

## Admin 2

### 1-Install ftpd service

```
radwa@radwa-VirtualBox:~$ sudo apt install vsftpd
[sudo] password for radwa:
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 7 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 3.0.5-0u
buntu1 [123 kB]
Fetched 123 kB in 1s (99.4 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 206065 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 → /li
b/systemd/system/vsftpd.service.
Processing triggers for man-db (2.10.2-1) ...
radwa@radwa-VirtualBox:~$
```

### 2-Enable port 21 and 20

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

### 3-Connect to ftp server and ls current directory

```
radwa@radwa-VirtualBox:~$ ftp localhost
Connected to localhost.
220 (vsFTPD 3.0.5)
Name (localhost:radwa): radwa
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 (|||9118|)
150 Here comes the directory listing.
drwxr-xr-x    2 1000    1000          4096 Feb 11 15:46 Desktop
drwxr-xr-x    2 1000    1000          4096 Feb 11 15:46 Documents
drwxr-xr-x    2 1000    1000          4096 Feb 11 15:46 Downloads
drwxr-xr-x    2 1000    1000          4096 Feb 11 15:46 Music
drwxr-xr-x    2 1000    1000          4096 Feb 11 15:46 Pictures
drwxr-xr-x    2 1000    1000          4096 Feb 11 15:46 Public
drwxr-xr-x    2 1000    1000          4096 Feb 11 15:46 Templates
drwxr-xr-x    2 1000    1000          4096 Feb 11 15:46 Videos
-rw-rw-r--    1 1000    1000          203 Feb 22 08:53 bgprocess.service
-rw-rw-r--    1 1000    1000           45 Feb 22 09:20 cronJob.sh
-rw-rw-r--    1 1000    1000           0 Feb 22 06:54 lab4.sh
-rw-r--r--    1 0        0           0 Feb 22 08:17 lab4_bash.service
```

### 4-enable ufw service

```
radwa@radwa-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
radwa@radwa-VirtualBox:~$
```

### 5-Block port 21 and port 20 using ufw

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

## 6-Try to connect to ftp service

```
radwa@radwa-VirtualBox:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:radwa): radwa
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 (|||22259|)
150 Here comes the directory listing.
drwxr-xr-x  2 1000    1000          4096 Feb 11 15:46 Desktop
drwxr-xr-x  2 1000    1000          4096 Feb 11 15:46 Documents
drwxr-xr-x  2 1000    1000          4096 Feb 11 15:46 Downloads
drwxr-xr-x  2 1000    1000          4096 Feb 11 15:46 Music
drwxr-xr-x  2 1000    1000          4096 Feb 11 15:46 Pictures
drwxr-xr-x  2 1000    1000          4096 Feb 11 15:46 Public
drwxr-xr-x  2 1000    1000          4096 Feb 11 15:46 Templates
drwxr-xr-x  2 1000    1000          4096 Feb 11 15:46 Videos
-rw-rw-r--  1 1000    1000          203 Feb 22 08:53 bgprocess.service
-rw-rw-r--  1 1000    1000           45 Feb 22 09:20 cronJob.sh
-rw-rw-r--  1 1000    1000           0 Feb 22 06:54 lab4.sh
```

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

```
radwa@radwa-VirtualBox:~$ tail /var/log/kern.log
Apr  1 05:04:16 radwa-VirtualBox kernel: [67470.155937] 09:04:16.436174 control
vbgIR3GuestCtrlDetectPeekGetCancelSupport: Supported (#1)
Apr  1 05:04:17 radwa-VirtualBox kernel: [67470.725526] usb 2-1: new full-speed
USB device number 6 using ohci-pci
Apr  1 05:04:17 radwa-VirtualBox kernel: [67471.514055] usb 2-1: New USB device
found, idVendor=80ee, idProduct=0021, bcdDevice= 1.00
Apr  1 05:04:17 radwa-VirtualBox kernel: [67471.514071] usb 2-1: New USB device
strings: Mfr=1, Product=3, SerialNumber=0
Apr  1 05:04:17 radwa-VirtualBox kernel: [67471.514073] usb 2-1: Product: USB Ta
blet
Apr  1 05:04:17 radwa-VirtualBox kernel: [67471.514075] usb 2-1: Manufacturer: V
irtualBox
Apr  1 05:04:18 radwa-VirtualBox kernel: [67471.739071] input: VirtualBox USB Ta
blet as /devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/0003:80EE:0021.0005/in
put/input11
Apr  1 05:04:18 radwa-VirtualBox kernel: [67471.798622] hid-generic 0003:80EE:00
21.0005: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:
00:06.0-1/input0
Apr  5 08:17:22 radwa-VirtualBox kernel: [67472.820380] 12:17:22.433120 timesync
vgsvcTimeSyncWorker: Radical host time change: 357 209 251 000 000ns (HostNow=1
680 697 042 433 000 000 ns HostLast=1 680 339 833 182 000 000 ns)
Apr  5 08:17:32 radwa-VirtualBox kernel: [67482.818433] 12:17:32.436088 timesync
vgsvcTimeSyncWorker: Radical guest time change: 357 193 335 533 000ns (GuestNow
```

## 8-Install nfs service on your system

```
radwa@radwa-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 7 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 amd64 1:2.6.1-1ubuntu1.2 [42.9 kB]
```

## 9-Enable nfs service on the firewall

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

## 10-Create and share /tmp/shares folder

>>mkdir /tmp/shares

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

## 11-Mount the remote share

```
radwa@radwa-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

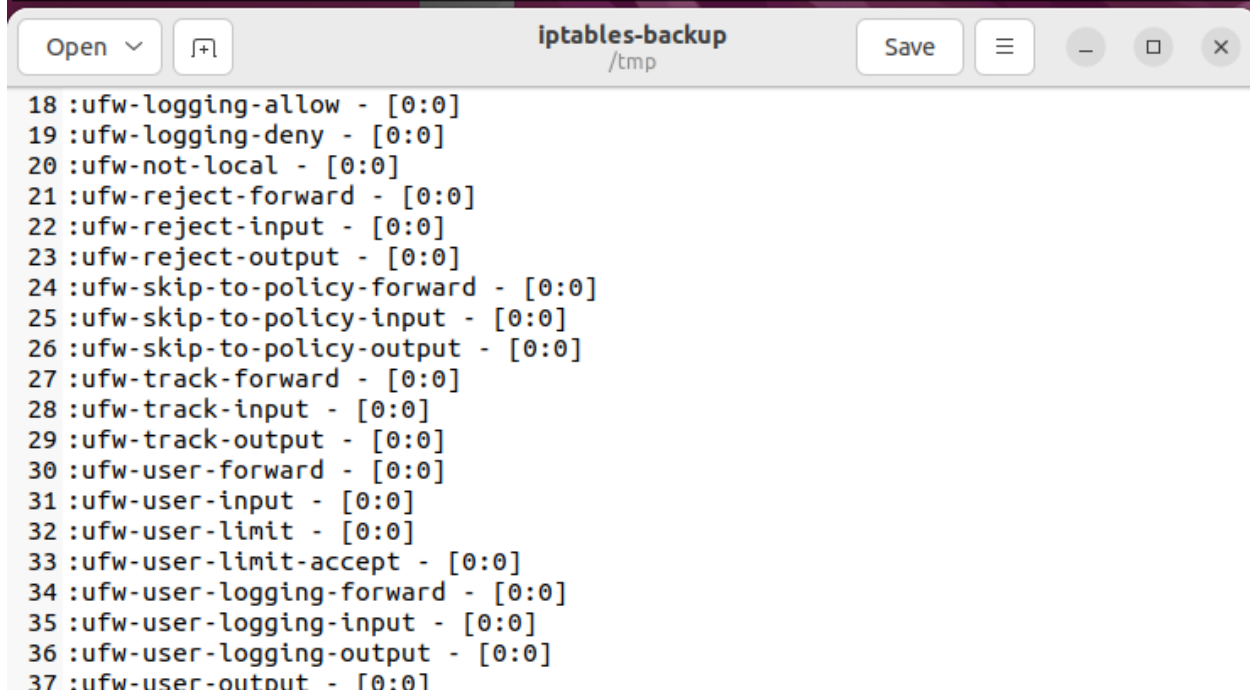
radwa@radwa-VirtualBox:~$ sudo mount -t nfs localhost:/tmp/shares /mnt
radwa@radwa-VirtualBox:~$
```

## 12-Copy some files to the remote share

```
radwa@radwa-VirtualBox:/$ scp /tmp/file.txt /mnt
radwa@radwa-VirtualBox:/$
```

## 13-Save iptables rules

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



```
Open ▾ [icon] iptables-backup /tmp Save [icon] [icon] [icon]
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]
29 :ufw-track-output - [0:0]
30 :ufw-user-forward - [0:0]
31 :ufw-user-input - [0:0]
32 :ufw-user-limit - [0:0]
33 :ufw-user-limit-accept - [0:0]
34 :ufw-user-logging-forward - [0:0]
35 :ufw-user-logging-input - [0:0]
36 :ufw-user-logging-output - [0:0]
37 :ufw-user-output - [0:0]
```