FTP Server Setup Guide with vsftpd on Linux

This guide provides a step-by-step approach to setting up an FTP server using vsftpd on a Linux environment. Each section covers installation, configuration, security settings, and usage, designed to assist users in deploying a secure and functional FTP server.

Step 1: Install vsftpd

1) Install vsftpd:
   Run the following command to install
   sudo apt install vsftpd
2) Check vsftpd service status:
   Verify if the service is active:
   sudo systemctl status vsftpd
   If not active, enable it using:
   sudo systemctl enable --now vsftpd

Step 2: Configure Firewall

1) FTP uses specific ports (20, 21) and a passive port range. Open these ports if using ufw:
   sudo ufw allow 20/tcp
   sudo ufw allow 21/tcp
   sudo ufw allow 990/tcp
   sudo ufw allow 5000:10000/tcp
   (configure your security grp inbound rules to allow traffic through these ports)

Step 3: Configure Users

1) Create a new public user for FTP access:
   - sudo adduser ftpuser
2) Disable SSH access for security:
   Edit the SSH config file: sudo nano /etc/ssh/sshd_config
   Add: DenyUsers ftpuser
   Restart SSH: sudo systemctl restart sshd

Step 4: Create FTP Folder and Set Permissions

1) Create FTP directory: sudo mkdir /ftp
2) Change owner of the FTP folder: sudo chown username /ftp

Step 5: Configure and Secure vsftpd

1) Edit vsftpd config file: sudo nano /etc/vsftpd.conf
2) Ensure the following settings are configured:
   anonymous_enable=NO
   local_enable=YES

write_enable=YES

3) Set passive port range:

pasv_min_port=5000

pasv_max_port=10000

4) Set default FTP directory:

local_root=/ftp

Step 6: Locking User into the Home Directory

For security purposes, it is essential to lock 'ftpuser' to their default directory, preventing access to other parts of the Linux server. To achieve this, vsftpd uses the chroot mechanism.

1) Open vsftpd config file and update the following lines:
Uncomment these lines if they are commented:

chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list

2) Add this line to allow writeable chroot (it is not in the file by default):

allow_writeable_chroot=YES

3) Set default file and directory permissions:
Set the following in vsftpd.conf:

local_umask=0002

Create the chroot list file and add the admin user(the user listed in the list can read all the files including root files, so if you want to restrict the user only to their specific directory skip this step):

sudo touch /etc/vsftpd.chroot_list

sudo nano /etc/vsftpd.chroot_list

4) Restart vsftpd for changes to take effect:

sudo systemctl restart --now vsftpd

Step 7: Secure vsftpd with SSL/TLS

1) Generate a self-signed certificate:

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

2) Configure vsftpd for SSL: Edit /etc/vsftpd.conf and set:

rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES force_local_data_ssl=YES
force_local_logins_ssl=YES ssl_ciphers=HIGH

Step 8: Connect to FTP Server

1) Use FTP client such as FileZilla: Enter server IP, username, and password.
2) Start transferring files between local and server directories using drag-and-drop.