Lab 3

1. **Install `ftpd` service on your laptop**

```
mariamkhaled@ubuntu22:~$ sudo apt install vsftpd
```

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

```
mariamkhaled@ubuntu22:~$ sudo iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
mariamkhaled@ubuntu22:~$ sudo iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
mariamkhaled@ubuntu22:~$
```

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

```
mariamkhaled@ubuntu22:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:mariamkhaled): mariamkhaled
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 (|||41096|)
150 Here comes the directory listing.
drwxr-xr-x    2 1006     1006         4096 Apr 05 15:36 Desktop
drwxr-xr-x    2 1006     1006         4096 Apr 05 15:36 Documents
drwxr-xr-x    2 1006     1006         4096 Apr 05 15:36 Downloads
drwxr-xr-x    2 1006     1006         4096 Apr 05 15:36 Music
drwxr-xr-x    2 1006     1006         4096 Apr 05 15:36 Pictures
drwxr-xr-x    2 1006     1006         4096 Apr 05 15:36 Public
drwxr-xr-x    2 1006     1006         4096 Apr 05 15:36 Templates
drwxr-xr-x    2 1006     1006         4096 Apr 05 15:36 Videos
drwx------    3 1006     1006         4096 Apr 05 15:36 snap
226 Directory send OK.
```

4. **enable ufw service**
5. **block port 20 and 21 (tcp) using ufw**

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

6. try to connect to ftp service.

```
mariamkhaled@ubuntu22:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:mariamkhaled): mariamkhaled
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

7. capture the ufw log to detect the blocked operation

```
mariamkhaled@ubuntu22:~$ sudo tail /var/log/kern.log
Apr  5 15:36:30 ubuntu22 kernel: [   17.248111] 13:36:30.222683 main     vbglR3GuestCtrlDetectPeek
GetCancelSupport: Supported (#1)
Apr  5 15:36:30 ubuntu22 kernel: [   17.952911] audit: type=1400 audit(1680701790.924:50): apparmo
r="DENIED" operation="capable" profile="/snap/snapd/18596/usr/lib/snapd/snap-confine" pid=1403 com
m="snap-confine" capability=12  capname="net_admin"
Apr  5 15:36:30 ubuntu22 kernel: [   17.955829] audit: type=1400 audit(1680701790.928:51): apparmo
r="DENIED" operation="capable" profile="/snap/snapd/18596/usr/lib/snapd/snap-confine" pid=1403 com
m="snap-confine" capability=38  capname="perfmon"
```

8. install nfs service on your system

```
mariamkhaled@ubuntu22:~$ sudo apt install nfs-kernel-server
```

9. enable nfs service on the firewall

```
mariamkhaled@ubuntu22:~$ echo '/tmp/shares *(rw)' | sudo tee -a /etc/exports
/tmp/shares *(rw)
mariamkhaled@ubuntu22:~$ sudo exports -a
sudo: exports: command not found
mariamkhaled@ubuntu22:~$ sudo exportfs -a
```

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

```
mariamkhaled@ubuntu22:~$ echo '/tmp/shares *(rw)' | sudo tee -a /etc/exports
/tmp/shares *(rw)
```

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

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

12. copy some files to the remote share

```
mariamkhaled@ubuntu22:~$ touch /tmp/file1.txt
mariamkhaled@ubuntu22:~$ scp /tmp/file1.txt /mnt
mariamkhaled@ubuntu22:~$
```

13. save iptables rules to /tmp/iptables-backup file

```
mariamkhaled@ubuntu22:~$ sudo iptables-save > /tmp/iptables-backup
mariamkhaled@ubuntu22:~$
```