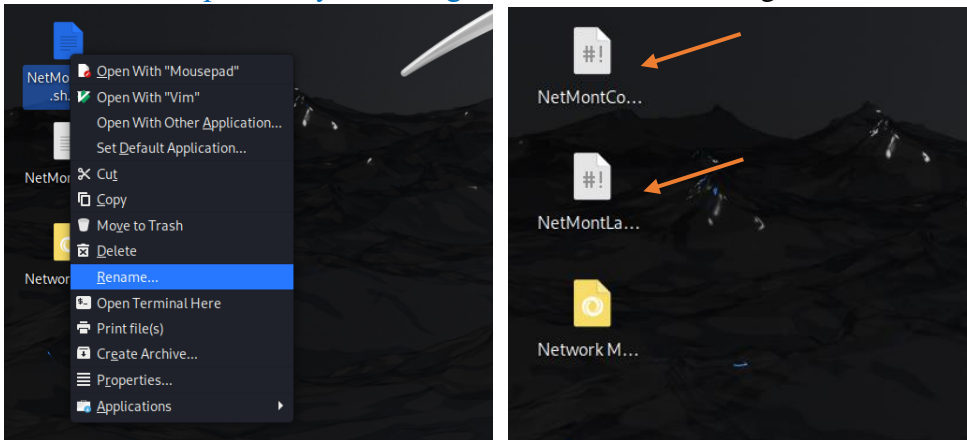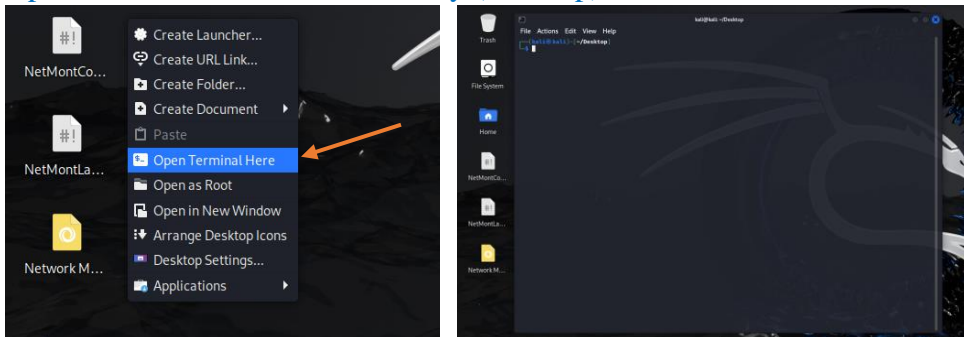- # Setting up the Network Monitoring Device.
1. Obtain a Raspberry PI (model B) with a Kali linux OS installed on it.
2. Copy the files "NetMontConfig.sh.txt", "NetMontLaunch.sh.txt", and "NetworkMonitoringDashboard.json" into the Desktop directory.

3. Rename the script files by removing ".txt": "NetMontConfig.sh", "NetMontLaunch.sh"

4. Open terminal in the same directory (Desktop).

5. Enter the following commands (one after the other) to turn the files into bash scripts:
   chmod +x NetMontConfig.sh NetMontLaunch.sh

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod +x NetMontConf.sh NetMontLaunch.sh
```

6. Now, To execute the Configuration file:
   bash NetMontConfig.sh

```
┌──(kali㉿kali)-[~/Desktop]
└─$ bash NetMontConf.sh
                              ─────Network Monitor Configuration─────────────────────────
─────────────────Installing Apache2 Server─────────────────
[sudo] password for kali: █
```

You may be asked to enter the password of the machine (default: kali).
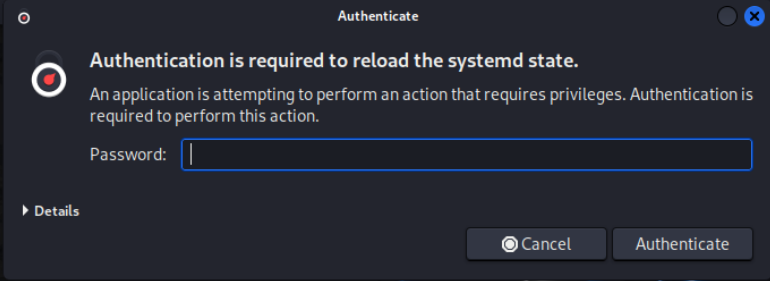You may be prompted with a question, respond with "Y".

7. Be patient:

```
Setting up Grafana ...
(Reading database ... 416698 files and directories currently installed.)
Preparing to unpack grafana_10.4.2_amd64.deb ...
Unpacking grafana (10.4.2) over (10.4.2) ...
Setting up grafana (10.4.2) ...
Restarting grafana-server service ... OK
Processing triggers for kali-menu (2023.4.7) ...
─────────────────Network Monitor Configuration Completed!─────────────

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

8. To Launch the System (Prometheus, Grafana, Exporters) enter the comand:
   bash NetMontLaunch.sh

Enter Password when needed.
And keep the terminal Open (Ctrl+c to close the monitoring system)

9. Keep the terminal open (Prometheus running):

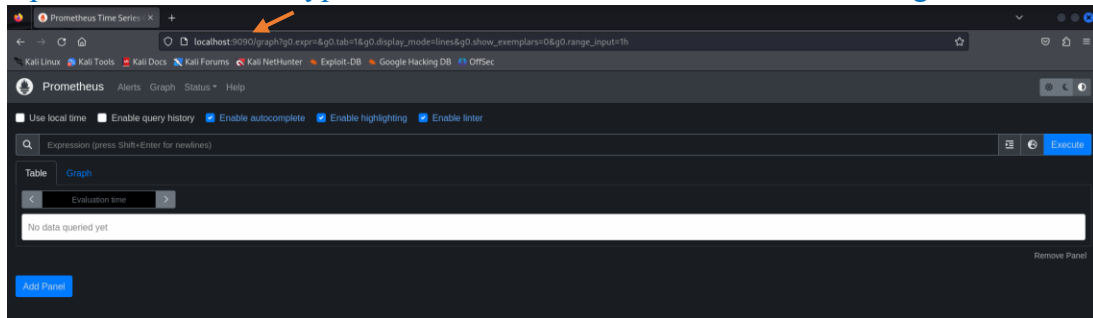
10. Open the browser and type "127.0.0.1:9090" to see Prometheus running.

11. Open the browser and type "127.0.0.1:3000" to open Grafana.
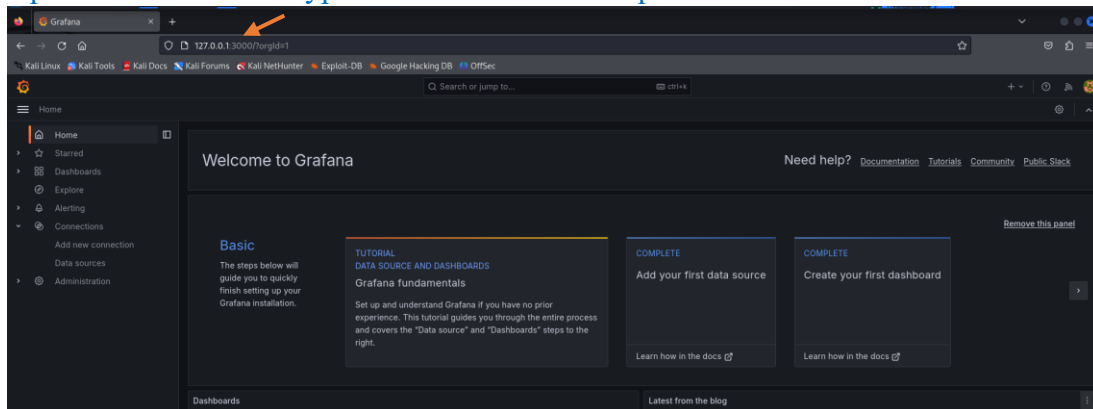
Now to setup the Dashboard:

12. To link Prometheus with Grafana: Press on connections then Data sources and select Prometheus
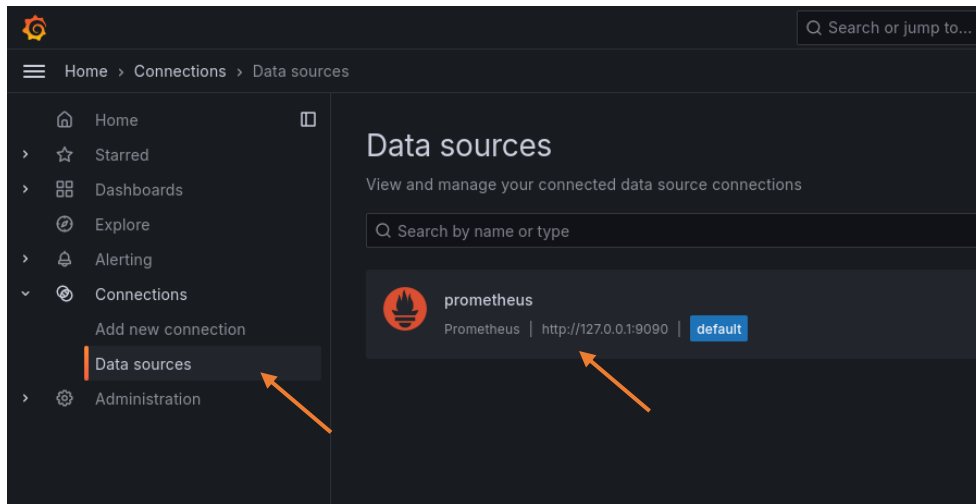
13. Add the connection "http://127.0.0.1:9090" and the scrape inetrvals "15s" "60s"
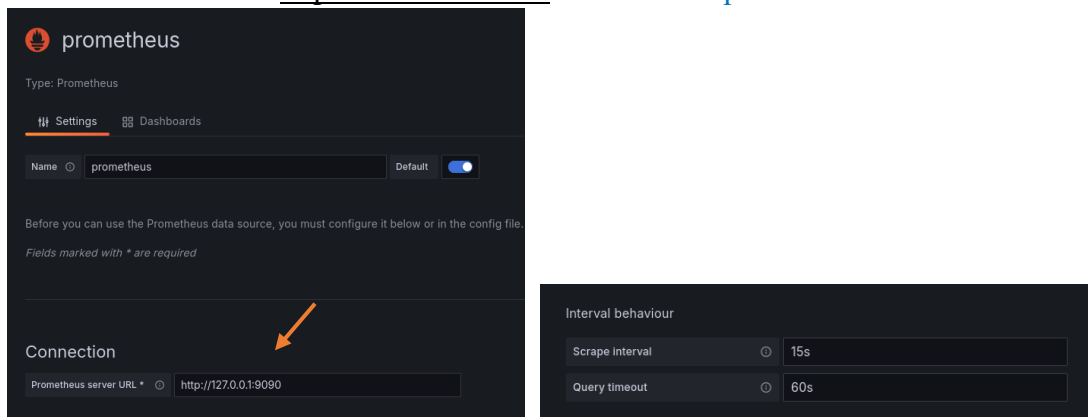
Then save&test
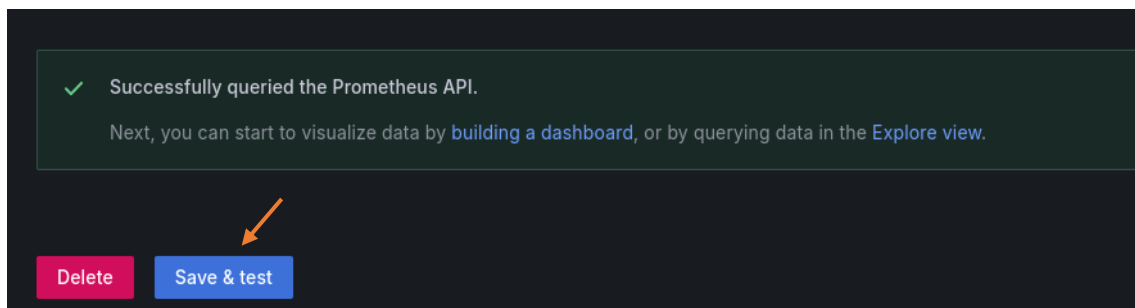
14. Under Dashboards, Press New then Import. And Upload Dashboard JSON file
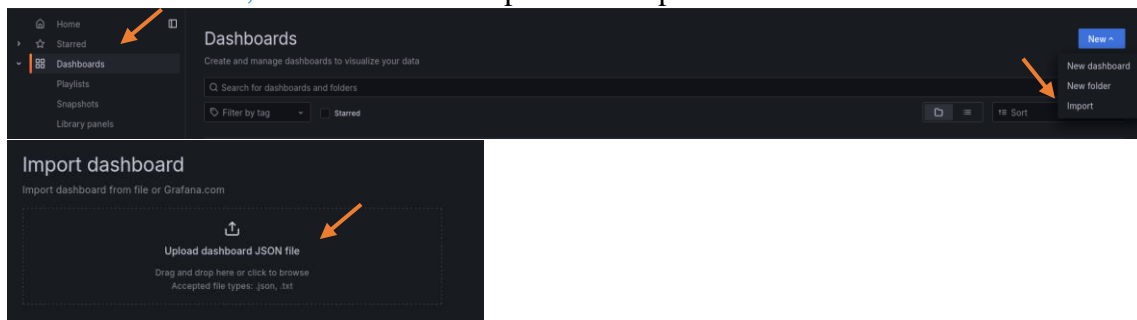
Select the "NetworkMonitoringDashboard.json" file.

15. Select Prometheus as Data source and Import:
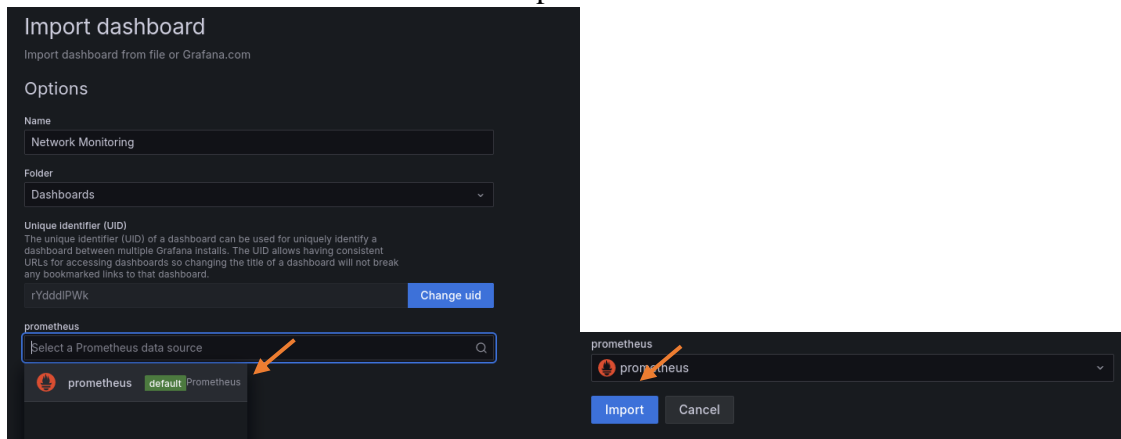
16. Now you can See the Dashboard "Network Monitoring" Under Dashboards:
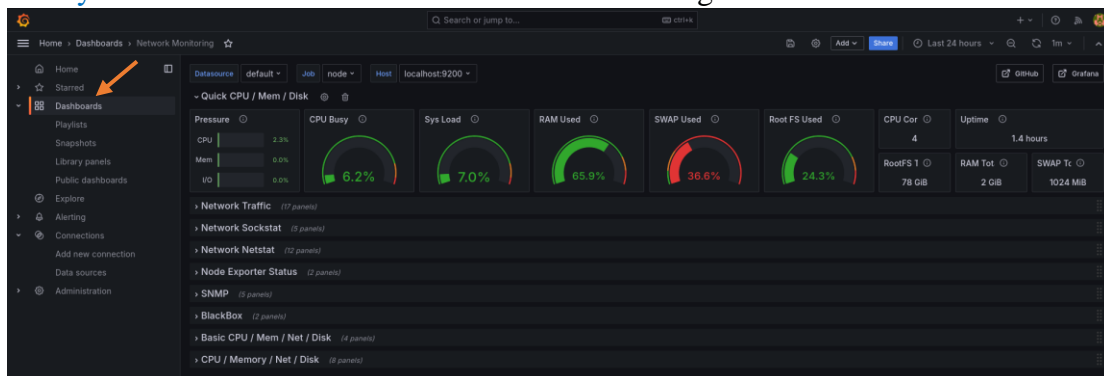
17. You may change the time range:
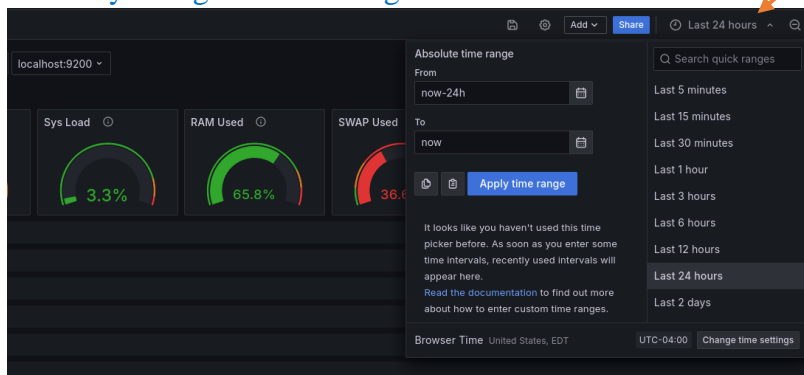
18. Explore all the metrics available:
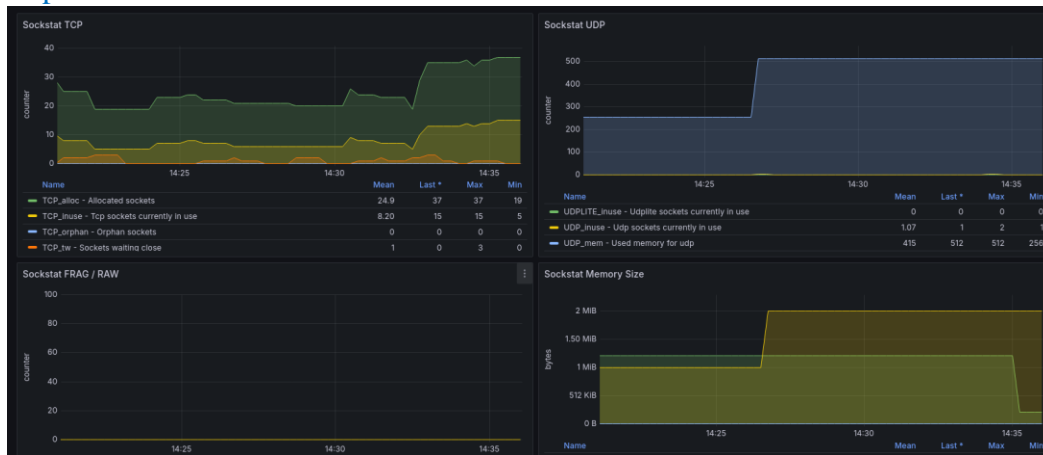
19. To stop the monitoring system: enter "Ctrl + c" in the terminal that's running Prometheus.

- Accessing the Network Monitoring System:
  System Configuration:
  1. ZeroTier:
     (RaspberryPi: 10.147.19.95):
     To create a virtual LAN:

     After accessing the official website on https://my.zerotier.com/ , sign up and create the virtual network.
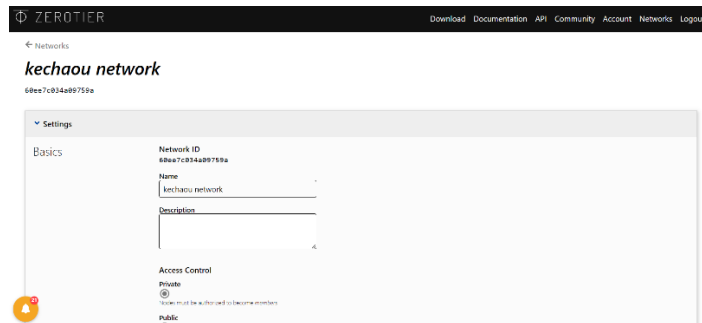
     A unique network ID is created and will be used to make other devices join the network.

     Here you can choose the Private ip to assign to the devices.

     Here are the devices connected to our network, including the raspberry pi.

Mentioning that zerotier is supported on linux and windows.

On the Monitoring Device run:

wget https://download.zerotier.com/debian/buster/pool/main/z/zerotier-one/zerotier-one_1.4.6_amd64.deb

sudo dpkg -i zerotier-one_1.4.6_amd64.deb

sudo update-rc.d zerotier-one enable

sudo zerotier-cli join 60ee7c034a09759a

2. to allow SSH on the Network Monitoring Device, run the commands:
sudo rm /etc/ssh/ssh_host_*
sudo dpkg-reconfigure openssh-server
sudo service ssh restart
for Remote desktop access:
sudo apt install xrdp -y
sudo adduser xrdp ssl-cert
sudo systemctl enable xrdp
sudo systemctl start xrdp
sudo systemctl start xrdp-sesman
sudo systemctl enable xrdp
sudo systemctl enable xrdp-sesman

That will allow access from your host device using:
ssh kali@10.147.19.95

```
C:\Users\DELL>ssh kali@10.147.19.95
kali@10.147.19.95's password:
Linux kali-raspberry-pi 5.15.44-Re4son-v7l+ #1 SMP Debian kali-pi (2022-07-03) armv7l

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Apr 27 13:12:32 2024 from 10.147.19.86
┌──(kali㉿kali-raspberry-pi)-[~]
└─$
```

User Configuration:

On a host device:

Install zerotier from: https://www.zerotier.com/download/

Then join the network:
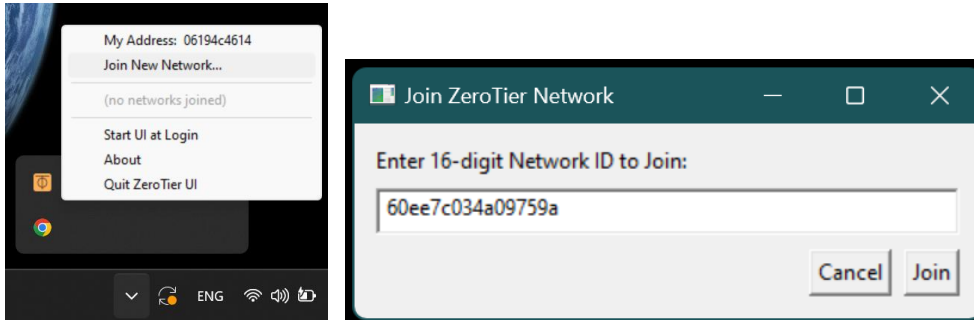
And wait for approval:
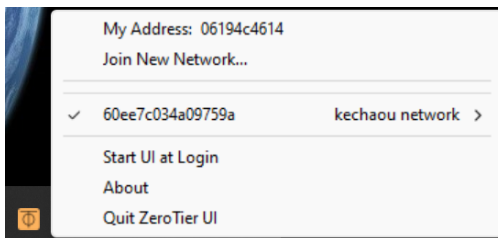
1. to test the connection from client device, use the ping command with the zerotier IP address:
   ping 10.147.19.95


```
C:\Users\DELL>ping 10.147.19.95

Pinging 10.147.19.95 with 32 bytes of data:
Reply from 10.147.19.95: bytes=32 time=232ms TTL=64
Reply from 10.147.19.95: bytes=32 time=55ms TTL=64
Reply from 10.147.19.95: bytes=32 time=67ms TTL=64
Reply from 10.147.19.95: bytes=32 time=73ms TTL=64

Ping statistics for 10.147.19.95:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 232ms, Average = 106ms
```

2. Now with access to the RaspberryPi Network, check the configuration set on the Monitoring system, type in the browser:
   http://10.147.19.95

Project Website:

1. The Home page:

    This page includes a Welcoming message and an Introduction to the project.
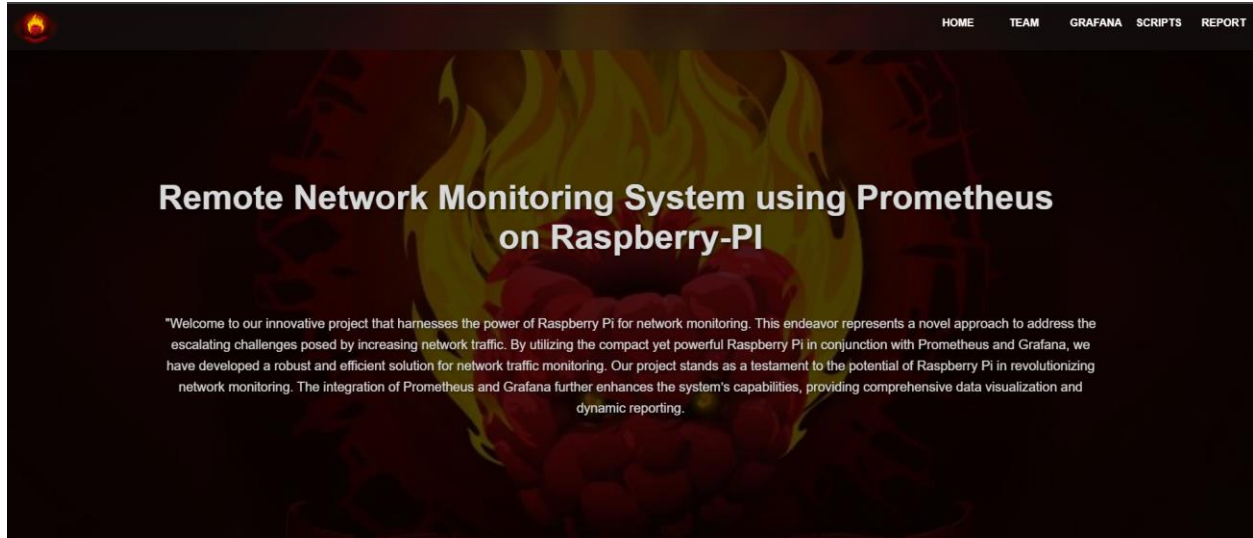
2. The Team page:

    This page includes the team members' names and links to their GitHub profiles.
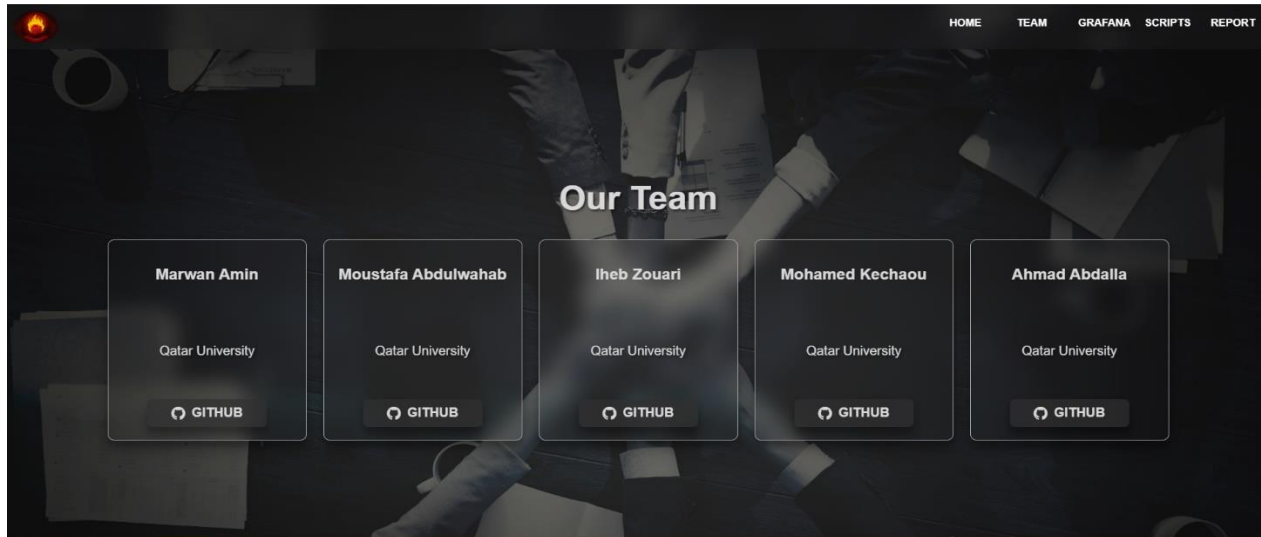
3. The Grafana page:

    This page includes a description about Grafana and a link to the Grafana page of the monitoring system.
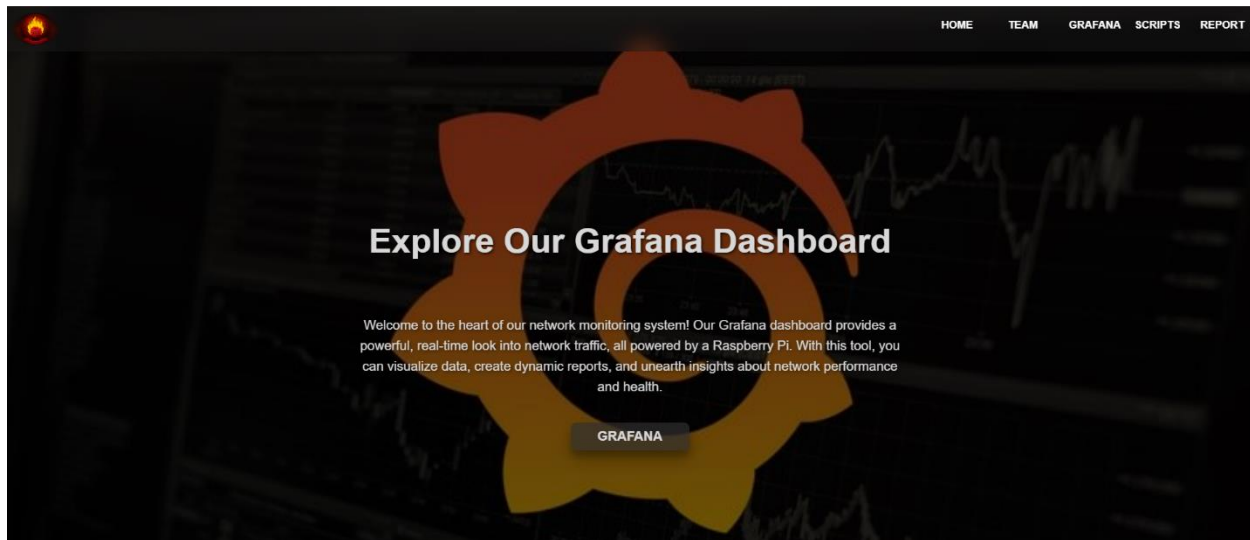
4. The Scripts page:

   This page includes the link to download a .zip file that has all the Scripts and Configuration files used for this project.
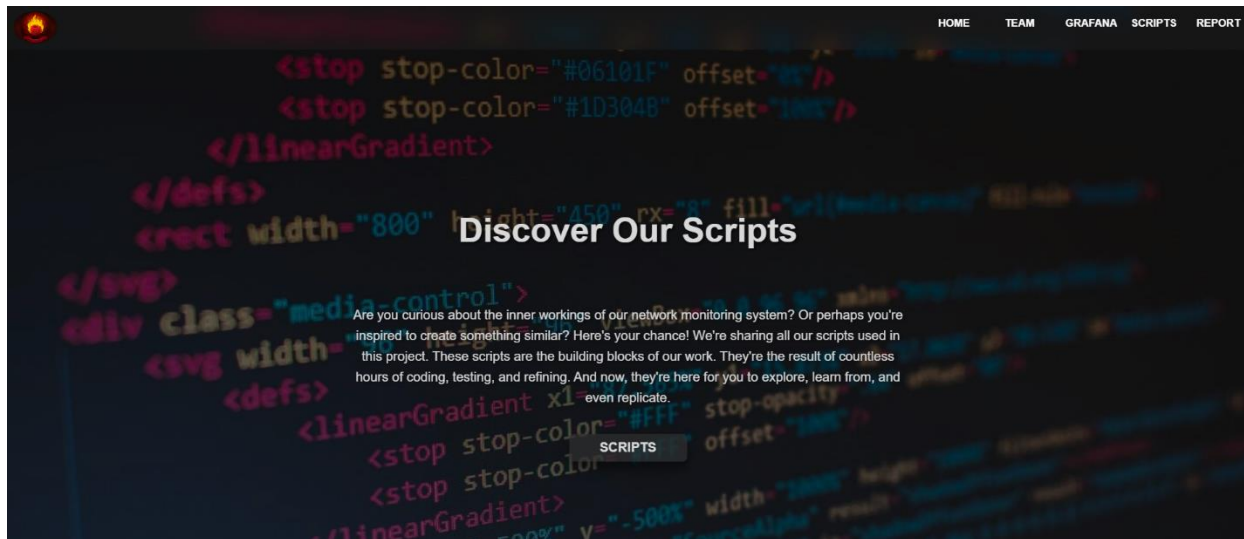
5. The Report page:

   This page includes the link to download the technical report and the link to this project's GitHub Repository for all the details of the project.
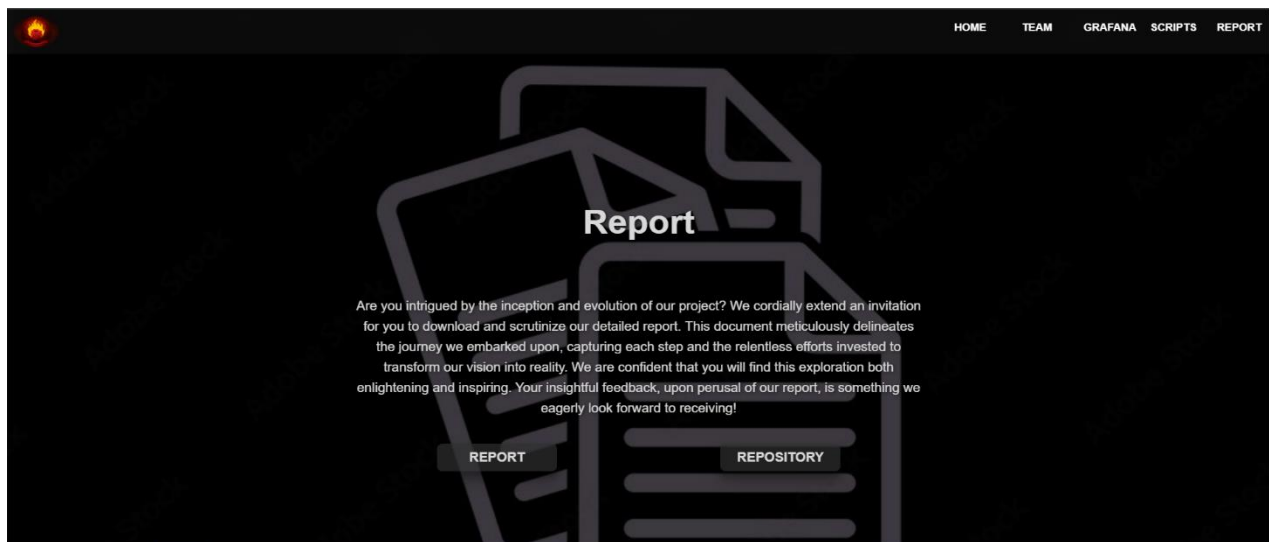
Grafana Dashboard:

1. Quick CPU / Mem / Disk: This section includes the metrics of the CPU, Mem, and Disk.

2. Network Traffic: This section includes 17 panels of network traffic metrics, for example:
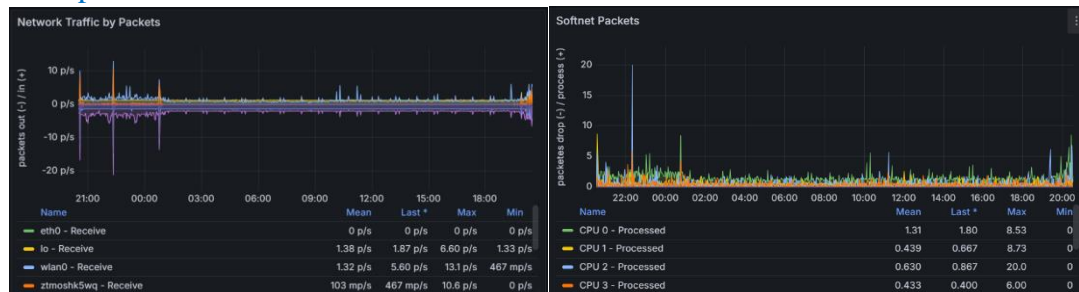
3. Network Traffic: This section includes 17 panels of network traffic metrics, for example:
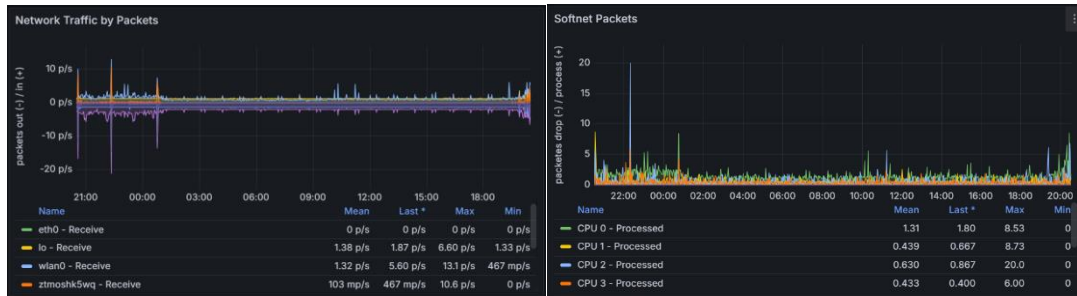
4. Network Stockstat: This section includes 5 panels of network stockstat metrics, like;
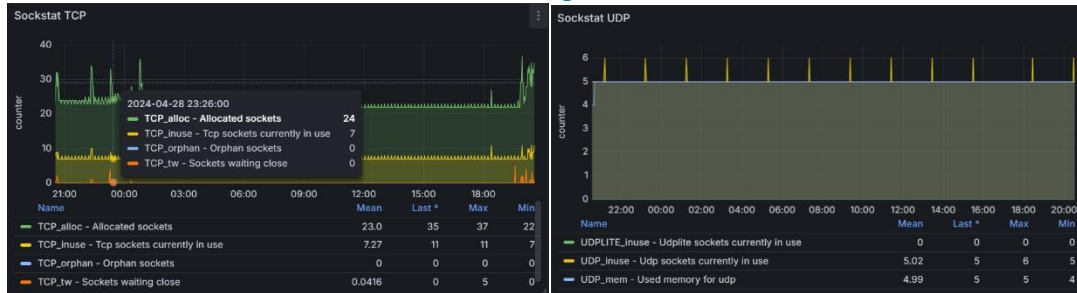
5. Network Netstat: This section includes 11 panels of network netstat metrics, like:

TCP In / Out
- InSegs - Segments received, including those received in error. This count includes segments receive...
- OutSegs - Segments sent, including those on current connections but excluding those containing onl...

TCP Errors
- ListenOverflows - Times the listen queue of a socket overflowed
- ListenDrops - SYNs to LISTEN sockets ignored
- TCPSynRetrans - SYN-SYN/ACK retransmits to break down retransmissions in SYN, fast/timeout retra...
- RetransSegs - Segments retransmitted - that is, the number of TCP segments transmitted containing ... 0.00

TCP Connections
	Mean
CurrEstab - TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT	8.96

TCP Direct Transition
- ActiveOpens - TCP connections that have made a direct transition to the SYN-SENT state from the CL... 0.00
- PassiveOpens - TCP connections that have made a direct transition to the SYN-RCVD state from the ... 0.0

6. Node Exporter Status: This section has a panel for the scrape time and a panel for the scrape successfulness.

Node Exporter Scrape Time
Name	Mean	Last *	Max	Min
arp - Scrape duration	540 µs	426 µs	6.82 ms	145 µs
bcache - Scrape duration	148 µs	72.9 µs	7.22 ms	30.1 µs
bonding - Scrape duration	217 µs	97.7 µs	7.64 ms	43.3 µs
btrfs - Scrape duration	175 µs	66.3 µs	13.4 ms	27.7 µs

Node Exporter Scrape
Name	Mean	Last *	Max	Min
arp - Scrape success	1	1	1	1
bcache - Scrape success	1	1	1	1
bonding - Scrape success	0	0	0	0
btrfs - Scrape success	1	1	1	1

7. SNMP: This section includes 5 panels of SNMP metrics and information:

Number of collection events

Total request errors
0

Time spent collecting m
0 s

Total PDU Errors
0

Version
0.19.0

8. Basic CPU / Mem / Net / Disk: This section includes 4 panels of CPU, Mem, Net, and Disk metrics:

9. CPU / Memory / Net / Disk: This section includes 8 panels of more metrics than the previous section:

Disk IOps

Name	Mean	Last *	Max	Min
mmcblk0 - Reads completed	0 io/s	0 io/s	0 io/s	0 io/s
mmcblk0 - Writes completed	7.22 io/s	12.7 io/s	19.7 io/s	0.267 io/s

I/O Usage Read / Write

Name	Mean	Last *	Max	Min
mmcblk0 - Successfully read bytes	4.17 B/s	0 B/s	3.00 kB/s	0 B/s
mmcblk0 - Successfully written bytes	36.9 kB/s	62.5 kB/s	264 kB/s	2.73 kB/s

I/O Utilization

Name	Mean	Last *	Max	Min
mmcblk0	1.18%	1.65%	51.2%	0.107%

CPU spent seconds in guests (VMs)

Name	Mean	Last *
Guest - Time spent running a virtual CPU for a guest operating system	0%	0%
GuestNice - Time spent running a niced guest (virtual CPU for guest operating system)	0%	0%