File server

The ftp or file transfer protocol is designed to transfer large file across the network .ftp works like client server model .FTP program allow the user to upload files to a server and download from them .any linux system can works as a ftp server.there are some packages that allows the linux system to work as a ftp server .A user can log into the account on that server and transfer files. a user can access only the Accounts directory of the server . there is a special type of account named ‘ftp’ that allow users to log into the server with the server with the user name “anonymous”.the account has its own directory and the directory is considered public because anybody in the network can access it. Any linux system can be configured to support anonymous login.
A ftp server software is based on two things

=>**ftp daemon**
=>**configuration file**

daemon is a program that continuously check ftp request from the remote user .when it get the request it manages the login and set the connection for the user account make the corresponding directory available for the user. for the anonymous ftp access the ftp daemon allow the remote user to login to this server using anonymous as the user name .and for the security purpose the linux system make the corresponding home directory as the root directory so that the user cannot access the rest of the computers files and folder .the user can only see its home directory and nits sub-directory. The remaining directory will remain hidden.

There are several ftp server packages for linux system among them the most popular is the vsftpd and proftpd

proftpd is a popular ftp daemon based on Apache web server design it has simple configuration and it supports virtual FTP hosts

another popular that is already already pre installed in many linux distribution is vsftpd(Very secure FTP server) .it support the anonymous Ftp support

installing the vsftpd :

in centos,fedora,redhat:

=>***sudo yum install vsftpd***

in debian based distribution:

=>***sudo apt install vsftpd***

if you want to start the server automatically
=>***chkconfig vsftpd on***

at the time of installation a ftp directory in the /var directory place you want to share the files is in the
/dev/ftp/pub directory

you can create sub directory in that once you connected to the network and the remote user can connect with your system and can download the files in the
pub directory and can upload the file if you give permission to that .all the default configuration is applied to the directories
but the vsftpd do not create any directory where you can upload the file .we generally called it a ‘incoming’ directory.
You have to create the directory and add to the default ftp user group and give the write access so the user can upload the file.so the user can upload files in that directory.

FTP USER:

normal user who have an account in the file server can gain full access by login with their credential . that user can transfer file (both upload and download) in all the directory thy have access to .you can also create users and have restricted their access to the publicly accessible folder.

Creating ftp server for anonymous user:

step 1:

open the firewall(if there any):
we need to open both ftp-data(port 20) and ftp(port 21)
=>***sudo ufw allow ftp-data***
=>***sudo ufw allow ftp***

STEP 2:

create a directory for sharing
=>***sudo mkdir -p /var/ftp/pub***

STEP3:

set the permission to nobody:nogroup

=>sudo chown nobody:nogroup /var/ftp/pub

STEP 4:

---

configure the anonymous access
=>vim /etc/vsftpd.conf
set the
=>anonymous_enable=YES

=>local_enable=NO
[we set the local enable to NO because we dont want to allow the local user to upload files via FTP]

step 5:

---

add some custom configuration bellow

first set the user directory
=>anon_root=/var/ftp
for stopping prompting password

=>no_anon_password=YES

this is the most inp thingn
show the user and group as ftp:ftp regardless the user
=>hide_ids=YES

STEP 6:

---

restart the server

=>***sudo service vsftpd restart***

Creating virtual ftp hosts:

STEP 1:

we have to go to the
/*etc/*vsftpd.conf file
and uncomment (if commented) this following

1)write_enable=YES
2)local_enable=YES

1)if you set the write_enable to YES the user can upload or write in server otherwise the user cant upload anything
2)local_enable set to YES will allow the local user accounts to connect to the file server if you don't uncomment the line. so if you install the ftp server and then if you try to access it using an ftp client you will not be able to connect to the server

STEP 2:

create a group

=>***sudo useradd <groupname>***
ex:
=>***sudo groupadd ftpgroup***

create a user and append in the group and set the home directory
=> ***sudo useradd -d <path> -g <group> <username>***

ex:
=>***sudo useradd -d /home/ftpfolder -g ftpgroup ftpuser***

add password:
=>***passwd <user>***
ex:
=>***passwd ftpuser***

STEP 3:

create corresponding folder:

=>***sudo mkdir -p home/forftp/file***

change the ownership to the user nad the group

=>***sudo chown -R ftpuser.ftpgroup /home/forftp/files***

give only the read permission to the ftp user home folder so that cant be deleted and
give write permission for the root and the corresponding user and only read permission for the otherwise
=>***sudo chmod 555 /home/forftp***
=>***sudo chmod 775 /home/forftp/files***

STEP 4:

=>***/bin/systemctl restart vsftpd.service***

or just

=>***service vsftpd restart***

to access the ftp server from the browser:

---

url(for normal user):

---

ftp://<user>:<password>@<ip/domainname>

<u>url for anonymous:</u>

ftp://<ip address>
or
ftp://<ftp/anonymous>:<ftp/anonymous>@ip