Installation

For the installation, you need to enter the following command:

sudo apt-get install vsftpd

After the successful installation, we will move to the configuration part for some security issues and user management.

Configuration

To begin with the configuration, open the *vsftpd.conf* file by typing:

sudo nano /etc/vsftpd.conf

Disable anonymous login and allow local users to write

The very first change we will be making in the config file is:

anonymous_enable=NO

This will prevent anonymous login from unidentified users. Which can prevent many security issues. Then just find the following lines and uncomment them:

local_enable=YES
write_enable=YES

The change above will allow local users to login and allow the users to write to the directory.

Chroot users

Now there are multiple options available for chrooting users. Search "chroot_local_users" and select one of these as per your needs:

chroot_local_user=YES
chroot_list_enable=NO

The above will chroot all the users.

chroot_local_user=NO
chroot_list_enable=YES

This will allow you to chroot some particular users. You will have to create a file /etc/vsftpd.chroot_list with a list of usernames that you want to chroot.

```
chroot_local_user=YES
chroot_list_enable=YES
```

All the users will be free of chroot except some. Create a file /etc/vsftpd.chroot_list with a list of usernames that you want under chroot.

Allowing and denying users from logging

To deny some particular users to login add these lines to the file:

```
userlist_deny=YES
userlist_file=/etc/vsftpd.denied_users
```

Then create a file *vsftpd.denied_users* and add denied users to it just by adding one user per line. The above will help to deny some particular users from login. You can allow some particular list of users by adding the following to the code:

```
userlist_deny=NO
userlist_enable=YES
userlist_file=/etc/vsftpd.allowed_users
```

Then create a file *vsftpd.allowed_users* and add all the usernames, one per line, that you want to allow.

Configuring TLS/SSL/FTPS

If you connect to your system remotely then you should go through these settings thoroughly, or else your passwords will be sent in plain text. Just make sure to add these options to your config file, some of them are already available check those and then change the options.

```
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
# Filezilla uses port 21 if you don't set any port
# in Servertype "FTPES - FTP over explicit TLS/SSL"
# Port 990 is the default used for FTPS protocol.
# Uncomment it if you want/have to use port 990.
# listen_port=990
```

This will be it with the basic configuration part.

To apply the above settings just close your config file and type:

sudo /etc/init.d/vsftpd restart

Restarting the service will use the new settings and you are done :