1. Generamos la key ssh con la siguiente comanda:
   ssh-keygen -t rsa -b 4096 -C "*your_email@example.com*"


```
1 dani@archdani ~/.ssh % ssh-keygen -t rsa -b 4096 -C "your_email@example.com"    :(
Generating public/private rsa key pair.
Enter file in which to save the key (/home/dani/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/dani/.ssh/id_rsa.
Your public key has been saved in /home/dani/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:9fdTsiPAROzDvAd+7bpfKXgC+7hSs3V2w8gD+K0h+N0 your_email@example.com
The key's randomart image is:
+---[RSA 4096]----+
|         . .     |
|         . .     |
|        ++       |
|        =*o      |
|      So++=.= .  |
|     . +===+O.Bo |
|      o.*=B+=o+  |
|      . ooooEoo. |
|       .o..o+.   |
+----[SHA256]-----+
```

2. Enviamos la clave al servidor y nos conectamos automaticamente:
   sudo ssh-copy-id -i ~/.ssh/id_rsa.pub funky@funkyserver
   ssh funky@funkyserver


```
dani@archdani ~/.ssh % sudo ssh-copy-id -i ~/.ssh/id_rsa.pub funky@funkyserver
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/dani/.ssh/id_rs
a.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out
any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted n
ow it is to install the new keys
funky@funkyserver's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'funky@funkyserver'"
and check to make sure that only the key(s) you wanted were added.

dani@archdani ~/.ssh % ssh funky@funkyserver
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-96-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Podeu actualitzar 114 paquets.
0 actualitzacions són actualitzacions de seguretat.

Last login: Fri Oct  6 17:30:22 2017
funky@funkyserver:~$
```
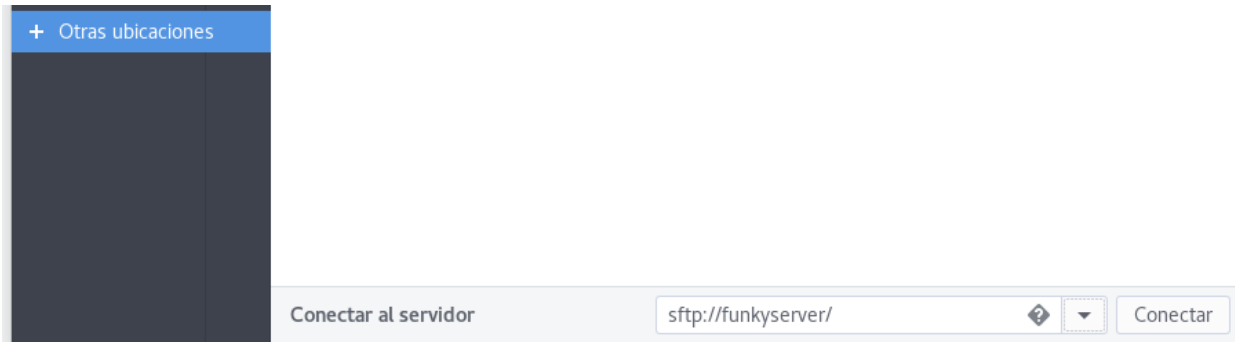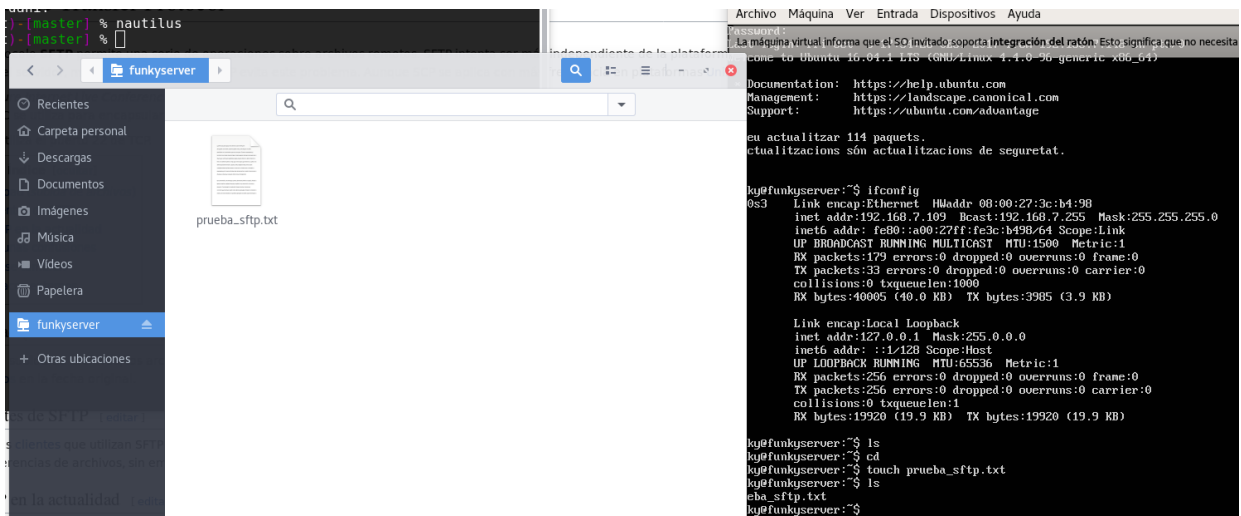
3.1 Acceder y navegar con nautilus por el servidor.
   Te vas al nautilus y en la barra de la izquierda te aparece "otras ubicaciones".
   Le das click y escribes "sftp://funkyserver" y le das enter para acceder.

Una vez estamos dentro, creamos un archivo de prueba y comprobamos que desde el cliente se puede visualizar.

3.2 Copiamos un archivo desde nuestra maquina al servidor.
   Del cliente al servidor:

   Del servidor al cliente:

3.3 Subir carpeta con todo lo de dentro.

4.1 Editamos el archivo sshd_config que hay en el servir con la siguiente orden: sudo nano /etc/ssh/sshd_config

4.2 Le damos acceso al usuario james solamente.
Añadir esta linia al fichero nombrado en el punto anterior.

Creamos el usuario james y le damos una passwd:
sudo useradd james
sudo passwd james

Intentamos pasar un archivo con funky:
Nos pide la contraseña y nos dice permiso denegado.

Intentamos pasarlo ahora con james:

```
dani@archdani ~ (git)-[master] % scp -P 1022 pruebaaa.txt james@funkyserver:~/
james@funkyserver's password:
pruebaaa.txt                                    100%      0     0.0KB/s   00:00
```

4.3 Denegamos acceso a un rango de ip's:
en el servidor añadimos al archivo "/etc/hosts.deny" la linia "sshd:
192.168.7.0/255.255.255.0"
Probamos a pasar un archivo y no nos deja, tambien probamos a acceder al servidor y no
deja. (he vuelto a permitir el acceso con el usuario funky).

```
dani@archdani ~ (git)-[master] % scp -P 1022 pruebaaa.txt james@funkyserver:~/
ssh_exchange_identification: read: Connection reset by peer
lost connection
1 dani@archdani ~ (git)-[master] % ssh funky@funkyserver
ssh: connect to host funkyserver port 22: Connection refused
255 dani@archdani ~ (git)-[master] % ssh -P 1022 funky@funkyserver
ssh: connect to host 1022 port 22: Invalid argument
255 dani@archdani ~ (git)-[master] % ssh -p 1022 funky@funkyserver
ssh_exchange_identification: read: Connection reset by peer
```