

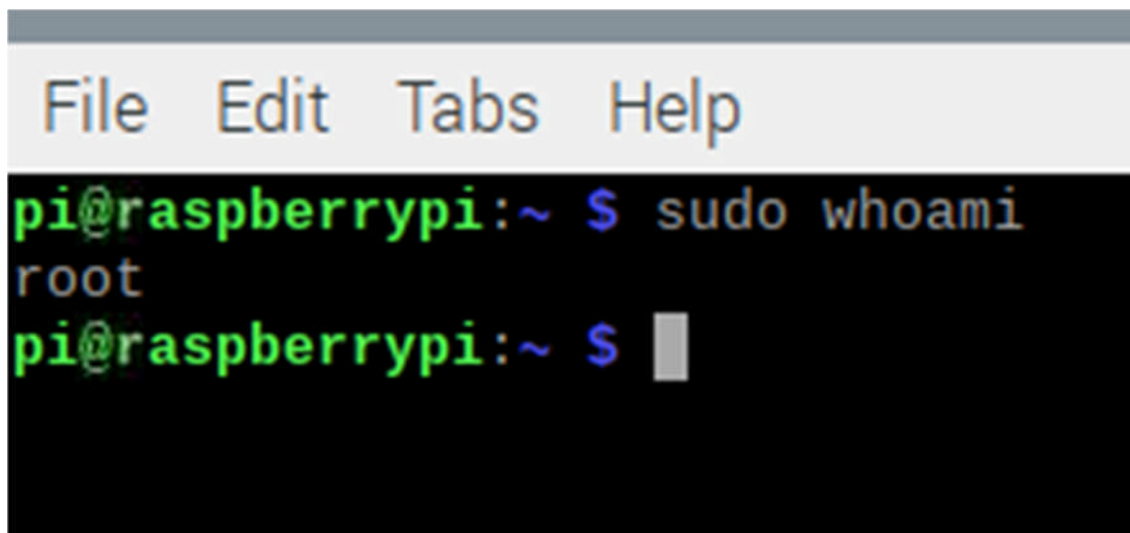
## EDUNET FOUNDATION-Class Exercise

### LAB-2: How to activate the firewall on the RPI

**Note: Description of commands available in PPT**

#### 1. Sudo

- If run sudo with command **whoami**,
- will get confirmation that you're running the command as root.
- sudo whoami root



```
File Edit Tabs Help
pi@raspberrypi:~ $ sudo whoami
root
pi@raspberrypi:~ $
```

#### 2. pwd

The Print Working Directory (pwd)

Where you currently are in the directory

```
File Edit Tabs Help

pi@raspberrypi:~ $ pwd
/home/pi
pi@raspberrypi:~ $
```

### 3. who and w

- **who** command display
  - logged in users
  - last time the system was booted
  - current run level
- **w** command prints
  - user id
  - user activities on the system.

```
File Edit Tabs Help

pi@raspberrypi:~ $ who
pi    tty7      2023-04-25 15:30 (:0)
pi    tty1      2023-04-25 15:30
pi@raspberrypi:~ $ w
 19:03:44 up 6 min,  2 users,  load average: 0.00, 0.16, 0.12
USER    TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
pi      tty7      :0                15:30    3:33m  3.10s  0.25s /usr/bin/lxsession -s LXDE-pi -e LXDE
pi      tty1      -                 15:30    3:33m  0.14s  0.11s -bash
pi@raspberrypi:~ $
```



#### 4. Last

- Shows recent logins for users
- Track down changes or other activity.

```
pi@raspberrypi:~ $ last
pi          tty1          Tue Apr 25 15:30      gone - no logout
pi          tty7          :0                   Tue Apr 25 15:30      gone - no logout
reboot     system boot  5.10.103-v7l+       Thu Jan 1 05:30      still running
pi          tty1          Tue Apr 25 14:33 -   down   (00:56)
pi          tty7          :0                   Tue Apr 25 14:33 -   15:30   (00:56)
reboot     system boot  5.10.103-v7l+       Thu Jan 1 05:30 -   15:30   (19472+10:00)
diwakar    pts/0         192.168.0.104       Tue Apr 25 14:28 -   down   (00:05)
pi          tty1          Tue Apr 25 12:55 -   down   (01:38)
pi          tty7          :0                   Tue Apr 25 12:55 -   14:33   (01:38)
reboot     system boot  5.10.103-v7l+       Thu Jan 1 05:30 -   14:33   (19472+09:03)
diwakar    pts/0         192.168.0.104       Tue Apr 25 11:13 -   12:55   (01:42)
pi          tty1          Tue Apr 25 11:06 -   crash   (-19472+05:36)
pi          tty7          :0                   Tue Apr 25 11:06 -   crash   (-19472+05:36)
reboot     system boot  5.10.103-v7l+       Thu Jan 1 05:30 -   14:33   (19472+09:03)
diwakar    pts/0         fe80::d835:7a1:4    Tue Apr 25 10:10 -   11:05   (00:55)
pi          tty1          Tue Apr 25 10:08 -   down   (00:57)
pi          tty7          :0                   Tue Apr 25 10:08 -   11:05   (00:57)
reboot     system boot  5.10.103-v7l+       Thu Jan 1 05:30 -   11:05   (19472+05:35)
pi          pts/0         fe80::d835:7a1:4    Tue Apr 25 09:53 -   10:07   (00:14)
pi          tty1          Mon Apr 24 15:46 -   down   (18:21)
pi          tty7          :0                   Mon Apr 24 15:46 -   10:07   (18:21)
reboot     system boot  5.10.103-v7l+       Thu Jan 1 05:30 -   10:07   (19472+04:37)
pi          pts/0         fe80::d835:7a1:4    Mon Apr 24 15:47 -   15:53   (00:06)
pi          tty1          Mon Apr 24 14:54 -   crash   (-19471+09:24)
pi          tty7          :0                   Mon Apr 24 14:54 -   crash   (-19471+09:24)
reboot     system boot  5.10.103-v7l+       Thu Jan 1 05:30 -   10:07   (19472+04:37)
pi          pts/0         192.168.0.106       Mon Apr 24 14:47 -   crash   (-19471+09:17)
pi          tty1          Mon Apr 24 14:47 -   crash   (-19471+09:17)
pi          tty7          :0                   Mon Apr 24 14:47 -   crash   (-19471+09:17)
reboot     system boot  5.10.103-v7l+       Thu Jan 1 05:30 -   10:07   (19472+04:37)
pi          pts/0         192.168.0.106       Mon Apr 24 14:46 -   14:47   (00:00)
```

#### 5. netstat -anp

- -a: shows the state for sockets.
- -n: shows IP addresses instead of hosts.
- -p: shows the program establishing the connection

```
File Edit Tabs Help
pi@raspberrypi:~ $ netstat -anp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.0.105:5900      192.168.0.104:53080     ESTABLISHED -
tcp        0      0 127.0.0.1:51590         127.0.0.1:37281        ESTABLISHED -
tcp        0      0 127.0.0.1:37281         127.0.0.1:51590        ESTABLISHED 706/vncserverui
tcp6       0      0 :::22                   :::*                     LISTEN      -
tcp6       0      0 :::1:631                 :::*                     LISTEN      -
tcp6       0      0 :::5900                   :::*                     LISTEN      -
udp        0      0 0.0.0.0:68              0.0.0.0:*               -
udp        0      0 0.0.0.0:631             0.0.0.0:*               -
udp        0      0 0.0.0.0:52942           0.0.0.0:*               -
udp        0      0 0.0.0.0:5353            0.0.0.0:*               -
udp6       0      0 :::5353                  :::*                     -
udp6       0      0 :::39297                 :::*                     -
raw6       0      0 :::58                    :::*                     7          -

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State      I-Node  PID/Program name  Path
unix   2      [ ]         DGRAM      -          19196   570/systemd       /run/user/1000/systemd/notify
unix   2      [ ACC ]     STREAM    LISTENING  19199   570/systemd       /run/user/1000/systemd/private
unix   2      [ ACC ]     STREAM    LISTENING  19204   570/systemd       /run/user/1000/gnupg/S.gpg-agent
unix   2      [ ACC ]     STREAM    LISTENING  19205   570/systemd       /run/user/1000/pulse/native
unix   2      [ ]         DGRAM      -          20724   644/lxpanel       /tmp/dhccpd-pi/libdhccpd-wpa-644.0
unix   2      [ ACC ]     STREAM    LISTENING  19206   570/systemd       /run/user/1000/gnupg/S.gpg-agent.ssh
unix   2      [ ACC ]     STREAM    LISTENING  19207   570/systemd       /run/user/1000/bus
unix   2      [ ]         DGRAM      -          20725   644/lxpanel       /tmp/dhccpd-pi/libdhccpd-wpa-644.1
```

## 6. UFW

- To install firewall in Rpi,  
**sudo apt install ufw**
- To enable the firewall at startup run:  
**sudo ufw enable**

```
pi@raspberrypi:~ $ sudo ufw enable
Firewall is active and enabled on system startup
pi@raspberrypi:~ $
```