

Mòdul 8: Desplegament d'Aplicacions Web

1.3_ACT02: Servidors de transferència de fitxers



ÍNDEX

Exercici1: Instal·lació d'un servidor FTP en Ubuntu.	2
Exercici2: Configuració bàsica d'un servidor FTP i usuaris anònims.	3
Exercici3: Configuració avançada – usuaris autenticats.....	6
Exercici4: Configuració avançada – usuaris autenticats II.....	11
Exercici 5: Modes de connexió actiu i passiu	18
Exercici 6: Configuració avançada – FTP Segur (FTPS)	21

Nota: Cada apartat dels diferents exercicis s'haurà de **demostrar** amb les captures de pantalla adients i/o amb explicacions pertinents que constatin la teva resposta, per exemple, amb enllaços web on hagi trobat la informació.

En aquests enllaços trobaràs tota la informació que necessites:

- **How to set up an FTP server on Ubuntu 14.04:** <https://es.godaddy.com/help/how-to-set-up-an-ftp-server-on-ubuntu-1404-12301>
- **Documentació oficial Ubuntu servidor FTP:** <https://help.ubuntu.com/14.04/serverguide/ftp-server.html>
- **Manual VSFTPD:** <http://manpages.ubuntu.com/manpages/trusty/en/man5/vsftpd.conf.5.html>

Exercici1: Instal·lació d'un servidor FTP en Ubuntu.

- Instal·la el servidor FTP "vsftpd" al teu servidor Ubuntu.

He fet `sudo apt install vsftpd`:

```
roajordi@roaserv:~$ sudo apt install vsftpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
vsftpd
```

- Respon les següents preguntes:
 - Que signifiquen les sigles VSFTPD?
[Significa VerySecure FTP Daemon. Traduït com a Dimoni d'FTP molt segur.](#)
 - On es troba l'arxiu de configuració de vsftpd? Quin nom té?
[En el directori /etc/ Hi trobem l'arxiu vsftpd.conf.](#)
 - Quins usuaris anònims té vsftpd? Estan habilitats per defecte? En cas de no estar habilitats, com els habilitaries?
[Els usuaris anònims no estan habilitats per defecte i per activar-ho s'ha de fer canviant la directiva anonymous_enable i posar-ho en YES. Té l'usuari anònim ftp i l'usuari anònim anonymous.](#)
 - Quin és el directori on es guarden, per defecte, els arxius del servidor FTP?
[Es guarden de forma predeterminada en la home de l'usuari de l'FTP. Per exemple /srv/ftp/.](#)

Exercici2: Configuració bàsica d'un servidor FTP i usuaris anònims.

- En el servidor, crea l'arxiu "prova.txt" dins del directori per defecte d'FTP. Connectat **via comandes** amb un usuari anònim (has d'habilitar l'accés en cas que no ho estigui) i intenta descarregar l'arxiu prova.txt al teu ordinador. Pots descarregar-lo?

```
roajordi@roaserv:/srv/ftp$ sudo touch prova.txt
roajordi@roaserv:/srv/ftp$ ls
prova.txt
```

Habilito els usuaris anònims:

```
GNU nano 2.9.3 /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
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
"
```

Em connecto:

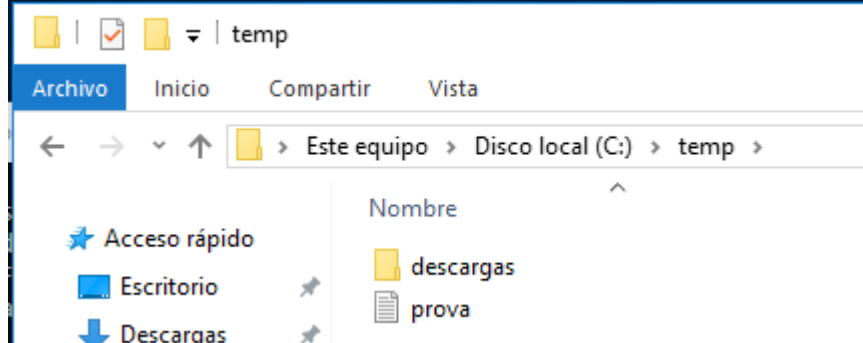
```

C:\Users\Jordi>ftp 200.200.1.10
Conectado a 200.200.1.10.
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
Usuario (200.200.1.10:(none)): anonymous
331 Please specify the password.
Contraseña:
230 Login successful.
ftp>
```

Mostro que puc veure l'arxiu i el descarrego ja que veiem que sí que em deixa descarregar-ho:

```
ftp> lcd c:\temp
Directorio local ahora C:\temp.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0      0      0 Dec 06 00:38 prova.txt
226 Directory send OK.
ftp: 70 bytes recibidos en 0.00segundos 70000.00a KB/s.
ftp> get prova.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for prova.txt (0 bytes).
226 Transfer complete.
ftp> _
```

Si vaig al directori temp veiem que s'ha descarregat allà ja que és a on he especificat:



Veiem com que ho podem descarregar correctament.

- En el client, crea l'arxiu "local.txt" dins de c:\temp\. Connectat via comandes amb un usuari anònim i pujar al servidor l'arxiu "local.txt". Pots pujar-lo?

Poso l'arxiu a temp:

```
c:\temp>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: E438-C3C4

Directorio de c:\temp

06/12/2020  01:53    <DIR>        .
06/12/2020  01:53    <DIR>        ..
18/11/2020  09:25    <DIR>        descargas
06/12/2020  01:53             0 local.txt
06/12/2020  01:47             0 prova.txt
                2 archivos                0 bytes
                3 dirs 32.319.066.112 bytes libres

c:\temp>_
```

Em connecto i ho intento pujar:

```
c:\temp>ftp 200.200.1.10
Conectado a 200.200.1.10.
220 (vsFTPD 3.0.3)
200 Always in UTF8 mode.
Usuario (200.200.1.10:(none)): anonymous
331 Please specify the password.
Contraseña:
230 Login successful.
ftp> lcd c:\temp
Directorio local ahora c:\temp.
ftp> put local.txt
200 PORT command successful. Consider using PASV.
550 Permission denied.
ftp> _
```

Veiem com no he pogut pujar l'arxiu ja que no hi tinc permisos per fer-ho o no tinc les directives necessàries per fer-ho.

- Canvia el missatge de benvinguda del servidor FTP per "Benvingut al servidor FTP de **<Nom Cognom>!!!**". Exemple: "Benvingut al servidor FTP de Marc Morales!!!". Demostra que funciona accedint via comandes.

Modifiquem l'arxiu vsftpd.conf i poso el ftpd_banner:

```
GNU nano 2.9.3 /etc/vsftpd.conf
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftpd_banner=Benvingut al servidor FTP de Jordi Roa!!!
#
```

Si des del client intento connectar, veiem com que ja em surt el missatge de benvinguda que he posat jo:

```
CA: Símbolo del sistema - ftp 200.200.1.10

c:\temp>ftp 200.200.1.10
Conectado a 200.200.1.10.
220 Benvingut al servidor FTP de Jordi Roa!!!
200 Always in UTF8 mode.
Usuario (200.200.1.10:(none)): _
```

Exercici3: Configuració avançada – usuaris autenticats.

Per defecte, **vsftpd** està configurat per autenticar als usuaris del sistema i permetre'ls descarregar arxius sempre que la directiva **local_enable** estigui a YES. Aquesta directiva permet que qualsevol compte d'usuari definit dins l'arxiu **/etc/passwd** pugui accedir al servidor FTP.

Per permetre que els usuaris puguin pujar arxius al servidor FTP canviarem la directiva **write_enable** a YES (ja que per defecte **vsftpd** només permet descarregar-los).

Poso **write_enable** a yes en l'arxiu **vsftpd.conf**:

```
GNU nano 2.9.3 /etc/vsftpd.conf
# 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
"
```

Usuaris sense engarjolar:

- Crea un usuari anomenat <inicial nom+cognom> (p.ex. **mmorales**).

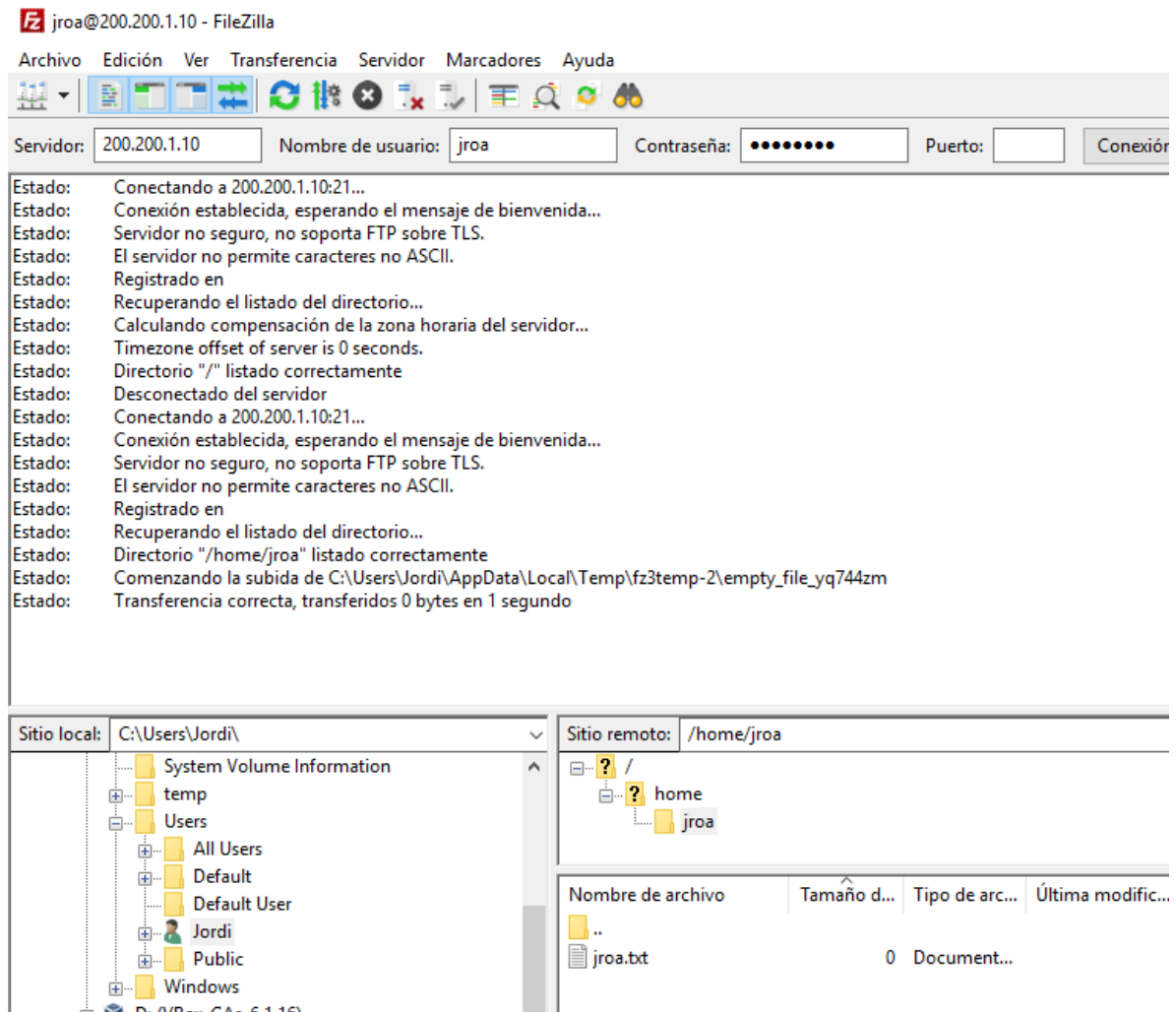
NOTA: Recorda fer-ho amb la comanda **adduser**.

Creació de l'usuari:

```
roajordi@roaserv:~$ sudo adduser jroa
Adding user `jroa' ...
Adding new group `jroa' (1001) ...
Adding new user `jroa' (1001) with group `jroa' ...
Creating home directory `/home/jroa' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for jroa
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
roajordi@roaserv:~$ _
```

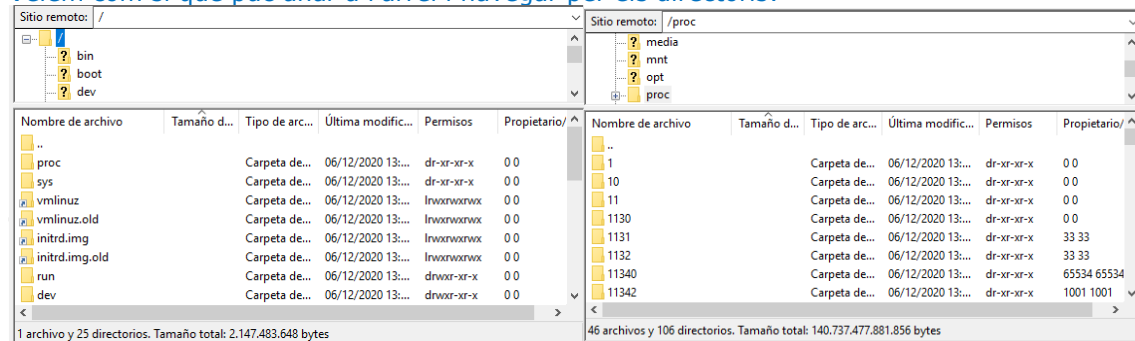
- Connectat al servidor FTP amb un client gràfic (p.ex FileZilla) i crea un arxiu anomenat <inicial nom+cognom>.txt (p.ex **mmorales.txt**).

Veiem com se m'ha creat correctament el .txt:



- Navega fins a l'arrel (/). Pots veure tots els directoris del sistema i navegar per ells?

Veiem com sí que puc anar a l'arrel i navegar per els directoris:



Usuaris engarjolats:

Hauràs pogut comprovar que, en l'apartat anterior "Usuaris sense engarjolar", un usuari pot navegar lliurement pel sistema d'arxius. Això és un perill i, per evitar-ho, hauríem de poder restringir l'usuari d'alguna manera perquè només pugui navegar pels directoris que nosaltres especifiquem.

Vsftpd permet fer aquesta restricció amb les anomenades garjoles "chroot". Quan aquestes garjoles estan habilitades, es restringeix els usuaris FTP al fet que només puguin navegar dins del seu directori HOME (de manera predeterminada).

Per engarjolar usuari canviem la directiva `chroot_local_user` a YES.

Modifiquem `vsftpd.conf` per fer-ho:

```
GNU nano 2.9.3 /etc/vsftpd.conf
# chroot_list_enable below.
#chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to th
# directory. If chroot_local_user is YES, then this list becomes a
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make
# the user does not have write access to the top level directory wi
# chroot)
chroot_local_user=YES
```

- Engarjola l'usuari que has creat abans (inicial nom+cognom) i connectat amb un client. Passa alguna cosa?

Veiem que ens surt el missatge de refusing to run with writable root inside chroot():

Comando: USER jroa

Respuesta: 331 Please specify the password.

Comando: PASS *****

Respuesta: 500 OOPS: vsftpd: refusing to run with writable root inside chroot()

Error: Error crítico: No se pudo conectar al servidor

A causa de la forma en què **vsftpd** protegeix el directori arrel de la garjola, l'usuari **no podrà escriure** dins del seu directori HOME. Per solucionar-ho hi ha dues maneres possibles.

1. Permetre l'accés d'escriptura a l'usuari dins de l'arrel de la seva garjola (directori HOME per defecte).

Per això hem de canviar la directiva `allow_writeable_chroot` a YES.

Posaré l'opció 2 ja que és més segur per el que veig.

2. Creant subdirectoris on es pugui escriure (més segur).

2.1. Comentar o canviar la directiva `allow_writeable_chroot` a NO.

```
GNU nano 2.9.3 /etc/vsftpd.conf
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
allow_writeable_chroot=NO
# You may activate the "-R" option to the builtin ls. This is disa
```

- 2.2. Crear la carpeta "**ftp**", establir els propietaris i eliminar els permisos d'escriptura a aquesta carpeta de la següent manera.

```
sudo mkdir /home/<usuari>/ftp
sudo chown nobody:nogroup /home/<usuari>/ftp
sudo chmod a-w /home/<usuari>/ftp
```

```
roajordi@roaserv:~$ sudo mkdir /home/jroa/ftp
roajordi@roaserv:~$ sudo chown nobody:nogroup /home/jroa/ftp/
roajordi@roaserv:~$ sudo chmod a-w /home/jroa/ftp/
roajordi@roaserv:~$ _
```

Resultat:

```
roajordi@roaserv:/home/jroa/ftp$ ls -la
total 8
dr-xr-xr-x 2 nobody nogroup 4096 dic  6 13:02 .
drwxr-xr-x 3 jroa    jroa    4096 dic  6 13:02 ..
roajordi@roaserv:/home/jroa/ftp$
```

- 2.3. Crear un directori on es puguin pujar els arxius i assignar-li propietats a l'usuari. En aquest cas, el directori l'anomenarem "files" i ho farem de la següent manera:

```
sudo mkdir /home/<usuari>/ftp/files
sudo chown <usuari>:<usuari> /home/<usuari>/ftp/files
```

```
roajordi@roaserv:/home/jroa/ftp$ sudo mkdir files
roajordi@roaserv:/home/jroa/ftp$ sudo chown jroa:jroa files/
roajordi@roaserv:/home/jroa/ftp$
```

Resultat:

```
roajordi@roaserv:/home/jroa/ftp$ ls -la
total 12
dr-xr-xr-x 3 nobody nogroup 4096 dic  6 13:06 .
drwxr-xr-x 3 jroa    jroa    4096 dic  6 13:02 ..
drwxr-xr-x 2 jroa    jroa    4096 dic  6 13:06 files
roajordi@roaserv:/home/jroa/ftp$ _
```

- 2.4. Canviar les directives **user_sub_token** i **local_root** de la següent manera:

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

NOTA: La directiva **local_root** serveix per indicar quin serà el directori que farà d'arrel (home) quan els usuaris es connectin al servidor FTP.

```

GNU nano 2.9.3 /etc/vsftpd.conf
# sites. However, some broken FTP clients such as "ncftp" and '
# the presence of the "-R" option, so there is a strong case fo
#ls_recurse_enable=YES
user_sub_token=$USER
local_root=/home/$USER/ftp

```

- Fes els canvis necessaris perquè l'usuari que hem creat (<inicial nom+cognom>) pugui connectar-se i penjar fitxers sense que **vsftpd** ens doni error. Fes-ho **sense utilitzar** la directiva **allow_writeable_chroota YES**. Comprova que pots crear fitxers com usuari del sistema dins de /home/<usuari>/ (nano/vi/touch). Comprova que, via FTP, pots crear arxius dins del directori /home/<usuari>/ftp/files.

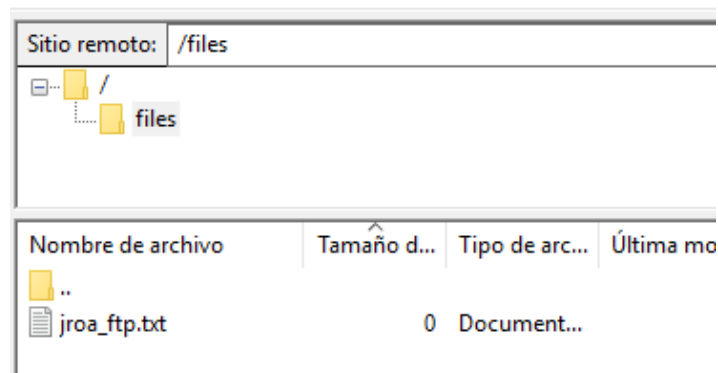
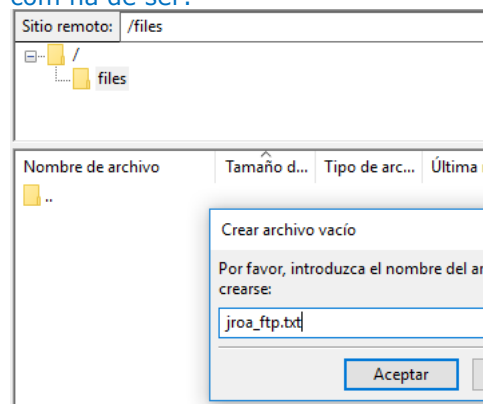
Com a usuari del sistema:

```

jroa@roaserv:~$ whoami
jroa
jroa@roaserv:~$ pwd
/home/jroa
jroa@roaserv:~$ touch jroa_home.txt
jroa@roaserv:~$ ls
ftp jroa_home.txt jroa.txt
jroa@roaserv:~$ _

```

Via FTP podem veure com he creat un arxiu al directori files que és el que m'apareix tal i com ha de ser:



Exercici4: Configuració avançada – usuaris autenticats II.

Canviant la directiva **allow_writeable_chroota YES**, fes el següent:

```
GNU nano 2.9.3 /etc/vsftpd.conf
allow_writeable_chroot=YES
# You may activate the "-R" option to the builtin ls. This is disa
```

- Crea la següent estructura de carpetes:
 - /informatica/ASIX/asix1
 - /informatica/ASIX/asix2
 - /informatica/DAW/daw1
 - /informatica/DAW/daw2

Estructura de carpetes creada:

```
roajordi@roaserv:/$ ls -R /informatica/
/informatica/:
asix  daw

/informatica/asix:
asix1 asix2

/informatica/asix/asix1:

/informatica/asix/asix2:

/informatica/daw:
daw1 daw2

/informatica/daw/daw1:

/informatica/daw/daw2:
roajordi@roaserv:/$ _
```

- Crea els següents grups amb els següents permisos a carpetes:
 - asix i daw
 - /informatica/: Poden accedir a aquest directori (cd) i veure els continguts que hi ha dins, així com llegir el contingut dels fitxers que hi hagi dins.

```
roajordi@roaserv:/$ sudo addgroup asix
[sudo] password for roajordi:
Adding group `asix' (GID 1002) ...
Done.
roajordi@roaserv:/$ sudo addgroup daw
Adding group `daw' (GID 1003) ...
Done.
roajordi@roaserv:/$ sudo chmod 774 informatica/
roajordi@roaserv:/$ _
```

- asix
 - /informatica/asix/: Tenen control total sobre aquesta carpeta (**només en aquesta carpeta**). Això significa que **no podran fer res** en altres directoris que es trobin dinsde /informatica/.

```
roajordi@roaserv:/$ sudo chown :asix /informatica/asix
roajordi@roaserv:/$ sudo chmod 770 /informatica/asix
roajordi@roaserv:/$ sudo ls -la informatica/asix
total 16
drwxrwx--- 4 root asix 4096 dic  6 14:45 .
drwxrwxr-- 4 root root 4096 dic  6 14:45 ..
drwxr-xr-x 2 root root 4096 dic  6 14:45 asix1
drwxr-xr-x 2 root root 4096 dic  6 14:45 asix2
roajordi@roaserv:/$
```

- daw
 - /informatica/daw/: Tenen control total sobre aquesta carpeta (**només en aquesta carpeta**). Això significa que **no podran fer res** en altres directoris que es trobin dinsde /informatica/.

```
roajordi@roaserv:/$ sudo chown :daw /informatica/daw
roajordi@roaserv:/$ sudo chmod 770 /informatica/daw
roajordi@roaserv:/$ sudo ls -la informatica/daw
total 16
drwxrwx--- 4 root daw  4096 dic  6 14:46 .
drwxrwxr-- 4 root root 4096 dic  6 14:45 ..
drwxr-xr-x 2 root root 4096 dic  6 14:46 daw1
drwxr-xr-x 2 root root 4096 dic  6 14:46 daw2
roajordi@roaserv:/$
```

- profes:
 - Poden fer qualsevol cosa dins de /informatica/ i en els fitxers i subdirectoris que hi hagi dintre (daw,asix,daw1,daw2, etc.).

```
roajordi@roaserv:/$ sudo addgroup profes
Adding group `profes' (GID 1004) ...
Done.
```

```
roajordi@roaserv:/$ sudo chown :profes /informatica/
roajordi@roaserv:/$ sudo chmod 770 /informatica/
roajordi@roaserv:/$
```

Per a que els permisos es passin als subdirectoris ho hem de fer de forma recursiva:

```
root@roaserv:/# sudo chmod -R 770 /informatica/
root@roaserv:/# _
```

- Crea els següents usuaris amb la següent configuració:
 - asix1: Pertany al grup ASIX i té control total a /informatica/ASIX/asix1 (**només en aquesta carpeta**). Això significa que **no podrà fer res** en altres directoris que es trobin dinsde /informatica/ASIX/. **Fes que tingui una contrasenya.**

```

roajordi@roaserv:/$ sudo adduser asix1
[sudo] password for roajordi:
Adding user `asix1' ...
Adding new group `asix1' (1005) ...
Adding new user `asix1' (1002) with group `asix1' ...
Creating home directory `/home/asix1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for asix1
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
roajordi@roaserv:/$ sudo usermod asix1 -g asix
roajordi@roaserv:/$ _
roajordi@roaserv:/$ sudo chown asix1: /informatica/asix/asix1
roajordi@roaserv:/$ sudo chmod 700 /informatica/asix/asix1
roajordi@roaserv:/$

```

- asix2: Pertany al grup ASIX i té control total a /informatica/ASIX/asix2 (**només en aquesta carpeta**). Això significa que **no podrà fer res** en altres directoris que es trobin dinsde /informatica/ASIX/.

[Veiem que l'usuari que surt ara és root ja que he fet sudo su.](#)

```

root@roaserv:/# sudo adduser asix2
Adding user `asix2' ...
Adding new group `asix2' (1006) ...
Adding new user `asix2' (1003) with group `asix2' ...
Creating home directory `/home/asix2' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for asix2
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@roaserv:/# sudo usermod asix2 -g asix
root@roaserv:/# sudo chown asix2: /informatica/asix/asix2
root@roaserv:/# sudo chmod 700 /informatica/asix/asix2
root@roaserv:/#

```

- o daw1: Pertany al grup DAW i té control total a /informatica/DAW/daw1 (**només en aquesta** carpeta). Això significa que **no podrà fer res** en altres directoris que es trobin dinsde /informatica/DAW/.

```
root@roaserv:/# sudo adduser daw1
Adding user `daw1' ...
Adding new group `daw1' (1007) ...
Adding new user `daw1' (1004) with group `daw1' ...
Creating home directory `/home/daw1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for daw1
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@roaserv:/# sudo usermod daw1 -g daw
root@roaserv:/# sudo chown daw1: /informatica/daw/daw1/
root@roaserv:/# sudo chmod 700 /informatica/daw/daw1/
root@roaserv:/# _
```

- o daw2: Pertany al grup DAW i té control total a /informatica/DAW/daw2 (**només en aquesta** carpeta). Això significa que **no podrà fer res** en altres directoris que es trobin dinsde /informatica/DAW/.

```
root@roaserv:/# sudo adduser daw2
adduser: The user `daw2' already exists.
root@roaserv:/#
root@roaserv:/# sudo usermod daw2 -g daw
root@roaserv:/# sudo chown daw2: /informatica/daw/daw2/
root@roaserv:/# sudo chmod 700 /informatica/daw/daw2/
root@roaserv:/#
```

- o **profe**: Pertany al grup **profes** i pot fer qualsevol cosa dins de/informatica/ i en els fitxers i subdirectoris que hi hagi dintre (daw, asix, daw1, daw2, etc.).

```
root@roaserv:/# sudo adduser profe
Adding user `profe' ...
Adding new group `profe' (1009) ...
Adding new user `profe' (1006) with group `profe' ...
Creating home directory `/home/profe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for profe
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@roaserv:/# sudo usermod profe -g profes
root@roaserv:/# sudo chown profe: /informatica/
root@roaserv:/# sudo chmod -R 700 /informatica/
root@roaserv:/# _
```

```

root@roaserv:/# sudo ls -la /informatica/
total 16
drwx----- 4 profe profes 4096 dic  6 14:45 .
drwxr-xr-x 24 root  root  4096 dic  6 14:45 ..
drwx----- 4 root  asix  4096 dic  6 14:45 asix
drwx----- 4 root  daw  4096 dic  6 14:46 daw
root@roaserv:/#

root@roaserv:/# sudo ls -la /informatica/asix/
total 16
drwx----- 4 root  asix  4096 dic  6 14:45 .
drwx----- 4 profe profes 4096 dic  6 14:45 ..
drwx----- 2 asix1 asix  4096 dic  6 14:45 asix1
drwx----- 2 asix2 asix  4096 dic  6 14:45 asix2
root@roaserv:/# _

root@roaserv:/# sudo ls -la /informatica/daw/
total 16
drwx----- 4 root  daw  4096 dic  6 14:46 .
drwx----- 4 profe profes 4096 dic  6 14:45 ..
drwx----- 2 daw1  daw  4096 dic  6 14:46 daw1
drwx----- 2 daw2  daw  4096 dic  6 14:46 daw2
root@roaserv:/# _

```

- Configura el teu servidor FTP perquè el directori /informatica/ sigui el directori arrel **de tots** els usuaris quan es connectin via FTP.
Modifico l'arxiu `vsftpd.conf` per canviar la directiva `local_root` tal i com veiem en la següent captura:

```

GNU nano 2.9.3 /etc/vsftpd.conf

local_root=/informatica
#

```

- Obre el client FTP (FileZilla) i comprova el següent:
Ho faig des de FileZilla client però la captura la poso del log de `vsftpd.log` ja que amb una sola línia, es veu si ha funcionat, l'usuari que ho ha fet, i l'arxiu.
 - Connectat amb l'usuari **profe** i fes el següent:
 - Intenta crear l'arxiu `informatica.txt` dins de `/informatica/`.

M'ho deixa fer:

```

Sun Dec  6 19:20:37 2020 [pid 12803] [profe] OK UPLOAD: Client "::ffff:200.200.1.5", "/informatica.txt", 0.00Kbyte/sec

```

- Intenta crear l'arxiu `asix.txt` dins de `/informatica/asix/`.

M'ho deixa fer:

```

Sun Dec  6 20:38:46 2020 [pid 12865] [profe] OK UPLOAD: Client "::ffff:200.200.1.5", "/asix/asix.txt", 0.00Kbyte/sec

```

- Intenta crear l'arxiu `asix1.txt` dins de `/informatica/asix/asix1/`.

Funciona:

```

Sun Dec  6 20:46:19 2020 [pid 12875] [profe] OK UPLOAD: Client "::ffff:200.200.1.5", "/asix/asix1/asix1.txt", 0.00Kbyte/sec

```

- Intenta crear l'arxiu `daw.txt` dins de `/informatica/daw/`.

Funciona:

```

Sun Dec  6 20:48:02 2020 [pid 12875] [profe] OK UPLOAD: Client "::ffff:200.200.1.5", "/daw/daw.txt", 0.00Kbyte/sec

```


- Intenta crear l'arxiu daw2.txt dins de /informatica/daw/daw2/.

Funciona

```
Sun Dec 6 20:49:03 2020 [pid 12875] [profe] OK UPLOAD: Client "::ffff:200.200.1.5", "/daw/daw2/daw2.txt", 0.00Kbyte/sec
```

- Connectat amb l'usuari **asix1** i fes el següent:
 - Intenta esborrar l'arxiu /informatica/informatica.txt.

No funciona:

```
Sun Dec 6 20:52:32 2020 [pid 12905] [asix1] FAIL DELETE: Client "::ffff:200.200.1.5", "/informatica.txt"
```

- Intenta accedir a /informatica/daw/.

No em deixa:

```
Comando: CWD /daw
Respuesta: 550 Failed to change directory.
Error: Error al recuperar el listado del directorio
```

- Intenta crear la carpeta "prova_asix1" dins de /informatica/asix/.

Funciona:

```
Sun Dec 6 21:01:32 2020 [pid 12994] [asix1] OK UPLOAD: Client "::ffff:200.200.1.5", "/asix/prova_asix1.txt", 0.00Kbyte/sec
```

- Intenta accedir a /informatica/asix/asix2/.

No funciona:

```
Comando: CWD /asix/asix2
Respuesta: 550 Failed to change directory.
Error: Error al recuperar el listado del directorio
```

- Intenta esborrar l'arxiu "asix1.txt" dins de /informatica/asix/asix1/.

Funciona:

```
Sun Dec 6 21:06:48 2020 [pid 12994] [asix1] OK DELETE: Client "::ffff:200.200.1.5", "/asix/asix1/asix1.txt"
```

- Connectat amb l'usuari **daw2** i fes el següent:
 - Intenta esborrar l'arxiu /informatica/informatica.txt.

Non funciona:

```
Sun Dec 6 21:09:07 2020 [pid 13015] [daw2] FAIL DELETE: Client "::ffff:200.200.1.5", "/informatica.txt"
```

- Intenta accedir a /informatica/asix/.

No funciona:

```
Comando: CWD asix
Respuesta: 550 Failed to change directory.
Error: Error al recuperar el listado del directorio
```

- Intenta crear la carpeta "prova_daw2" dins de /informatica/daw/.

Funciona:

```
Sun Dec 6 21:15:06 2020 [pid 13015] [daw2] OK UPLOAD: Client "::ffff:200.200.1.5", "/daw/prova_daw2.txt", 0.00Kbyte/sec
```

- Intenta accedir a /informatica/daw/daw1/.

No funciona:

```
Comando: CWD daw1
Respuesta: 550 Failed to change directory.
Error: Error al recuperar el listado del directorio
```

- Intenta esborrar l'arxiu "daw2.txt" dins de /informatica/daw/daw2/.

Funciona:

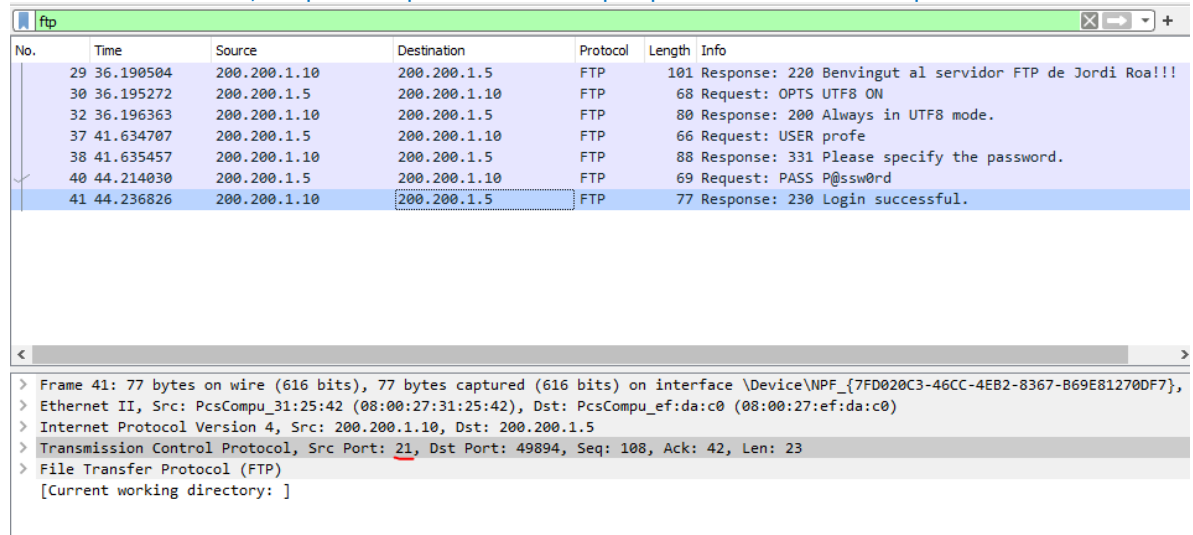
```
Sun Dec 6 21:21:53 2020 [pid 13015] [daw2] OK DELETE: Client "::ffff:200.200.1.5", "/daw/daw2/daw2.txt"
```

Exercici 5: Modes de connexió actiu i passiu

En aquest exercici hauràs d'investigar els diferents modes de connexió FTP (actiu i passiu). Per fer-ho fes servir el programa WireShark i aplica el filtre `ip.addr eq <ip servidor> and ip.addr eq <ip client>` perquè et sigui més fàcil veure les trames que intervien en una comunicació FTP.

Connectat via comandes i contesta aquestes preguntes:

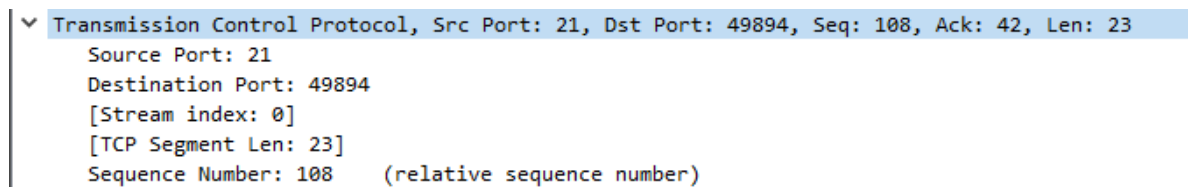
- En quin mode es fa la connexió FTP?
Es fa en mode actiu, ho puc comprovar sobretot perquè estem utilitzat en port 21.



No.	Time	Source	Destination	Protocol	Length	Info
29	36.190504	200.200.1.10	200.200.1.5	FTP	101	Response: 220 Benvingut al servidor FTP de Jordi Roa!!!
30	36.195272	200.200.1.5	200.200.1.10	FTP	68	Request: OPTS UTF8 ON
32	36.196363	200.200.1.10	200.200.1.5	FTP	80	Response: 200 Always in UTF8 mode.
37	41.634707	200.200.1.5	200.200.1.10	FTP	66	Request: USER profe
38	41.635457	200.200.1.10	200.200.1.5	FTP	88	Response: 331 Please specify the password.
40	44.214030	200.200.1.5	200.200.1.10	FTP	69	Request: PASS P@ssw0rd
41	44.236826	200.200.1.10	200.200.1.5	FTP	77	Response: 230 Login successful.

Frame 41: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{7FD020C3-46CC-4EB2-8367-B69E81270DF7},
 Ethernet II, Src: PcsCompu_31:25:42 (08:00:27:31:25:42), Dst: PcsCompu_ef:da:c0 (08:00:27:ef:da:c0)
 Internet Protocol Version 4, Src: 200.200.1.10, Dst: 200.200.1.5
 Transmission Control Protocol, Src Port: 21, Dst Port: 49894, Seq: 108, Ack: 42, Len: 23
 File Transfer Protocol (FTP)
 [Current working directory:]

- Quins ports utilitza el client i el servidor per transferir dades?
Tal i com veiem en la següent captura, el client utilitza el port 49894 i el servidor utilitza el port 21.



Transmission Control Protocol, Src Port: 21, Dst Port: 49894, Seq: 108, Ack: 42, Len: 23

Source Port: 21
Destination Port: 49894
[Stream index: 0]
[TCP Segment Len: 23]
Sequence Number: 108 (relative sequence number)

Connectat amb el FileZilla client i contesta les següents preguntes:

- En quin mode es fa la connexió FTP?
Un cop iniciada la sessió amb filezilla client veiem que s'ha fet en mode passiu. De fet, ens ho mostra tal i com veiem en la següent captura amb la comanda PASV.

No.	Time	Source	Destination	Protocol	Length	Info
31	8.303957	200.200.1.5	200.200.1.10	FTP	66	Request: USER profe
32	8.305120	200.200.1.10	200.200.1.5	FTP	88	Response: 331 Please specify the password.
33	8.306598	200.200.1.5	200.200.1.10	FTP	69	Request: PASS P@ssw0rd
35	8.356526	200.200.1.10	200.200.1.5	FTP	77	Response: 230 Login successful.
36	8.369039	200.200.1.5	200.200.1.10	FTP	59	Request: PWD
38	8.370198	200.200.1.10	200.200.1.5	FTP	88	Response: 257 "/" is the current directory
39	8.371040	200.200.1.5	200.200.1.10	FTP	62	Request: TYPE I
40	8.373083	200.200.1.10	200.200.1.5	FTP	85	Response: 200 Switching to Binary mode.
41	8.373925	200.200.1.5	200.200.1.10	FTP	60	Request: PASV
42	8.375142	200.200.1.10	200.200.1.5	FTP	105	Response: 227 Entering Passive Mode (200,200,1,10,239,106)
43	8.377827	200.200.1.5	200.200.1.10	FTP	60	Request: LIST
47	8.382188	200.200.1.10	200.200.1.5	FTP	93	Response: 150 Here comes the directory listing.
49	8.383209	200.200.1.10	200.200.1.5	FTP	78	Response: 226 Directory send OK.

- Quins ports utilitza el client i el servidor per transferir dades?

El servidor utilitza el port 61290.

File Transfer Protocol (FTP)

227 Entering Passive Mode (200,200,1,10,239,106).\r\n

Response code: Entering Passive Mode (227)

Response arg: Entering Passive Mode (200,200,1,10,239,106).

Passive IP address: 200.200.1.10

Passive port: 61290

[Current working directory: /]

[Command: LIST]

[Command frame: 43]

El client utilitza el port 49903.

> Transmission Control Protocol, Src Port: 21, Dst Port: 49903, Seq: 246, Ack: 67, Len: 51

File Transfer Protocol (FTP)

- Fes que el servidor FTP **no permeti** connexions FTP en mode passiu. Quins ports utilitza, ara, el client i el servidor per transferir dades?

Per a que no permeti les connexions FTP en mode passiu he hagut de modificar vsftpd.conf i posar la directiva pasv_enable a NO.

```
GNU nano 2.9.3 /etc/vsftpd.conf

#chown_uploads=YES
#chown_username=whoever
pasv_enable=NO
# You may override where the log file goes if you like. The default
# below
```

El client utilitza el port 49978 i el servidor el port 21.

```
> Transmission Control Protocol, Src Port: 49978, Dst Port: 21, Seq: 47, Ack: 181, Len: 5
  Source Port: 49978
  Destination Port: 21
  [Stream index: 2]
  [TCP Segment Len: 5]
  Sequence Number: 47 (relative sequence number)
  Sequence Number (raw): 3685920392
  [Next Sequence Number: 52 (relative sequence number)]
  Acknowledgment Number: 181 (relative ack number)
  Acknowledgment number (raw): 2414964048
  0101 .... = Header length: 20 bytes (5)
```

- Fes que el servidor FTP **permeti** connexions FTP en mode passiu. Escull com a port mínim el 6969 i màxim el 7000. Quins ports utilitza, ara, el client i el servidor per transferir dades?

```
GNU nano 2.9.3 /etc/vsftpd.conf
pasv_enable=YES
pasv_min_port=6969
pasv_max_port=7000
# You may override where the log file goes if you like. The defa
```

El servidor utilitza el port 6983.

```

File Transfer Protocol (FTP)
  227 Entering Passive Mode (200,200,1,10,27,71).\r\n
    Response code: Entering Passive Mode (227)
    Response arg: Entering Passive Mode (200,200,1,10,27,71).
    Passive IP address: 200.200.1.10
    Passive port: 6983
[Current working directory: /]
[Command: LIST]
[Command frame: 24]
```

I el client utilitza el port 49983.

```
> Transmission Control Protocol, Src Port: 21, Dst Port: 49983, Seq: 246, Ack: 67, Len: 49
```

Exercici 6: Configuració avançada – FTP Segur (FTPS)

Fes que el teu **servidor FTP** sigui segur amb SSL (FTPS). Per això has de crear un certificat (autofirmat) i configurar el teu servidor FTP perquè sigui segur.

- Crear el certificat amb el nom **"ftp.crt"** i amb la clau **"ftp.key"**. Aquests dos arxius es guardaran/generaran a **/etc/ssl/certs/ftp/**.

Creo el certificat:

```
root@roaserv:/# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/certs/ftp/ftp.key -out /etc/ssl/certs/ftp/ftp.crt
Can't load /root/.rnd into RNG
140674549510592:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/root/.rnd
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/ssl/certs/ftp/ftp.key'
-----
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]:ES
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@roaserv:/# _
```

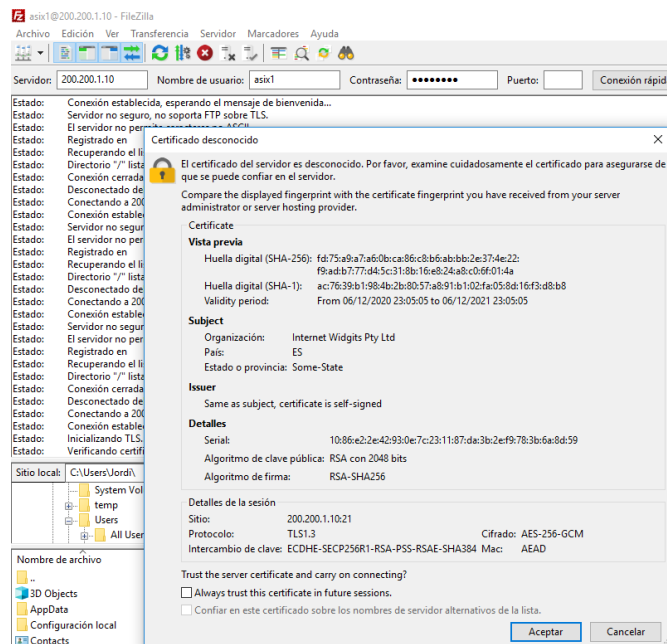
- Configura el servidor FTP perquè sigui segur (utilitzi SSL).
Modifiquem vsftpd.conf com veiem a la captura que he fet:

```
GNU nano 2.9.3 /etc/vsftpd.conf

local_root=/informatica
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ftp/ftp.crt
rsa_private_key_file=/etc/ssl/certs/ftp/ftp.key
ssl_enable=YES
```

- Connectat al servidor FTP amb el client FileZilla amb l'usuari **asix1** però, aquesta vegada, de manera segura i torna a utilitzar el WireShark(com has fet en l'exercici 4) per comprovar si pots veure les credencials dels usuaris.

Veiem com ara ja ens salta el certificat:



Veiem com ara que he posat el certificat ja no veiem la informació:

[illegible]