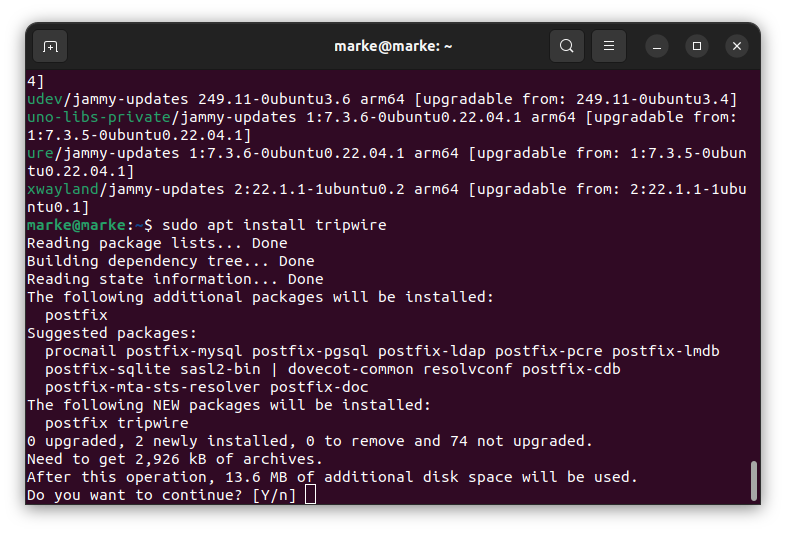
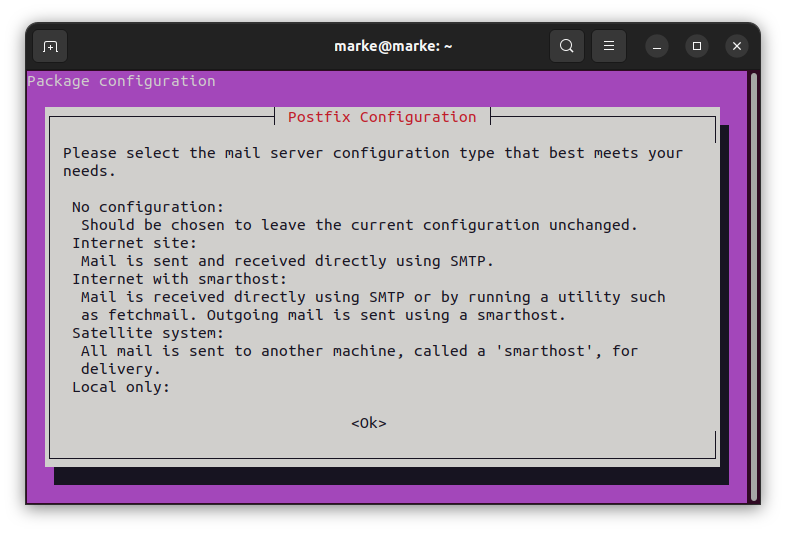
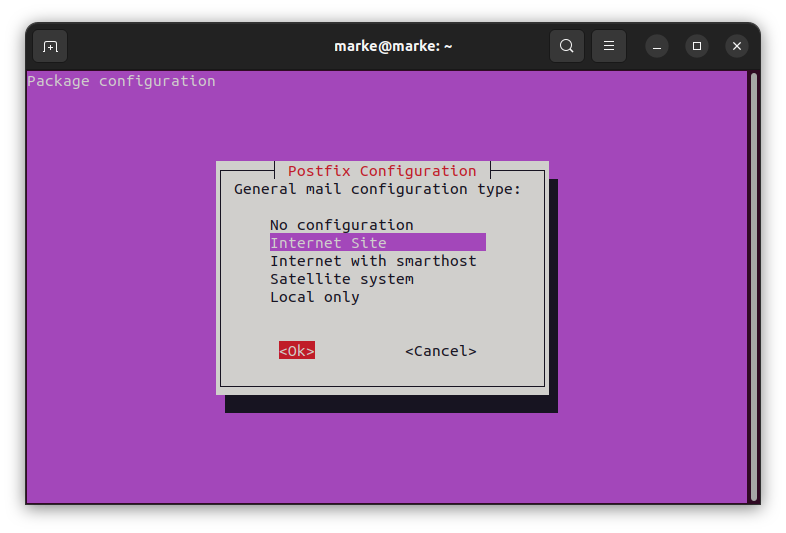
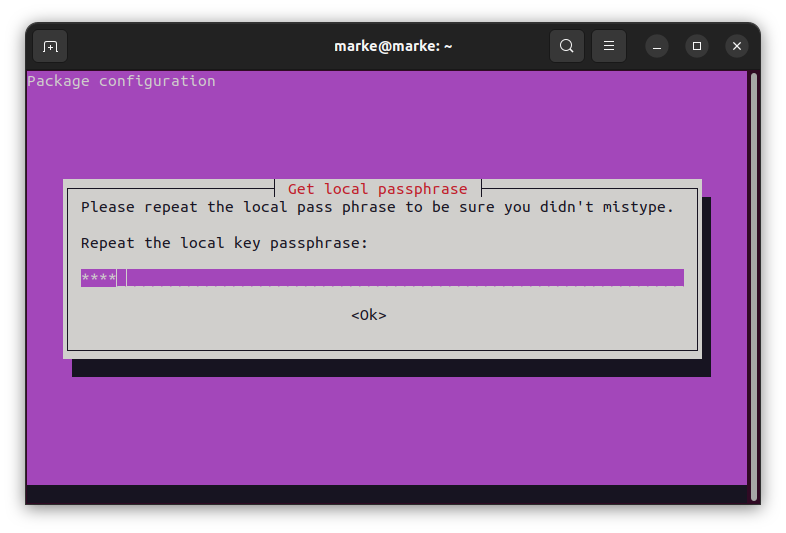
**WEEK 3-1:**

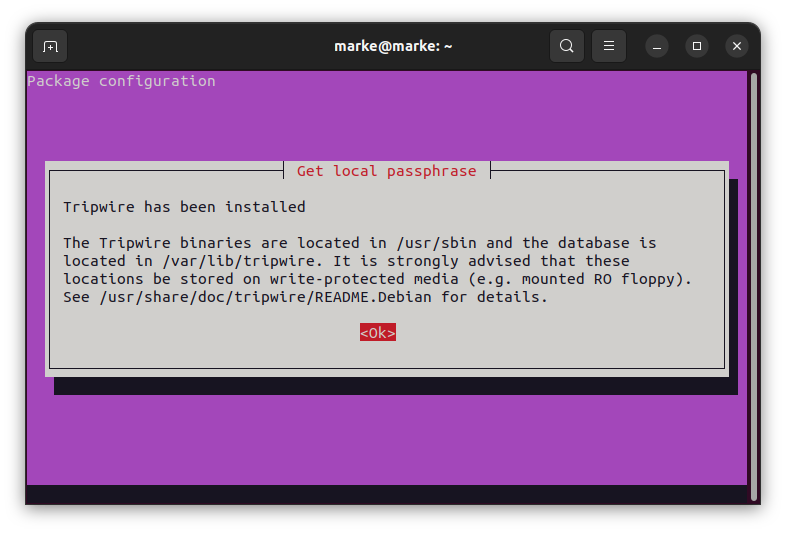
Install Tripwire and show advanced configuration

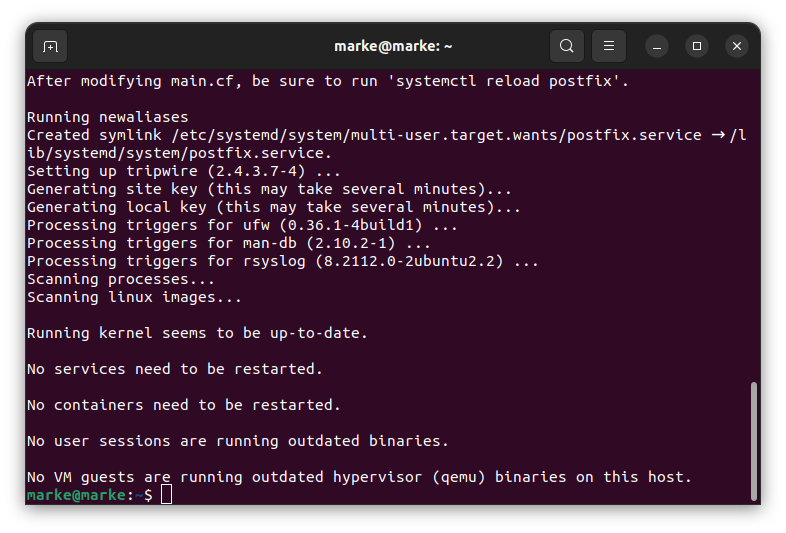
****



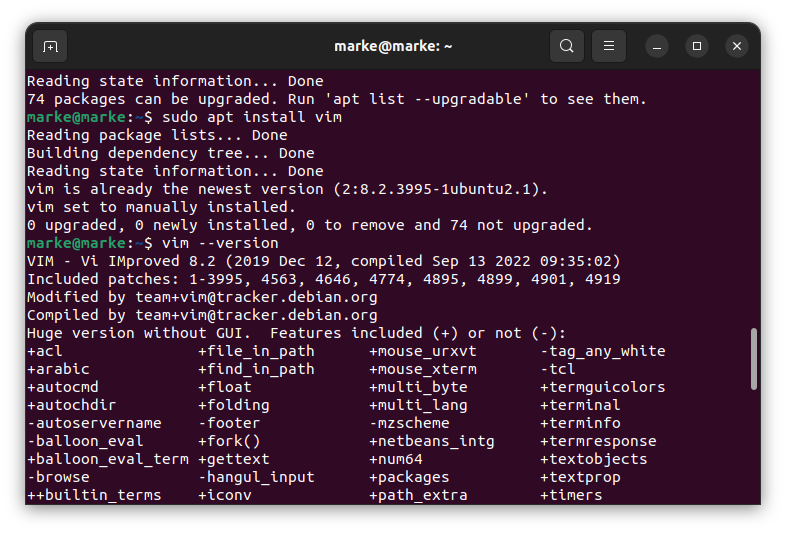


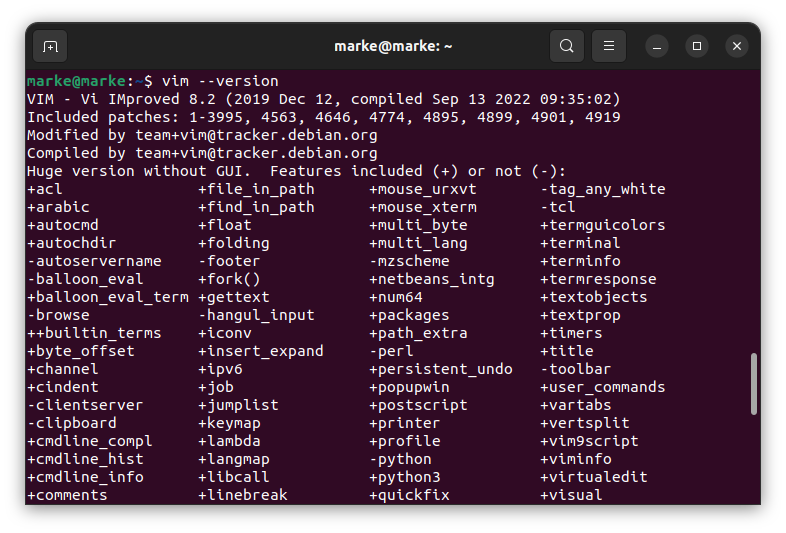


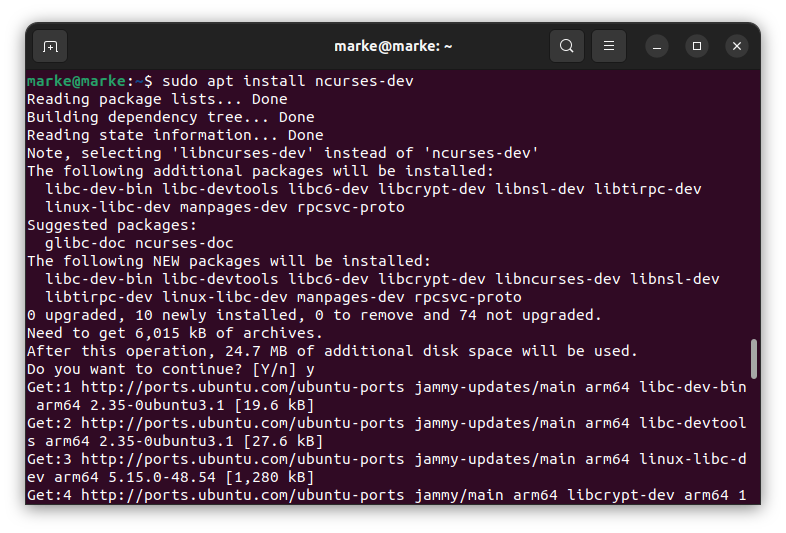


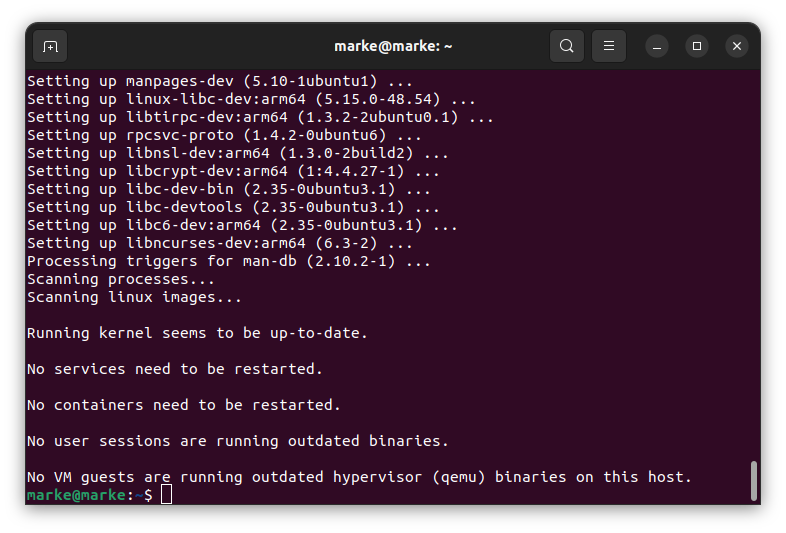


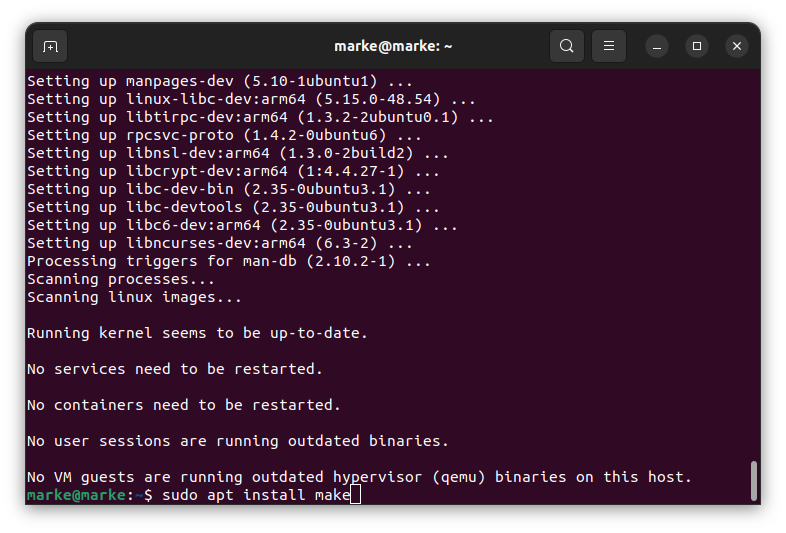
vim

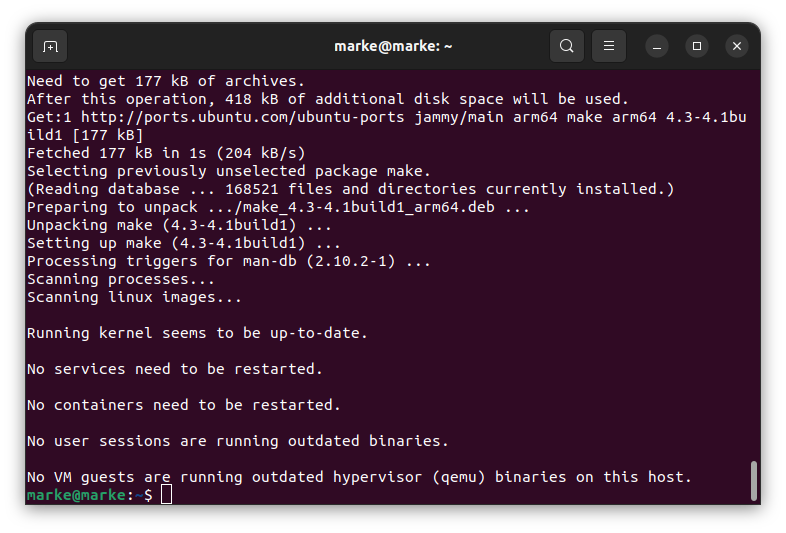


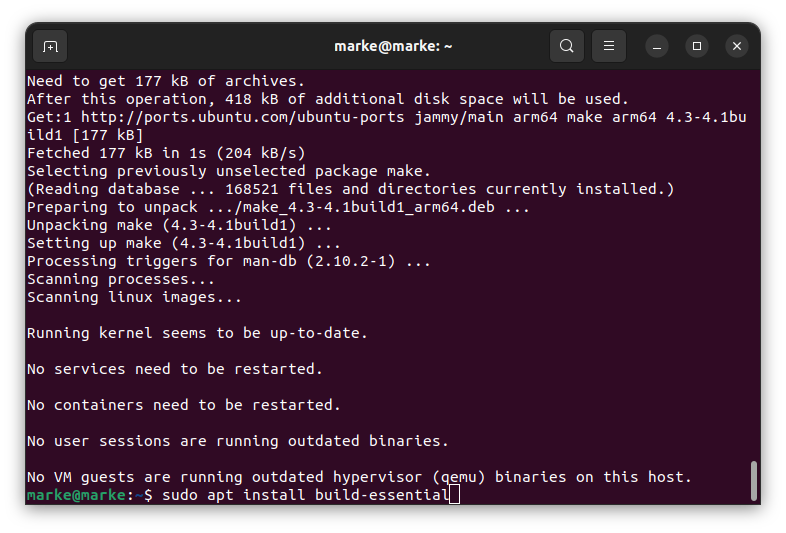


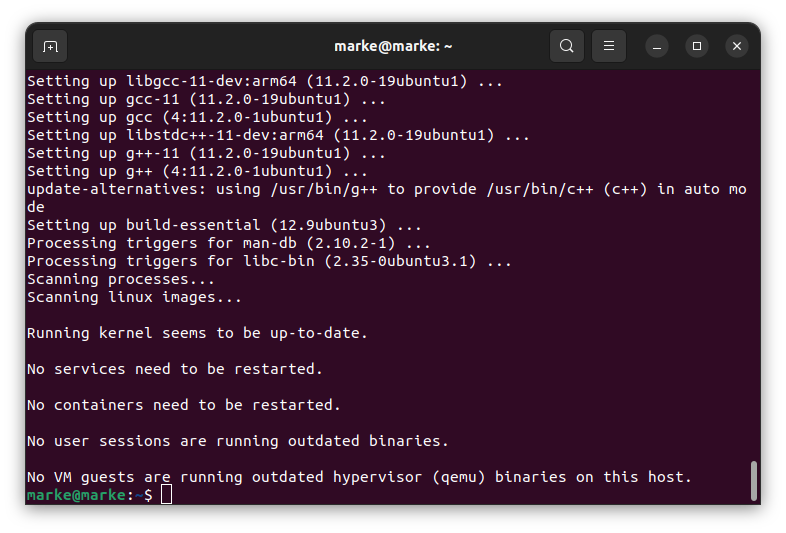


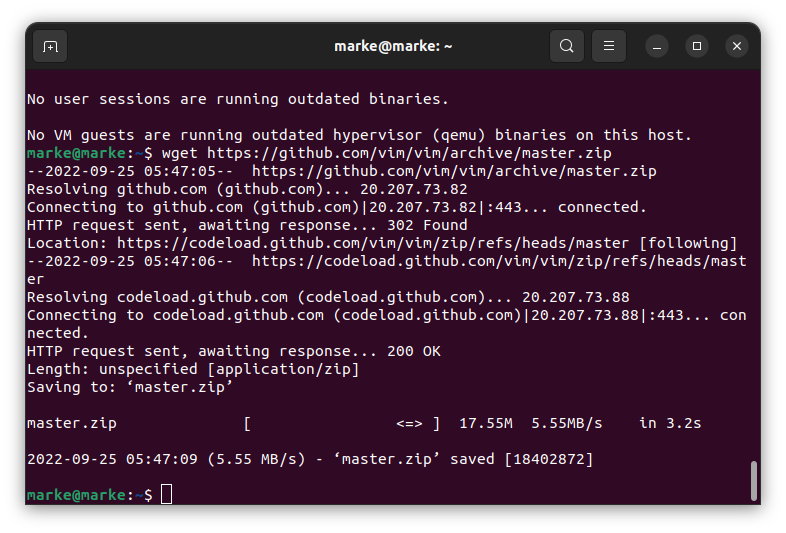


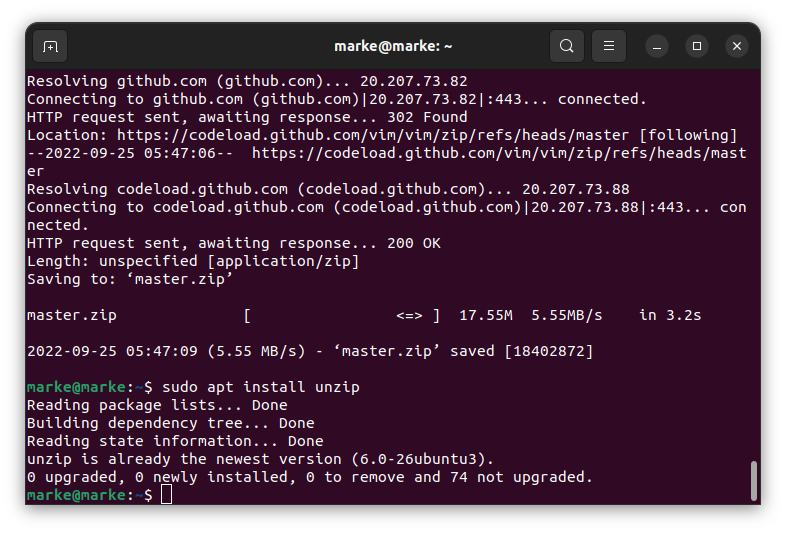


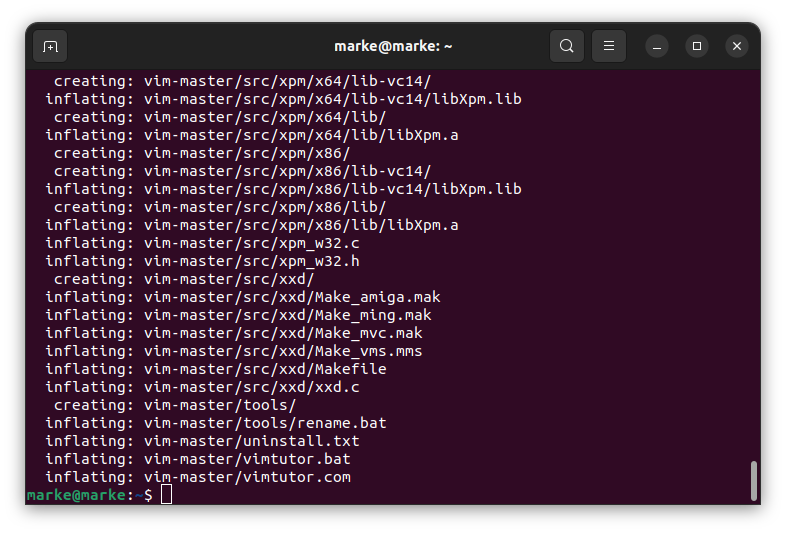


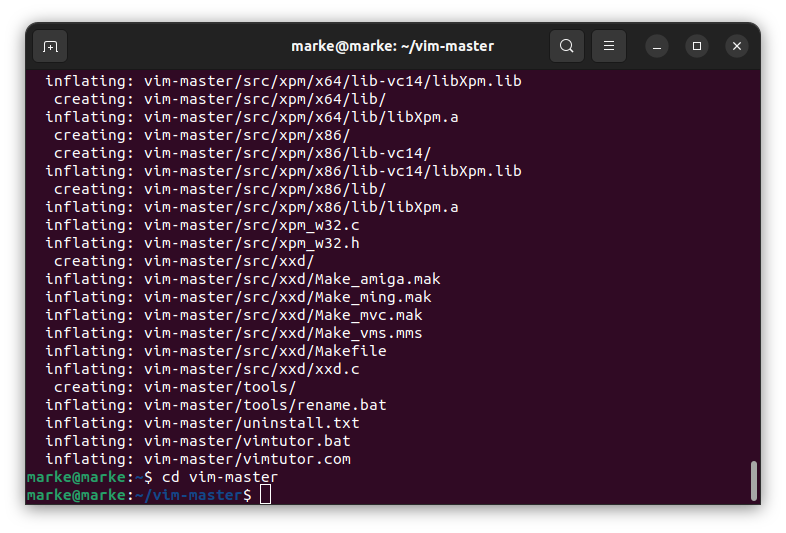


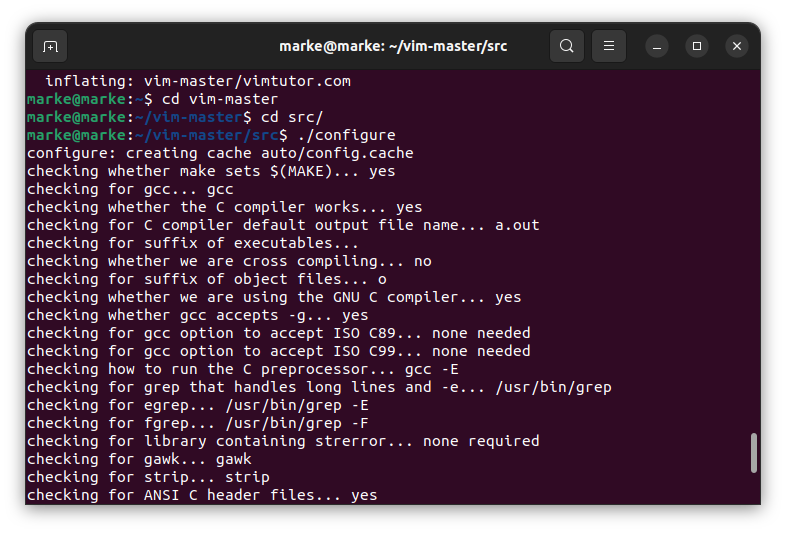


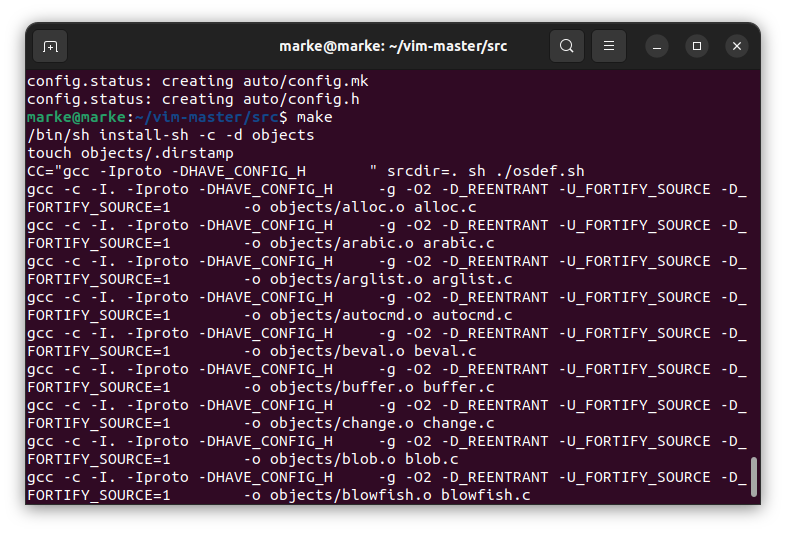




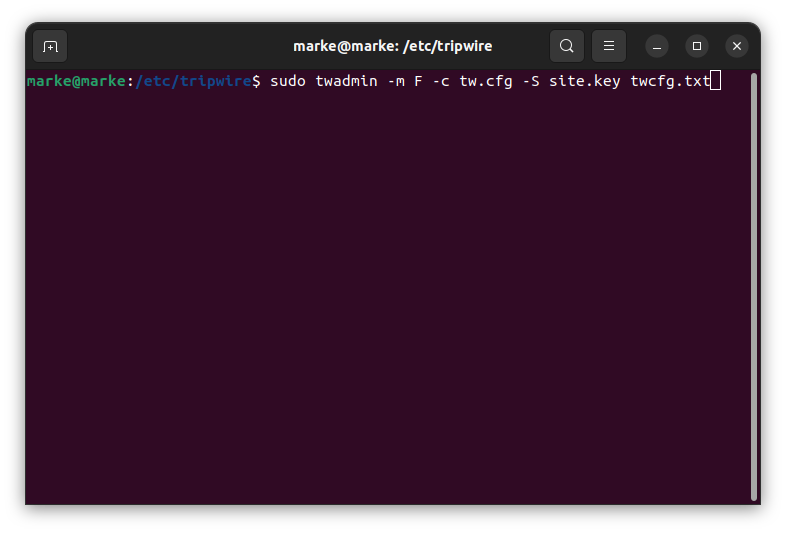


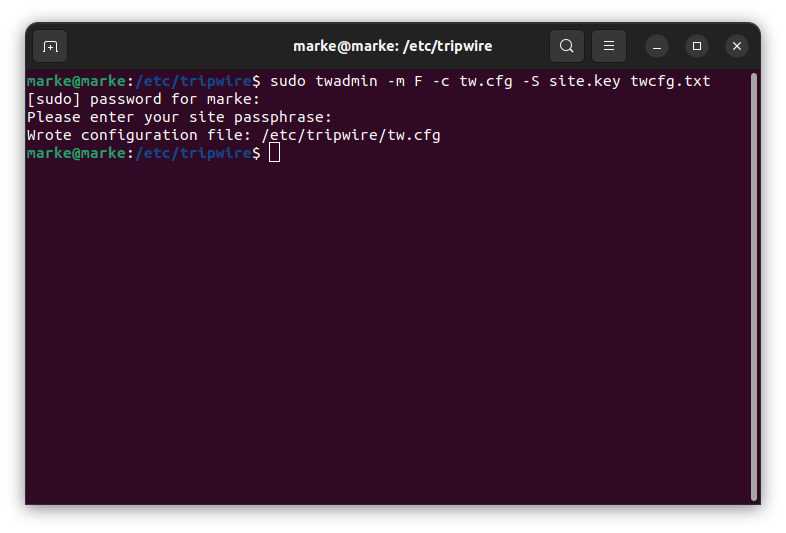














#!/usr/bin/perl

# Tripwire Policy File customize tool

# ----------------------------------------------------------------

# Copyright (C) 2003 Hiroaki Izumi

# This program is free software; you can redistribute it and/or

# modify it under the terms of the GNU General Public License

# as published by the Free Software Foundation; either version 2

# of the License, or (at your option) any later version.

# This program is distributed in the hope that it will be useful,

# but WITHOUT ANY WARRANTY; without even the implied warranty of

# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

# GNU General Public License for more details.

# You should have received a copy of the GNU General Public License

# along with this program; if not, write to the Free Software

# Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

# ----------------------------------------------------------------

# Usage:

# perl twpolmake.pl {Pol file}

# ----------------------------------------------------------------

#

$POLFILE=$ARGV[0];

open(POL,"$POLFILE") or die "open error: $POLFILE" ;

my($myhost,$thost) ;

my($sharp,$tpath,$cond) ;

my($INRULE) = 0 ;

while (<POL>) {

chomp;

if (($thost) = /^HOSTNAME\s\*=\s\*(.\*)\s\*;/) {

$myhost = `hostname` ; chomp($myhost) ;

if ($thost ne $myhost) {

$\_="HOSTNAME=\"$myhost\";" ;

}

}

elsif ( /^{/ ) {

$INRULE=1 ;

}

elsif ( /^}/ ) {

$INRULE=0 ;

}

elsif ($INRULE == 1 and ($sharp,$tpath,$cond) = /^(\s\*\#?\s\*)(\/\S+)\b(\s+->\s+.+)$/) {

$ret = ($sharp =~ s/\#//g) ;

if ($tpath eq '/sbin/e2fsadm' ) {

$cond =~ s/;\s+(tune2fs.\*)$/; \#$1/ ;

}

if (! -s $tpath) {

$\_ = "$sharp#$tpath$cond" if ($ret == 0) ;

}

else {

$\_ = "$sharp$tpath$cond" ;

}

}

print "$\_\n" ;

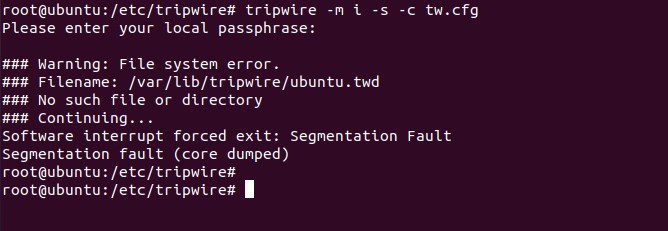
}

close(POL) ;

Create Tripwire database:

tripwire -m i -s -c tw.cfg

as expected false error but just continue

[](https://i0.wp.com/techdirectarchive.com/wp-content/uploads/2022/03/false-error.jpg?ssl=1)You can print database using the command:

# twprint -m d -d /var/lib/tripwire/server-01.twd

## Step 4: Updating the database

# tripwire --update --accept-all

executing checking manually

root@ubuntu:~# tripwire -m c -s -c /etc/tripwire/tw.cfg

Open Source Tripwire(R) 2.4.3.7 Integrity Check Report

Report generated by: root

Report created on: Thu 24 Mar 2022 11:51:38 AM PDT

Database last updated on: Never

===============================================================================

Report Summary:

===============================================================================

Host name: ubuntu

Host IP address: 127.0.1.1

Host ID: None

Policy file used: /etc/tripwire/tw.pol

Configuration file used: /etc/tripwire/tw.cfg

Database file used: /var/lib/tripwire/ubuntu.twd

Command line used: tripwire -m c -s -c /etc/tripwire/tw.cfg

===============================================================================

Rule Summary:

===============================================================================

-------------------------------------------------------------------------------

Section: Unix File System

-------------------------------------------------------------------------------

Rule Name Severity Level Added Removed Modified

--------- -------------- ----- ------- --------

Other binaries 66 0 0 0

Tripwire Binaries 100 0 0 0

Other libraries 66 0 0 0

Root file-system executables 100 0 0 0

Tripwire Data Files 100 0 0 0

System boot changes 100 0 0 0

Root file-system libraries 100 0 0 0

(/lib)

Critical system boot files 100 0 0 0

Other configuration files 66 0 0 0

(/etc)

Boot Scripts 100 0 0 0

Security Control 66 0 0 0

Root config files 100 0 0 0

Devices & Kernel information 100 0 0 0

(/dev)

Invariant Directories 66 0 0 0

Total objects scanned: 54913

Total violations found: 0

===============================================================================

Object Summary:

===============================================================================

-------------------------------------------------------------------------------

# Section: Unix File System

-------------------------------------------------------------------------------

No violations.

===============================================================================

Error Report:

===============================================================================

No Errors

-------------------------------------------------------------------------------

\*\*\* End of report \*\*\*

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc. Tripwire is a registered

trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;

for details use --version. This is free software which may be redistributed

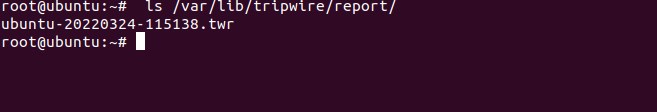
or modified only under certain conditions; see COPYING for details.

All rights reserved.

root@ubuntu:~#

since there are no errors encountered, Tripwire data files are located on  : /var/lib/tripwire/<servername>.twd Scan results are saved under /var/lib/tripwire/report/ directory:

# ls /var/lib/tripwire/report/

[](https://i0.wp.com/techdirectarchive.com/wp-content/uploads/2022/03/pRINT-report.jpg?ssl=1)

To print this report, use the syntax:

twprint -m r -t [0-4] -r /path/to/reportfile.twr

The -t measure indicates the report verbosity, with 0 displaying a single line summary of the contents and 4 displaying all gathered characteristics for all altered objects. If no report level is supplied on the command line or via the REPORTLEVEL config file option, the report level defaults to 3. Example: we used our path from the screenshot above

twprint -m r -t 4 -r /var/lib/tripwire/report/ubuntu-20220324-115138.twr

report is shown below:

oot@ubuntu:~# twprint -m r -t 4 -r /var/lib/tripwire/report/ubuntu-20220324-115138.twr

Note: Report is not encrypted.

Open Source Tripwire(R) 2.4.3.7 Integrity Check Report

Report generated by: root

Report created on: Thu 24 Mar 2022 11:51:38 AM PDT

Database last updated on: Never

===============================================================================

Report Summary:

===============================================================================

Host name: ubuntu

Host IP address: 127.0.1.1

Host ID: None

Policy file used: /etc/tripwire/tw.pol

Configuration file used: /etc/tripwire/tw.cfg

Database file used: /var/lib/tripwire/ubuntu.twd

Command line used: tripwire -m c -s -c /etc/tripwire/tw.cfg

===============================================================================

Rule Summary:

===============================================================================

-------------------------------------------------------------------------------

Section: Unix File System

-------------------------------------------------------------------------------

Rule Name Severity Level Added Removed Modified

--------- -------------- ----- ------- --------

Other binaries 66 0 0 0

Tripwire Binaries 100 0 0 0

Other libraries 66 0 0 0

Root file-system executables 100 0 0 0

Tripwire Data Files 100 0 0 0

System boot changes 100 0 0 0

Root file-system libraries 100 0 0 0

(/lib)

Critical system boot files 100 0 0 0

Other configuration files 66 0 0 0

(/etc)

Boot Scripts 100 0 0 0

Security Control 66 0 0 0

Root config files 100 0 0 0

Devices & Kernel information 100 0 0 0

(/dev)

Invariant Directories 66 0 0 0

Total objects scanned: 54913

Total violations found: 0

===============================================================================

Object Summary:

===============================================================================

-------------------------------------------------------------------------------

# Section: Unix File System

-------------------------------------------------------------------------------

No violations.

===============================================================================

Object Detail:

===============================================================================

-------------------------------------------------------------------------------

Section: Unix File System

-------------------------------------------------------------------------------

No violations.

===============================================================================

Error Report:

===============================================================================

No Errors

-------------------------------------------------------------------------------

\*\*\* End of report \*\*\*

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc. Tripwire is a registered

trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;

for details use --version. This is free software which may be redistributed

or modified only under certain conditions; see COPYING for details.

All rights reserved.

root@ubuntu:~#

Also, note that you can update this report manually:

tripwire -m u -a -s -c /etc/tripwire/tw.cfg -r /var/lib/tripwire/report/ubuntu-20220324-115138.twr

## Step 5: Updating a policy

Policy update mode allows you to make changes to your current Tripwire policy without sacrificing your previous baselines.

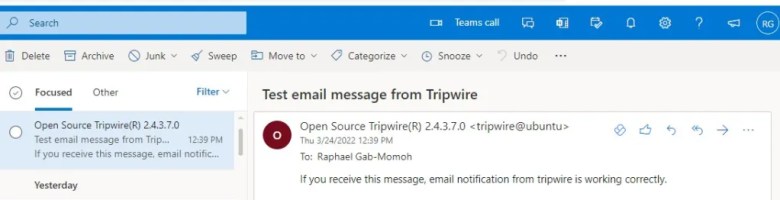
tripwire --update-policy updated-policy.txt

As part of the update process, this will do a check against the new policy. If this check finds changes, the default approach is to show the changes and then quit without altering the policy or database.

## Step 6: Testing email configuration

To test email configuration: tripwire --test --email user@domain.tld

This sends a test email to the supplied address, using the config file’s email settings.

[](https://i0.wp.com/techdirectarchive.com/wp-content/uploads/2022/03/tripwire-email.jpg?ssl=1)

## Summary

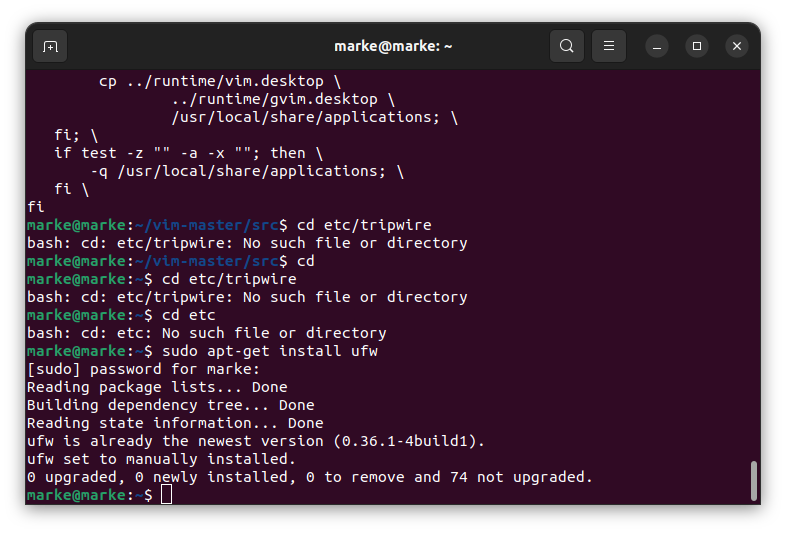
We went through the steps to install Tripwire, which is an open-source intrusion detection system as it monitors your vital system files and reports in real time to see if they’ve been tampered with or destroyed by a hacker or by accident.

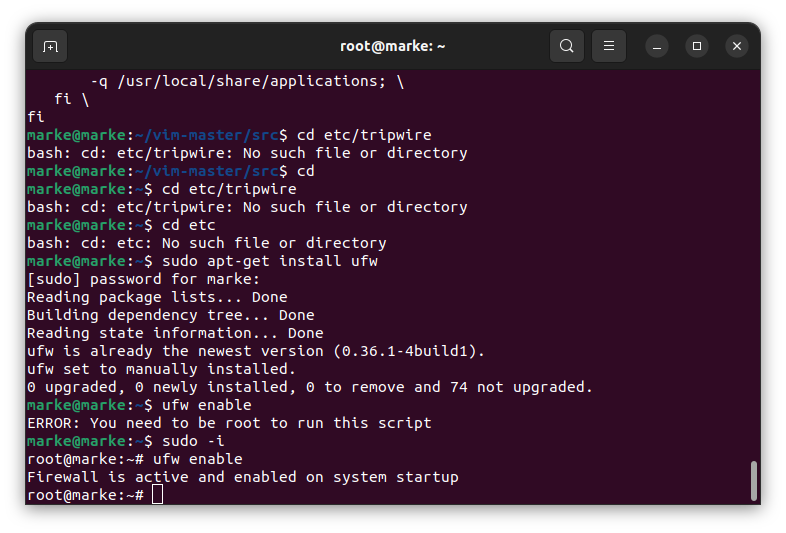
**WEEK 3-2:**

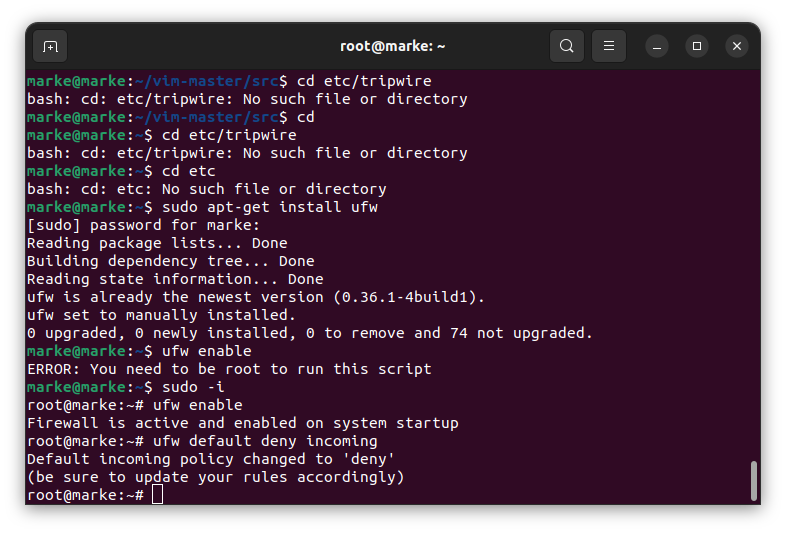
MANUALLY CONFIGURING A FIREWALL IN UBUNTU:

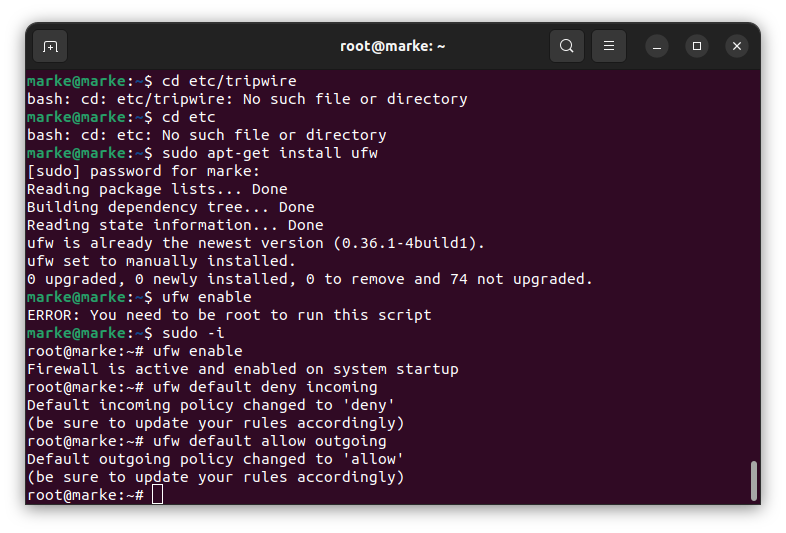
HERE WE ARE INSTALLING UFW WHICH IS AN UNCOMPLICATED FIREWALL.

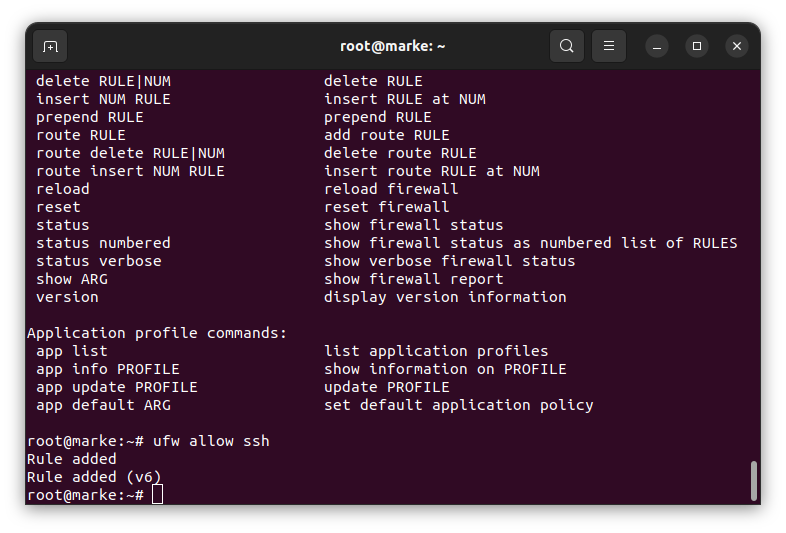
Firewall









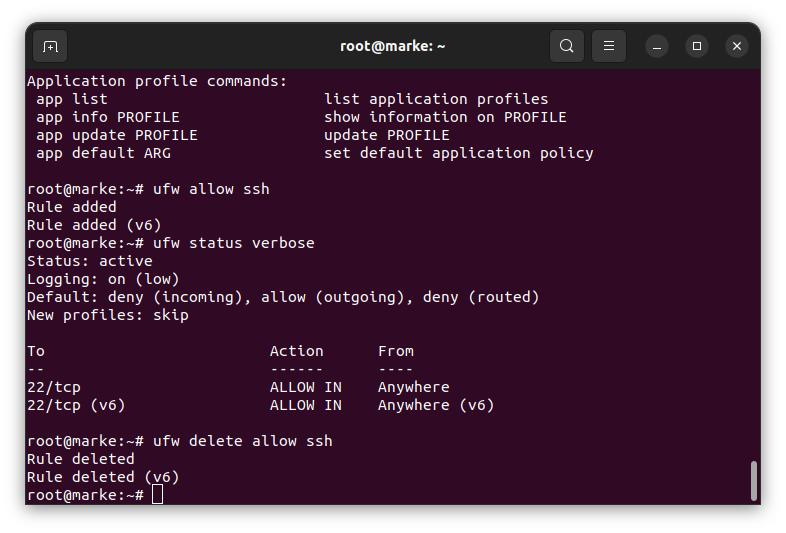


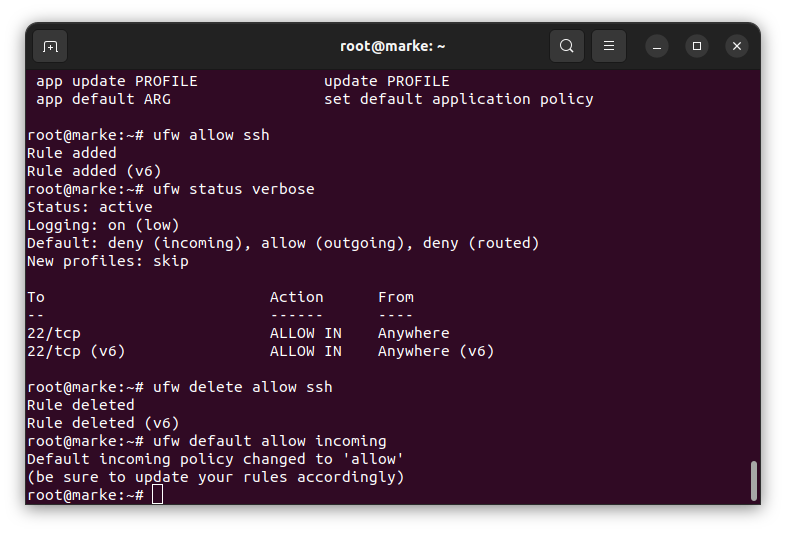
 #ufw status verbose

Is used to ensure that the firewall is saved.

#ufw delete allow ssh

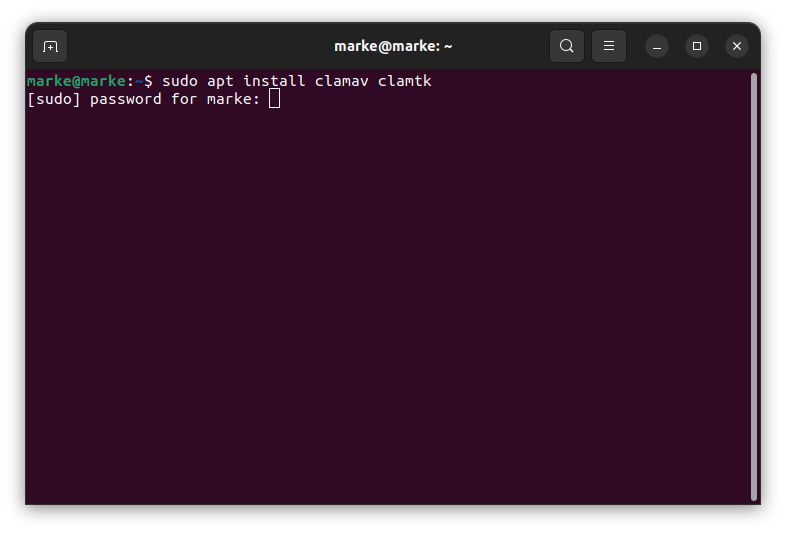
Is used to delete the rules.

 Above we have deleted the rules and then enabled back the incoming.

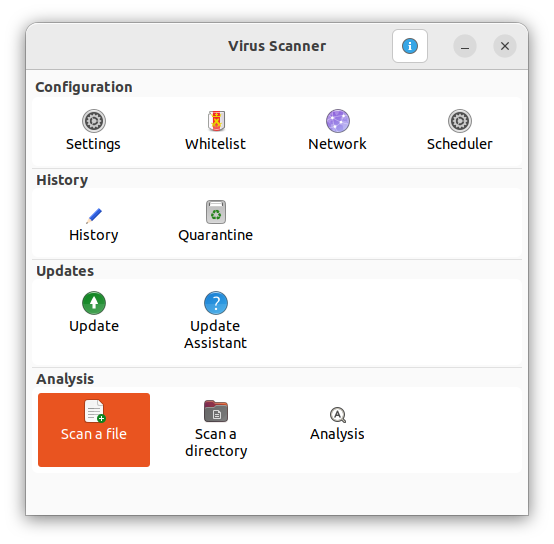


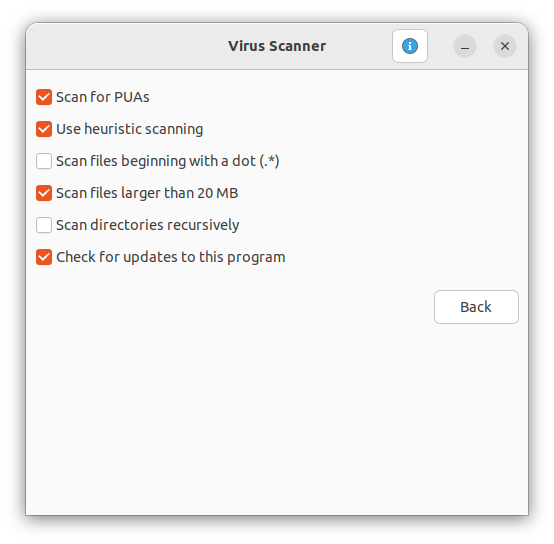
**WEEK 3-3:**

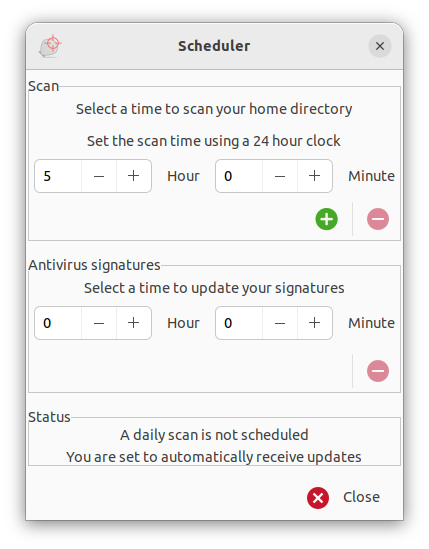
Install an Antivirus and show advanced configuration

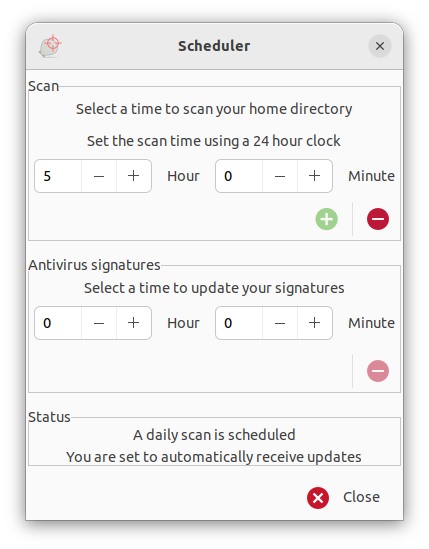


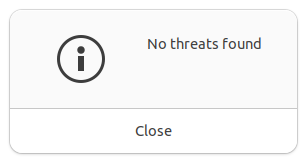
After installing the clamtk we launch the clamtk to configure the anti-virus:

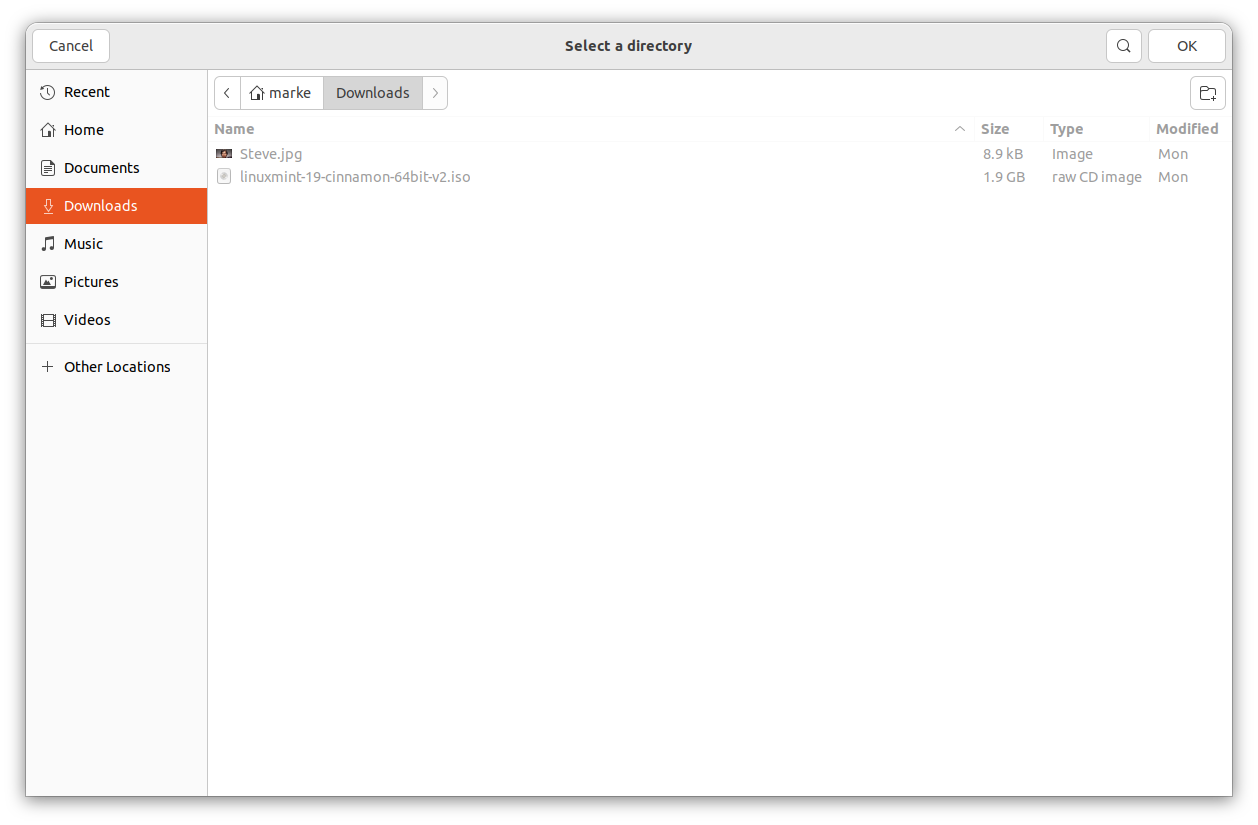








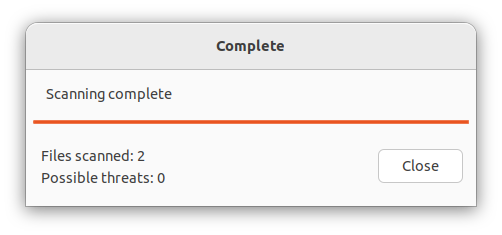


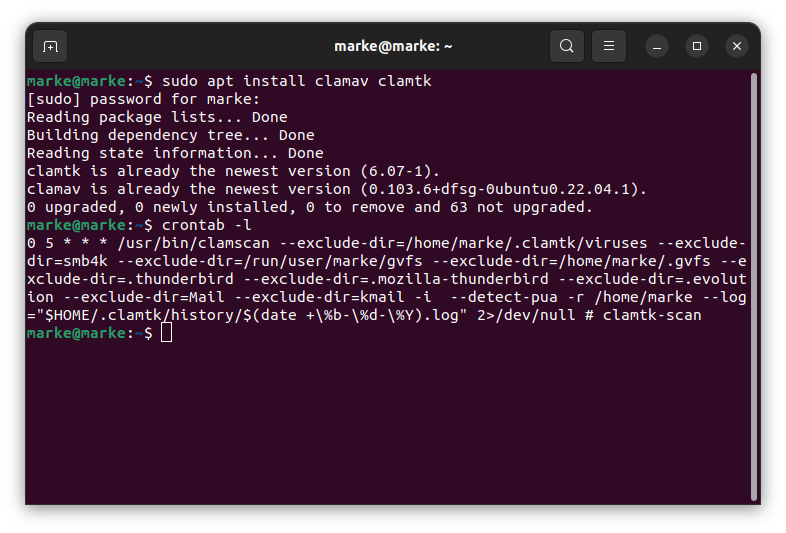


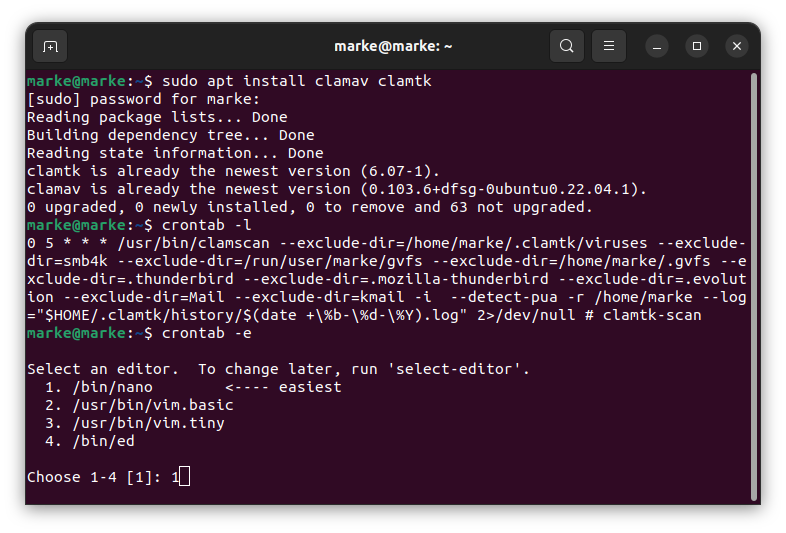
To check for the listed scheduled time for scan in terminal type in “crontab -l”:

here we can see that the scheduled scan is at 9 in the morning everyday.

If the GUI interface doesnt work for us we can do this with the command prompt with the below command:



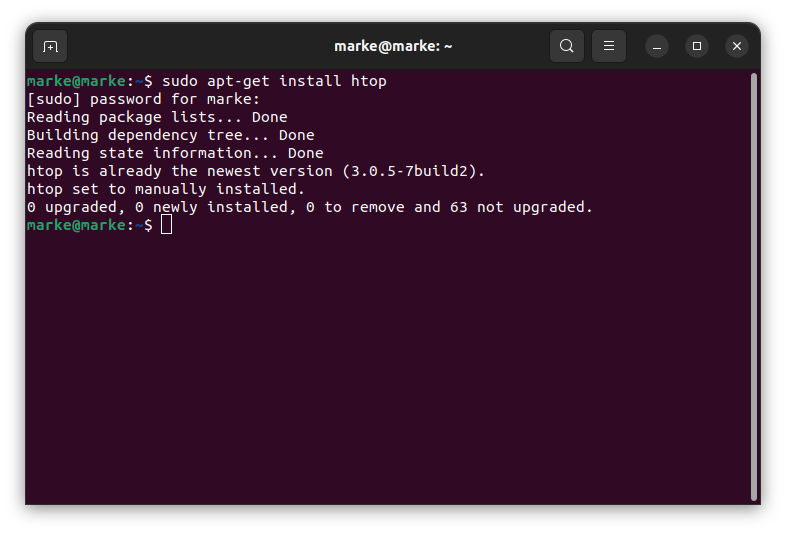


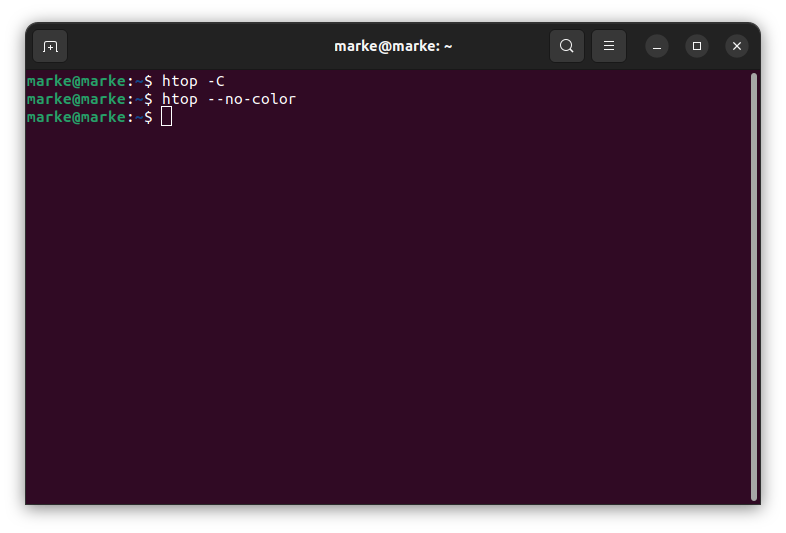
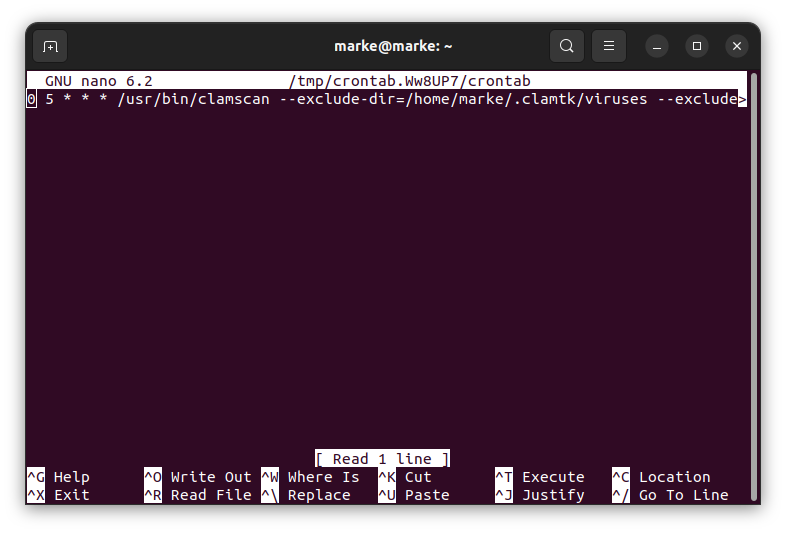


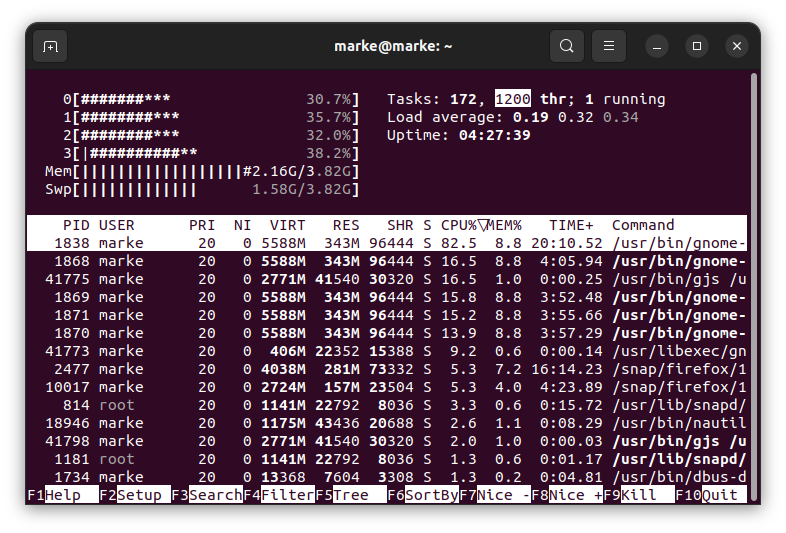
**WEEK 3-4:**

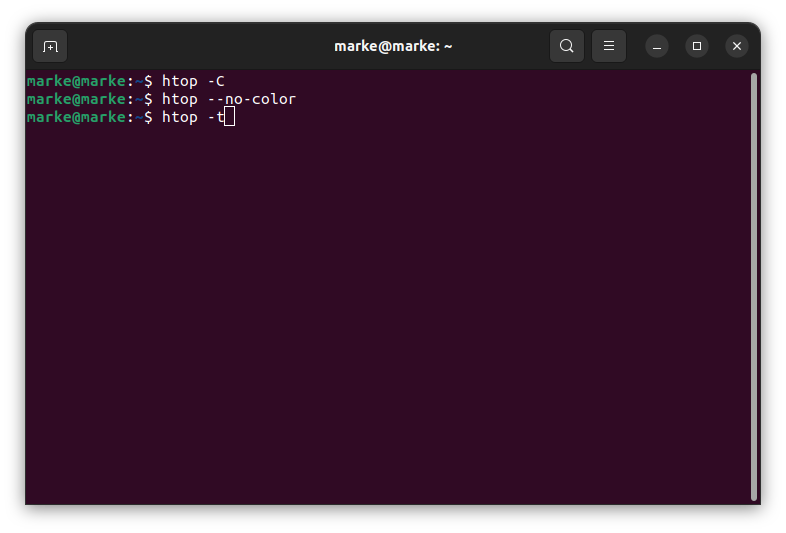
Install htop and demonstrate use.

One can use a monochrome color scheme, run:  
htop -C  
htop --no-color



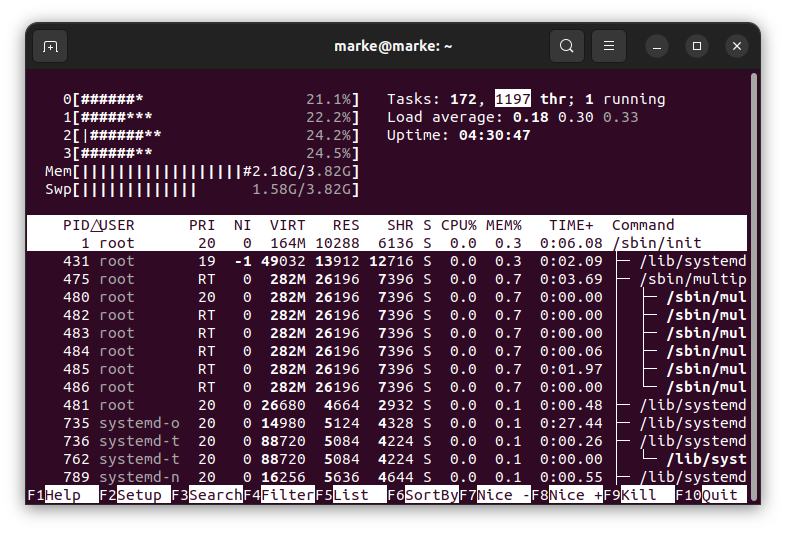






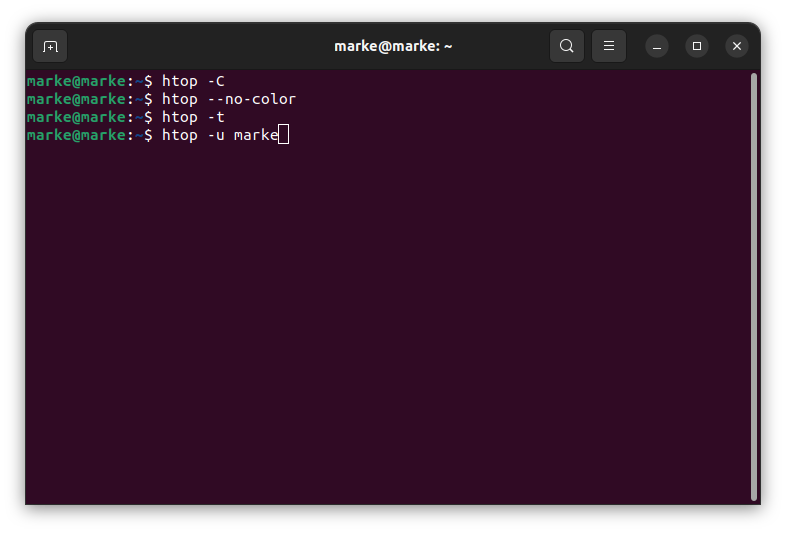
Want to see the tree view by default when running htop? Try:

$htop -t



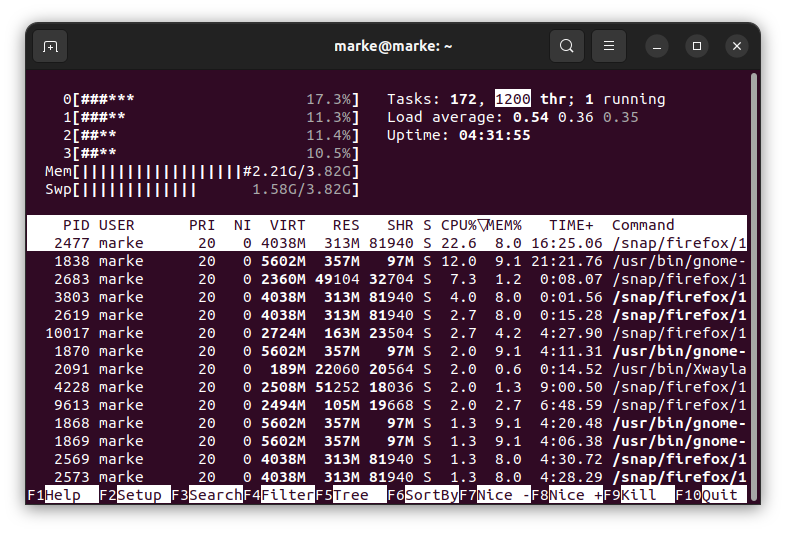
Let us see only processes of a given user named neeraja:

$htop -u neeraja

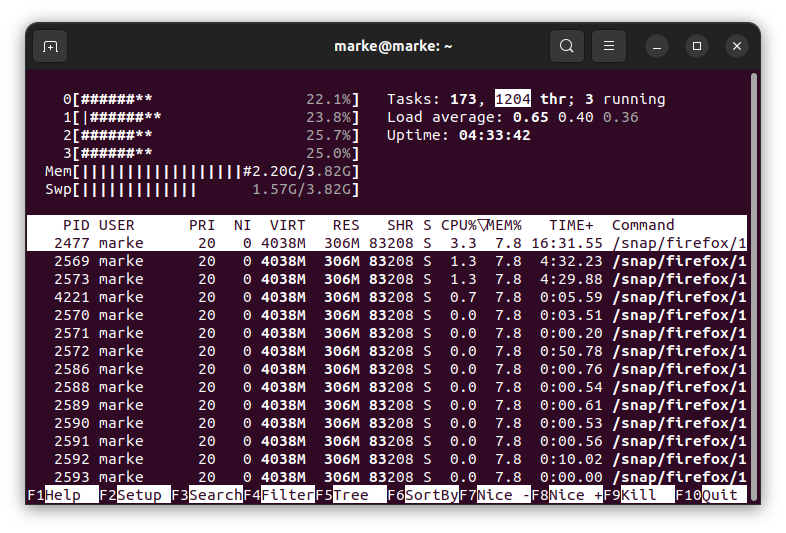


Limit and show process for only the given PIDs:

$htop -p PID



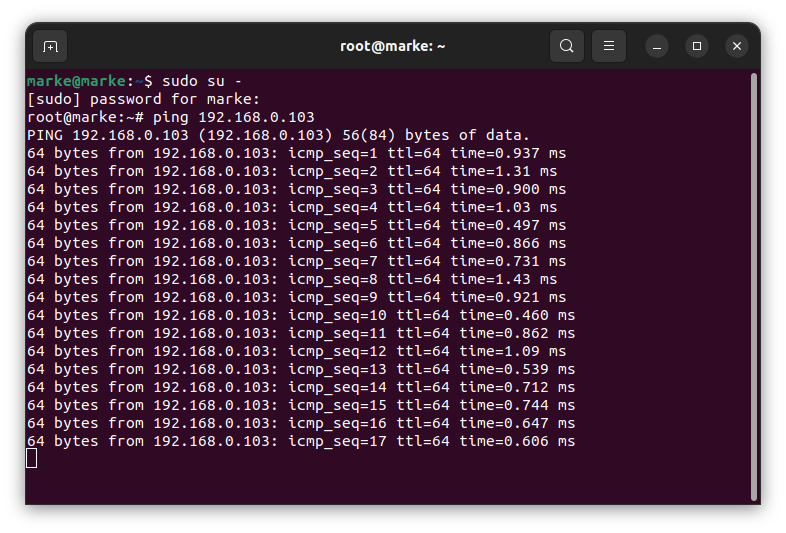




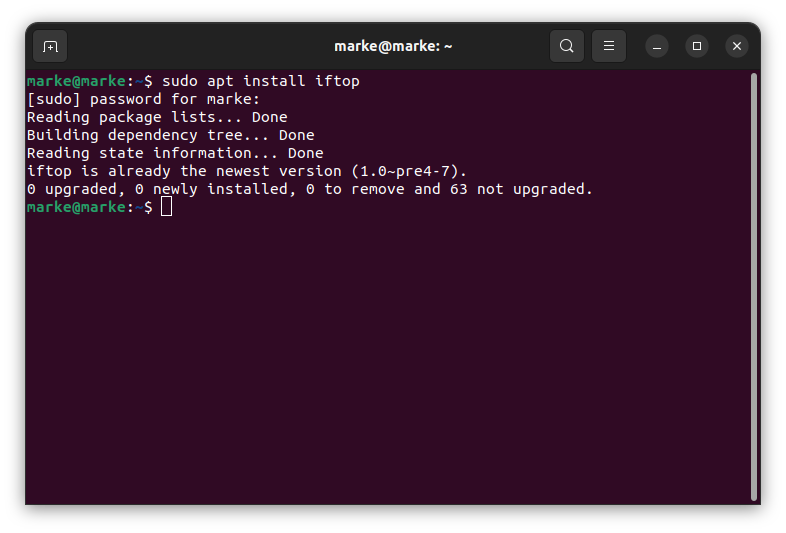
**WEEK 3-5:**

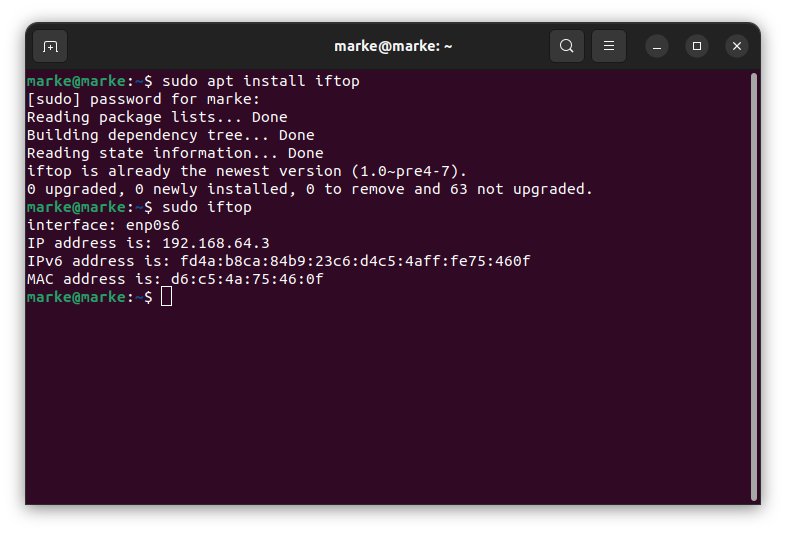
Install top and demonstrate use.

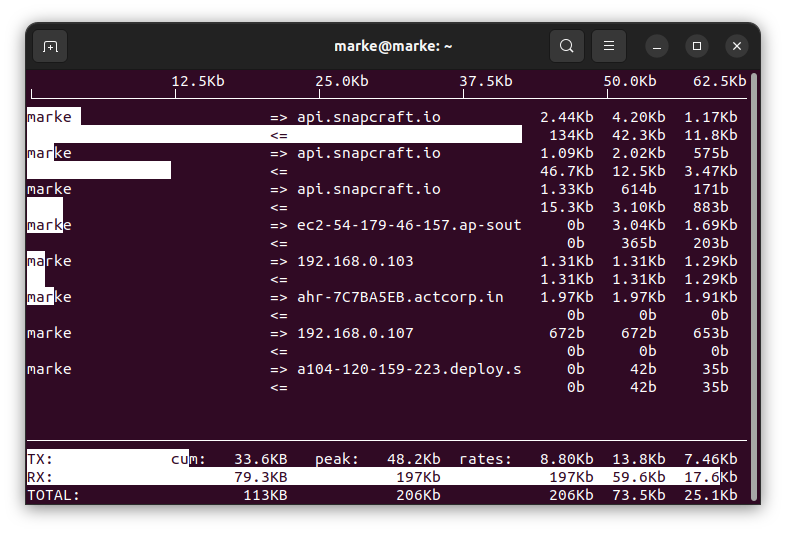
Since top is available from htop we can directly use it to ping the other machine by using the ip address



**WEEK 3-6:** Install iftop and demonstrate use.

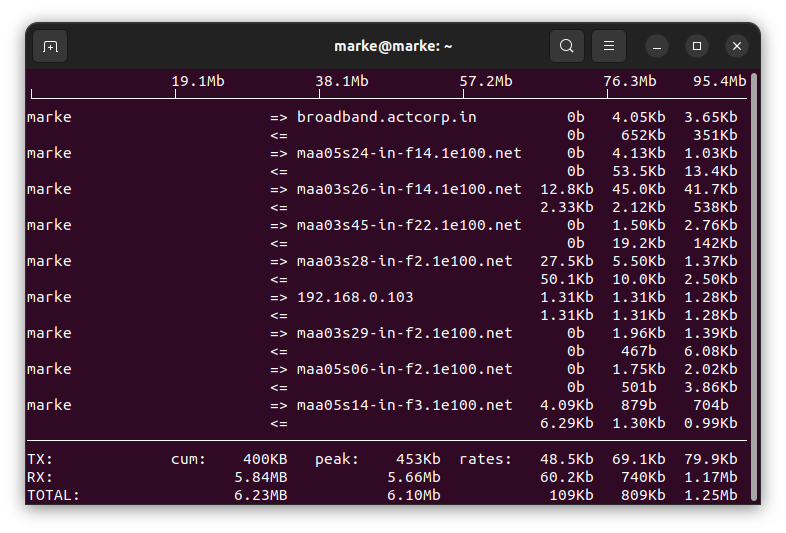
 Sample output of iftop command which shows bandwidth of default interface as shown below.



 run the following [ifconfig command](https://www.tecmint.com/ifconfig-command-examples/" \t "_blank) or [ip command](https://www.tecmint.com/ip-command-examples/" \t "_blank) to find all attached network interfaces on your Linux system.

Then use the -i flag to specify the interface you want to monitor. For example the command below used to monitor bandwidth on the wireless interface on the test computer.

$ sudo iftop -i enp0s3



While running iftop you can use the keys like S, D to see more information like source, destination etc. Please do run man iftop if you want to explore more options and tricks. Press ‘q‘ to quit from running windows.

**WEEK 3-7:**

SLURM ASSESSMENT:

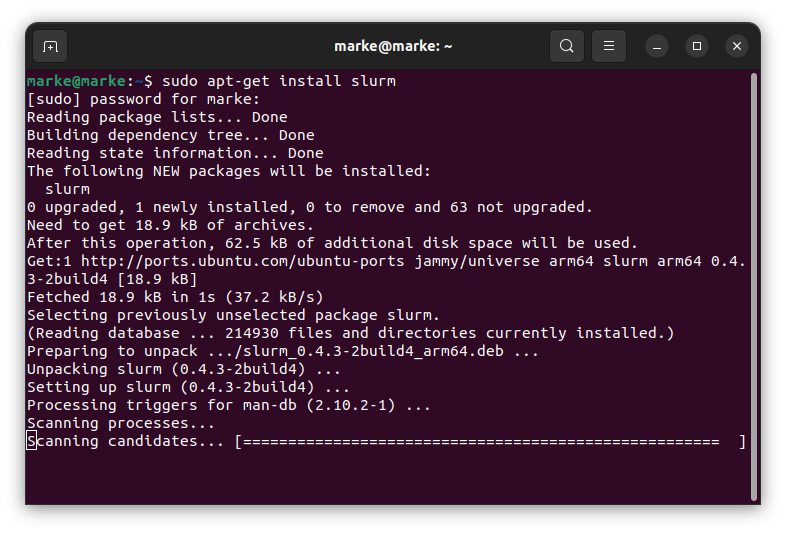
## To Monitor Network Load in Ubuntu With slurm Tool

The slurm tool displays device statistics together with an ascii graph. Installation of slurm to Monitor Network Load in Ubuntu is explained in this manual.

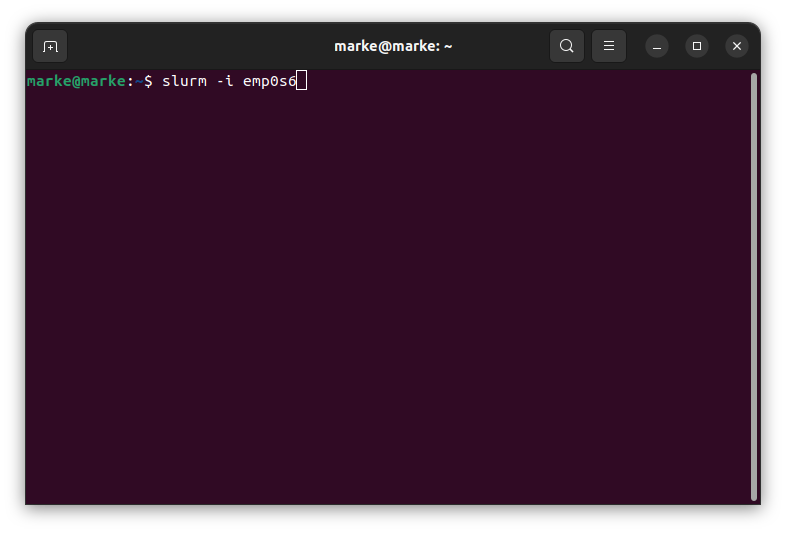
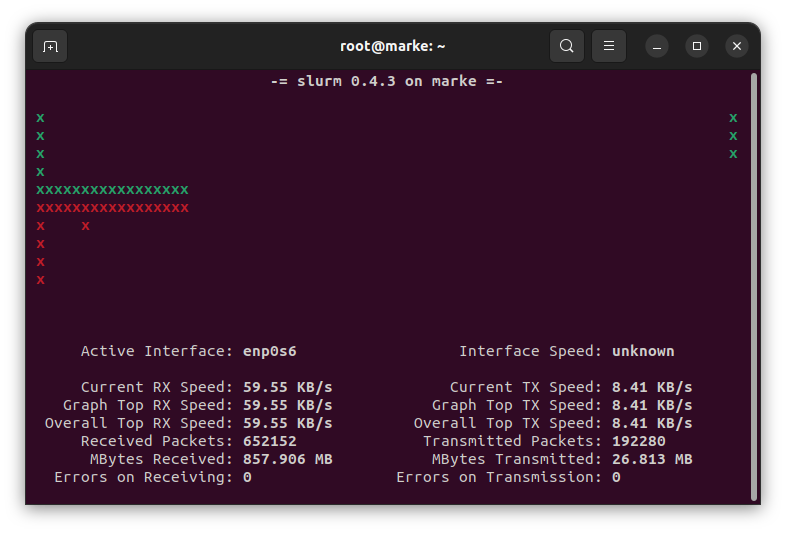
**It provides three key functions**  
1.Allocates the resources.  
2. Provides a framework for starting, executing, and monitoring work.  
3. Manages the queue of pending jobs.

### To install slurm

Run the following command to install slurm.

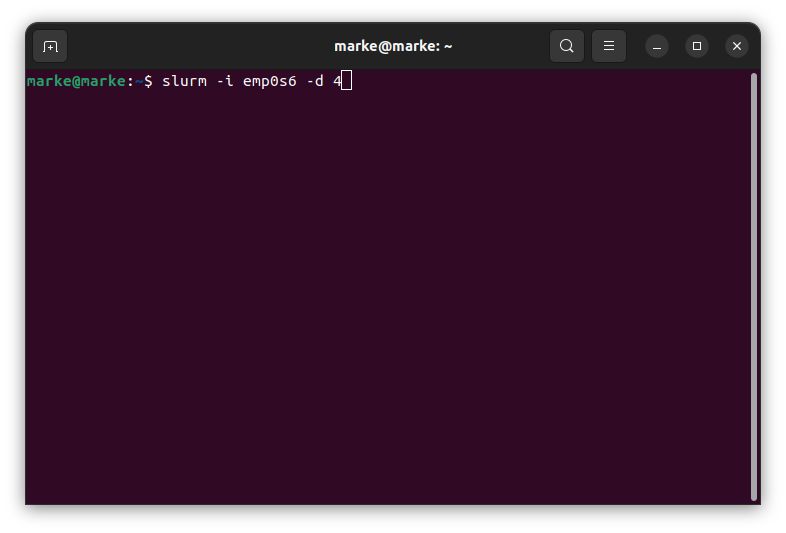


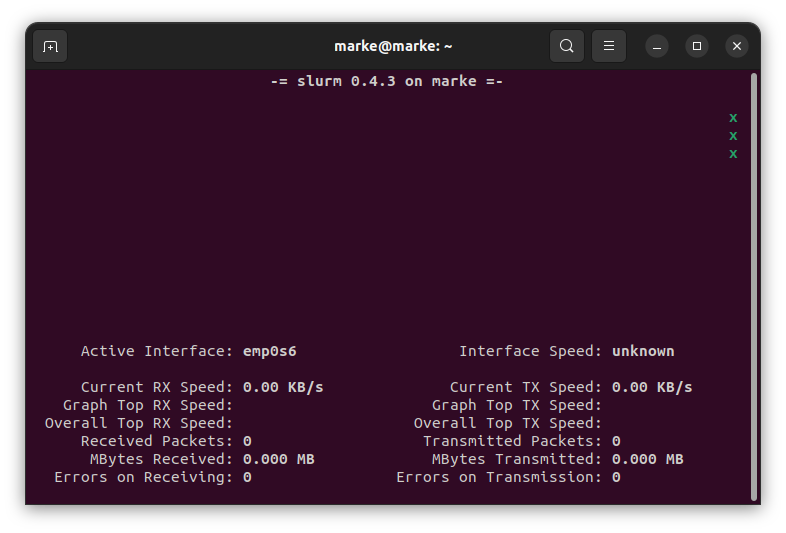
Run the following command to select the interface that is to be monitor. The -i option is used to select the interface



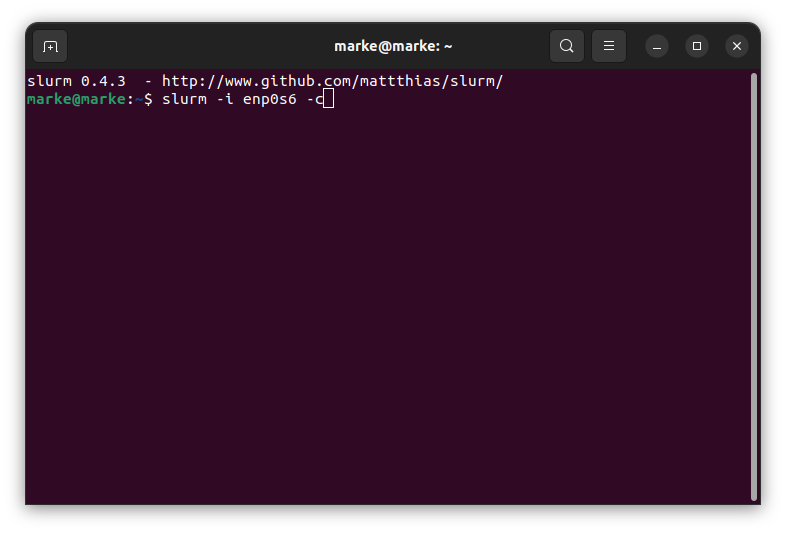


To Set delay between screen updates, use the following command.



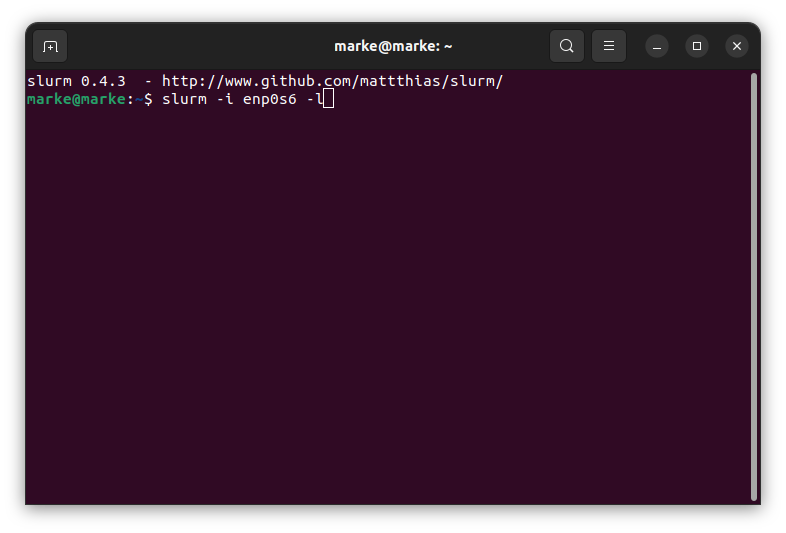


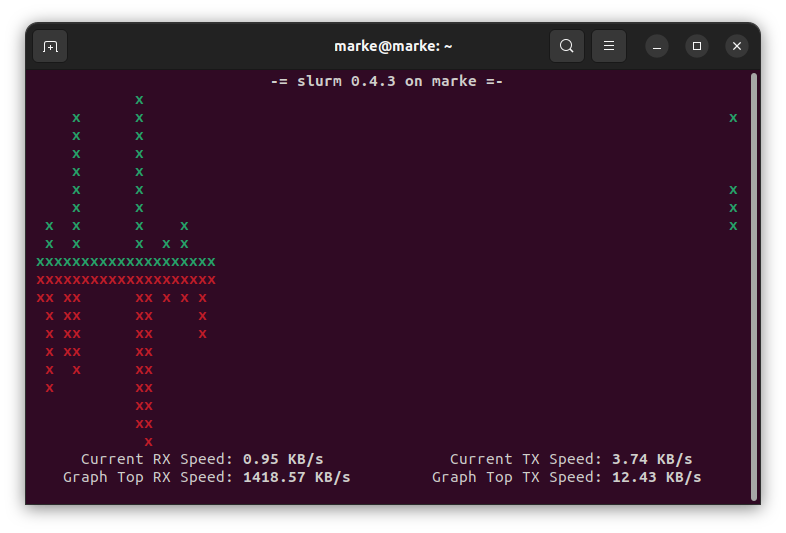
To start slurm in classic graph, execute the following command.





Utilise the following command to start slurm in a large split graph mode:



 Various option available in slurm are

c - Classic mode showing one graph  
s - Split graph mode showing uploads and downloads (default)  
l - Same as split graph, but larger. Some text omitted.  
L - TX/RX LED mode  
m - Cycle among classic (c), split (s), and large split (l)  
q - Quit

**WEEK 3-8:**

TCPTRACK:



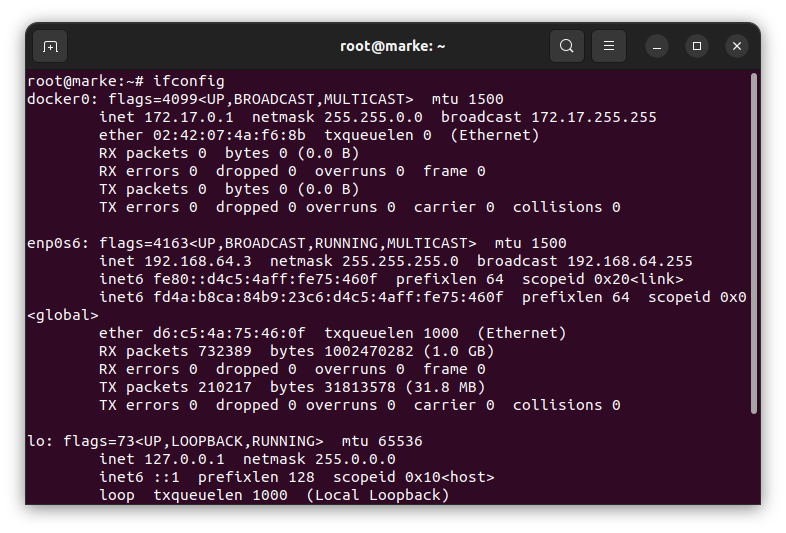
 In my VM there was no ifconfig so I had to download it as follows:

Command 'ifconfig' not found, but can be installed with:

apt install net-tools:

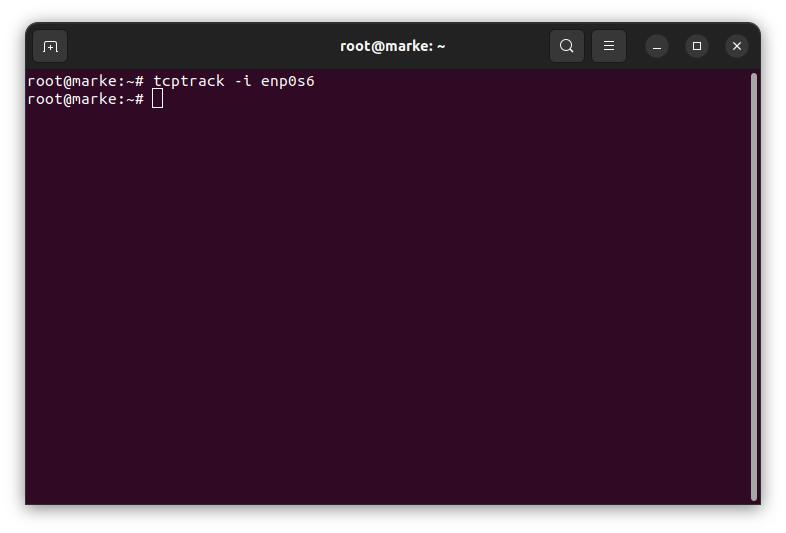


ifconfig is used here to know the name of our interface:

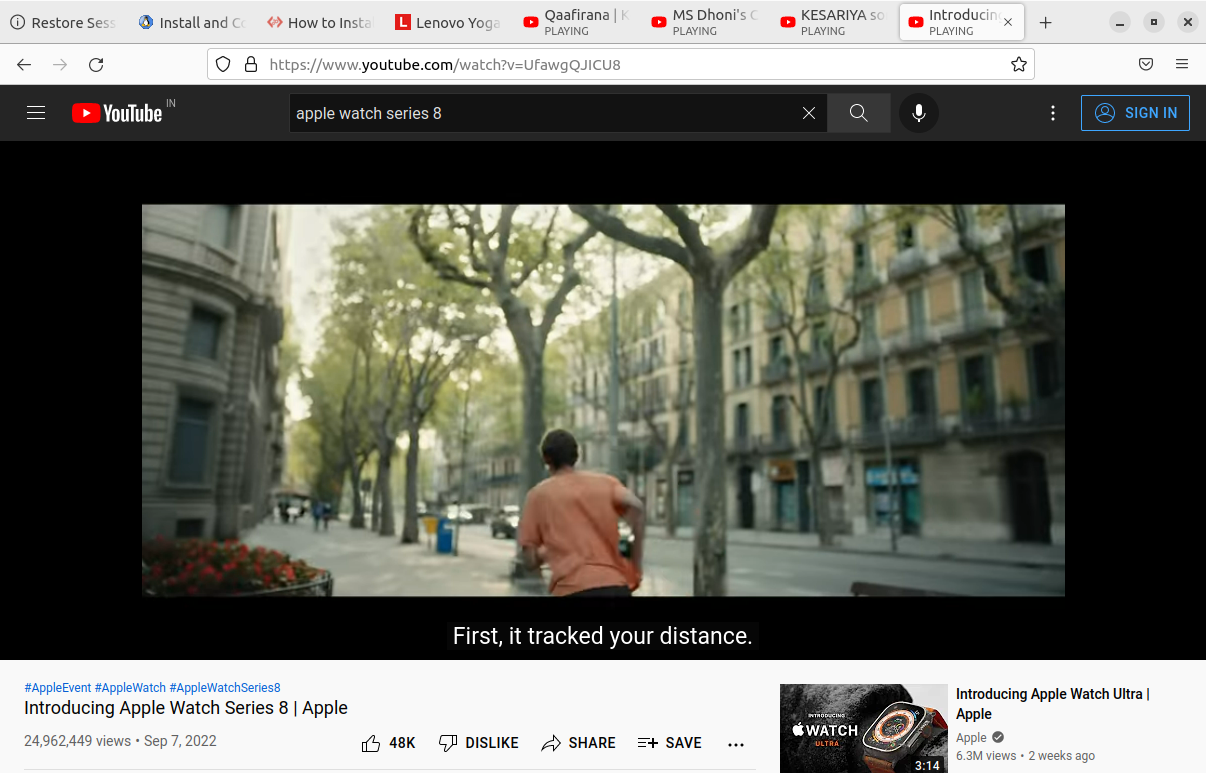


The interface name of my VM is enp0s6.

Here we track the tcp packets for our interface by using the following statement:



’ve opened a youtube video to track the tcp packets



The below is the tracked tcp connnection using tcptrack:

