COS 301 CAPSTONE PROJECT

Denendr User Manual

Advance & Dark nITes

Ruslynn Appana

Jeandre Botha

Muhammed Carrim

Sisa Khoza

Christiaan Opperman



Table of Contents

[1. Introduction 3](#_Toc14247156)

[1.1. System Overview 3](#_Toc14247157)

[1.2. System Configuration 3](#_Toc14247158)

[2. Getting Started 3](#_Toc14247159)

[3. Using the System 4](#_Toc14247160)

[3.1. Sign in window 4](#_Toc14247161)

[3.2. Register window 4](#_Toc14247162)

[3.3. Home window 5](#_Toc14247163)

[3.4. User Management window 5](#_Toc14247164)

[3.5. Change User window 6](#_Toc14247165)

[3.6. IP list window 6](#_Toc14247166)

[3.7. Log window 7](#_Toc14247167)

[4. Troubleshooting 7](#_Toc14247168)

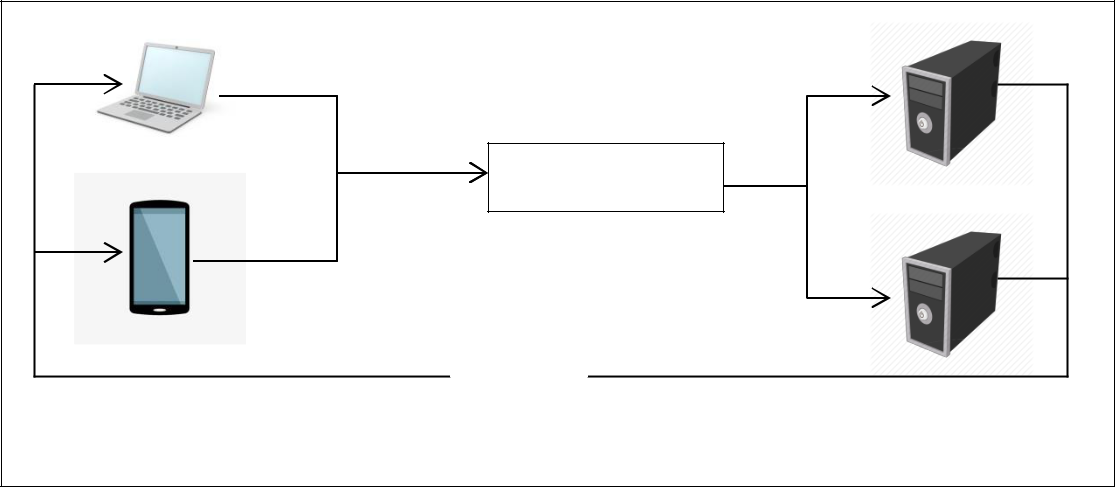
# Introduction

## 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.

## System Configuration



|  |  |  |
| --- | --- | --- |
|  | Request |  |
|  | Defendr Server |  |
|  | Request |  |
|  | Forward |  |
|  | Answer |  |
| Third party’s client | Servers |  |
|  |  |

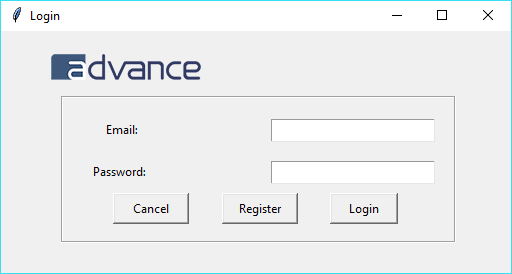
There are three main components in this system, namely: servers on which back-end applications run, normal devices that the client uses to connect to the third party application and a server on which Defendr executes. The servers on which back-end applications run and the normal devices that the client 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.

# 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

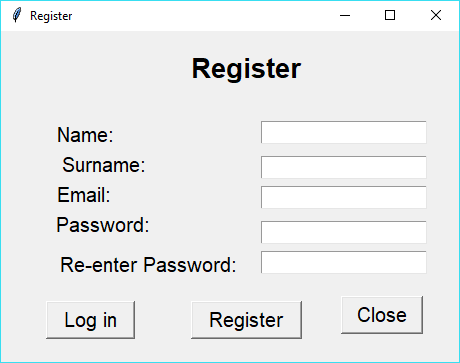
# Getting Started

* 1. Sign in window

****

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.

* 1. Register window



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.

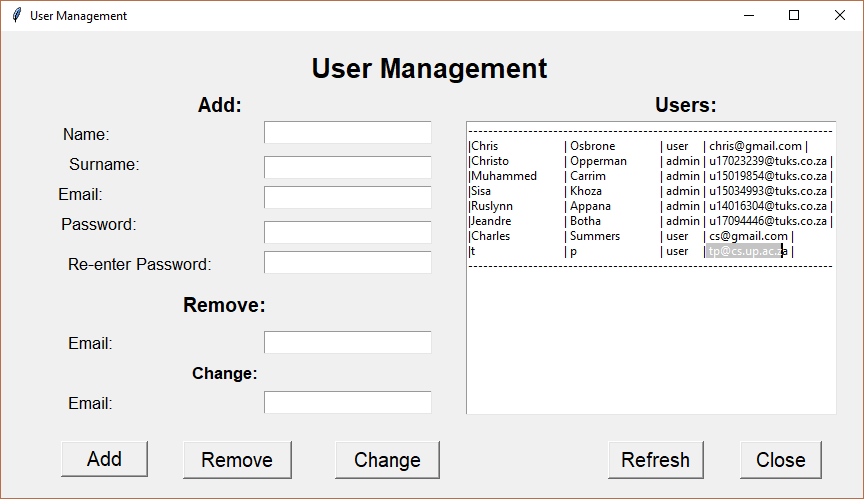
# Using the System

* 1. Home window



After logging in the, this window will appear. 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. They will also have the option to Log out. Note that only admin users can access the user management window.

* 1. User Management Window

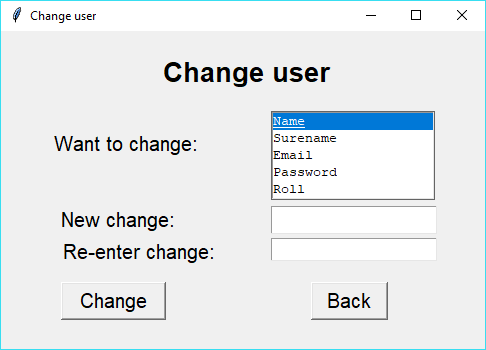


This window has four main functions, namely adding a user, removing a user, changing a user’s details or displaying all users. To display all users, the user must click the refresh button.

* To add a user, the user is required to fill in the aforementioned details in Section 2.2. The user will then click on the add button to complete the adding process.
* To remove a user, the user will simply have to insert the e-mail address of the user that needs to be removed and click on the remove button.
* Similarly, to change a user’s details the user will be required to insert the e-mail address of the user that needs to be changed and will then have to click on the change button. This will direct them to the change user window.

Additionally there is also a back button to return the user to the home window.

* 1. Change User window



This window allows the user to change specific details for user accounts, such as name, surname, e-mail address, password and the role of the user. To use this functionality the user is required to select the details that he/she wants to change. The user has to enter the corrected details twice for clarity purposes. The user than has to click the change button. Once this has been completed the user can use the back button to return to the user management window.

* 1. IP list window



This window enables the user to see blacklisted IP addresses and add or remove blacklisted IP addresses from the list.

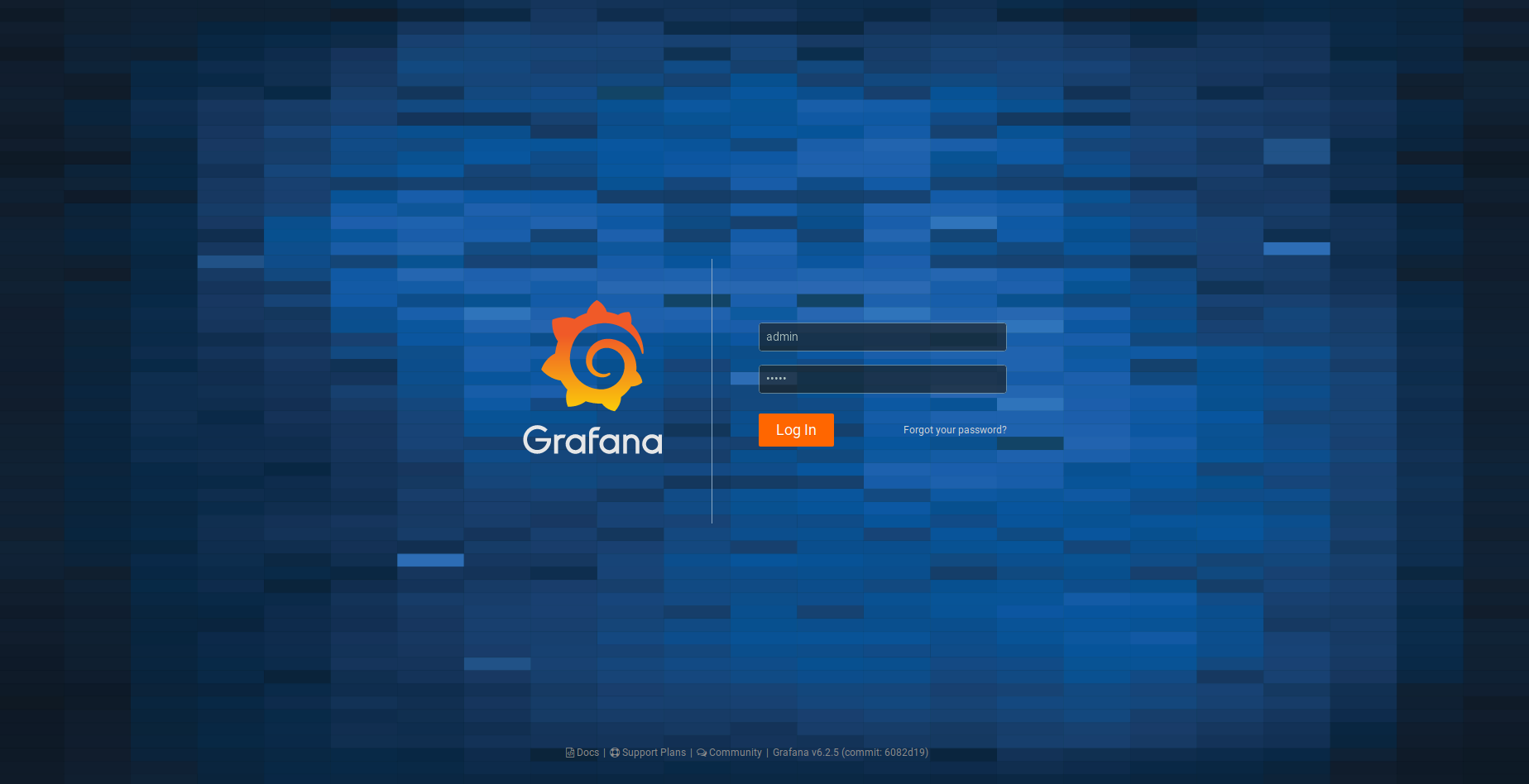
* 1. Log window



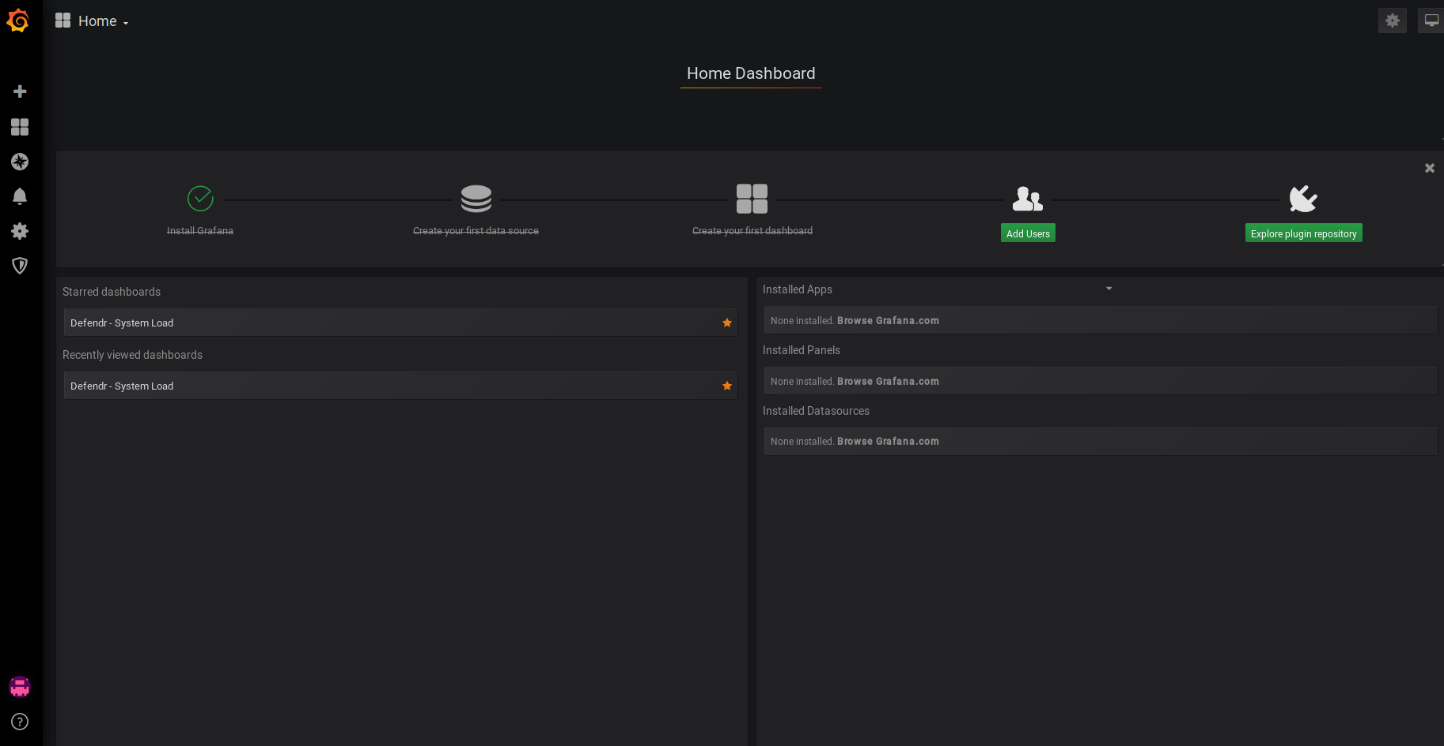
This window enables the user to see either all the packets that went through the system or packets for specific IP addresses. This is achieved through two queries to the database, namely find (to show all packets) and query (to find packets for a specific IP address).

* 1. Metrics window

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.

- Dashboard

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

* Create > Dashboard, Folder, Import
* Dashboards > Home, Manage, Playlists, Snapshots
* Explore
* Alerting > Alert Rules, Notifications Channels
* Configuration > Data Sources, Users, Teams, Plugins, Preferences, API Keys
* Server Admin > Users, Orgs, Settings, Stats
* Dashboards

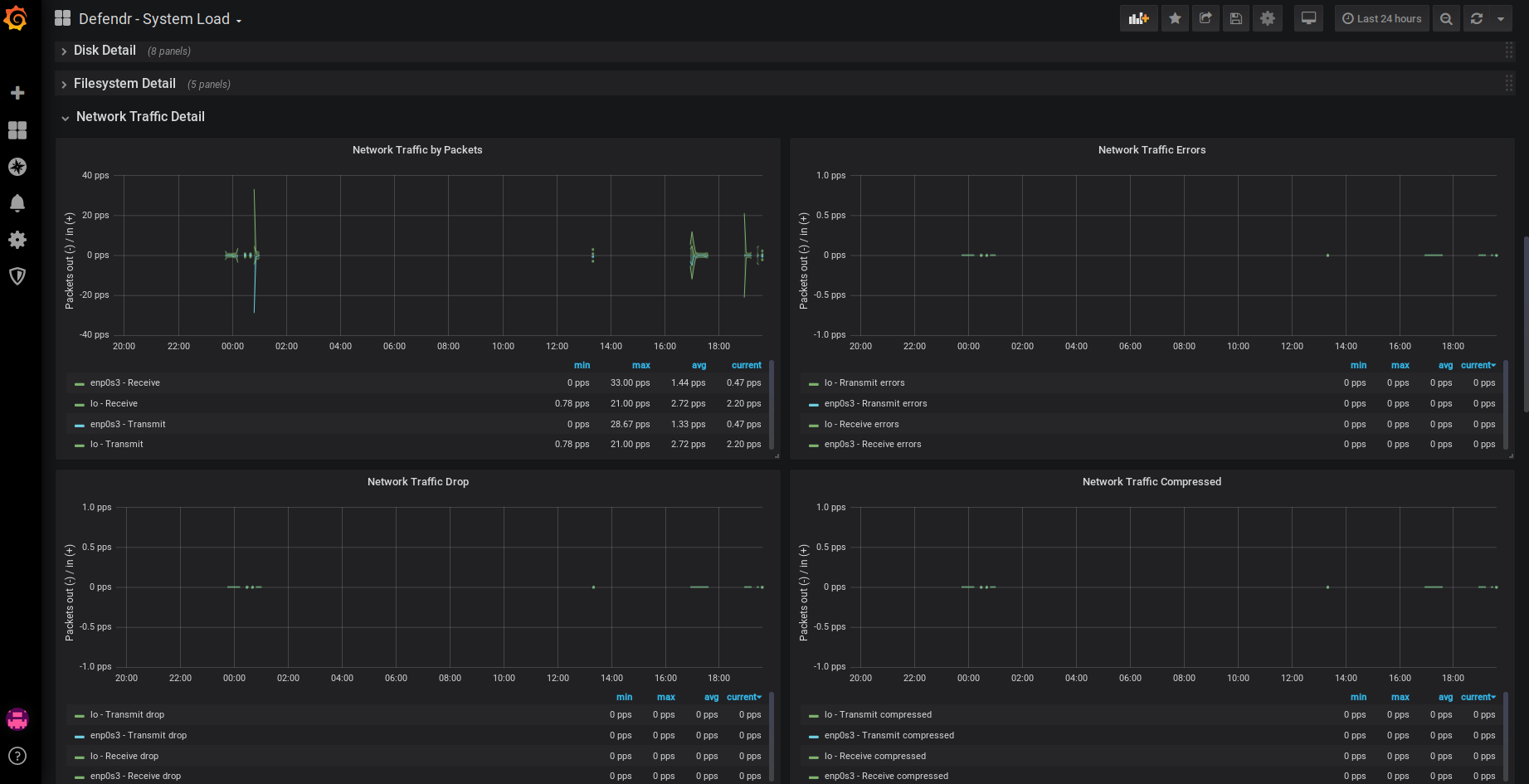
- Dashboard 

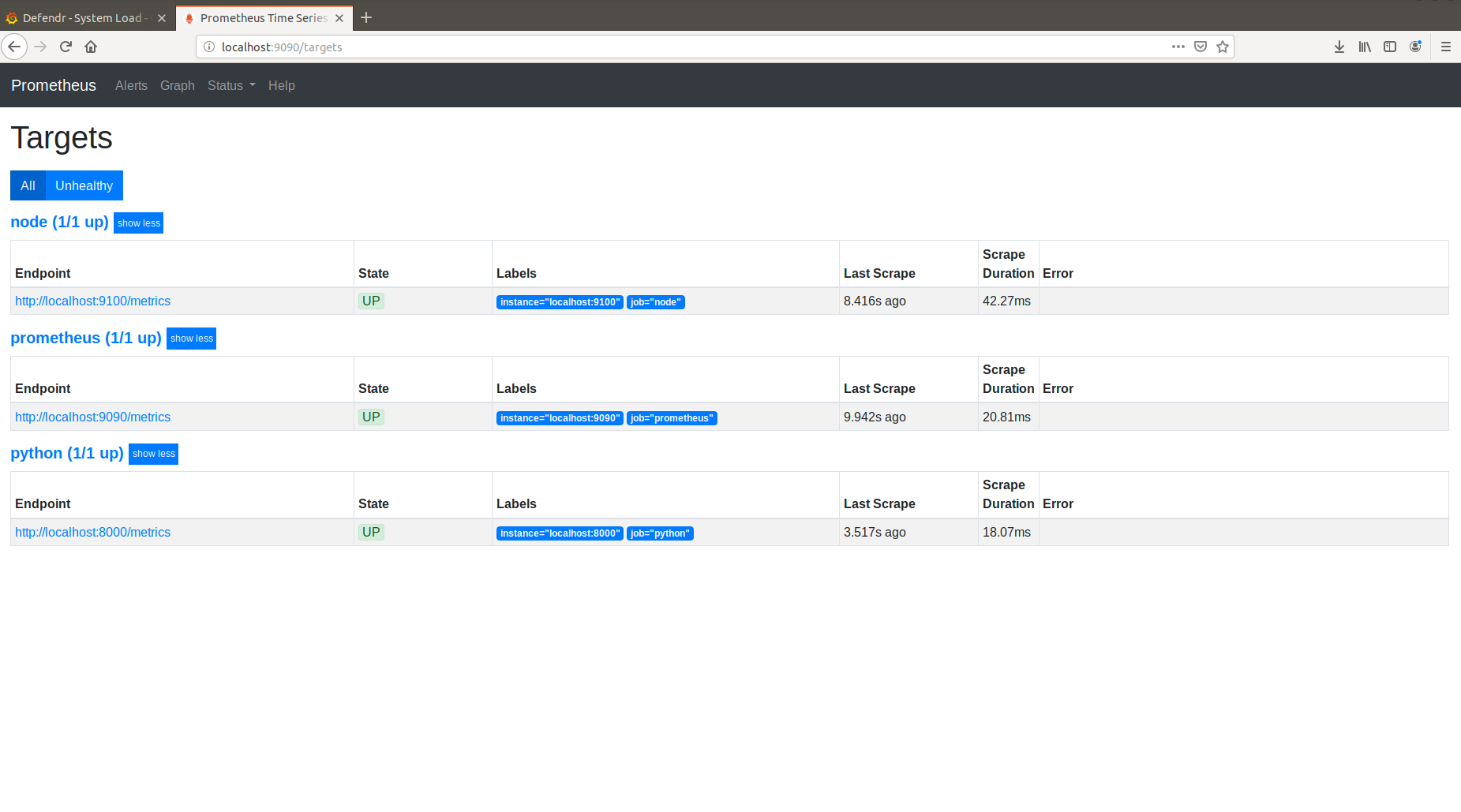
- Defendr – System Load

grf

grf

- Defendr – System Load (Expanded)



gr

* 1. Load balancing
  2. Adding backends

# Troubleshooting

In the unlikely event that the user is ever confronted with a terminal with the following issue,



The error can easily be fixed by navigating to the installation directory (default is /home/darknites/Defendr/) and opening the command line terminal in said directory. Simply then enter the command “sudo mount -t bpf bpf /sys/fs/bpf/” without the quotations and press enter. If confronted with a request for the user password, enter the server password obtained from the server admin and press enter.

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.