System Admin II :Lab3

- Install ftpd services on your device

```
maysara@Linux-Ubuntu:~$ sudo apt install vsftpd
[sudo] password for maysara:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-5.15.0-60 linux-headers-5.15.0-60-generic
  linux-image-5.15.0-60-generic linux-modules-5.15.0-60-generic
  linux-modules-extra-5.15.0-60-generic systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 230 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 3.0.5-0u
buntu1 [123 kB]
```

- Enable port 20 and 21 (tcp) using iptables command using input chain

```
maysara@Linux-Ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 20 -j ACCEPT
maysara@Linux-Ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
```

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

```
maysara@Linux-Ubuntu:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:maysara): maysara
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
```

- Enable ufw service

```
maysara@Linux-Ubuntu:~$ sudo ufw enable
[sudo] password for maysara:
Firewall is active and enabled on system startup
maysara@Linux-Ubuntu:~$
```

- Block port 20 and 21 (tcp) using ufw

```
maysara@Linux-Ubuntu:~$ sudo ufw deny 20/tcp
Rule added
Rule added (v6)
maysara@Linux-Ubuntu:~$ sudo ufw deny 21/tcp
Rule added
Rule added (v6)
maysara@Linux-Ubuntu:~$
```

- Try to connect to ftp service

```
maysara@Linux-Ubuntu:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:maysara): maysara
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 (|||34902|)
150 Here comes the directory listing.
drwxr-xr-x    3 1000     1000         4096 Mar 04 13:21 Desktop
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:43 Documents
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:43 Downloads
drwxr-xr-x    2 1000     1000         4096 Feb 01 13:43 Music
```

- Capture the ufw log to detect the blocked operations

```
maysara@Linux-Ubuntu:~$ tail /var/log/kern.log
tail: cannot open '/var/log/kern.log' for reading: Permission denied
maysara@Linux-Ubuntu:~$ sudo tail /var/log/kern.log
[sudo] password for maysara:
Apr 11 22:37:19 Linux-Ubuntu kernel: [   27.941728]  exe="/usr/bin/dbus-daemon"
sauid=102 hostname=? addr=? terminal=?'
Apr 11 22:37:19 Linux-Ubuntu kernel: [   27.942051] audit: type=1107 audit(16812
45439.527:54): pid=609 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freed
esktop/PolicyKit1/Authority" interface="org.freedesktop.PolicyKit1.Authority" me
mber="CheckAuthorization" mask="send" name=":1.4" pid=1769 label="snap.snap-stor
e.snap-store" peer_pid=632 peer_label="unconfined"
Apr 11 22:37:19 Linux-Ubuntu kernel: [   27.942051]  exe="/usr/bin/dbus-daemon"
sauid=102 hostname=? addr=? terminal=?'
Apr 11 22:37:19 Linux-Ubuntu kernel: [   27.944440] audit: type=1107 audit(16812
45439.531:55): pid=609 uid=102 auid=4294967295 ses=4294967295 subj=unconfined ms
g='apparmor="DENIED" operation="dbus_method_call"  bus="system" path="/org/freed
esktop/PolicyKit1/Authority" interface="org.freedesktop.DBus.Properties" member=
"GetAll" mask="send" name=":1.4" pid=1769 label="snap.snap-store.snap-store" pee
r_pid=632 peer_label="unconfined"
Apr 11 22:37:19 Linux-Ubuntu kernel: [   27.944440]  exe="/usr/bin/dbus-daemon"
sauid=102 hostname=? addr=? terminal=?'
```

- Install nfs service on your system

```
maysara@Linux-Ubuntu:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-5.15.0-60 linux-headers-5.15.0-60-generic
  linux-image-5.15.0-60-generic linux-modules-5.15.0-60-generic
  linux-modules-extra-5.15.0-60-generic systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove them.
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 238 not upgraded.
Need to get 615 kB of archives.
After this operation, 2,235 kB of additional disk space will be used.
```

- Enable nfs service of the firewall

```
maysara@Linux-Ubuntu:~$ sudo ufw allow 2024/tcp
Rule added
Rule added (v6)
maysara@Linux-Ubuntu:~$
```

- Create and share /tmp/shares folder using exports command and etc/exports file

```
Rule added (v6)
maysara@Linux-Ubuntu:~$ sudo echo "/tmp/shares *(rw)" | sudo tee -a /etc/exports
/tmp/shares *(rw)
maysara@Linux-Ubuntu:~$ sudo exportfs -a
exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check' specified for expo
rt "*:/tmp/shares".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x

maysara@Linux-Ubuntu:~$
```

- Mount the remote share on /mnt folder

```
maysara@Linux-Ubuntu:~$ sudo mount -t nfs localhost:/tmp/shares /mnt
maysara@Linux-Ubuntu:~$
```

- Copy some files to remote share

```
maysara@Linux-Ubuntu:~$ scp /tmp/file.txt /mnt
cp: cannot stat '/tmp/file.txt': No such file or directory
maysara@Linux-Ubuntu:~$ touch /tmp/file.txt
maysara@Linux-Ubuntu:~$ scp /tmp/file.txt /mnt
maysara@Linux-Ubuntu:~$
```

- Save iptables run to /tmp/iptables-backup file

```
maysara@Linux-Ubuntu:~$ sudo iptables-save > /tmp/iptables-backup
maysara@Linux-Ubuntu:~$
```