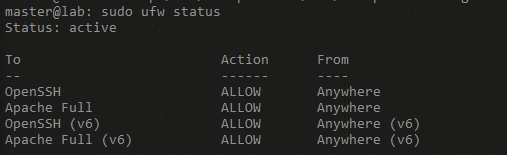
sudo apt update

sudo apt upgrade

sudo apt install vsftpd

sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original

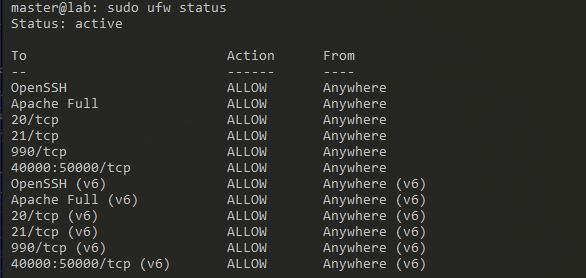
sudo ufw status



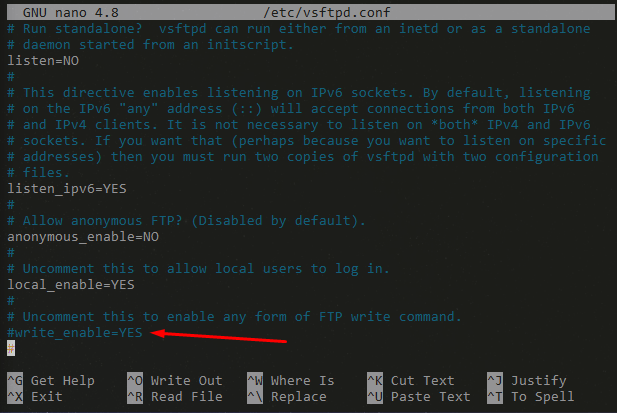
sudo ufw enable

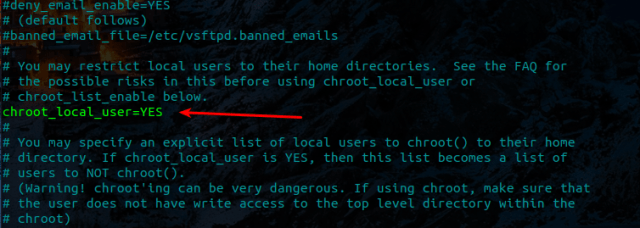
sudo ufw allow 20/tcp && sudo ufw allow 21/tcp && sudo ufw allow 22/tcp && sudo ufw allow 990/tcp && sudo ufw allow 40000:50000/tcp

sudo ufw status



sudo nano /etc/vsftpd.conf





Guarda todos los cambios con CTRL O para guardar, Enter para aceptar y CTRL X para salir.

sudo service vsftpd restart

sudo service vsftpd status

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

Una vez abierto el archivo de configuración desplázate al final del mismo y con un ‘#’ comenta las siguientes líneas: #rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeol.pem

#rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key

Una vez que comentes estas dos líneas, vuelve al final del archivo y agrega las siguiente líneas:

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

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

Dentro del archivo busca ssl\_enable y cambiamos su valor a YES:

ssl\_enable=YES

Para terminar la configuración agrega las siguientes líneas de código al final del archivo:

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

Guarda los cambios y reinicia el servidor ejecutando el comando:

sudo systemctl restart vsftpd

