LAB 3

- **STEP-1**: Install ftpd service on your laptop

Commands

- `sudo apt install vsftpd`

```
hager@hager-VirtualBox:~$ sudo apt install vsftpd
[sudo] password for hager:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

- **STEP-2**: Enable port 21 and 20 (tcp) using iptables command using INPUT chain

Commands

- `sudo iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT`
- `sudo iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT`

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

- **STEP-3**: Connect to ftp server (e.g: localhost) and browse the current directory

Commands

- `ftp localhost`
- `ls`

```
hager@hager-VirtualBox:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:hager): hager
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 (|||11559|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Desktop
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Documents
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Downloads
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Music
drwxr-xr-x    3 1000     1000         4096 Mar 04 12:22 Pictures
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Public
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Templates
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Videos
drwx------    4 1000     1000         4096 Mar 04 13:01 snap
226 Directory send OK.
```

- **STEP-4**: Enable ufw service

Commands

- `sudo ufw enable`

```
hager@hager-VirtualBox:~$ sudo ufw enable
[sudo] password for hager:
Firewall is active and enabled on system startup
```

- **STEP-5**: Block port 20 and 21 (tcp) using ufw

Commands

- `sudo ufw deny 20/tcp`
- `sudo ufw deny 21/tcp`

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

- **STEP-6**: Try to connect to ftp service

Commands

- `ftp localhost`
- `ls`

```
hager@hager-VirtualBox:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:hager): hager
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 (|||55404|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Desktop
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Documents
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Downloads
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Music
drwxr-xr-x    3 1000     1000         4096 Mar 04 12:22 Pictures
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Public
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Templates
drwxr-xr-x    2 1000     1000         4096 Mar 01 02:06 Videos
drwx------    4 1000     1000         4096 Mar 04 13:01 snap
226 Directory send OK.
```

- **STEP-7**: Capture the ufw log to detect the blocked operation

Commands

- `tail /var/log/kern.log`

```
hager@hager-VirtualBox:~$ tail /var/log/kern.log
Apr  5 13:38:46 hager-VirtualBox kernel: [   44.293147] audit: type=1400 audit(
1680694726.531:50): apparmor="DENIED" operation="capable" class="cap" profile="
/snap/snapd/18596/usr/lib/snapd/snap-confine" pid=939 comm="snap-confine" capab
ility=38  capname="perfmon"
Apr  5 13:39:15 hager-VirtualBox kernel: [   71.142922] rfkill: input handler d
isabled
Apr  5 13:41:37 hager-VirtualBox kernel: [  213.281429] audit: type=1400 audit(
1680694897.331:51): apparmor="DENIED" operation="capable" class="cap" profile="
/snap/snapd/18596/usr/lib/snapd/snap-confine" pid=1400 comm="snap-confine" capa
bility=12  capname="net_admin"
Apr  5 13:41:37 hager-VirtualBox kernel: [  213.281441] audit: type=1400 audit(
1680694897.331:52): apparmor="DENIED" operation="capable" class="cap" profile="
/snap/snapd/18596/usr/lib/snapd/snap-confine" pid=1400 comm="snap-confine" capa
bility=38  capname="perfmon"
Apr  5 13:41:37 hager-VirtualBox kernel: [  213.462083] rfkill: input handler e
nabled
Apr  5 13:41:46 hager-VirtualBox kernel: [  222.745469] rfkill: input handler d
isabled
Apr  5 13:42:02 hager-VirtualBox kernel: [  238.578156] audit: type=1326 audit(
1680694922.631:53): auid=1000 uid=1000 gid=1000 ses=3 subj=snap.snapd-desktop-i
ntegration.snapd-desktop-integration pid=2014 comm="snapd-desktop-i" exe="/snap
/snapd-desktop-integration/57/usr/bin/snapd-desktop-integration" sig=0 arch=c00
0003e syscall=314 compat=0 ip=0x7f36bbfb5a3d code=0x50000
Apr  5 14:21:01 hager-VirtualBox kernel: [ 2574.595726] ohci-pci 0000:00:06.0:
frame counter not updating; disabled
Apr  5 14:21:01 hager-VirtualBox kernel: [ 2574.595758] ohci-pci 0000:00:06.0:
HC died; cleaning up
Apr  5 14:21:01 hager-VirtualBox kernel: [ 2577.080368] usb 1-1: USB disconnect
```

- **STEP-8**: Install nfs service on your system

Commands

- `sudo apt install nfs-kernel-server`

```
hager@hager-VirtualBox:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

- **STEP-9**: Enable nfs service on the firewall

Commands

- `sudo ufw allow 2049/tcp`
- `sudo ufw allow 2049/udp`

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

- **STEP-10**: Create and share /tmp/shares folder using exportfs command and /etc/exports file

Commands

- `mkdir /tmp/shares`
- `sudo echo "/tmp/shares *(rw)" | sudo tee -a /etc/exports`
- `sudo exportfs -a`

```
hager@hager-VirtualBox:~$ mkdir /tmp/shares
```

```
hager@hager-VirtualBox:~$ sudo echo "/tmp/shares *(rw)" | sudo tee -a /etc/expo
rts
/tmp/shares *(rw)
```

```
hager@hager-VirtualBox:~$ sudo exportfs -a
exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' spe
fied for export "*:/tmp/shares".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x
```

- **STEP-11**: Mount the remote share on /mnt folder (you can using localhost as well)

Commands

- `sudo mount -t nfs localhost:/tmp/shares /mnt`

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

- **STEP-12**: Copy some files to the remote share

Commands

- `scp /tmp/filetest.txt /mnt`

```
hager@hager-VirtualBox:/$ scp /tmp/filetest.txt /mnt
```

- **STEP-13**: Save iptables rules to /tmp/iptables-backup file

Commands

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

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