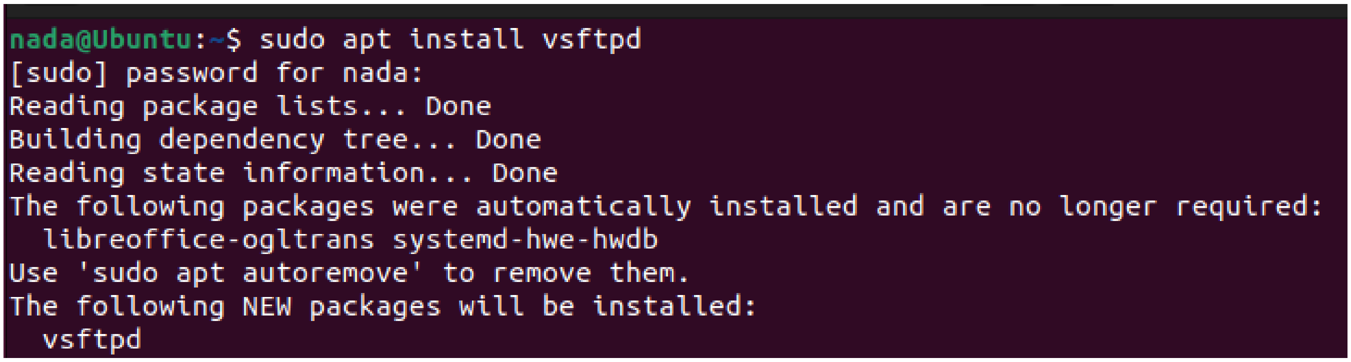
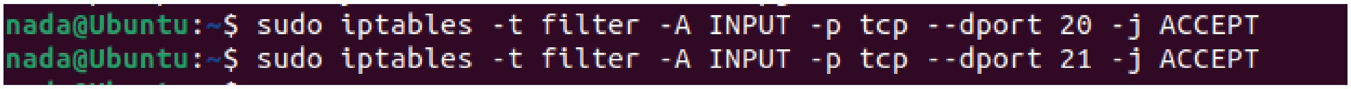
Lab 3

- Install ftpd service on your laptop.



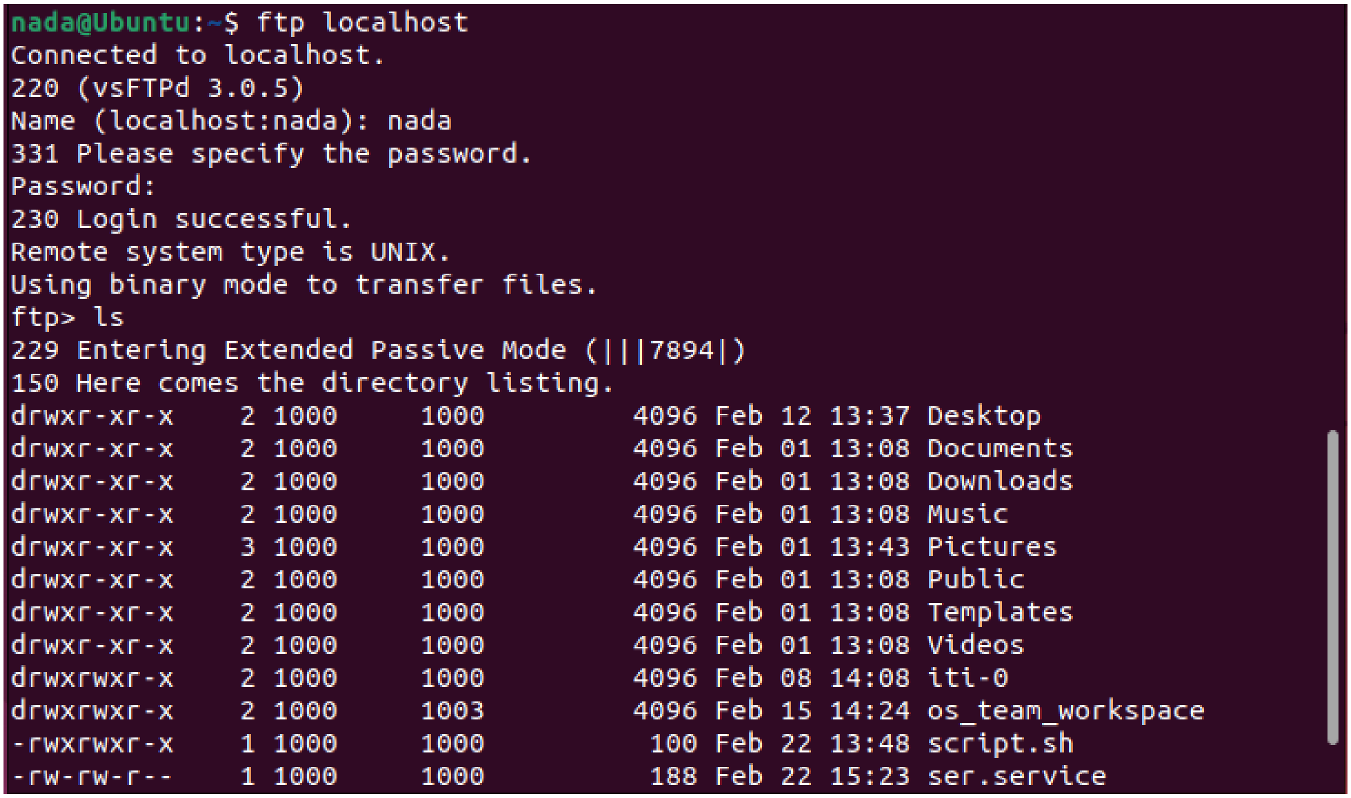
```
nada@Ubuntu:~$ sudo apt install vsftpd
[sudo] password for nada:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libreoffice-ogltrans systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
```

- Enable port 21 and 20 (tpc) using the iptables command using INPUT chain.



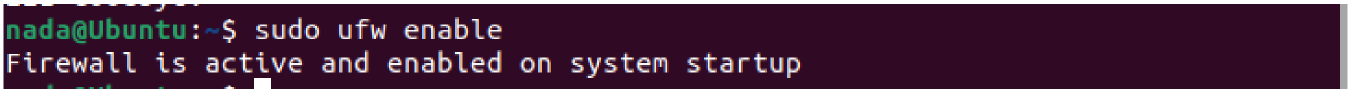
```
nada@Ubuntu:~$ sudo iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
nada@Ubuntu:~$ sudo iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
```

- connect to ftp server (e.g: localhost) and browse the current directory.



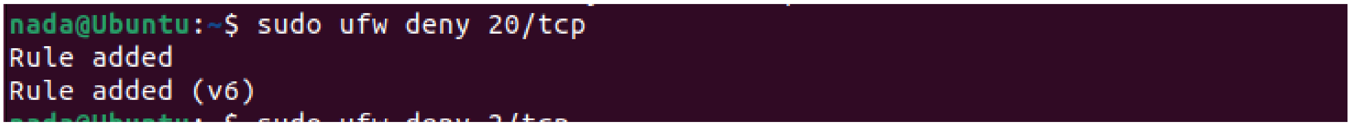
```
nada@Ubuntu:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:nada): nada
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||7894|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Feb 12 13:37 Desktop
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Documents
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Music
drwxr-xr-x    3 1000     1000         4096 Feb 01 13:43 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Public
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Videos
drwxrwxr-x    2 1000     1000         4096 Feb 08 14:08 iti-0
drwxrwxr-x    2 1000     1003         4096 Feb 15 14:24 os_team_workspace
-rwxrwxr-x    1 1000     1000          100 Feb 22 13:48 script.sh
-rw-rw-r--    1 1000     1000          188 Feb 22 15:23 ser.service
```

- Enable ufw service.

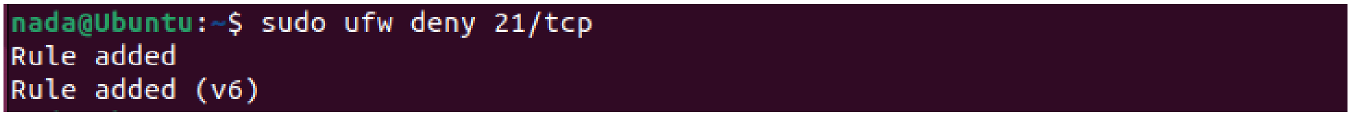


```
nada@Ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

- Block port 21 and 20 (tcp) using ufw

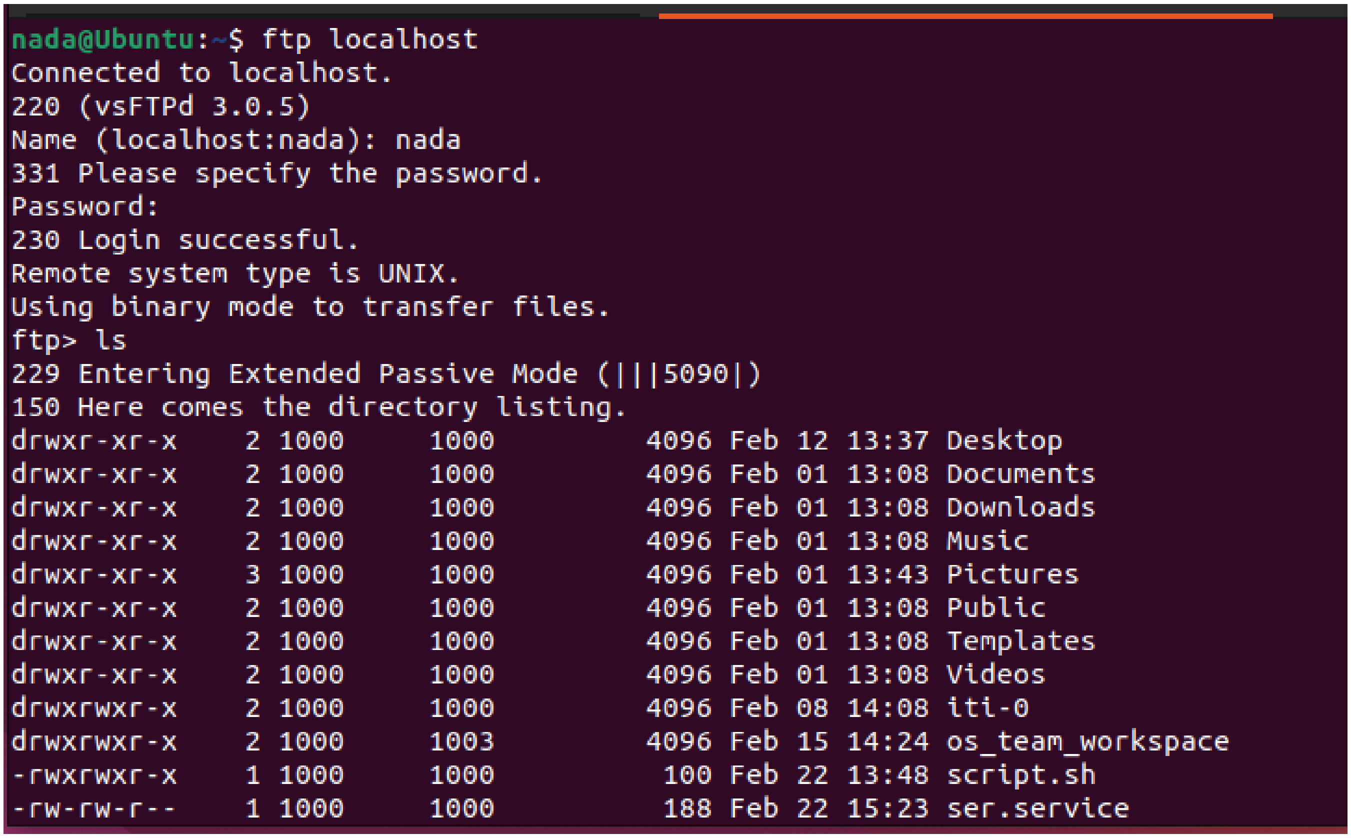


```
nada@Ubuntu:~$ sudo ufw deny 20/tcp
Rule added
Rule added (v6)
```



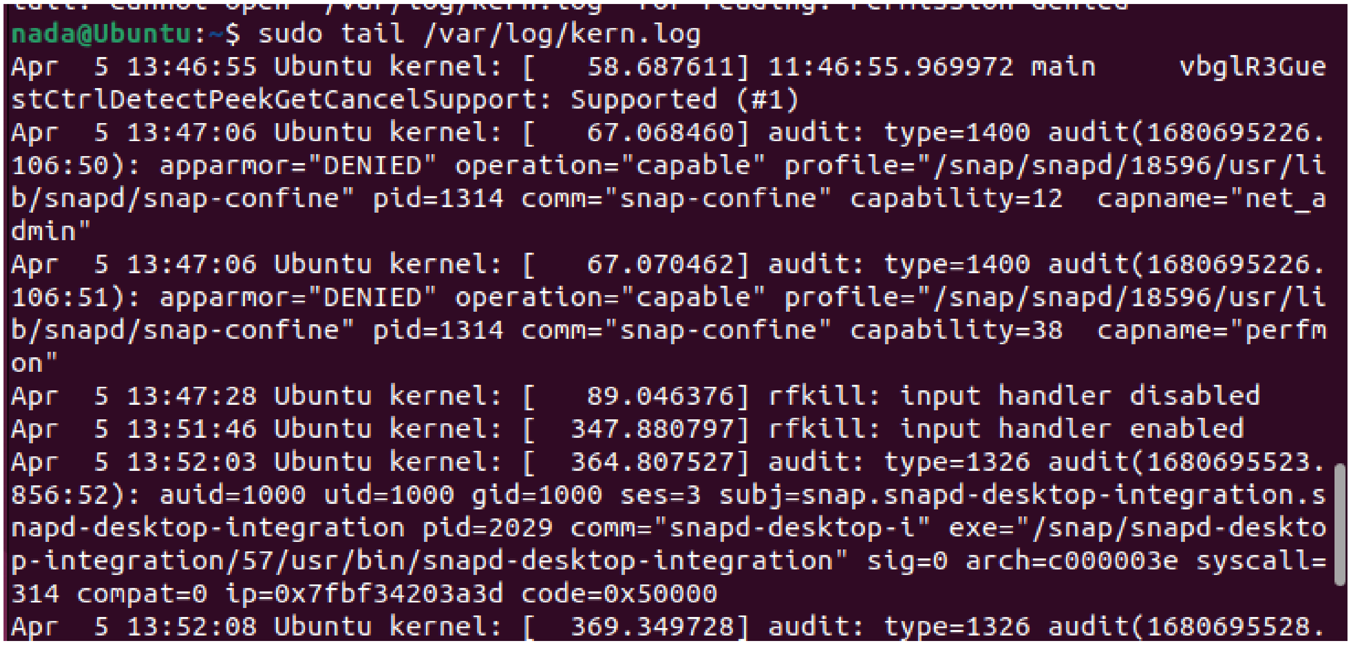
```
nada@Ubuntu:~$ sudo ufw deny 21/tcp
Rule added
Rule added (v6)
```

- Try connecting to ftp service.



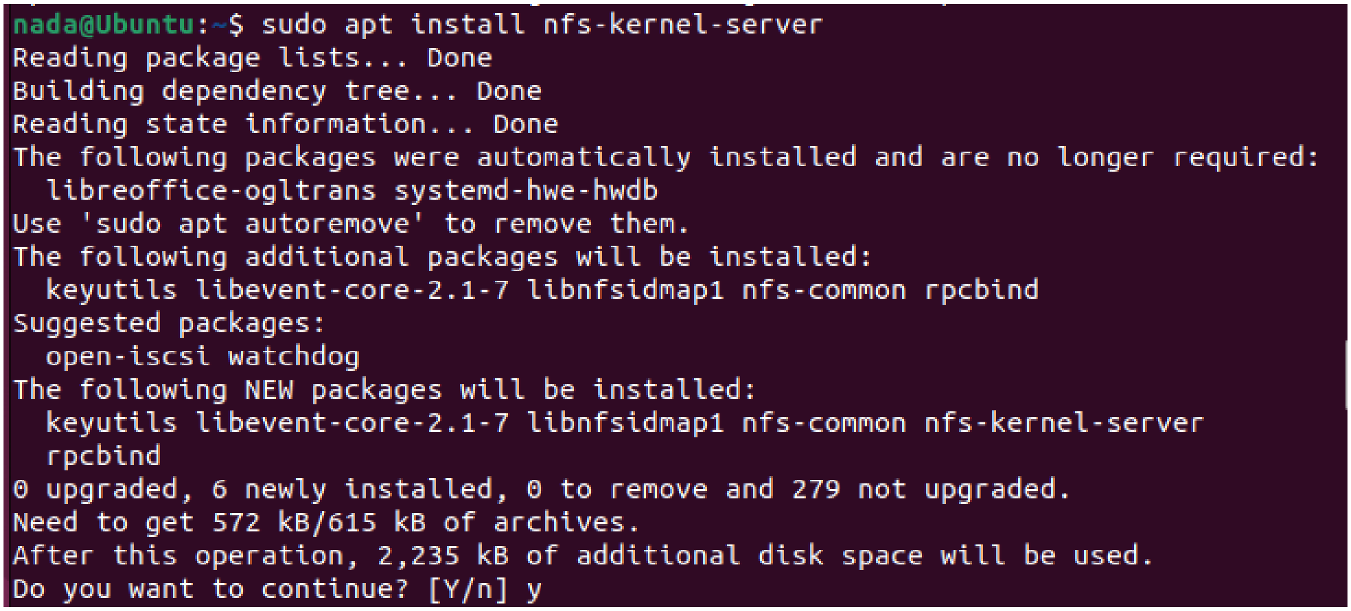
```
nada@Ubuntu:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:nada): nada
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||5090|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Feb 12 13:37 Desktop
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Documents
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Music
drwxr-xr-x    3 1000     1000         4096 Feb 01 13:43 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Public
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:08 Videos
drwxrwxr-x    2 1000     1000         4096 Feb 08 14:08 iti-0
drwxrwxr-x    2 1000     1003         4096 Feb 15 14:24 os_team_workspace
-rwxrwxr-x    1 1000     1000          100 Feb 22 13:48 script.sh
-rw-rw-r--    1 1000     1000          188 Feb 22 15:23 ser.service
```

- Capture the ufw log to delete the blocked operation



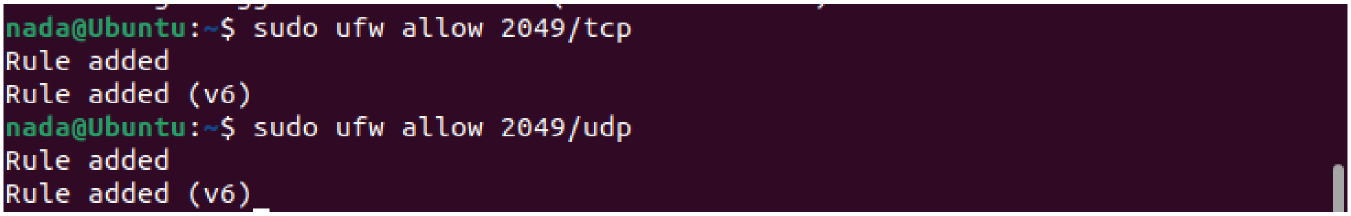
```
tail: cannot open '/var/log/kern.log' for reading: Permission denied
nada@Ubuntu:~$ sudo tail /var/log/kern.log
Apr  5 13:46:55 Ubuntu kernel: [   58.687611] 11:46:55.969972 main     vbglR3GuestCtrlDetectPeekGetCancelSupport: Supported (#1)
Apr  5 13:47:06 Ubuntu kernel: [   67.068460] audit: type=1400 audit(1680695226.106:50): apparmor="DENIED" operation="capable" profile="/snap/snapd/18596/usr/lib/snapd/snap-confine" pid=1314 comm="snap-confine" capability=12  capname="net_admin"
Apr  5 13:47:06 Ubuntu kernel: [   67.070462] audit: type=1400 audit(1680695226.106:51): apparmor="DENIED" operation="capable" profile="/snap/snapd/18596/usr/lib/snapd/snap-confine" pid=1314 comm="snap-confine" capability=38  capname="perfmon"
Apr  5 13:47:28 Ubuntu kernel: [   89.046376] rfkill: input handler disabled
Apr  5 13:51:46 Ubuntu kernel: [  347.880797] rfkill: input handler enabled
Apr  5 13:52:03 Ubuntu kernel: [  364.807527] audit: type=1326 audit(1680695523.856:52): auid=1000 uid=1000 gid=1000 ses=3 subj=snap.snapd-desktop-integration.snapd-desktop-integration pid=2029 comm="snapd-desktop-i" exe="/snap/snapd-desktop-integration/57/usr/bin/snapd-desktop-integration" sig=0 arch=c000003e syscall=314 compat=0 ip=0x7fbf34203a3d code=0x50000
Apr  5 13:52:08 Ubuntu kernel: [  369.349728] audit: type=1326 audit(1680695528.
```

- Install nfs service on your system.



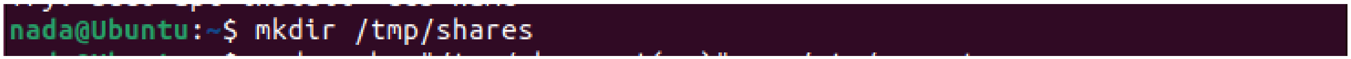
```
nada@Ubuntu:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libreoffice-ogltrans systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  keyutils libevent-core-2.1-7 libnfsidmap1 nfs-common rpcbind
Suggested packages:
  open-iscsi watchdog
The following NEW packages will be installed:
  keyutils libevent-core-2.1-7 libnfsidmap1 nfs-common nfs-kernel-server
  rpcbind
0 upgraded, 6 newly installed, 0 to remove and 279 not upgraded.
Need to get 572 kB/615 kB of archives.
After this operation, 2,235 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

- Enable nfs service on the firewall.

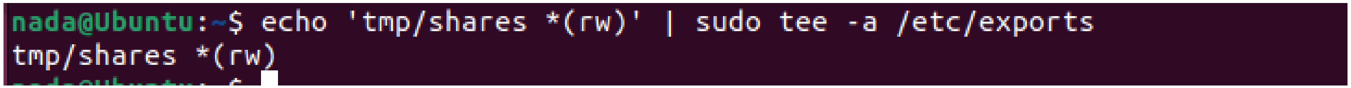


```
nada@Ubuntu:~$ sudo ufw allow 2049/tcp
Rule added
Rule added (v6)
nada@Ubuntu:~$ sudo ufw allow 2049/udp
Rule added
Rule added (v6)
```

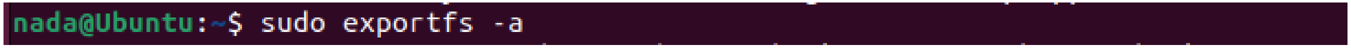
- Create and share /tmp/shares folder using exportfs command and etc/exports file



```
nada@Ubuntu:~$ mkdir /tmp/shares
```

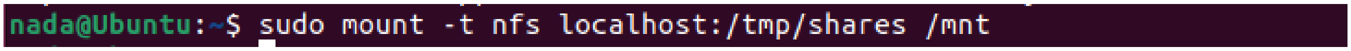


```
nada@Ubuntu:~$ echo 'tmp/shares *(rw)' | sudo tee -a /etc/exports
tmp/shares *(rw)
```



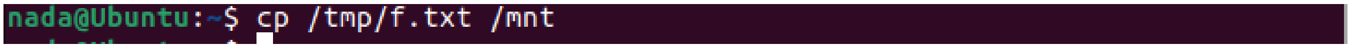
```
nada@Ubuntu:~$ sudo exportfs -a
```

- Mount the remote share on /mnt folder



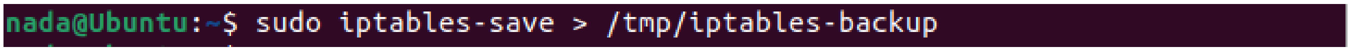
```
nada@Ubuntu:~$ sudo mount -t nfs localhost:/tmp/shares /mnt
```

- Copy some files to the remote share.



```
nada@Ubuntu:~$ cp /tmp/f.txt /mnt
```

- save iptables rule to /tmp/iptables-backup file.



```
nada@Ubuntu:~$ sudo iptables-save > /tmp/iptables-backup
```