

Lab 3

- Install `ftpd` service on your laptop

`sudo apt-get update && sudo apt-get install vsftpd`

- enable port 21 and 20 (tcp) using iptables command using INPUT chain
- connect to ftp server (e.g: localhost) and browse the current directory

```
hager@ubuntu22: ~  
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 (|||41884|)  
150 Here comes the directory listing.  
drwxr-xr-x  2 1000    1000          4096 Feb  01 12:09 Desktop  
drwxr-xr-x  2 1000    1000          4096 Feb  01 12:09 Documents  
drwxr-xr-x  3 1000    1000          4096 Feb 11 15:06 Downloads  
drwxr-xr-x  2 1000    1000          4096 Feb  01 12:09 Music  
drwxr-xr-x  3 1000    1000          4096 Mar 28 13:14 Pictures  
drwxr-xr-x  2 1000    1000          4096 Feb  01 12:09 Public  
drwxr-xr-x  2 1000    1000          4096 Feb  01 12:09 Templates  
drwxr-xr-x  2 1000    1000          4096 Feb  01 12:09 Videos  
-rw-r--r--  1 0        0              0 Feb 22 14:40 bg_process.service  
-rw-r--r--  1 0        0              0 Mar  4 13:03 f1.txt  
-rw-r--r--  1 0        0              0 Mar  4 13:03 f2.txt  
drwxrwxr-x  2 1000    1000          4096 Feb  08 14:32 iti-0  
drwxrwsr-x  2 1000    10000         4096 Feb 15 13:51 os_team_workspace  
-rwxrwxr-x  1 1000    1000          100 Feb 22 13:59 script.sh  
-rw-rw-r--  1 1000    1000          104 Feb 22 13:48 script1.sh  
-rw-rw-r--  1 1000    1000              0 Feb 22 14:50 ser.service  
-rw-rw-r--  1 1000    1000          188 Feb 22 15:02 ser_bg.service  
drwxr-xr-x  4 1000    1000          4096 Feb 11 13:14 snap
```

- enable ufw service
- block port 20 and 21 (tcp) using ufw

```
hager@ubuntu22:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
hager@ubuntu22:~$ sudo ufw deny 20/tcp  
Rule added  
Rule added (v6)  
hager@ubuntu22:~$ sudo ufw deny 21/tcp  
Rule added  
Rule added (v6)  
hager@ubuntu22:~$
```

- try to connect to ftp service.

`ftp localhost`

- capture the ufw log to detect the blocked operation

```
hager@ubuntu22:~$ sudo tail /var/log/kern.log
Apr  5 14:19:19 ubuntu22 kernel: [ 21.558883] 12:19:19.843017 main      vbglR3GuestCt
lDetectPeekGetCancelSupport: Supported (#1)
Apr  5 14:19:21 ubuntu22 kernel: [ 23.197466] audit: type=1400 audit(1680697161.476:
0): apparmor="DENIED" operation="capable" profile="/snap/snapd/18596/usr/lib/snapd/sna
p-confine" pid=1446 comm="snap-confine" capability=12  capname="net_admin"
Apr  5 14:19:21 ubuntu22 kernel: [ 23.221542] audit: type=1400 audit(1680697161.500:
1): apparmor="DENIED" operation="capable" profile="/snap/snapd/18596/usr/lib/snapd/sna
p-confine" pid=1446 comm="snap-confine" capability=38  capname="perfmon"
Apr  5 14:19:27 ubuntu22 kernel: [ 28.843479] rfkill: input handler disabled
Apr  5 14:22:39 ubuntu22 kernel: [ 218.711913] rfkill: input handler enabled
Apr  5 14:22:44 ubuntu22 kernel: [ 224.001894] audit: type=1326 audit(1680697364.735:
2): auid=1000 uid=1000 gid=1000 ses=4 subj=snap.snapd-desktop-integration.snapd-deskto
p-integration pid=2057 comm="snapd-desktop-i" exe="/snap/snapd-desktop-integration/57/u
sr/bin/snapd-desktop-integration" sig=0 arch=c000003e syscall=314 compat=0 ip=0x7f89c42
5a3d code=0x50000
Apr  5 14:22:48 ubuntu22 kernel: [ 227.543903] ISO 9660 Extensions: Microsoft Joliet
level 3
Apr  5 14:22:48 ubuntu22 kernel: [ 227.544377] ISO 9660 Extensions: RRIP_1991A
Apr  5 14:22:49 ubuntu22 kernel: [ 229.051237] rfkill: input handler disabled
Apr  5 14:24:41 ubuntu22 kernel: [ 340.331380] loop17: detected capacity change from
to 149488
```

- install `nfs` service on your system

```
sudo apt install nfs-kernel-server
```

- enable `nfs` service on the firewall

```
hager@ubuntu22:~$ sudo ufw allow 2049/tcp
Rule added
Rule added (v6)
hager@ubuntu22:~$ sudo ufw allow 2049/udp
Rule added
Rule added (v6)
```

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

```
mkdir /tmp/shares
```

```
hager@ubuntu22:~$ sudo sh -c 'echo "/mnt/backups primary(rw,sync,no_root_squash)" >> /e
tc/exports'
hager@ubuntu22:~$
```

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

```
hager@ubuntu22:~$ sudo mount -t nfs localhost:/tmp/shares /mnt
```

- copy some files to the remote share

```
scp /tmp/file.txt /mnt
```

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

```
sudo iptables-save > /tmp/iptables-backup
```