Lab 3

1. Install ftpd service on your laptop
    - Sudo apt install vsftpd

2. Enable port 21 and 20 (tcp) using iptables command using input chain
    - Sudo iptables -t filter -a input -p tcp --dport 20 -j accept
    - Sudo iptables -t filter -a input -p tcp --dport 21 -j accept

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

4. Enable ufw service
    - Sudo ufw enable

5. Block port 20 and 21 (tcp) using ufw
    - Sudo ufw deny 20/tcp
    - Sudo ufw deny 21/tcp

6. Try to connect to ftp service
    - Ftp localhost

7. Capture the ufw log to detect the blocked operation
    - tail /var/log/kern.log

8. Install nfs service on your system
    - Sudo apt install nfs-kernel-server

9. Enable nfs service on the firewall
    - Sudo ufw allow 2049/tcp

10. create and share /tmp/shares folder using exportfs command and /etc/exports file
    - Mkdir /tmp/shares
    - sudo echo "/tmp/shares *(rw)" | sudo tee -a /etc/exports
    - sudo exportfs -a

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

- Sudo mount -t nfs localhost:/tmp/shares /mnt

12.Copy some files to the remote share

- Scp /tmp/filetest.txt /mnt

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

- Sudo iptables-save > /tmp/iptables-backup