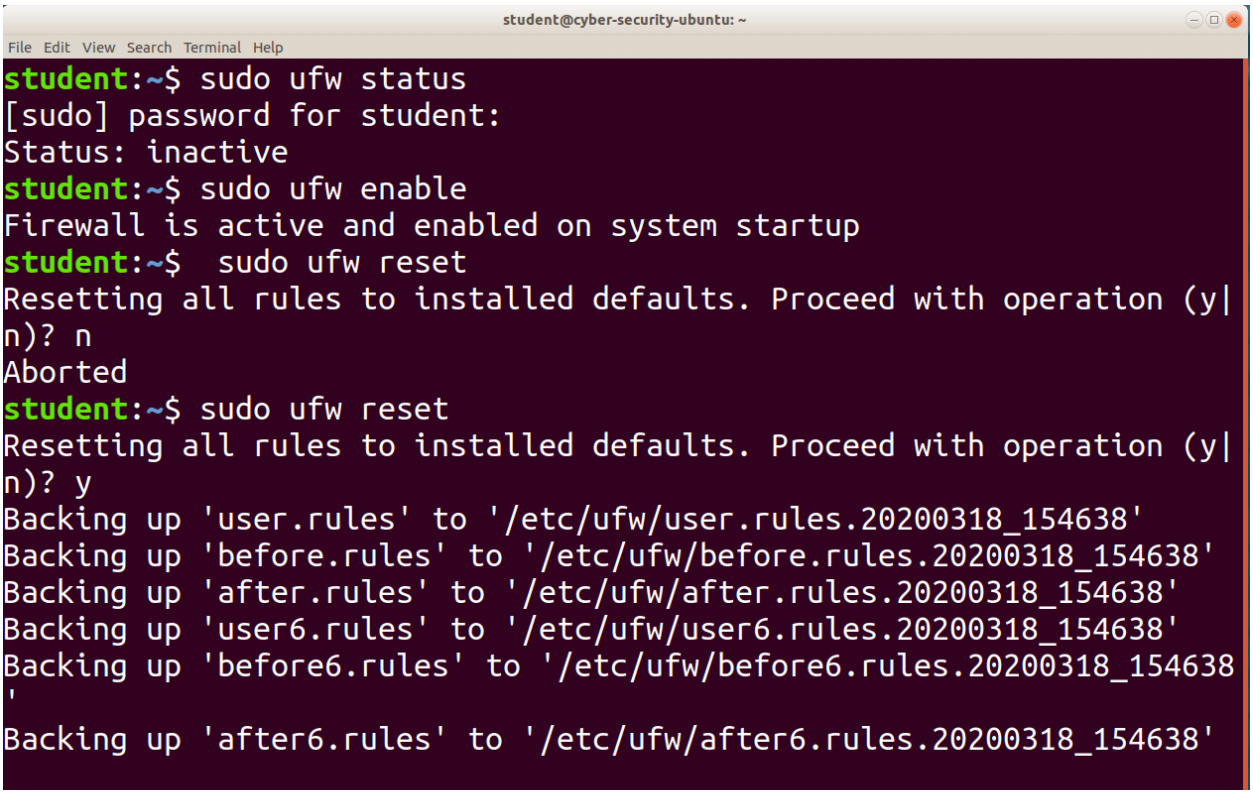

Install UFW

- Set up firewall with sudo ufw enable

```
Status: active
student:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip
student:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
  Nginx Full
  Nginx HTTP
  Nginx HTTPS
  Postfix
  Postfix SMTPS
  Postfix Submission
student:~$ sudo ufw app info 'Apache Full'
Profile: Apache Full
Title: Web Server (HTTP,HTTPS)
Description: Apache v2 is the next generation of the omnipresent Apac
he web
server.

Ports:
  80,443/tcp
student:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
student:~$
```

- Once installation is complete; check ufw status with sudo ufw status verbose
- List all application profiles available on server with sudo ufw app list
- You can discover more information about a specific profile using audo app info ‘Apache Full’
- Add a new rule to allow incoming ssh connections

```
on with the other options.
student:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 204 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,316 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 n
curses-term all 6.1-1ubuntu1.18.04 [248 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 o
penssh-sftp-server amd64 1:7.6p1-4ubuntu0.3 [45.6 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 o
penssh-server amd64 1:7.6p1-4ubuntu0.3 [333 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 s
sh-import-id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 0s (1,841 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
(Reading database ... 231997 files and directories currently installe
d.)
Preparing to unpack .../ncurses-term_6.1-1ubuntu1.18.04_all.deb ...
Unpacking ncurses-term (6.1-1ubuntu1.18.04) ...
Selecting previously unselected package openssh-sftp-server.
```

- Install ssh server;
- configure ufw firewall to all incoming ssh connections

```
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor pr
   Active: active (running) since Wed 2020-03-18 17:15:17 EDT; 3min 58
 Main PID: 5984 (sshd)
    Tasks: 1 (limit: 4856)
   CGroup: /system.slice/ssh.service
           └─5984 /usr/sbin/sshd -D

Mar 18 17:15:17 cyber-security-ubuntu systemd[1]: Starting OpenBSD Sec
Mar 18 17:15:17 cyber-security-ubuntu sshd[5984]: Server listening on
Mar 18 17:15:17 cyber-security-ubuntu sshd[5984]: Server listening on
Mar 18 17:15:17 cyber-security-ubuntu systemd[1]: Started OpenBSD Secu
```

- check ssh service status and what port ssh is listening on

```
student:~$ ^C
student:~$ ^C
student:~$ sudo ufw allow 5984/tcp
Rule added
Rule added (v6)
student:~$
```

```
student:~$ sudo ufw disable
Firewall stopped and disabled on system startup
student:~$ telnet localhost
Trying ::1...
Trying 127.0.0.1...
Trying 127.0.1.1...
telnet: Unable to connect to remote host: Connection refused
student:~$ sudo ufw enable
Firewall is active and enabled on system startup
student:~$ apt-get install telnetd
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Per
mission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-fronten
d), are you root?
student:~$ sudo apt-get install telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  openbsd-inetd tcpd
The following NEW packages will be installed:
  openbsd-inetd tcpd telnetd
0 upgraded, 3 newly installed, 0 to remove and 204 not upgraded.
Need to get 89.8 kB of archives.
After this operation, 294 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

- use telnet to check localhost
- however, the first time I tried the connection was refused so I had to manually install telnet with sudo get-install telnetd

```
student:~$ sudo ufw allow 23/tcp
Rule added
Rule added (v6)
student:~$
```

- allow the standard telnet port 23 to be open

```
  command 'pork' from deb pork

Try: sudo apt install <deb name>

student:~$ sudo nmap -sTU -O 172.17.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-18 17:46 EDT
Nmap scan report for cyber-security-ubuntu (172.17.0.1)
Host is up (0.00011s latency).
Not shown: 1994 closed ports
PORT     STATE         SERVICE
22/tcp   open          ssh
23/tcp   open          telnet
80/tcp   open          http
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.10
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
student:~$
```

- use sudo nmap -sTU -O <IP address> to check what ports are open; alternative to using telnet command
- ifconfig verified that the host IP address is 172.17.0.1

```
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
student:~$ sudo ufw allow dns
ERROR: Could not find a profile matching 'dns'
student:~$ sudo ufw allow DNS
ERROR: Could not find a profile matching 'DNS'
student:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
5984/tcp                   ALLOW       Anywhere
23/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
5984/tcp (v6)              ALLOW       Anywhere (v6)
23/tcp (v6)                ALLOW       Anywhere (v6)

student:~$ sudo ufw allow ftp
Rule added
Rule added (v6)
student:~$ sudo ufw allow dns
ERROR: Could not find a profile matching 'dns'
student:~$
```

```
5984/tcp                   ALLOW       Anywhere
23/tcp                     ALLOW       Anywhere
21/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
5984/tcp (v6)              ALLOW       Anywhere (v6)
23/tcp (v6)                ALLOW       Anywhere (v6)
21/tcp (v6)                ALLOW       Anywhere (v6)

student:~$ sudo ufw deny 5984/tcp
Rule updated
Rule updated (v6)
student:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
5984/tcp                   DENY        Anywhere
23/tcp                     ALLOW       Anywhere
21/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
5984/tcp (v6)              DENY        Anywhere (v6)
23/tcp (v6)                ALLOW       Anywhere (v6)
21/tcp (v6)                ALLOW       Anywhere (v6)
```

```
21/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
5984/tcp (v6)              DENY        Anywhere (v6)
23/tcp (v6)                ALLOW       Anywhere (v6)
21/tcp (v6)                ALLOW       Anywhere (v6)

student:~$ sudo ufw disable
Firewall stopped and disabled on system startup
student:~$ sudo sed -i '/ufw-before-input.*icmp/s/ACCEPT/DROP/g' /etc/u
fw/before.rules
student:~$ sudo ufw enable
Firewall is active and enabled on system startup
student:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
5984/tcp                   DENY        Anywhere
23/tcp                     ALLOW       Anywhere
21/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
5984/tcp (v6)              DENY        Anywhere (v6)
23/tcp (v6)                ALLOW       Anywhere (v6)
21/tcp (v6)                ALLOW       Anywhere (v6)

student:~$
```

- use command:
- sudo sed -i '/ufw-before-input.*icmp/s/ACCEPT/DROP/g' /etc/ufw/before.rules
- to change rules and deny inbound ICMP from outside localhost
- or use sudo ufw deny <port>/tcp