Lab 3 System Admin 2

- install ftpd service on your laptop.

```
vboxuser@Ubuntuu:~$ sudo apt install vsftpd
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 205 not upgraded.
Need to get 123 kB of archives.
After this operation, 326 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 vsftpd amd64 3.0.5-0
ubuntu1 [123 kB]
Fetched 123 kB in 1s (148 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 232721 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) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /l
ib/systemd/system/vsftpd.service.
Processing triggers for man-db (2.10.2-1) ...
vboxuser@Ubuntuu:~$
```

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

```
vboxuser@Ubuntuu:~$ sudo iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEP
T
vboxuser@Ubuntuu:~$ sudo iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEP
T
```

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

```
vboxuser@Ubuntuu:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:vboxuser): vboxuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
Rhythmbox
g Extended Passive Mode (|||22121|)
omes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Feb 25 12:18 Desktop
drwxr-xr-x    2 1000     1000         4096 Feb 01 20:29 Documents
drwxr-xr-x    2 1000     1000         4096 Feb 01 20:29 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 01 20:29 Music
drwxr-xr-x    2 1000     1000         4096 Feb 01 20:29 Pictures
drwxr-xr-x    2 1000     1000         4096 Feb 01 20:29 Public
drwxr-xr-x    2 1000     1000         4096 Feb 01 20:29 Templates
drwxr-xr-x    2 1000     1000         4096 Feb 01 20:29 Videos
-rw-r--r--    1 0        0             340 Feb 25 12:38 bg_process.service
-rw-rw-r--    1 1000     1000            0 Feb 25 12:40 bg_script.service
-rw-rw-r--    1 1000     1000     20480000 Mar 03 04:08 disk.img
-rw-r--r--    1 0        0               0 Mar 03 04:33 file1
-rw-r--r--    1 0        0               0 Mar 03 04:33 file2
drwxrwxr-x    2 1000     1000         4096 Feb 08 14:53 iti-0
drwx------    5 1000     1000         4096 Mar 28 17:21 snap
226 Directory send OK.
```

- enable ufw service.

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

- block port 21 and 21 (tcp) using ufw.

```
vboxuser@Ubuntuu:~$ sudo ufw deny 20/tcp
Rule added
Rule added (v6)
vboxuser@Ubuntuu:~$ sudo ufw deny 21/tcp
Rule added
Rule added (v6)
```

- try to connect to ftp service.

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

- capture the ufw log to detect the blocked operation.

```
vboxuser@Ubuntuu:~$ sudo tail /var/log/kern.log
Apr  7 15:59:21 Ubuntuu kernel: [   68.132796] loop17: detected capacity change
 from 0 to 8
Apr  7 16:00:20 Ubuntuu kernel: [  126.060309] audit: type=1400 audit(168087602
0.854:53): apparmor="DENIED" operation="capable" class="cap" profile="/snap/sna
pd/18596/usr/lib/snapd/snap-confine" pid=1000 comm="snap-confine" capability=12
  capname="net_admin"
Apr  7 16:00:20 Ubuntuu kernel: [  126.060542] audit: type=1400 audit(168087602
0.854:54): apparmor="DENIED" operation="capable" class="cap" profile="/snap/sna
pd/18596/usr/lib/snapd/snap-confine" pid=1000 comm="snap-confine" capability=38
  capname="perfmon"
Apr  7 16:01:32 Ubuntuu kernel: [  197.037251] rfkill: input handler disabled
Apr  7 16:01:37 Ubuntuu kernel: [  201.905356] rfkill: input handler enabled
Apr  7 16:03:00 Ubuntuu kernel: [  285.271450] rfkill: input handler disabled
Apr  7 16:03:59 Ubuntuu kernel: [  345.182730] rfkill: input handler enabled
Apr  7 16:04:23 Ubuntuu kernel: [  369.192410] rfkill: input handler disabled
Apr  7 16:06:00 Ubuntuu kernel: [  466.034000] audit: type=1326 audit(168087636
0.485:55): auid=1000 uid=1000 gid=1000 ses=3 subj=snap.snapd-desktop-integratio
n.snapd-desktop-integration pid=2283 comm="snapd-desktop-i" exe="/snap/snapd-de
sktop-integration/49/usr/bin/snapd-desktop-integration" sig=0 arch=c000003e sys
call=314 compat=0 ip=0x7fbd6c10b73d code=0x50000
```

- install nfs service on your system.

```
vboxuser@Ubuntuu:~$ 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 205 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://us.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-core-2.1-7
amd64 2.1.12-stable-1build3 [93.9 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnfsidmap1
 amd64 1:2.6.1-1ubuntu1.2 [42.9 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 rpcbind amd64 1.2.6-
2build1 [46.6 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 keyutils amd64 1.6.1
-2ubuntu3 [50.4 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 nfs-common a
md64 1:2.6.1-1ubuntu1.2 [241 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 nfs-kernel-s
```

- enable nfs service on the firewall.

```
vboxuser@Ubuntuu:~$ sudo ufw allow 2049/tcp
Rule added
Rule added (v6)
vboxuser@Ubuntuu:~$ sudo ufw allow 2049/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
vboxuser@Ubuntuu:~$ sudo ufw allow 2049/udp
Rule added
Rule added (v6)
```

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

```
vboxuser@Ubuntuu:~$ sudo nano /etc/exports
vboxuser@Ubuntuu:~$ sudo exportfs -a
```

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

```
vboxuser@Ubuntuu:~$ sudo mkdir /mnt/myshare
vboxuser@Ubuntuu:~$ sudo mount localhost:/tmp/shares /mnt/myshare
```

- copy some files to the remote share.
  - Sudo cp /home/vboxuser/Desktop/iti-0/file2.html /mnt/myshare
- save iptables rules to /tmp/iptables-backup file.
  - Sudo iptables-save > /tmp/iptables-backup