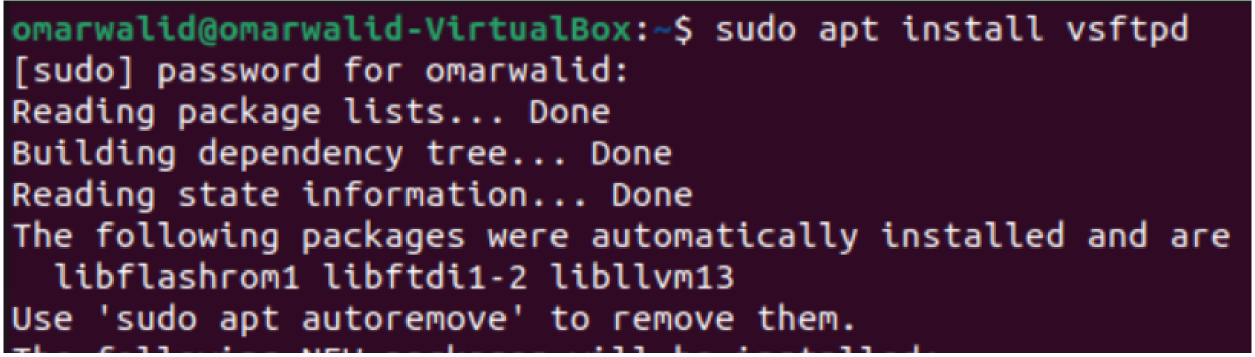
System Admin II Lab3

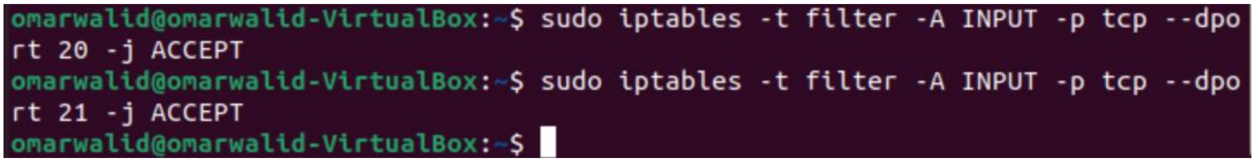
Lab Objectives:

- Install `ftpd` service on your laptop



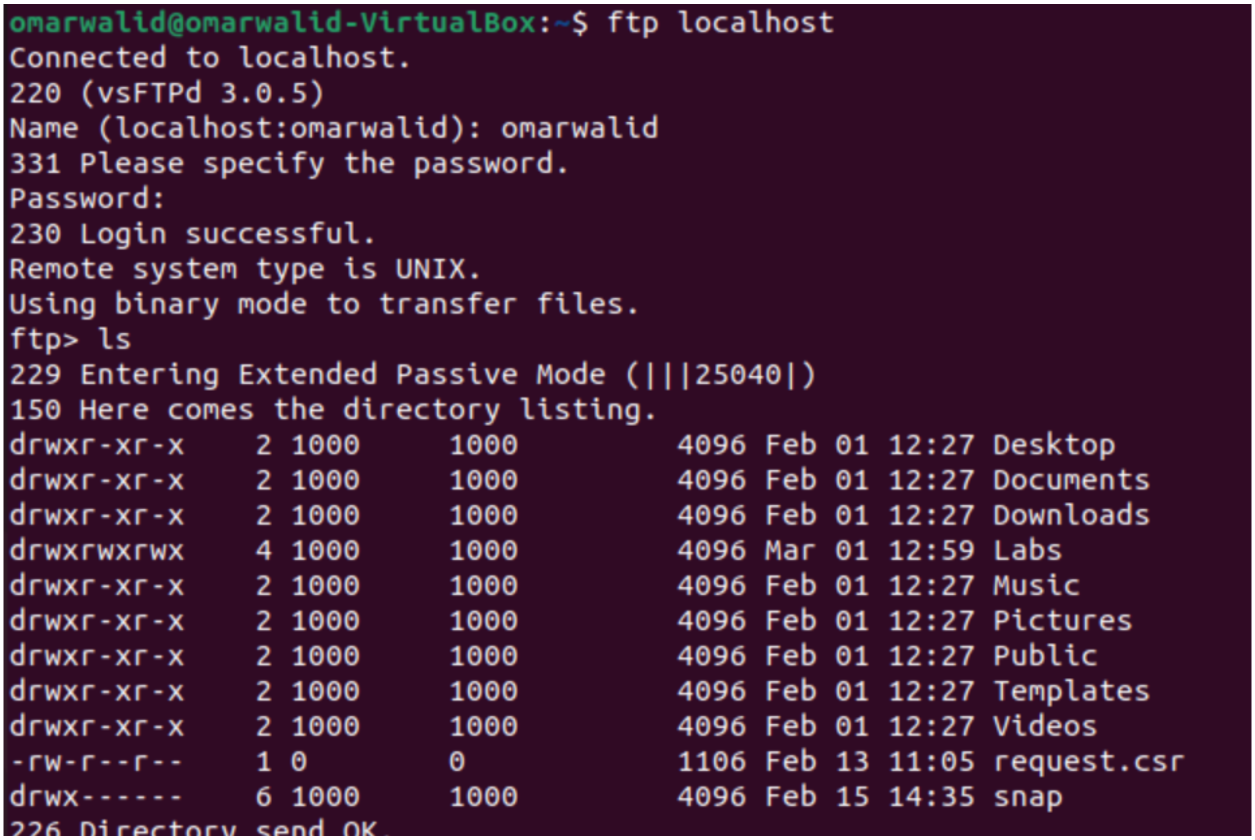
```
omarwalid@omarwalid-VirtualBox:~$ sudo apt install vsftpd
[sudo] password for omarwalid:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are
  libflashrom1 libftdi1-2 libllvm13
Use 'sudo apt autoremove' to remove them.
```

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



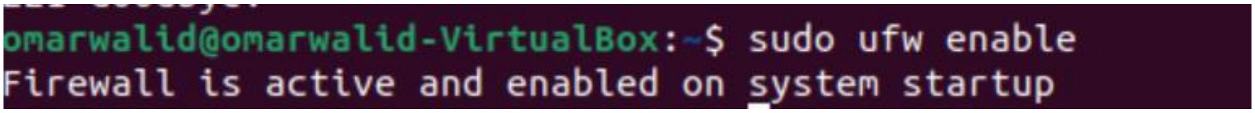
```
omarwalid@omarwalid-VirtualBox:~$ sudo iptables -t filter -A INPUT -p tcp --dpo
rt 20 -j ACCEPT
omarwalid@omarwalid-VirtualBox:~$ sudo iptables -t filter -A INPUT -p tcp --dpo
rt 21 -j ACCEPT
omarwalid@omarwalid-VirtualBox:~$ 
```

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



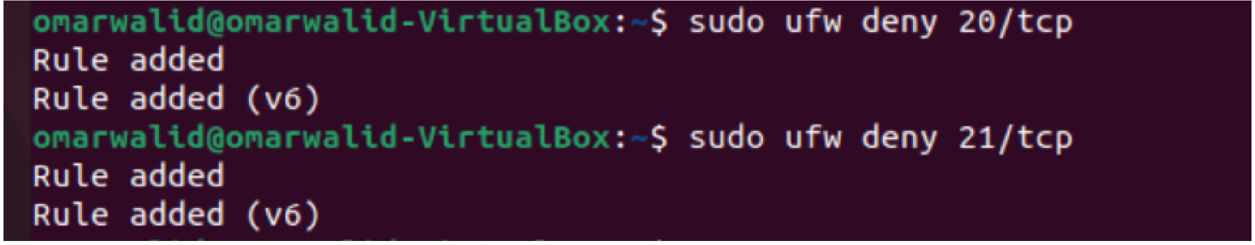
```
omarwalid@omarwalid-VirtualBox:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:omarwalid): omarwalid
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||25040|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Feb 01 12:27 Desktop
drwxr-xr-x    2 1000     1000         4096 Feb 01 12:27 Documents
drwxr-xr-x    2 1000     1000         4096 Feb 01 12:27 Downloads
drwxrwxrwx    4 1000     1000         4096 Mar 01 12:59 Labs
drwxr-xr-x    2 1000     1000         4096 Feb 01 12:27 Music
drwxr-xr-x    2 1000     1000         4096 Feb 01 12:27 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 01 12:27 Public
drwxr-xr-x    2 1000     1000         4096 Feb 01 12:27 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 01 12:27 Videos
-rw-r--r--    1 0        0            1106 Feb 13 11:05 request.csr
drwx------    6 1000     1000         4096 Feb 15 14:35 snap
226 Directory send OK.
```

- enable `ufw` service



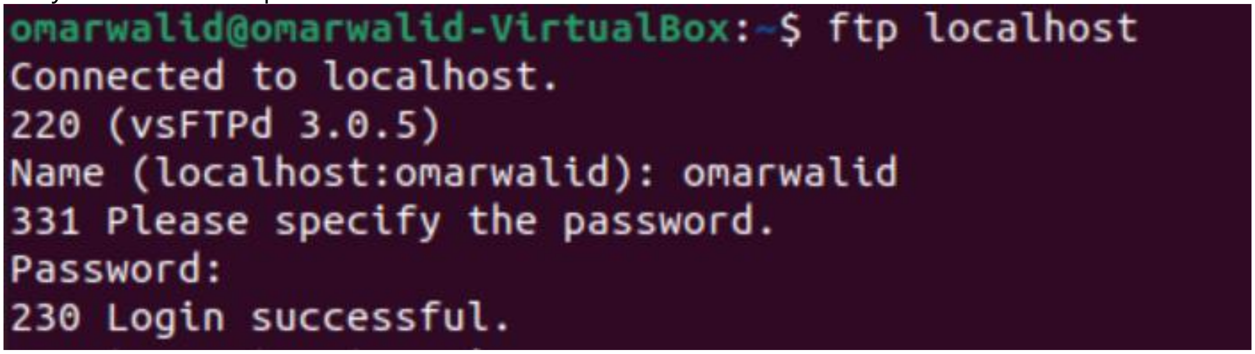
```
omarwalid@omarwalid-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

- block port 20 and 21 (tcp) using ufw



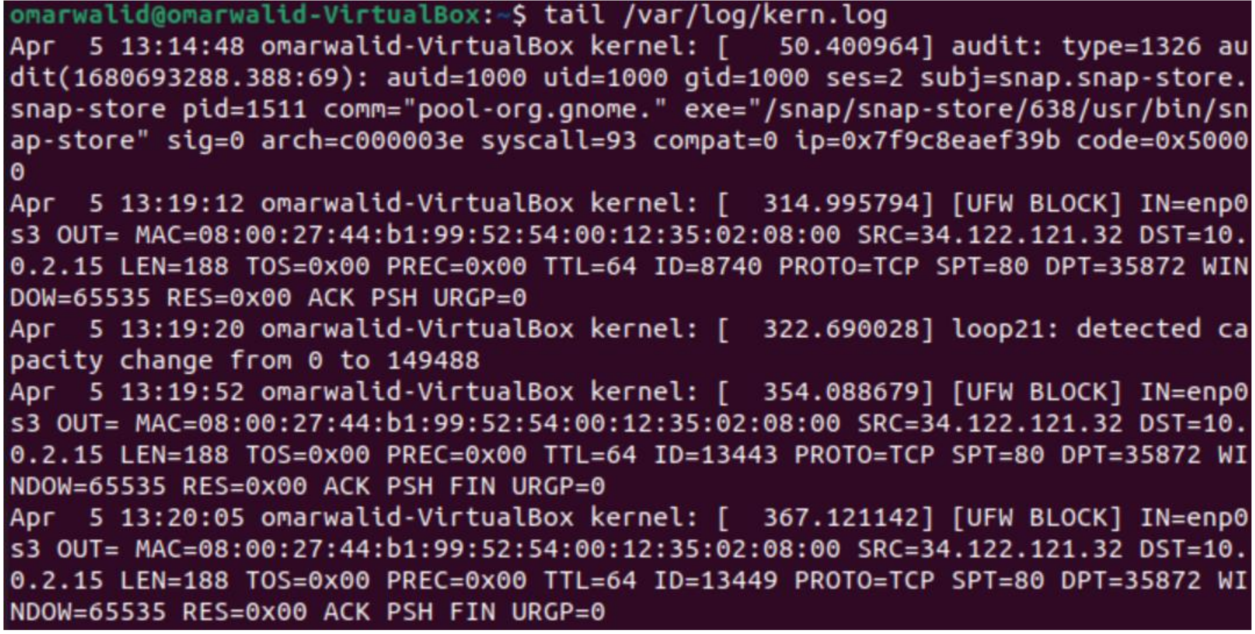
```
omarwalid@omarwalid-VirtualBox:~$ sudo ufw deny 20/tcp
Rule added
Rule added (v6)
omarwalid@omarwalid-VirtualBox:~$ sudo ufw deny 21/tcp
Rule added
Rule added (v6)
```

- try to connect to ftp service.



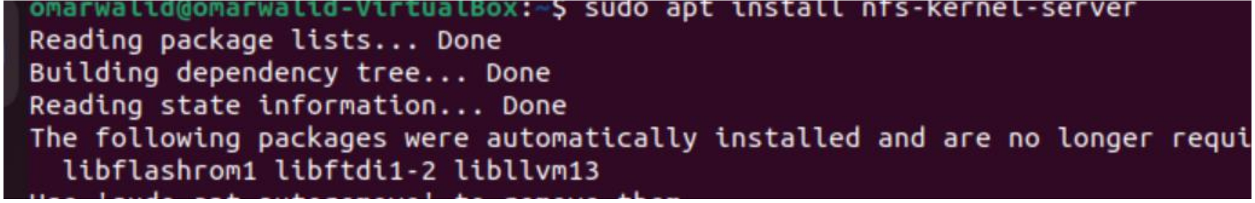
```
omarwalid@omarwalid-VirtualBox:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:omarwalid): omarwalid
331 Please specify the password.
Password:
230 Login successful.
```

- capture the ufw log to detect the blocked operation



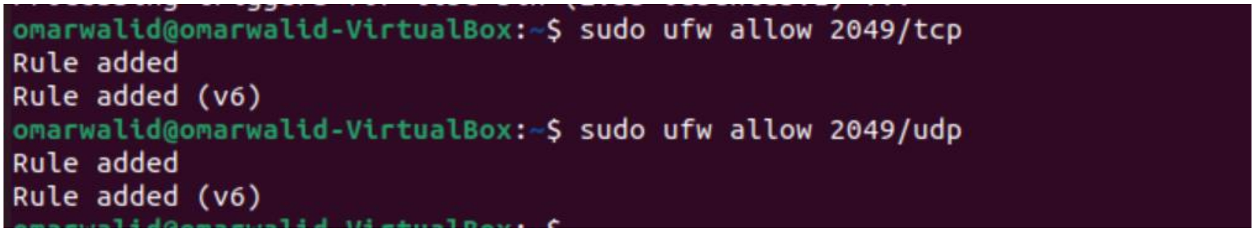
```
omarwalid@omarwalid-VirtualBox:~$ tail /var/log/kern.log
Apr  5 13:14:48 omarwalid-VirtualBox kernel: [   50.400964] audit: type=1326 au
dit(1680693288.388:69): auid=1000 uid=1000 gid=1000 ses=2 subj=snap.snap-store.
snap-store pid=1511 comm="pool-org.gnome." exe="/snap/snap-store/638/usr/bin/sn
ap-store" sig=0 arch=c000003e syscall=93 compat=0 ip=0x7f9c8eaef39b code=0x5000
0
Apr  5 13:19:12 omarwalid-VirtualBox kernel: [  314.995794] [UFW BLOCK] IN=enp0
s3 OUT= MAC=08:00:27:44:b1:99:52:54:00:12:35:02:08:00 SRC=34.122.121.32 DST=10.
0.2.15 LEN=188 TOS=0x00 PREC=0x00 TTL=64 ID=8740 PROTO=TCP SPT=80 DPT=35872 WIN
DOW=65535 RES=0x00 ACK PSH URGP=0
Apr  5 13:19:20 omarwalid-VirtualBox kernel: [  322.690028] loop21: detected ca
pacity change from 0 to 149488
Apr  5 13:19:52 omarwalid-VirtualBox kernel: [  354.088679] [UFW BLOCK] IN=enp0
s3 OUT= MAC=08:00:27:44:b1:99:52:54:00:12:35:02:08:00 SRC=34.122.121.32 DST=10.
0.2.15 LEN=188 TOS=0x00 PREC=0x00 TTL=64 ID=13443 PROTO=TCP SPT=80 DPT=35872 WI
NDOW=65535 RES=0x00 ACK PSH FIN URGP=0
Apr  5 13:20:05 omarwalid-VirtualBox kernel: [  367.121142] [UFW BLOCK] IN=enp0
s3 OUT= MAC=08:00:27:44:b1:99:52:54:00:12:35:02:08:00 SRC=34.122.121.32 DST=10.
0.2.15 LEN=188 TOS=0x00 PREC=0x00 TTL=64 ID=13449 PROTO=TCP SPT=80 DPT=35872 WI
NDOW=65535 RES=0x00 ACK PSH FIN URGP=0
```

- install `nfs` service on your system



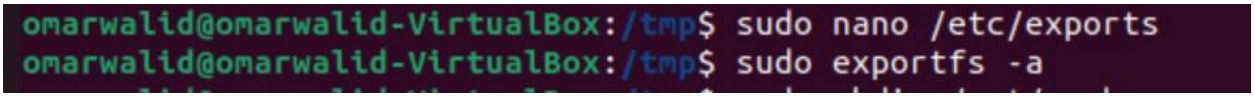
```
omarwalid@omarwalid-VirtualBox:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer requi
  libflashrom1 libftdi1-2 libllvm13
```

- enable nfs service on the firewall



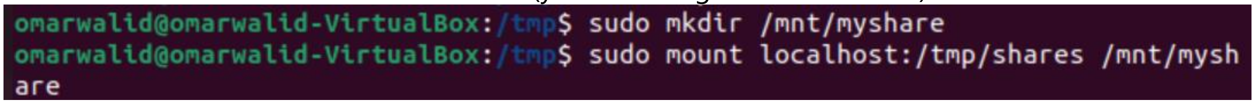
```
omarwalid@omarwalid-VirtualBox:~$ sudo ufw allow 2049/tcp
Rule added
Rule added (v6)
omarwalid@omarwalid-VirtualBox:~$ sudo ufw allow 2049/udp
Rule added
Rule added (v6)
```

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



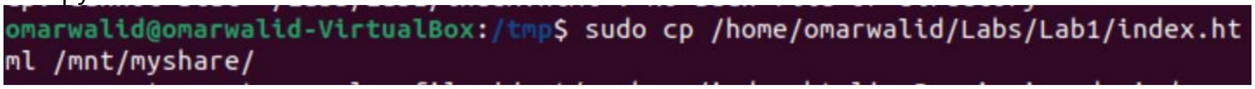
```
omarwalid@omarwalid-VirtualBox:/tmp$ sudo nano /etc/exports
omarwalid@omarwalid-VirtualBox:/tmp$ sudo exportfs -a
```

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



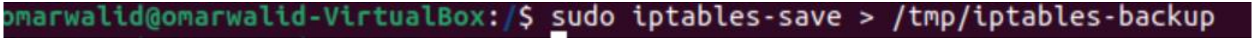
```
omarwalid@omarwalid-VirtualBox:/tmp$ sudo mkdir /mnt/myshare
omarwalid@omarwalid-VirtualBox:/tmp$ sudo mount localhost:/tmp/shares /mnt/mysh
are
```

- copy some files to the remote share



```
omarwalid@omarwalid-VirtualBox:/tmp$ sudo cp /home/omarwalid/Labs/Lab1/index.ht
ml /mnt/myshare/
```

- save `iptables` rules to `/tmp/iptables-backup` file



```
omarwalid@omarwalid-VirtualBox:/$ sudo iptables-save > /tmp/iptables-backup
```