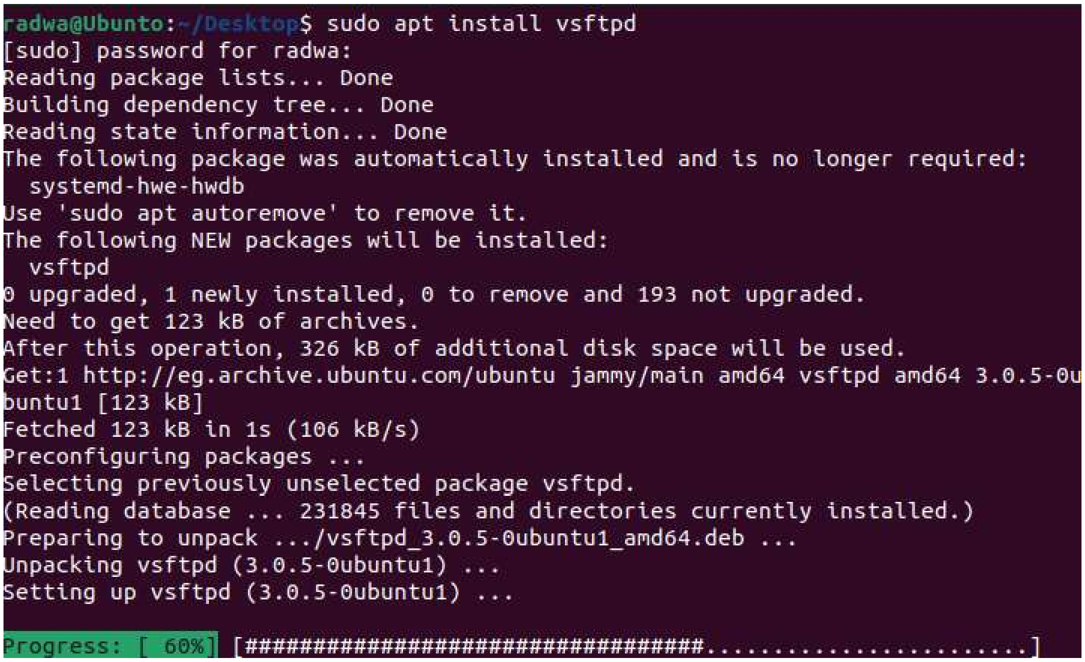
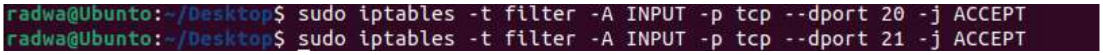
- **Install ftpd service on your laptop**



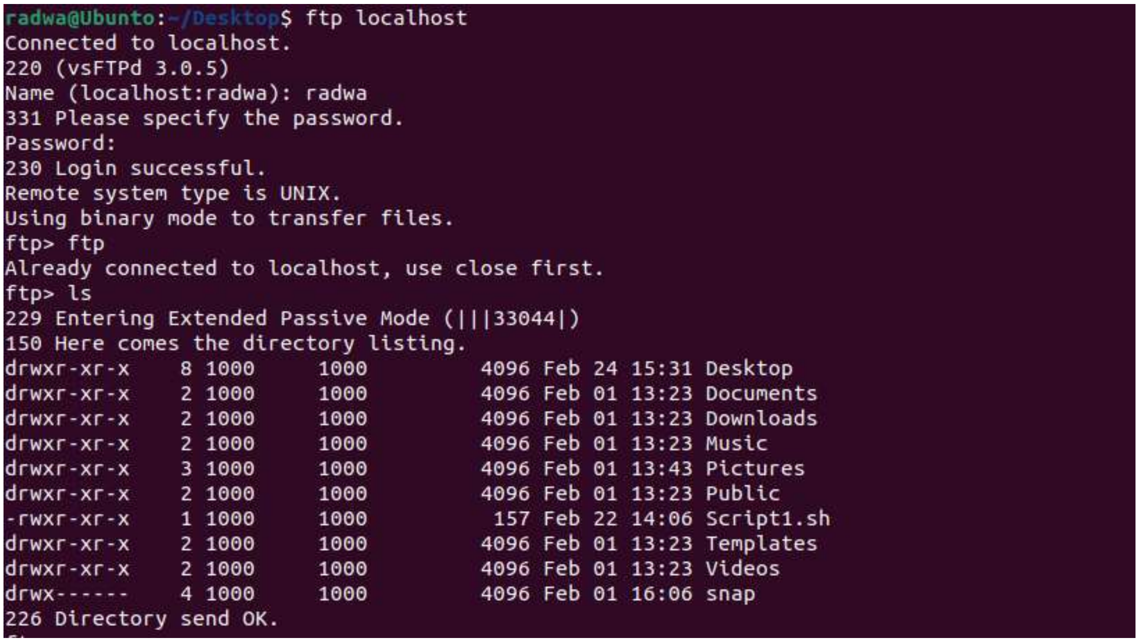
```
radwa@Ubunto:~/Desktop$ sudo apt install vsftpd
[sudo] password for radwa:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 193 not upgraded.
Need to get 123 kB of archives.
After this operation, 326 kB of additional disk space will be used.
Get:1 http://eg.archive.ubuntu.com/ubuntu jammy/main amd64 vsftpd amd64 3.0.5-0u
buntu1 [123 kB]
Fetched 123 kB in 1s (106 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 231845 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0ubuntu1_amd64.deb ...
Unpacking vsftpd (3.0.5-0ubuntu1) ...
Setting up vsftpd (3.0.5-0ubuntu1) ...

Progress: [ 60%] [##################################........................]
```

- **enable port 21 and 20 (tcp) using iptables command using INPUT chain**



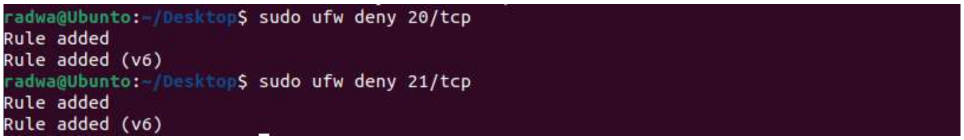
```
radwa@Ubunto:~/Desktop$ sudo iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
radwa@Ubunto:~/Desktop$ sudo iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
```

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



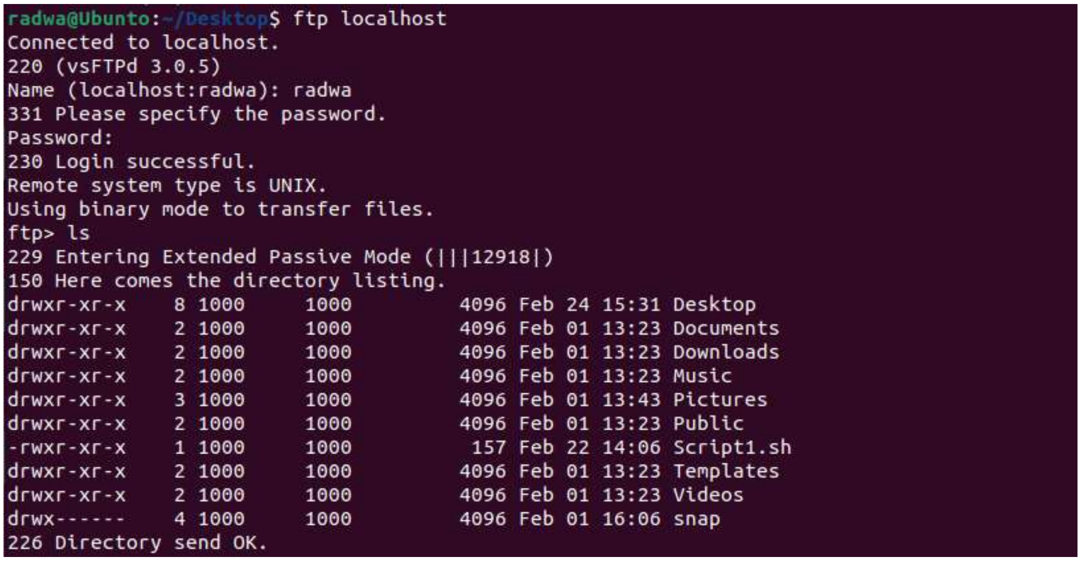
```
radwa@Ubunto:~/Desktop$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:radwa): radwa
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ftp
Already connected to localhost, use close first.
ftp> ls
229 Entering Extended Passive Mode (|||33044|)
150 Here comes the directory listing.
drwxr-xr-x    8 1000     1000         4096 Feb 24 15:31 Desktop
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Documents
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Music
drwxr-xr-x    3 1000     1000         4096 Feb 01 13:43 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Public
-rwxr-xr-x    1 1000     1000          157 Feb 22 14:06 Script1.sh
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Videos
drwx------    4 1000     1000         4096 Feb 01 16:06 snap
226 Directory send OK.
```

- **block port 20 and 21 (tcp) using ufw**



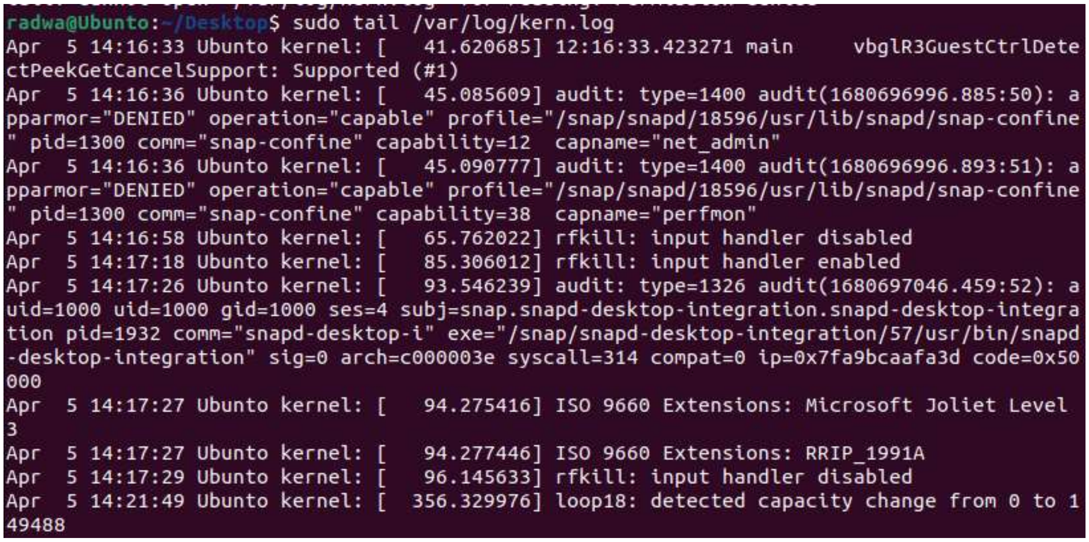
```
radwa@Ubunto:~/Desktop$ sudo ufw deny 20/tcp
Rule added
Rule added (v6)
radwa@Ubunto:~/Desktop$ sudo ufw deny 21/tcp
Rule added
Rule added (v6)
```

- **try to connect to ftp service.**



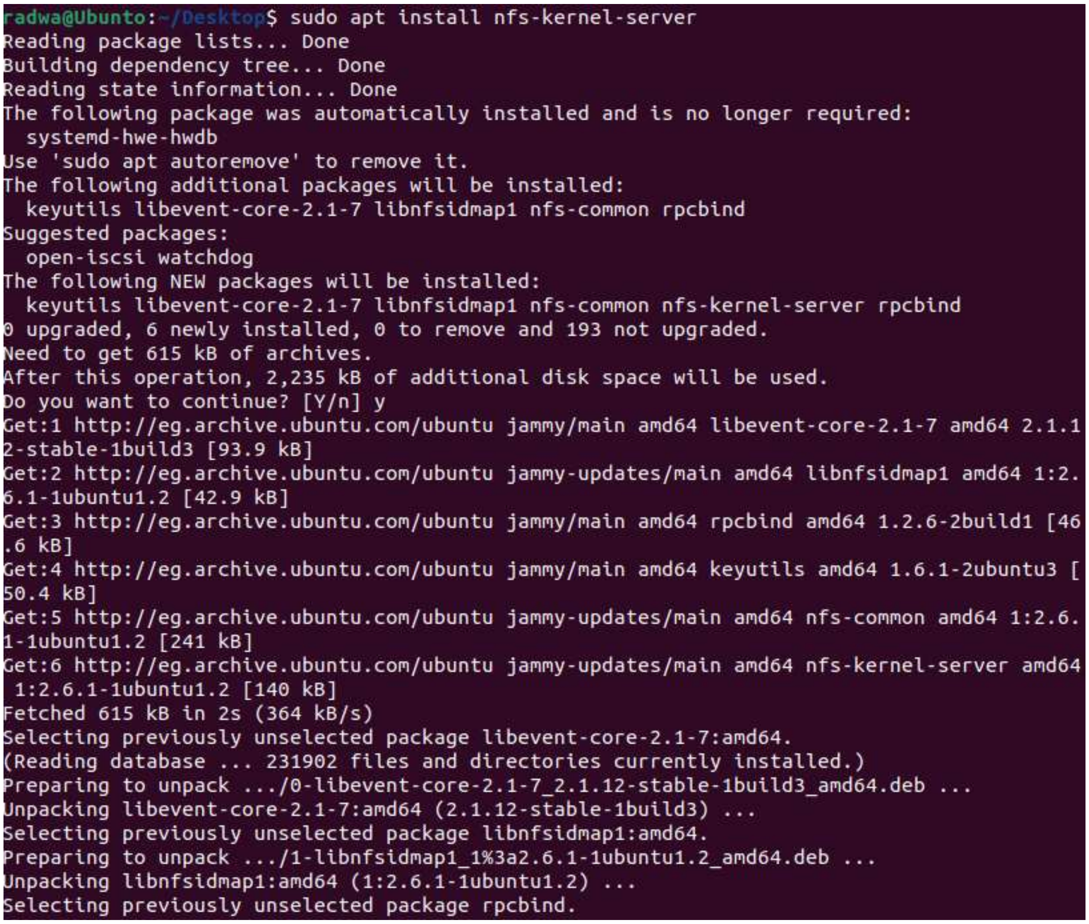
```
radwa@Ubunto:~/Desktop$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:radwa): radwa
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||12918|)
150 Here comes the directory listing.
drwxr-xr-x    8 1000     1000         4096 Feb 24 15:31 Desktop
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Documents
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Music
drwxr-xr-x    3 1000     1000         4096 Feb 01 13:43 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Public
-rwxr-xr-x    1 1000     1000          157 Feb 22 14:06 Script1.sh
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:23 Videos
drwx------    4 1000     1000         4096 Feb 01 16:06 snap
226 Directory send OK.
```

- **capture the ufw log to detect the blocked operation**



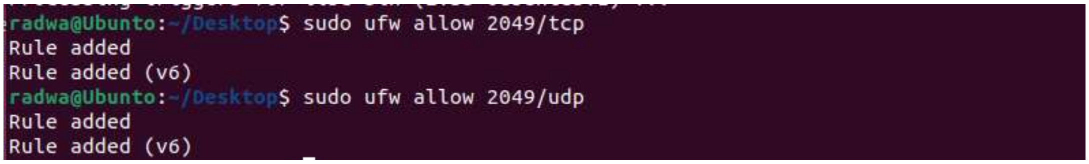
```
radwa@Ubunto:~/Desktop$ sudo tail /var/log/kern.log
Apr  5 14:16:33 Ubunto kernel: [   41.620685] 12:16:33.423271 main     vbglR3GuestCtrlDete
ctPeekGetCancelSupport: Supported (#1)
Apr  5 14:16:36 Ubunto kernel: [   45.085609] audit: type=1400 audit(1680696996.885:50): a
pparmor="DENIED" operation="capable" profile="/snap/snapd/18596/usr/lib/snapd/snap-confine
" pid=1300 comm="snap-confine" capability=12  capname="net_admin"
Apr  5 14:16:36 Ubunto kernel: [   45.090777] audit: type=1400 audit(1680696996.893:51): a
pparmor="DENIED" operation="capable" profile="/snap/snapd/18596/usr/lib/snapd/snap-confine
" pid=1300 comm="snap-confine" capability=38  capname="perfmon"
Apr  5 14:16:58 Ubunto kernel: [   65.762022] rfkill: input handler disabled
Apr  5 14:17:18 Ubunto kernel: [   85.306012] rfkill: input handler enabled
Apr  5 14:17:26 Ubunto kernel: [   93.546239] audit: type=1326 audit(1680697046.459:52): a
uid=1000 uid=1000 gid=1000 ses=4 subj=snap.snapd-desktop-integration.snapd-desktop-integra
tion pid=1932 comm="snapd-desktop-i" exe="/snap/snapd-desktop-integration/57/usr/bin/snapd
-desktop-integration" sig=0 arch=c000003e syscall=314 compat=0 ip=0x7fa9bcaafa3d code=0x50
000
Apr  5 14:17:27 Ubunto kernel: [   94.275416] ISO 9660 Extensions: Microsoft Joliet Level
3
Apr  5 14:17:27 Ubunto kernel: [   94.277446] ISO 9660 Extensions: RRIP_1991A
Apr  5 14:17:29 Ubunto kernel: [   96.145633] rfkill: input handler disabled
Apr  5 14:21:49 Ubunto kernel: [  356.329976] loop18: detected capacity change from 0 to 1
49488
```

- **install nfs service on your system**



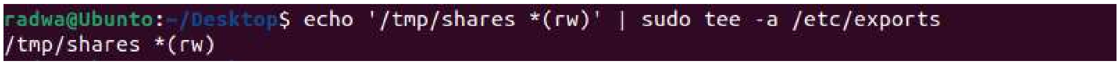
```
radwa@Ubunto:~/Desktop$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove it.
The following 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 193 not upgraded.
Need to get 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
Get:1 http://eg.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-core-2.1-7 amd64 2.1.1
2-stable-1build3 [93.9 kB]
Get:2 http://eg.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnfsidmap1 amd64 1:2.
6.1-1ubuntu1.2 [42.9 kB]
Get:3 http://eg.archive.ubuntu.com/ubuntu jammy/main amd64 rpcbind amd64 1.2.6-2build1 [46
.6 kB]
Get:4 http://eg.archive.ubuntu.com/ubuntu jammy/main amd64 keyutils amd64 1.6.1-2ubuntu3 [
50.4 kB]
Get:5 http://eg.archive.ubuntu.com/ubuntu jammy-updates/main amd64 nfs-common amd64 1:2.6.
1-1ubuntu1.2 [241 kB]
Get:6 http://eg.archive.ubuntu.com/ubuntu jammy-updates/main amd64 nfs-kernel-server amd64
 1:2.6.1-1ubuntu1.2 [140 kB]
Fetched 615 kB in 2s (364 kB/s)
Selecting previously unselected package libevent-core-2.1-7:amd64.
(Reading database ... 231902 files and directories currently installed.)
Preparing to unpack .../0-libevent-core-2.1-7_2.1.12-stable-1build3_amd64.deb ...
Unpacking libevent-core-2.1-7:amd64 (2.1.12-stable-1build3) ...
Selecting previously unselected package libnfsidmap1:amd64.
Preparing to unpack .../1-libnfsidmap1_1%3a2.6.1-1ubuntu1.2_amd64.deb ...
Unpacking libnfsidmap1:amd64 (1:2.6.1-1ubuntu1.2) ...
Selecting previously unselected package rpcbind.
```

- **enable nfs service on the firewall**



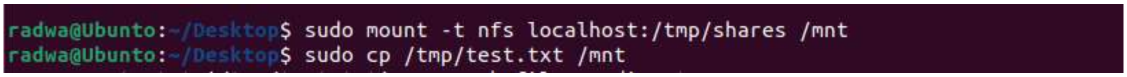
```
radwa@Ubunto:~/Desktop$ sudo ufw allow 2049/tcp
Rule added
Rule added (v6)
radwa@Ubunto:~/Desktop$ sudo ufw allow 2049/udp
Rule added
Rule added (v6)
```

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



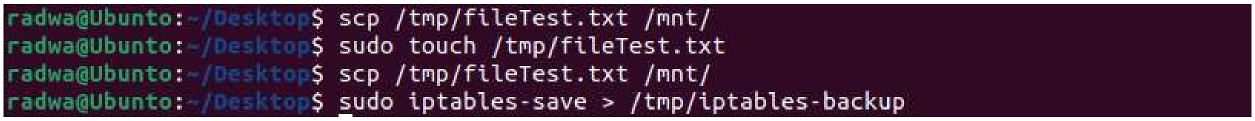
```
radwa@Ubunto:~/Desktop$ echo '/tmp/shares *(rw)' | sudo tee -a /etc/exports
/tmp/shares *(rw)
```

- **mount the remote share on /mnt folder (you can using localhost as well)**

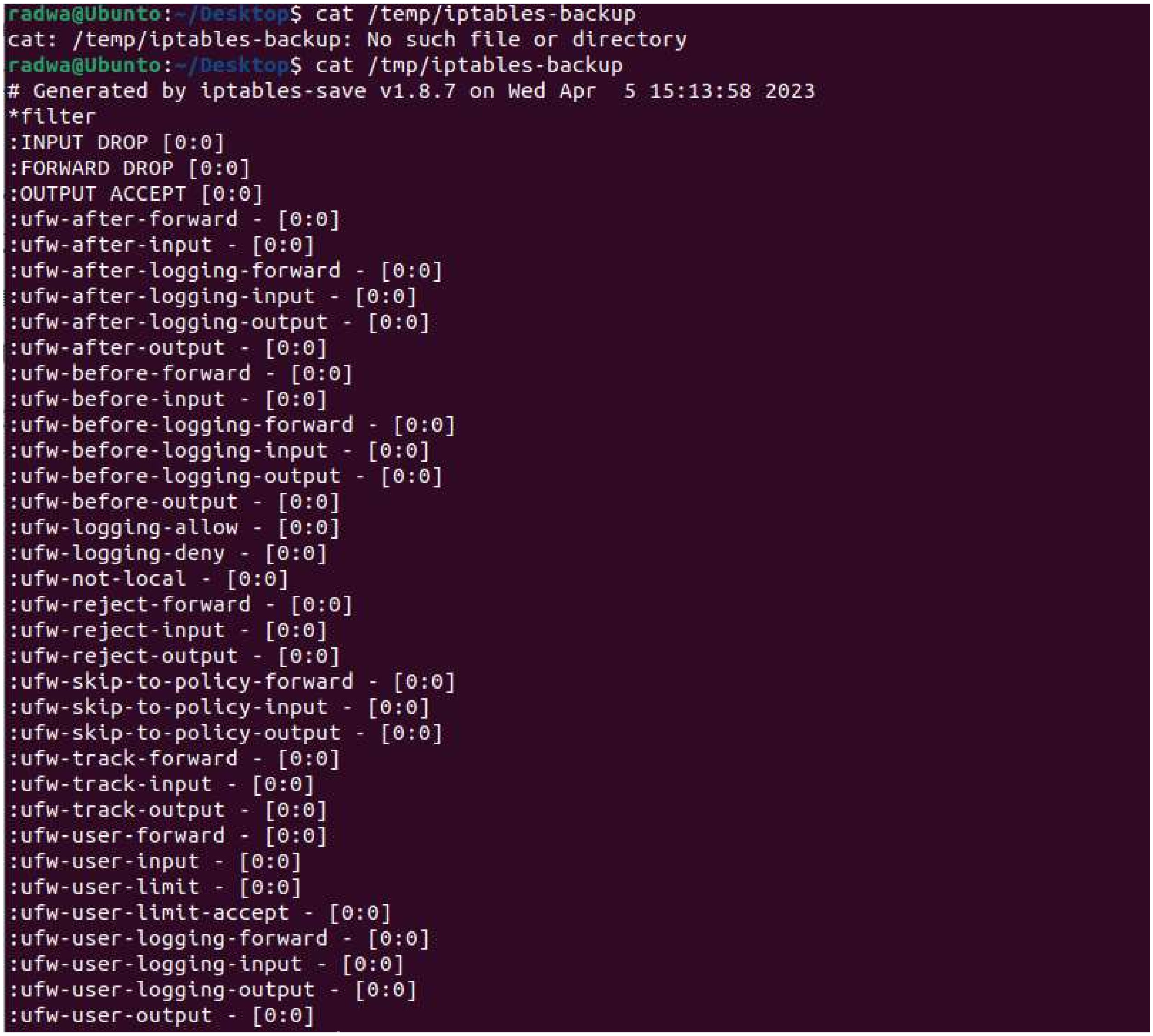


```
radwa@Ubunto:~/Desktop$ sudo mount -t nfs localhost:/tmp/shares /mnt
radwa@Ubunto:~/Desktop$ sudo cp /tmp/test.txt /mnt
```

- **copy some files to the remote share**
- **save iptables rules to /tmp/iptables-backup file**



```
radwa@Ubunto:~/Desktop$ scp /tmp/fileTest.txt /mnt/
radwa@Ubunto:~/Desktop$ sudo touch /tmp/fileTest.txt
radwa@Ubunto:~/Desktop$ scp /tmp/fileTest.txt /mnt/
radwa@Ubunto:~/Desktop$ sudo iptables-save > /tmp/iptables-backup
```



```
radwa@Ubunto:~/Desktop$ cat /temp/iptables-backup
cat: /temp/iptables-backup: No such file or directory
radwa@Ubunto:~/Desktop$ cat /tmp/iptables-backup
# Generated by iptables-save v1.8.7 on Wed Apr  5 15:13:58 2023
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:ufw-after-forward - [0:0]
:ufw-after-input - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-before-input - [0:0]
:ufw-before-logging-forward - [0:0]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-output - [0:0]
:ufw-logging-allow - [0:0]
:ufw-logging-deny - [0:0]
:ufw-not-local - [0:0]
:ufw-reject-forward - [0:0]
:ufw-reject-input - [0:0]
:ufw-reject-output - [0:0]
:ufw-skip-to-policy-forward - [0:0]
:ufw-skip-to-policy-input - [0:0]
:ufw-skip-to-policy-output - [0:0]
:ufw-track-forward - [0:0]
:ufw-track-input - [0:0]
:ufw-track-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-input - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
:ufw-user-logging-forward - [0:0]
:ufw-user-logging-input - [0:0]
:ufw-user-logging-output - [0:0]
:ufw-user-output - [0:0]
```