

## 1-Install ftpd service

```
samar@samar-VirtualBox:~$ sudo apt install vsftpd
[sudo] password for samar:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 248 not upgraded.
Need to get 123 kB of archives.
After this operation, 326 kB of additional disk space will be used.
Get:1 http://eg.archive.ubuntu.com/ubuntu jammy/main amd64 vsftpd amd64 3.0.5-0ubuntu1 [123 kB]
Fetched 123 kB in 1s (175 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 175772 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 → /lib/systemd/system/vsftpd.service.
Processing triggers for man-db (2.10.2-1) ...
```

## 2-enable port 20 and 21

```
Processing triggers for man-db (2.10.2-1) ...
samar@samar-VirtualBox:~$ sudo iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
[sudo] password for samar:
samar@samar-VirtualBox:~$ sudo iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
samar@samar-VirtualBox:~$
```

## 3-connect to ftp server

```
samar@samar-VirtualBox:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:samar): samar
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ftp
Already connected to localhost, use close first.
ftp> ls
229 Entering Extended Passive Mode (|||23671|)
150 Here comes the directory listing.
drwxr-xr-x  2 1000    1000          4096 Feb 01 13:34 Desktop
drwxr-xr-x  2 1000    1000          4096 Feb 01 13:34 Documents
drwxr-xr-x  2 1000    1000          4096 Feb 01 13:34 Downloads
drwxr-xr-x  2 1000    1000          4096 Feb 01 13:34 Music
drwxr-xr-x  2 1000    1000          4096 Feb 01 13:34 Pictures
drwxr-xr-x  2 1000    1000          4096 Feb 01 13:34 Public
drwxr-xr-x  2 1000    1000          4096 Feb 01 13:34 Templates
drwxr-xr-x  2 1000    1000          4096 Feb 01 13:34 Videos
-rw-rw-r--  1 1000    1000           10 Feb 01 16:38 file1.txt
drwxrwxr-x  2 1000    1000          4096 Feb 01 16:14 iti
drwxrwxr-x  2 1000    1000          4096 Feb 01 16:36 iti-0
drwxrwxr-x  2 1000    1000          4096 Feb 08 14:57 iti0
drwxrwxr-x  2 1000    1000          4096 Feb 01 16:07 iti1
drwxrwxr-x  2 1000    1000          4096 Feb 01 16:07 iti2
-rw-rw-r--  1 1000    1000           0 Feb 01 16:25 logfile.log
```

4-enable ufw service

5-block port 20 and 21

```
samar@samar-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
samar@samar-VirtualBox:~$ sudo ufw deny 20/tcp
sudo: ufw: command not found
samar@samar-VirtualBox:~$ sudo ufw deny 20/tcp
Rule added
Rule added (v6)
samar@samar-VirtualBox:~$ sudo ufw deny 21/tcp
Rule added
Rule added (v6)
samar@samar-VirtualBox:~$
```

6-try to connect to ftp service

```
samar@samar-VirtualBox:~$ ftp localhost
Connected to localhost.
220 (vsFTPD 3.0.5)
Name (localhost:samar): samar
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 (|||50218|)
150 Here comes the directory listing.
drwxr-xr-x  2 1000    1000          4096 Feb  1 13:34 Desktop
drwxr-xr-x  2 1000    1000          4096 Feb  1 13:34 Documents
drwxr-xr-x  2 1000    1000          4096 Feb  1 13:34 Downloads
drwxr-xr-x  2 1000    1000          4096 Feb  1 13:34 Music
drwxr-xr-x  2 1000    1000          4096 Feb  1 13:34 Pictures
drwxr-xr-x  2 1000    1000          4096 Feb  1 13:34 Public
drwxr-xr-x  2 1000    1000          4096 Feb  1 13:34 Templates
drwxr-xr-x  2 1000    1000          4096 Feb  1 13:34 Videos
-rw-rw-r--  1 1000    1000           10 Feb  1 16:38 file1.txt
drwxrwxr-x  2 1000    1000          4096 Feb  1 16:14 iti
drwxrwxr-x  2 1000    1000          4096 Feb  1 16:36 iti-0
drwxrwxr-x  2 1000    1000          4096 Feb  1 16:07 iti0
drwxrwxr-x  2 1000    1000          4096 Feb  1 16:07 iti1
drwxrwxr-x  2 1000    1000          4096 Feb  1 16:07 iti2
-rw-rw-r--  1 1000    1000           0 Feb  1 16:25 logfile.log
drwxrwxr-x  2 1000    1000          4096 Feb 12 23:11 mydir1
drwxrwxr-x  2 1000    1000          4096 Feb 12 23:11 mydir2
```

## 7-capture the ufw log to detect the blocked operation

```
samar@samar-VirtualBox:~$ tail /var/log/kern.log
Mar 30 13:23:01 samar-VirtualBox kernel: [68771.767284] audit: type=1326 audit(1680175381.823:233): auid=1000 uid=1000 gid=1000 ses=24 subj=? pid=83856 comm="firefox" exe="/snap/firefox/2487/usr/lib/firefox/firefox" sig=0 arch=c000003e syscall=314 compat=0 ip=0x7f9fb055073d code=0x50000
Apr  1 13:24:09 samar-VirtualBox kernel: [69915.300277] audit: type=1326 audit(1680348249.379:234): auid=1000 uid=1000 gid=1000 ses=24 subj=? pid=15663 comm="pool-org.gnome." exe="/snap/snap-store/638/usr/bin/snap-store" sig=0 arch=c000003e syscall=93 compat=0 ip=0x7f3ac587339b code=0x50000
Apr  1 13:33:58 samar-VirtualBox kernel: [70504.404841] usb 2-1: USB disconnect, device number 22
Apr  1 13:33:59 samar-VirtualBox kernel: [70504.986360] usb 2-1: new full-speed USB device number 23 using ohci-pci
Apr  1 13:33:59 samar-VirtualBox kernel: [70505.672370] usb 2-1: New USB device found, idVendor=80ee, idProduct=0021, bcdDevice= 1.00
Apr  1 13:33:59 samar-VirtualBox kernel: [70505.672387] usb 2-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
Apr  1 13:33:59 samar-VirtualBox kernel: [70505.672394] usb 2-1: Product: USB Tablet
Apr  1 13:33:59 samar-VirtualBox kernel: [70505.672398] usb 2-1: Manufacturer: VirtualBox
Apr  1 13:33:59 samar-VirtualBox kernel: [70505.897513] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/0003:80EE:0021.0016/input/input28
```

## 8-install nfs service

```
samar@samar-VirtualBox:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
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 248 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://eg.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-core-2.1-7 amd64 2.1.12-stable-1build3 [93.9 kB]
Get:2 http://eg.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnfsidmap1 amd64 1:2.6.1-1ubuntu1.2 [42.9 kB]
Get:3 http://eg.archive.ubuntu.com/ubuntu jammy/main amd64 rpcbind amd64 1.2.6-
```

## 9-enable nfs service on the firewall

```
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
samar@samar-VirtualBox:~$ sudo ufw allow 2049/tcp
Rule added
Rule added (v6)
samar@samar-VirtualBox:~$ sudo ufw allow 2049/udp
Rule added
Rule added (v6)
```

## 10-create and share /tmp/shares folder using exportfs command and /etc/exportfs file

```
exportfs: failed to stat tmp/shares: No such file or directory
samar@samar-VirtualBox:~$ echo '/tmp/shares *(rw)' | sudo tee -a /etc/exports
/tmp/shares *(rw)
tee: /tmp/shares: Is a directory
/tmp/shares *(rw)
```

## 11-Mount the remote share on /mnt folder

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

exportfs: /etc/exports [2]: Neither 'subtree_check' or 'no_subtree_check' specified for export "*/tmp/shares".
    Assuming default behaviour ('no_subtree_check').
    NOTE: this default has changed since nfs-utils version 1.0.x

exportfs: /etc/exports [3]: Neither 'subtree_check' or 'no_subtree_check' specified for export "*/tmp/shares".
    Assuming default behaviour ('no_subtree_check').
    NOTE: this default has changed since nfs-utils version 1.0.x

exportfs: duplicated export entries:
    tmp/shares *(rw)
    tmp/shares *(rw)
```

## 12-Copy some files to the remote share

## 13-and save iptablesrules to /tmp/iptables-backup file

```
13-1- save the rules to a file
samar@samar-VirtualBox:~$ scp /tmp/file.txt/mnt
usage: scp [-346ABCOpqRrsTv] [-c cipher] [-D sftp_server_path] [-F ssh_c
        [-i identity_file] [-J destination] [-l limit]
        [-o ssh_option] [-P port] [-S program] source ... target
samar@samar-VirtualBox:~$ sudo iptables-save > /tmp/iptables-backup
[sudo] password for samar:
```

```
1 # Generated by iptables-save v1.8.7 on Tue Apr 11 16:22:34 2023
2 *filter
3 :INPUT DROP [0:0]
4 :FORWARD DROP [0:0]
5 :OUTPUT ACCEPT [0:0]
6 :ufw-after-forward - [0:0]
7 :ufw-after-input - [0:0]
8 :ufw-after-logging-forward - [0:0]
9 :ufw-after-logging-input - [0:0]
10 :ufw-after-logging-output - [0:0]
11 :ufw-after-output - [0:0]
12 :ufw-before-forward - [0:0]
13 :ufw-before-input - [0:0]
14 :ufw-before-logging-forward - [0:0]
15 :ufw-before-logging-input - [0:0]
16 :ufw-before-logging-output - [0:0]
17 :ufw-before-output - [0:0]
18 :ufw-logging-allow - [0:0]
19 :ufw-logging-deny - [0:0]
20 :ufw-not-local - [0:0]
21 :ufw-reject-forward - [0:0]
22 :ufw-reject-input - [0:0]
23 :ufw-reject-output - [0:0]
24 :ufw-skip-to-policy-forward - [0:0]
25 :ufw-skip-to-policy-input - [0:0]
26 :ufw-skip-to-policy-output - [0:0]
27 :ufw-track-forward - [0:0]
28 :ufw-track-input - [0:0]
```