### **Step 1: Update System Packages**

**sudo apt update**

### Step 2: Install vsftpd Server on Ubuntu

**sudo apt install vsftpd**

**sudo systemctl start vsftpd**

**sudo systemctl enable vsftpd**

### Step 3: Backup Configuration Files

**Backup configuration file  
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf\_default**

### Step 4: Create FTP User

**sudo useradd -m testuser**

**sudo passwd testuser**

### Step 5: Configure Firewall to Allow FTP Traffic

**sudo ufw allow 20/tcp**

**sudo ufw allow 21/tcp**

### Step 6: Connect to Ubuntu FTP Server

**sudo ftp ubuntu-ftp #ubuntu-ftp —> your hostname**

### Configuring and Securing Ubuntu vsftpd Server

### Change Default Directory

**sudo mkdir /srv/ftp/new\_location**

**sudo usermod -d /srv/ftp/new\_location ftp\**

**sudo systemctl restart vsftpd.service**

### Authenticate FTP Users

**sudo nano /etc/vsftpd.conf**

**Find the entry labeled *write\_enable=NO*, and change the value to “YES.”**

**sudo systemctl restart vsftpd.service**

### Securing FTP

### Limit User Access

**sudo nano /etc/vsftpd.conf**

**chroot\_local\_user=YES**

**chroot\_list\_file=/etc/vsftpd.chroot\_list**

### Create a User List File

**sudo nano /etc/vsftpd.chroot\_list**

**#add one user per line**

**sudo systemctl restart vsftpd.service**

### Encrypt Traffic With FTPS

**sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem**

**sudo nano /etc/vsftpd.conf**

##ssl\_enable=NO to ssl\_enable=YES

**ssl\_enable=YES**

**rsa\_cert\_file=/etc/ssl/private/vsftpd.pem**

**rsa\_private\_key\_file=/etc/ssl/private/vsftpd.pem**

**allow\_anon\_ssl=NO**

**force\_local\_data\_ssl=YES**

**force\_local\_logins\_ssl=YES**

**ssl\_tlsv1=YES**

**ssl\_sslv2=NO**

**ssl\_sslv3=NO**

**require\_ssl\_reuse=NO**

**ssl\_ciphers=HIGH**

**pasv\_min\_port=40000**

**pasv\_max\_port=50000**

**## Save and exit**

**sudo systemctl restart vsftpd.service**