

Defendr User Manual

Advance & Dark nITes

Ruslynn Appana
Jeandre Botha
Muhammed Carrim
Sisa Khoza
Christiaan Opperman



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA



Table of Contents

1. Introduction.....	3
1.1. System Overview	3
1.2. System Configuration	3
1.3. Installation.....	3
2. Getting Started	4
2.1. Signing in	4
2.2. Registering	4
3. Using the System	5
3.1. Exploring the home window	5
3.2. Managing users	6
3.3. Changing user details	7
3.4. IP blacklisting	7
3.5. Viewing traffic logs	8
3.6. Viewing System metrics	8
3.7. Load balancing.....	13
3.8. Adding service backends	13
4. Troubleshooting	13
4.1 Missing bpf maps	13
4.2 Grafana is not showing any data	14

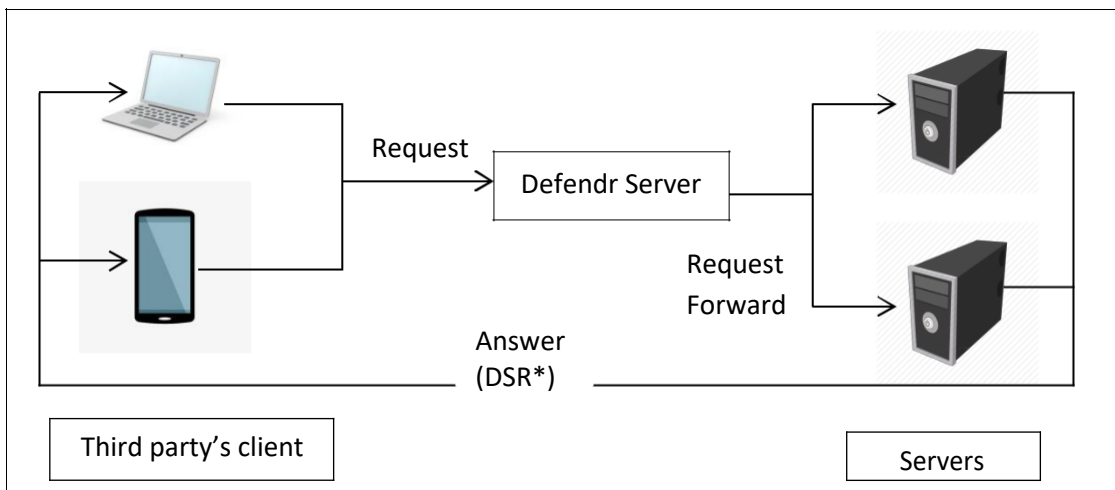
1. Introduction

1.1. System Overview

The purpose of this system is to protect third party applications from malicious users. The system implements this by detecting DDOS attacks and dropping the packets that are associated with an attack. It also provides load balancing features to control the load for each pool of resources that it is connected to.

The user interacts with the system via an intuitive graphical user interface where the user can to add and remove IP addresses to a white- and blacklist, see packets that traversed the system, view metrics (such as drop rates, packet sizes etc.) and remove and add back-end applications.

1.2. System Configuration



*Direct Server Return

There are three main components in this system, namely: servers on which back-end applications run, normal devices that the client uses to connect to the third party application and a server on which Defendr executes. The servers on which back-end applications run and the normal devices that the client uses to connect to the third party application is beyond the scope of this user manual. Defendr runs on a server that intercepts the packages after they have left the third party's client, but before they reach the application.

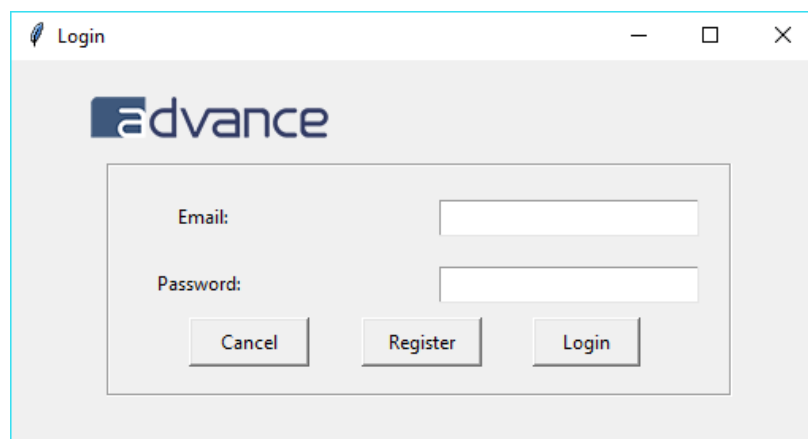
1.3. Installation

1. The entire Defendr package can be found on <https://github.com/cos301-2019-se/Defendr.git>

2. Open the terminal
3. Type the following commands:
 - `sudo nano /etc/ld.so.conf`
4. In the ld.so.conf file type this in: `"include /usr/local/lib"`
5. Navigate into the root Defendr Folder
6. Open the terminal
7. Run the command: `"chmod +x installcommands.sh"`
8. Run the command: `"./installcommands.sh"`
9. Follow instructions on the screen

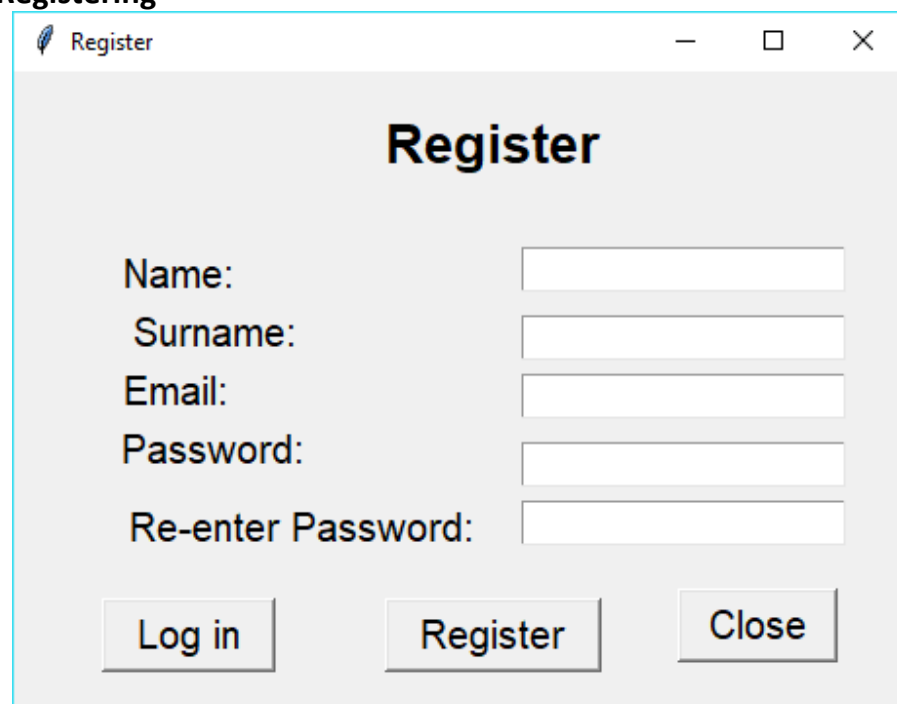
2. Getting Started

2.1. Signing in



After the program installs, this window will appear on the screen. For first time users of the system; please click on the register button to register yourself as a user of the system as explained in section 2.2. Otherwise, log in with your credentials.

2.2. Registering



This window is for registering new users to the system. A user will be requested to fill in:

- His/Her name
- Surname
- A valid Email address
- A Password and
- Confirm password

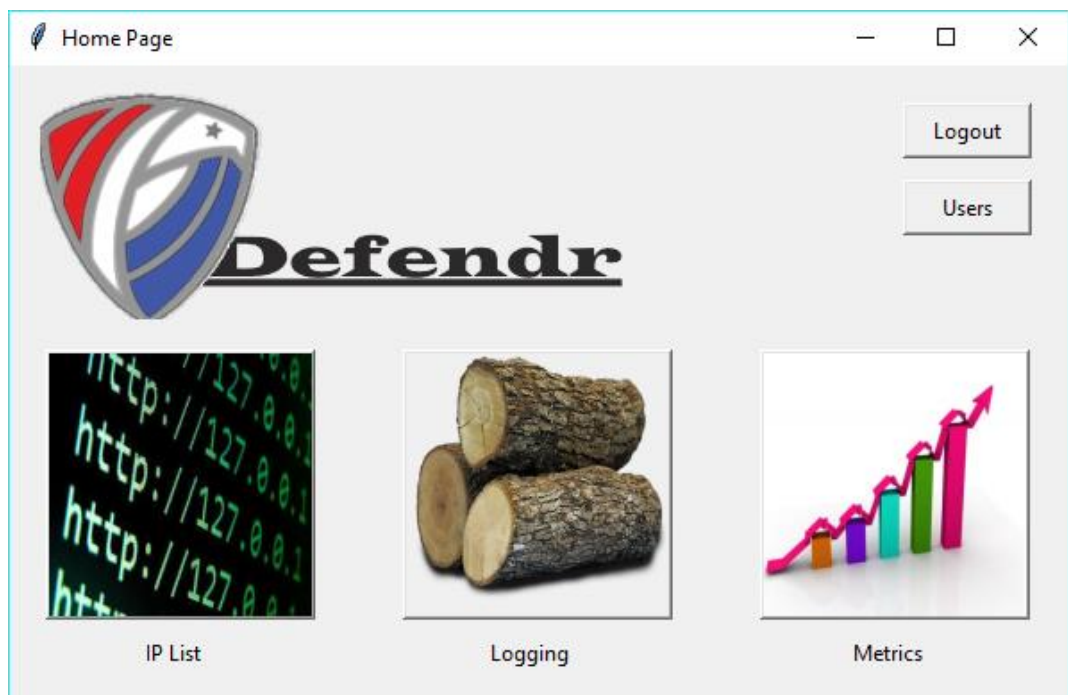
Please note that the password must contain:

- An uppercase character
- A lowercase character
- A symbol and
- A number

After the user has completed their details, they will have to click the register button. This will register the user by default as a non-admin user unless they are the first user of the system. Once registration is successful, the user will be directed to the home screen. The login button will return the user to the login window, whilst the close button will close the system.

3. Using the System

3.1. Exploring the home window



After successfully signing in as described in 2. *Getting started*, the home window will open. This is the main hub of the application, from here a user

can navigate to the IP List window, Logs window, metrics window or user management window.

- **To view and add blacklisted IPs**, click on the **IP List** icon.
- **To view system logs**, click on the **Logging** icon.
- **To view the system metrics**, click on the **Metrics** icon.
- **To log out**, click the **Logout** button.
- **To open the user management plane**, click the **Users** button. (admin only)

3.2. Managing users

The screenshot shows a 'User Management' window with the following components:

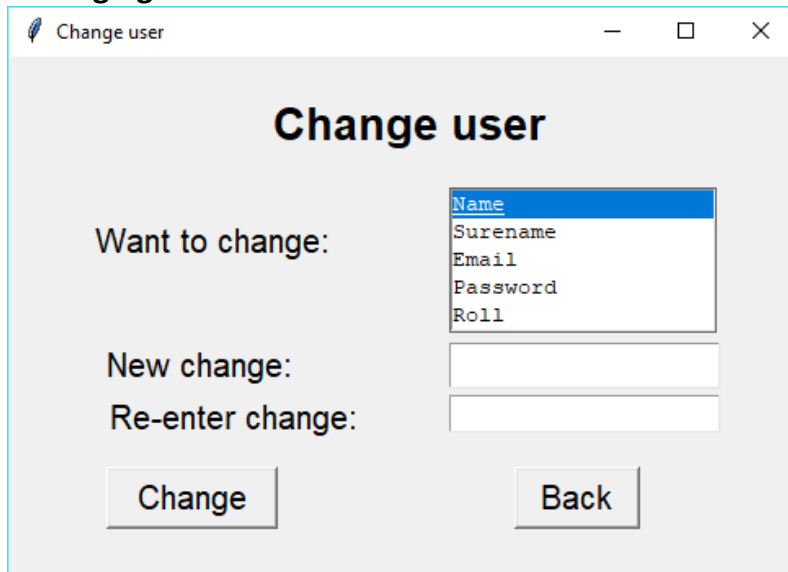
- Add:** Fields for Name, Surname, Email, Password, and Re-enter Password.
- Remove:** Field for Email.
- Change:** Field for Email.
- Buttons:** Add, Remove, Change, Refresh, and Close.
- Users:** A table listing existing users.

Users:			
Chris	Osbrone	user	chris@gmail.com
Christo	Opperman	admin	u17023239@tuks.co.za
Muhammed	Carrim	admin	u15019854@tuks.co.za
Sisa	Khoza	admin	u15034993@tuks.co.za
Ruslynn	Appana	admin	u14016304@tuks.co.za
Jeandre	Botha	admin	u17094446@tuks.co.za
Charles	Summers	user	cs@gmail.com
t	p	user	tp@cs.up.ac.za

The user management plane has four main functions:

1. adding new users
 2. removing users
 3. changing a user's details and
 4. displaying all users.
- **To display all registered users**, click the **refresh** button.
 - **To add a new user**, fill in the aforementioned details in Section 2.2 and then click on the **Add** button to complete the adding process.
 - **To remove a user**, provide the e-mail address of the user that needs to be removed in the **Email** field under the **Remove** heading and click the **Remove** button.
 - **To change a user's details**, insert the e-mail address of the user that needs to be changed in the **Email** field under the **Change** heading and click on the change button which will open the change user window.
 - **To go back to the main page**, click on **Close** button.


3.3. Changing user details



This window allows the user to change specific details for user accounts, such as

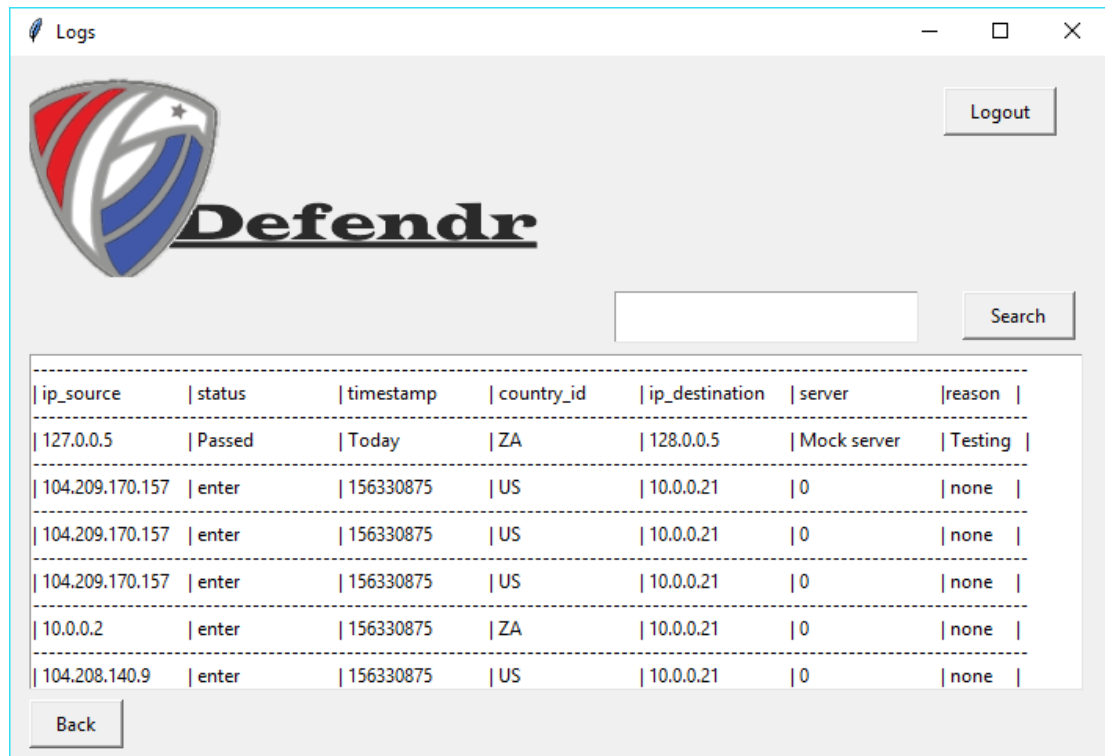
- Name
 - Surname
 - e-mail address
 - password
 - the role of a user
- **To change user detail**, select desired field from the list of fields, then enter the new value for the given field in the **New change** fields and re-enter the value in the **Re-enter change** field. Now click the **Change** button to make the change.
 - **To return to the user management plane**, click the **Back** button

3.4. IP blacklisting



- **To manually blacklist IP address**, enter the IP address to be blacklisted in the field next to the **Add IP** button then click on **Add IP**.
- **To remove a blacklisted IP address**, enter the IP address to be removed from the blacklist in the field next to the **Add IP** button then click on **Remove IP**.
- **To view currently blacklisted IP addresses**, click **List Blacklisted**.
- **To log out**, click **Logout**.
- **To go back to the main window**, click **Back**
- **To close defender**, click **Close**

3.5. Viewing traffic logs



ip_source	status	timestamp	country_id	ip_destination	server	reason
127.0.0.5	Passed	Today	ZA	128.0.0.5	Mock server	Testing
104.209.170.157	enter	156330875	US	10.0.0.21	0	none
104.209.170.157	enter	156330875	US	10.0.0.21	0	none
104.209.170.157	enter	156330875	US	10.0.0.21	0	none
10.0.0.2	enter	156330875	ZA	10.0.0.21	0	none
104.208.140.9	enter	156330875	US	10.0.0.21	0	none

This window enables the user to see either all the packets that went through the system or packets for specific IP addresses.

- **To view all incoming packets**, leave the search field empty and click **Search**.
- **To view packets with a specific source IP address**, enter the desired IP address in the search field and click **Search**.
- **To log out**, click **Logout**.
- **To go back to the main window**, click **Back**

3.6. Viewing System metrics

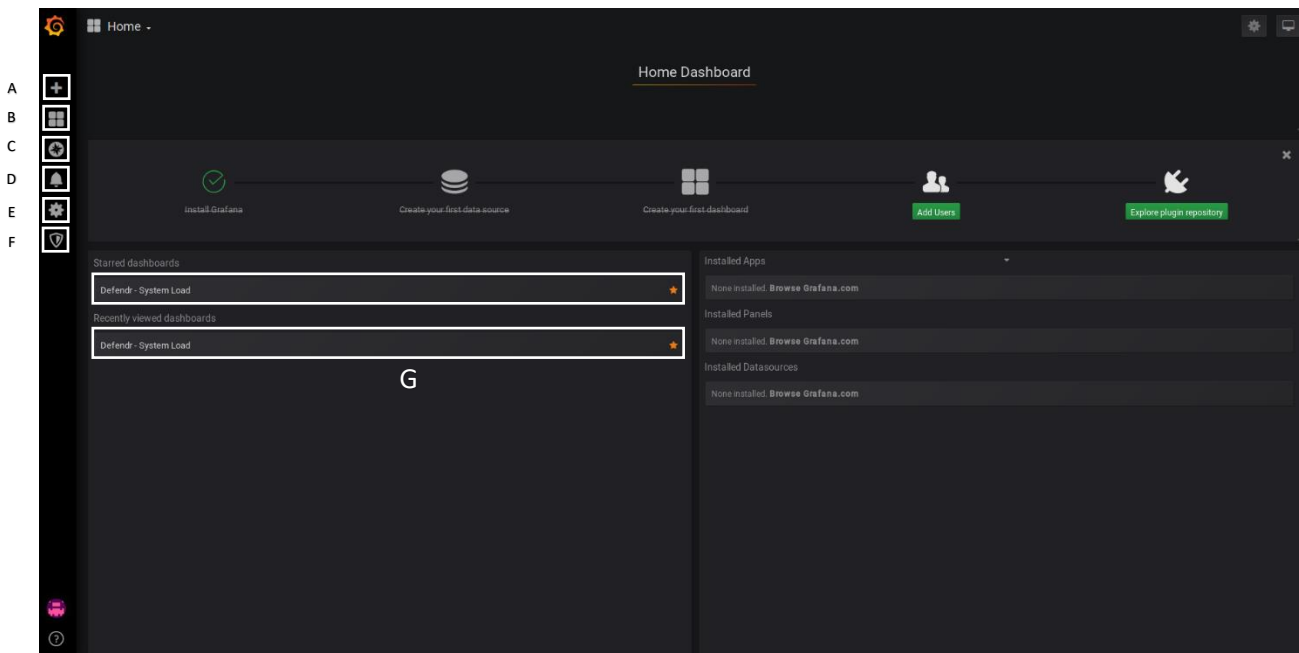
The metrics window has jurisdiction over system load and individual resource monitoring.

- Sign-in



On click of the Metrics button (as shown in Section 3.1) a Grafana sign-in page will open in a browser. The default username is **admin**, and the default password is **admin**. You will be prompted to provide a more secure password at the first successful sign-in.

- B/G)Home Dashboard

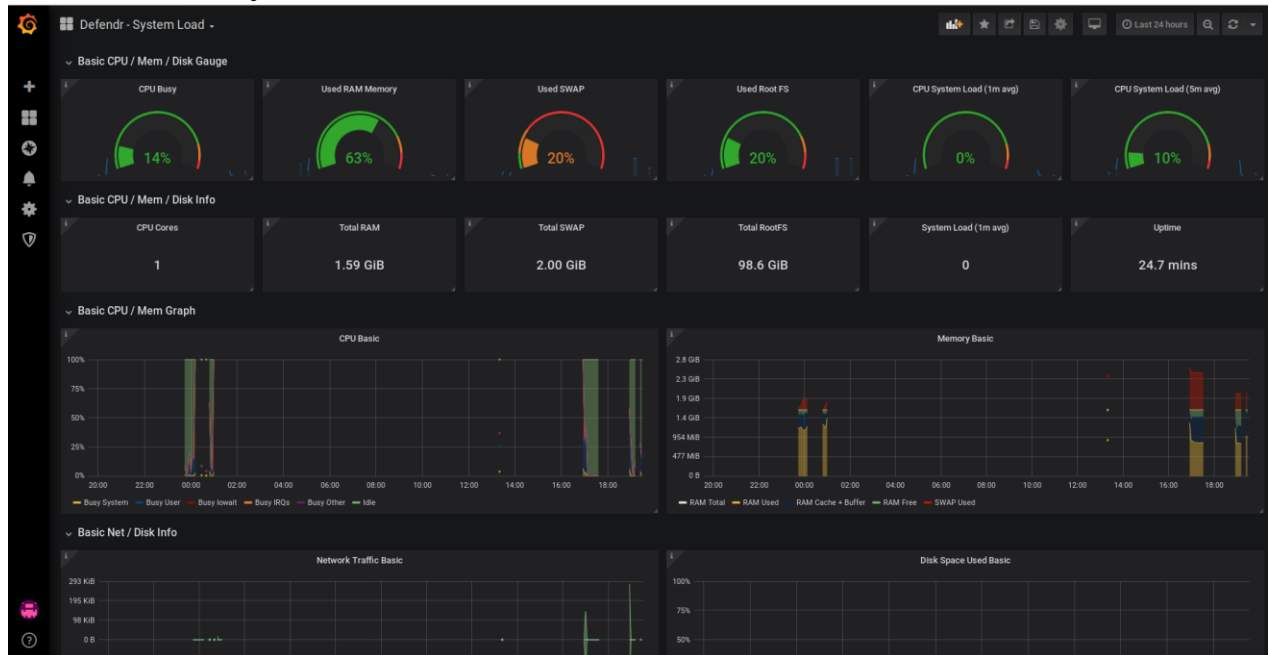


The dashboard is a centralised portal to access metrics and configuration:

- A. Create > Dashboard, Folder, Import
- B. Dashboards > Home, Manage, Playlists, Snapshots
- C. Explore
- D. Alerting > Alert Rules, Notifications Channels
- E. Configuration > Data Sources, Users, Teams, Plugins, Preferences, API Keys

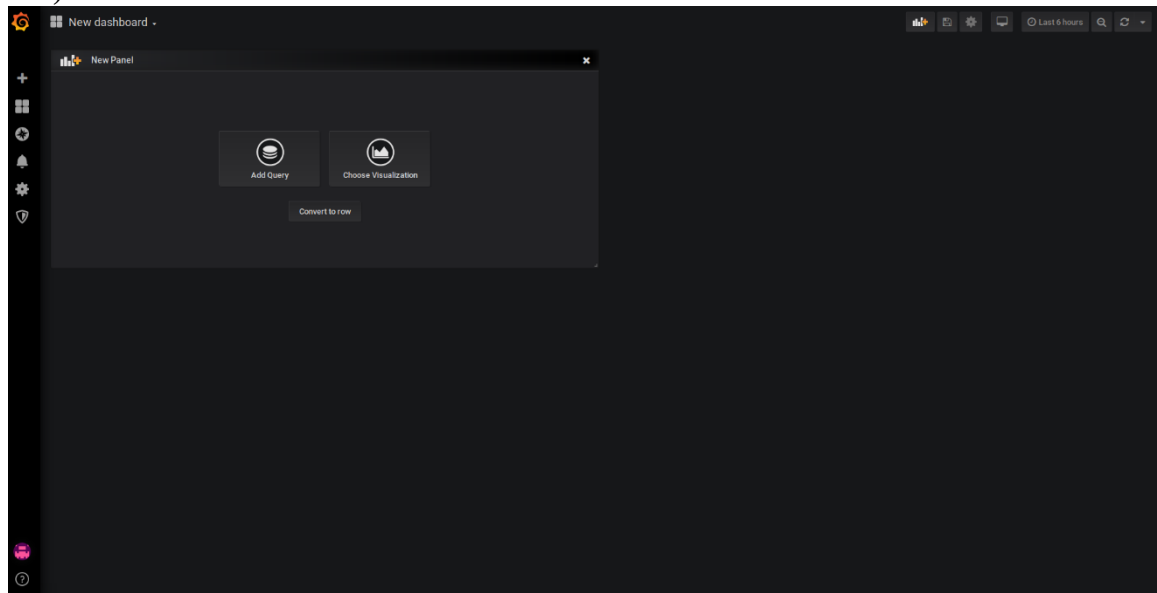
- F. Server Admin > Users, Orgs, Settings, Stats
- G. Dashboards

- G) Defendr – System Load



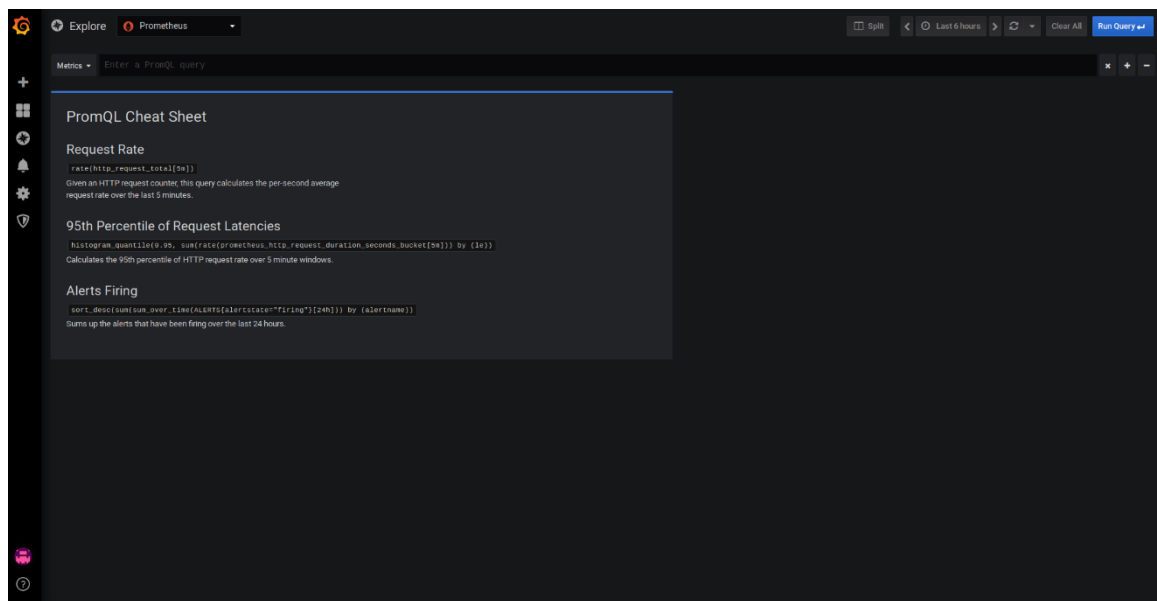
This window is the **Defendr -System Load**. This page will display the usage statistics as provided by the Prometheus and its exporters. This enables a unified monitoring tool for system load statistics.

- A) New dashboard



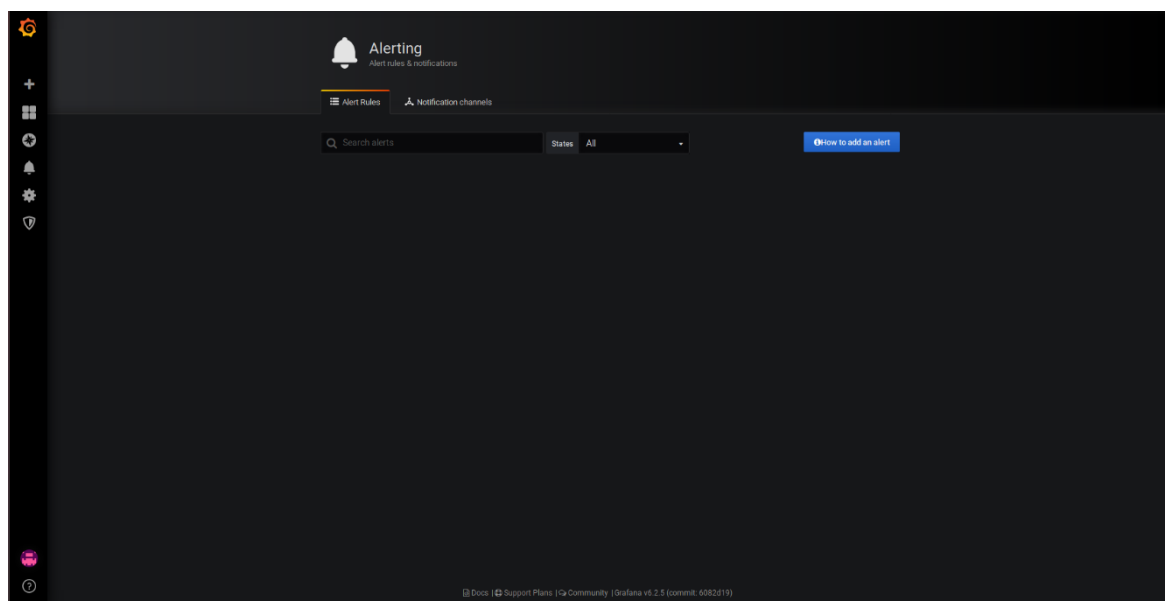
The **New Dashboard** page allows a user to create and customise a new dashboard. It also allows the querying of data from a data source.

- C) Explore



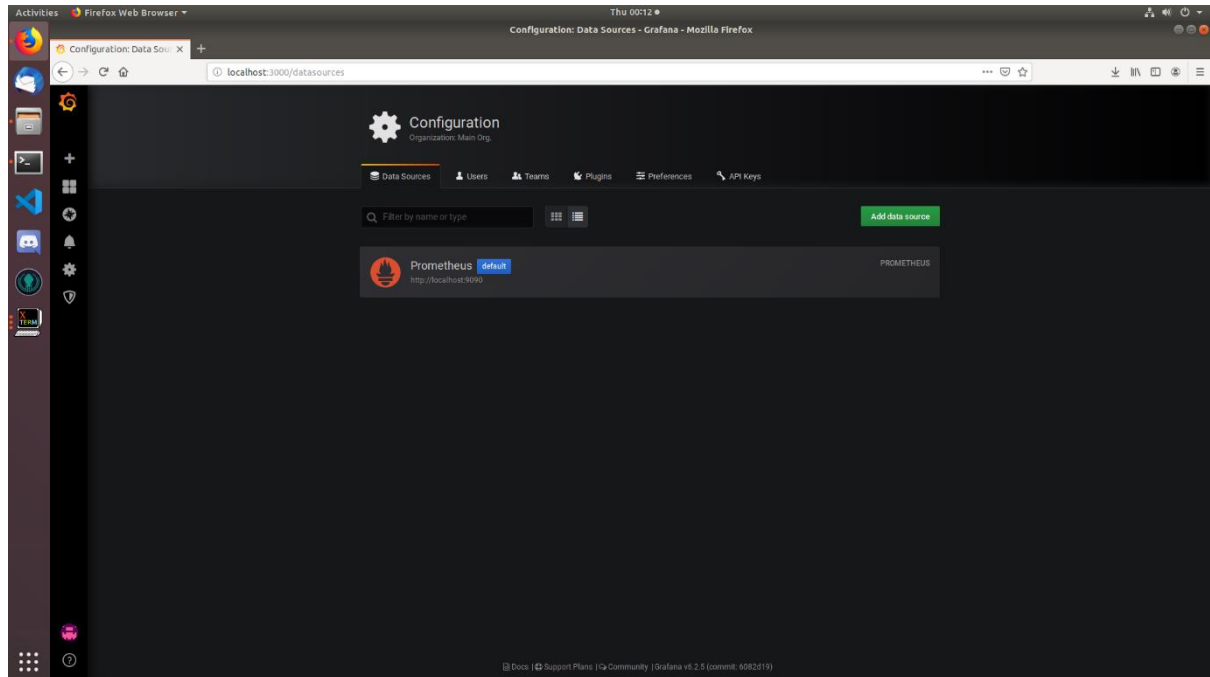
Explore is an information hub that give a user tIPs to better benefit from Grafana.

- D) Alerting



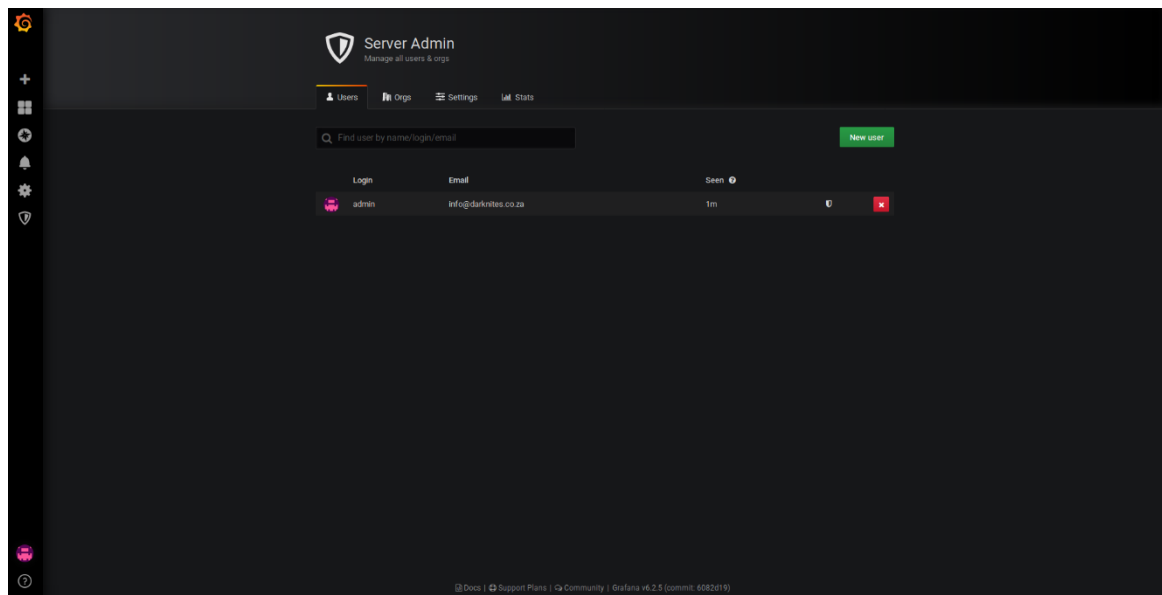
Alerting is a featured provided by Grafana to allow real-time updates to another communication channel, e.g. e-mail, Slack, Webhook etc., based on rules attached to a dashboard. One such example could be when the system is under a greater-than-normal network load.

- E) Configuration



The **Configuration** page allows a user to add and remove other metrics reporting systems that Grafana can gather data from to graph. At current Prometheus will be visible by default.

- F) Server Admin



Server Admin is a page to carry out administrative tasks on Grafana. The system administrator will be able to

- create or remove users
- establish organisations (user privileges)
- change settings view Grafana logs.

3.7. Load balancing

Load balancing will automatically start when the Defendr application is installed

3.8. Adding service backends

To add a new backend:

1. Start up the desired machine that contains the service instance.
2. Copy the "serviceInstance" folder from the downloaded Defendr package to any location on the machine.
3. Open and navigate to serviceInstance/src/main/resources/
4. Open the file application.properties.
5. Change the property "app.name" to the applications IP address.
6. Change the property "client.instance_id" to the machine's own IP address.
7. Return to the "serviceInstance" root folder : serviceInstance/
8. Open the command line terminal in this location. (rightclick in the folder and click on "Open Terminal Here")
9. In the command line terminal type "gradle clean build" without the quotations and press enter.
10. After the build finishes, in the terminal, type "java -jar build/libs/serviceInstance.jar" without quotations and press enter.
11. The backend will now automatically register itself with the Defendr application.

4. Troubleshooting

4.1 Missing bpf maps

In the unlikely event that the following error appears in a pop up terminal while opening the Defendr application

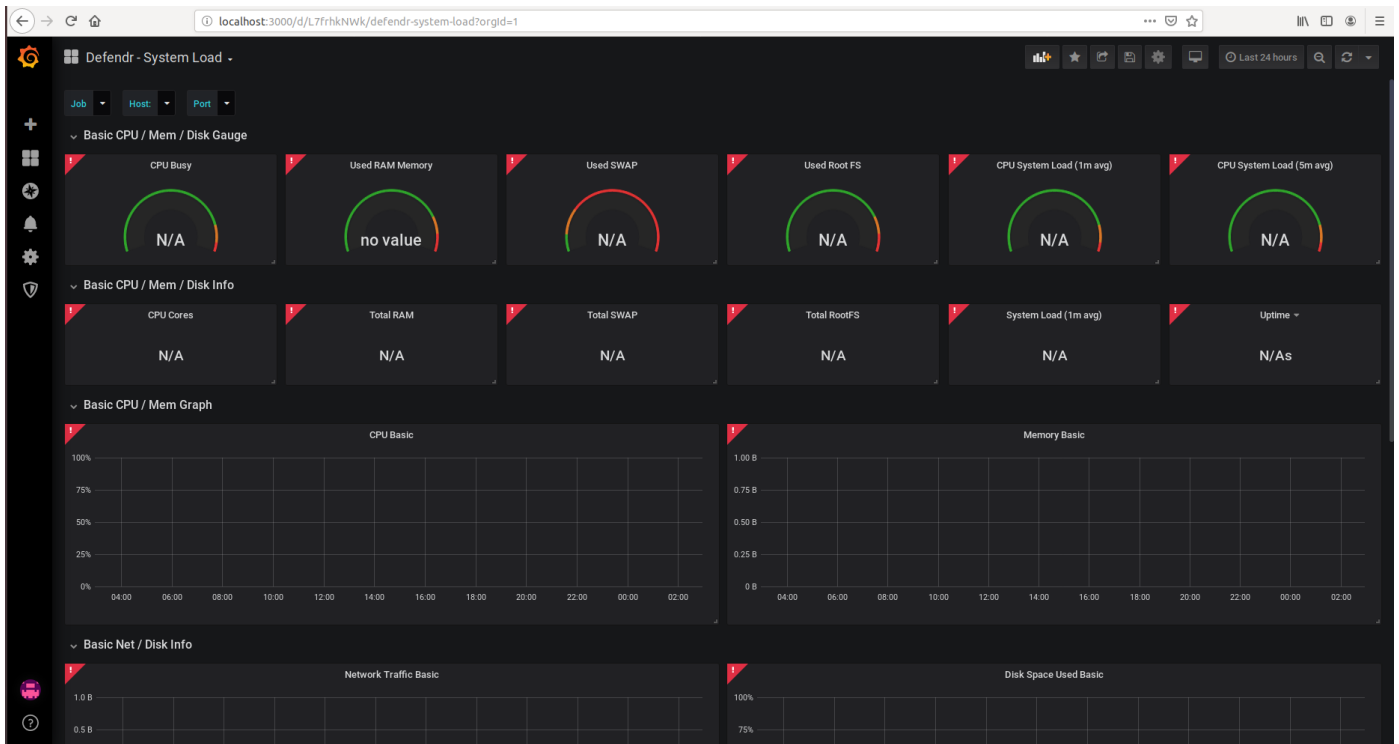
```
ERR: specified path /sys/fs/bpf/ddos_blacklist is not on BPF FS
```

Mount the bpf file system by entering the command "sudo mount -t bpf bpf /sys/fs/bpf/" without the quotations within the terminal and press enter. If confronted with a request for the user password, enter the server password obtained from the server admin and press enter. The application can now be safely restarted.

In the event that the system interface becomes unresponsive the interface can simply be closed without doing any harm and restarted. This will not affect the system in any way.

4.2 Grafana is not showing any data

At time an improper start-up of a server may cause a disruption in the proper display of metrics. This may be due to delays or disruptions in service start-ups. A Defendr restart may cause the system to return to normal functionality, however for persistent cases more steps can be taken to investigate and remediate.



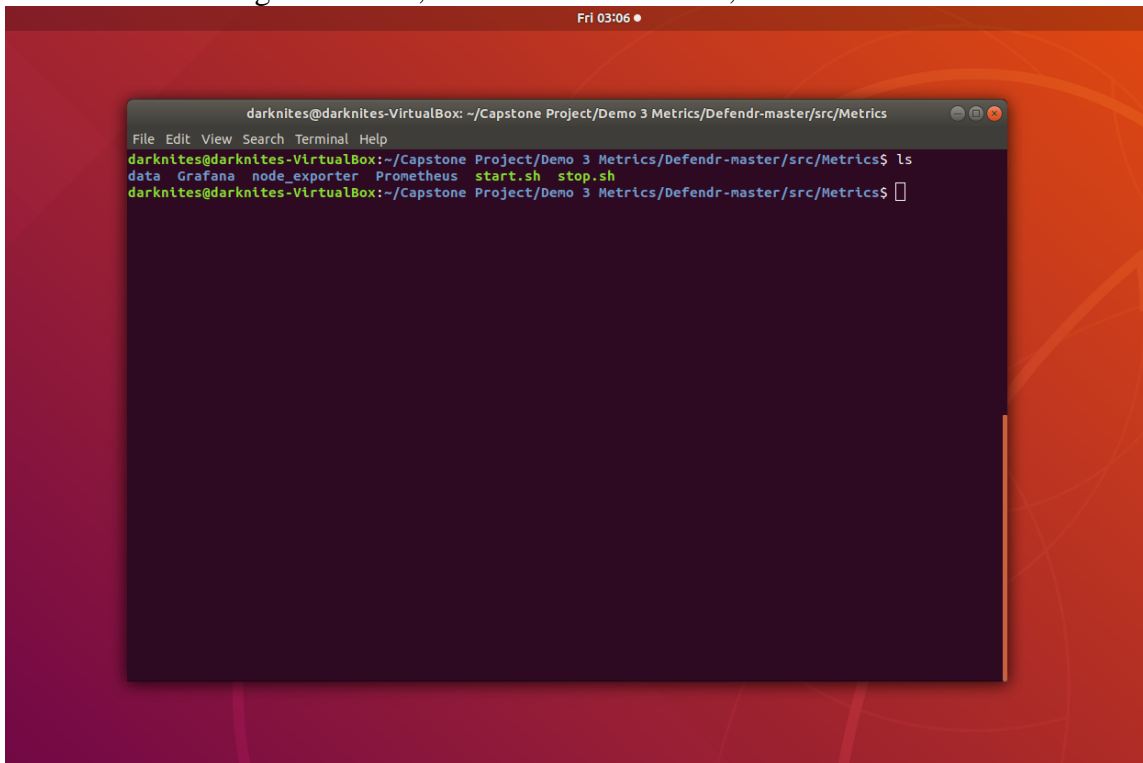
To determine the cause, open a browser and navigate to:

- <http://localhost:9190>*
- <http://localhost:9090>*
- <http://localhost:3000>*

*curl <address> can be used in terminal as well

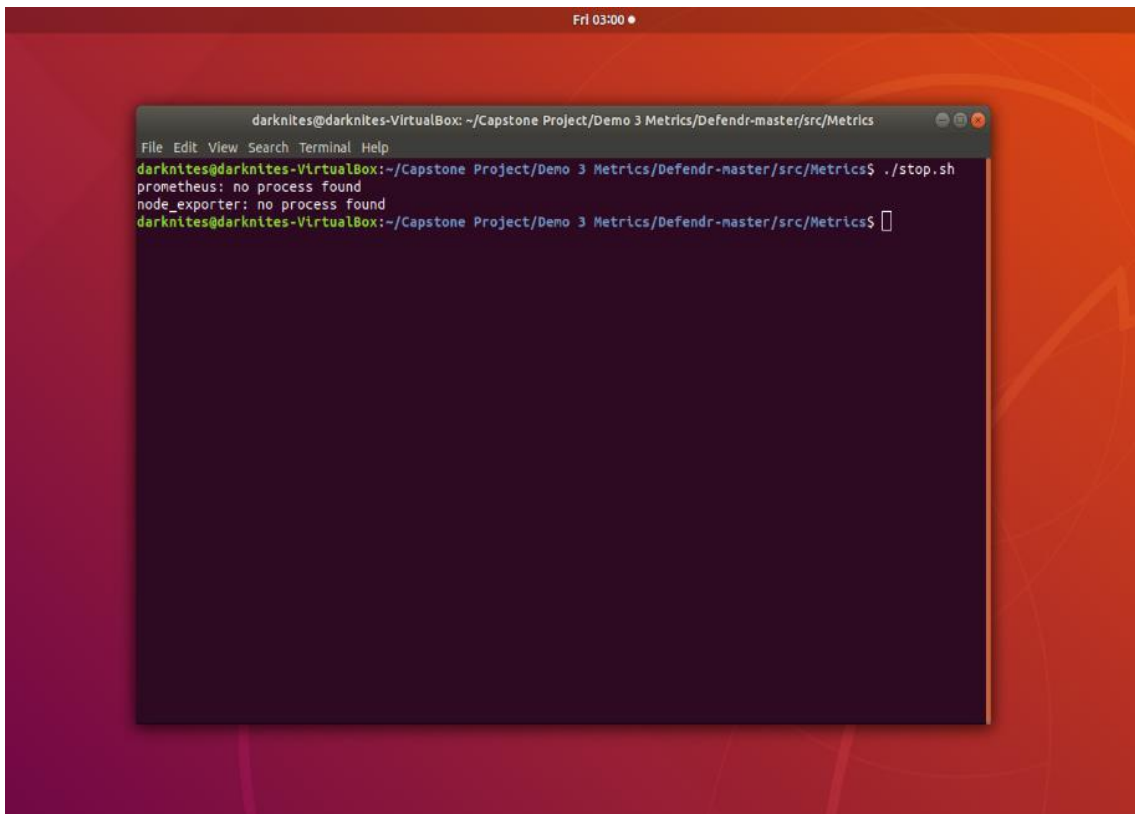
If no response is received, please try the following:

- Open a terminal in “/Defendr/src/Interfaces/Metrics”. This is the working directory and all the following commands, unless otherwise stated, will start here.



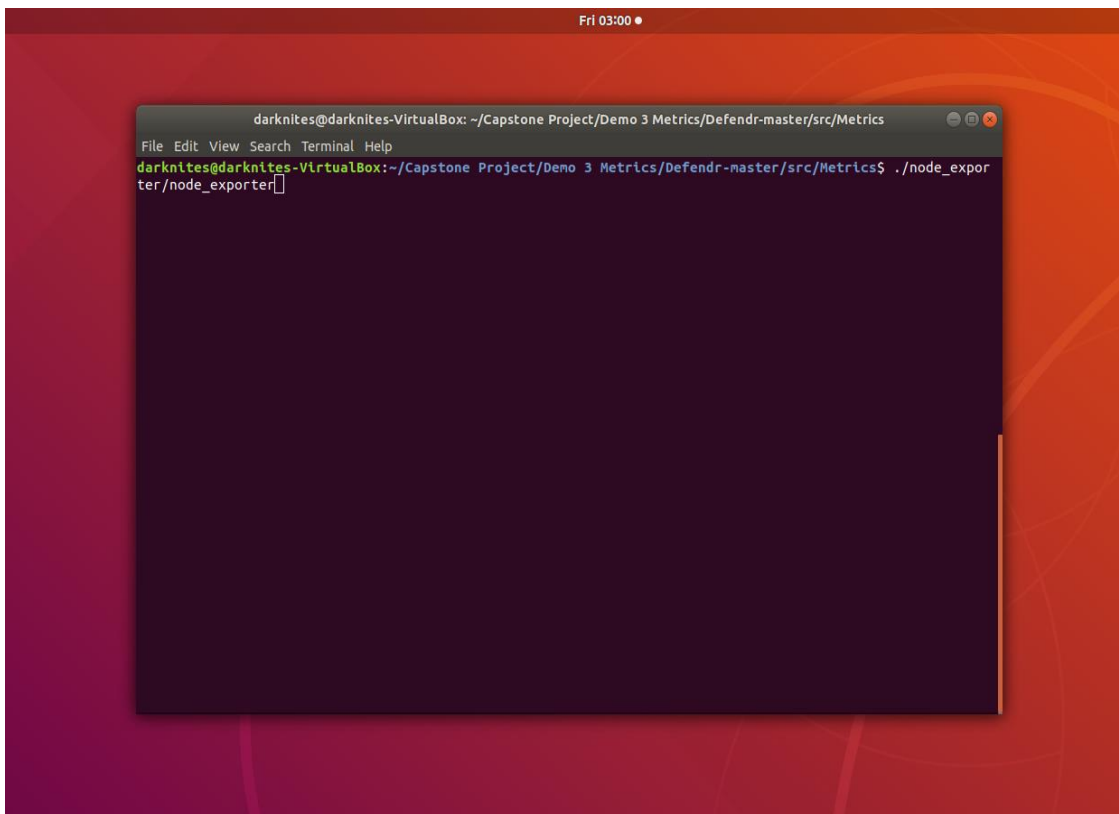
A screenshot of a terminal window titled "darknites@darknites-VirtualBox: ~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics". The terminal shows the command `ls` being executed, which lists the contents of the directory: `data`, `Grafana`, `node_exporter`, `Prometheus`, `start.sh`, and `stop.sh`. The prompt is `darknites@darknites-VirtualBox:~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics$`.

- Enter “./stop.sh”. Any rouge servers will stop. If a no process message appears, that just means the particular service was not running.

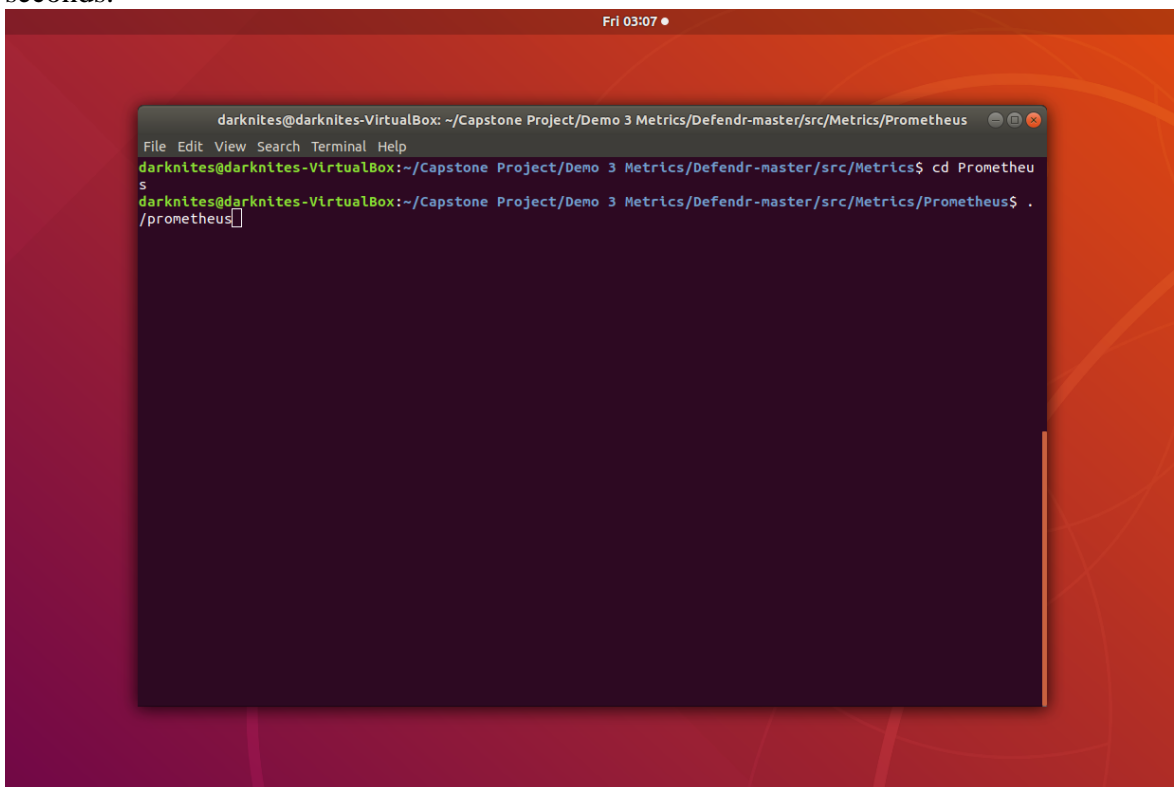


A screenshot of a terminal window titled "darknites@darknites-VirtualBox: ~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics". The terminal shows the command `./stop.sh` being executed. The output of the script is: `prometheus: no process found` and `node_exporter: no process found`. The prompt is `darknites@darknites-VirtualBox:~/Capstone Project/Demo 3 Metrics/Defendr-master/src/Metrics$`.

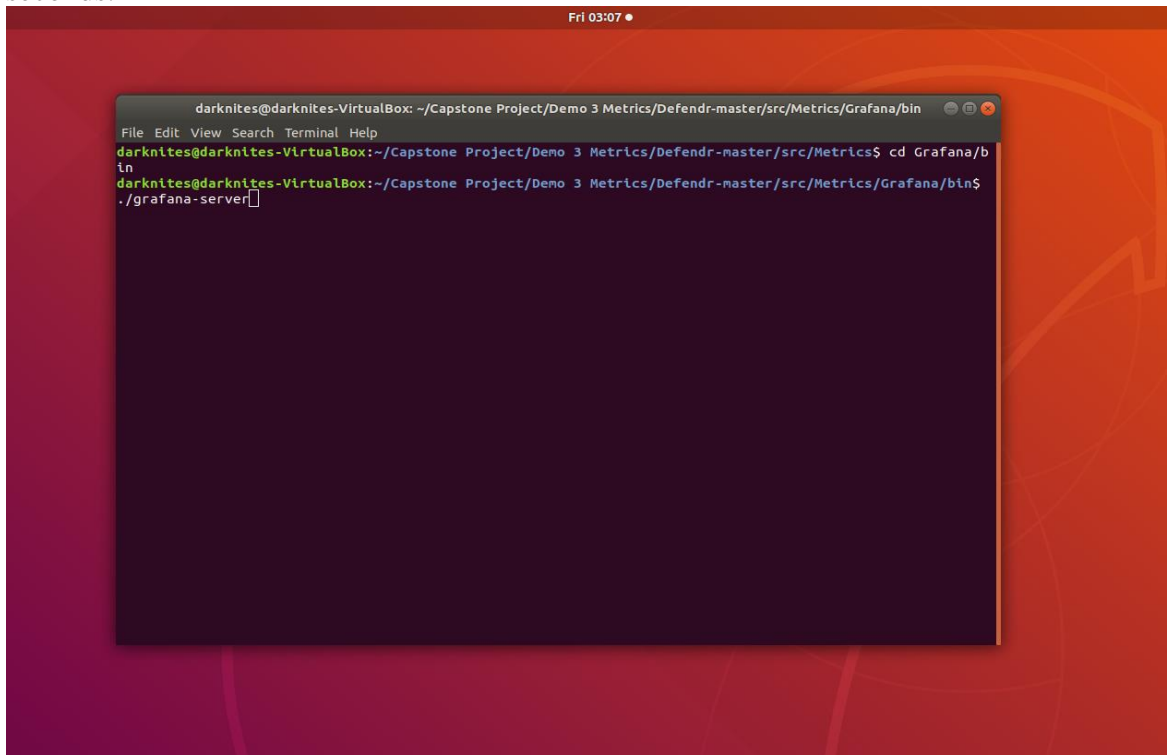
- Open a terminal and enter “./node_exporter/node_exporter”. Allow 5 seconds.



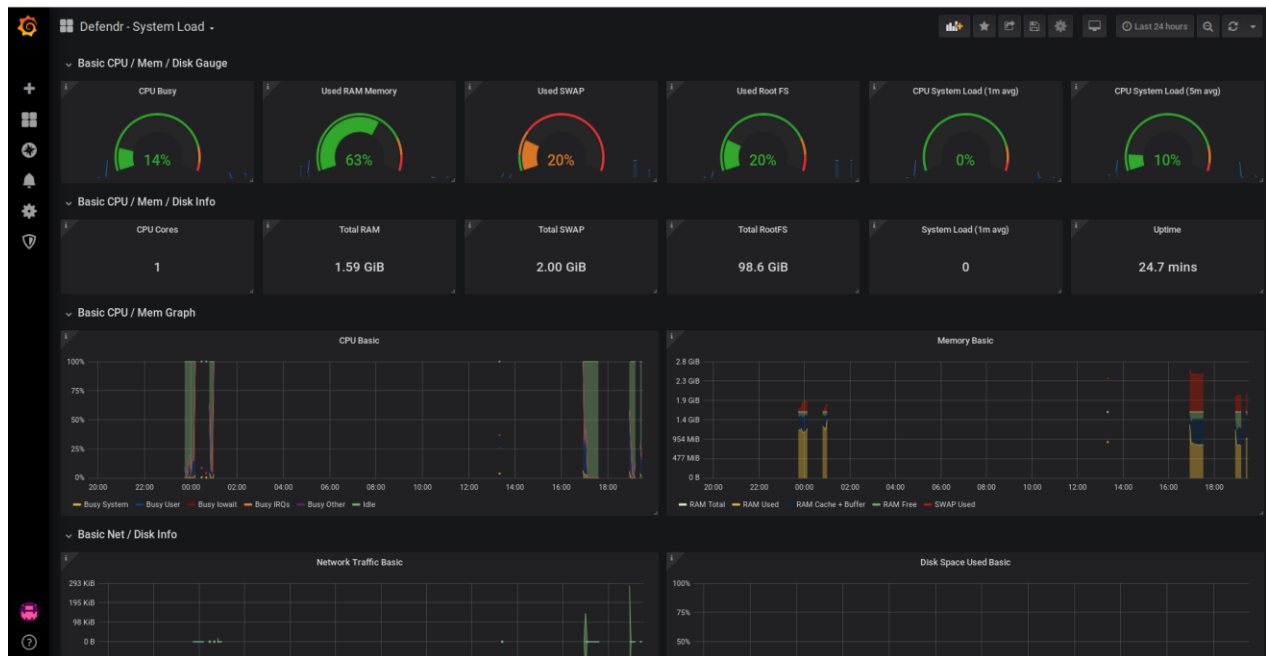
- Open a terminal and enter “cd Prometheus”. Then enter “./prometheus”. Allow 5 seconds.



- Open a terminal and enter “cd Grafana/bin”. Then enter “./grafana-server”. Allow 5 seconds.



- Open a browser, and navigate to “<http://localhost:3000>”



Provided the above services started with no errors, Grafana log-in should be displayed and metrics accessible again.