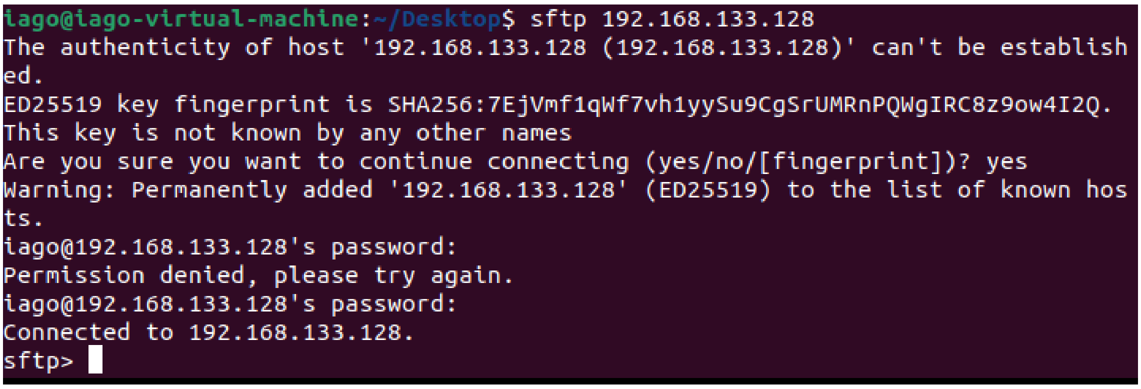


```
iago@iago-virtual-machine:~/Desktop$ sudo ufw allow ssh
```



```
iago@iago-virtual-machine:~/Desktop$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: enable>
    Drop-In: /etc/systemd/system/ssh.service.d
             └─00-socket.conf
     Active: active (running) since Thu 2022-11-17 19:15:04 CET; 6min ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 5225 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCES>
   Main PID: 5226 (sshd)
      Tasks: 1 (limit: 2240)
     Memory: 3.0M
        CPU: 197ms
     CGroup: /system.slice/ssh.service
             └─5226 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

nov 17 19:16:34 iago-virtual-machine sshd[5257]: Failed password for root from>
nov 17 19:16:36 iago-virtual-machine sshd[5257]: Connection closed by authenti>
nov 17 19:16:42 iago-virtual-machine sshd[5259]: Failed password for root from>
nov 17 19:16:45 iago-virtual-machine sshd[5259]: pam_unix(sshd:auth): authenti>
nov 17 19:16:47 iago-virtual-machine sshd[5259]: Failed password for root from>
nov 17 19:16:47 iago-virtual-machine sshd[5259]: Connection closed by authenti>
nov 17 19:19:59 iago-virtual-machine sshd[5307]: Accepted password for iago fr>
nov 17 19:19:59 iago-virtual-machine sshd[5307]: pam_unix(sshd:session): sessi>
nov 17 19:20:00 iago-virtual-machine sshd[5307]: pam_env(sshd:session): deprec>
nov 17 19:20:23 iago-virtual-machine sshd[5301]: fatal: Timeout before authent>
lines 1-26/26 (END)
```

Por último, accedemos al servicio



```
iago@iago-virtual-machine:~/Desktop$ sftp 192.168.133.128
The authenticity of host '192.168.133.128 (192.168.133.128)' can't be establish
ed.
ED25519 key fingerprint is SHA256:7EjVmf1qWf7vh1yySu9CgSrUMRnPQWgIRC8z9ow4I2Q.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.133.128' (ED25519) to the list of known hos
ts.
iago@192.168.133.128's password:
Permission denied, please try again.
iago@192.168.133.128's password:
Connected to 192.168.133.128.
sftp>
```