COS 301 CAPSTONE PROJECT

Denendr User Manual

Advance & Dark nITes

Ruslynn Appana

Jeandre Botha

Muhammed Carrim

Sisa Khoza

Christiaan Opperman



**Table of Contents**

|  |  |  |  |
| --- | --- | --- | --- |
| [1.](#page3) | [Introduction ....................................................................................................................................](#page3) | | [2](#page3) |
|  | [1.1.](#page3) | [System Overview.....................................................................................................................](#page3) | [2](#page3) |
|  | [1.2.](#page3) | [System Configuration ..............................................................................................................](#page3) | [2](#page3) |
|  | [1.3.](#page3) | [Installation ..............................................................................................................................](#page3) | [2](#page3) |
|  | [1.3.1 Dependencies .........................................................................................................................](#page3) | | [2](#page3) |
|  | [1.3.2 Dowload .................................................................................................................................](#page4) | | [3](#page4) |
| [2.](#page4) | [Getting started ................................................................................................................................](#page4) | | [3](#page4) |
| [3.](#page4) | [Using the System .............................................................................................................................](#page4) | | [3](#page4) |
|  | [3.1.](#page4) | [Sign in window ........................................................................................................................](#page4) | [3](#page4) |
|  | [3.2.](#page4) | [Home window .........................................................................................................................](#page4) | [3](#page4) |
|  | [3.3.](#page4) | [IP list window ..........................................................................................................................](#page4) | [3](#page4) |
|  | [3.4.](#page5) | [Log window ............................................................................................................................](#page5) | [4](#page5) |
| [4.](#page5) | [Troubleshooting ..............................................................................................................................](#page5) | | [4](#page5) |

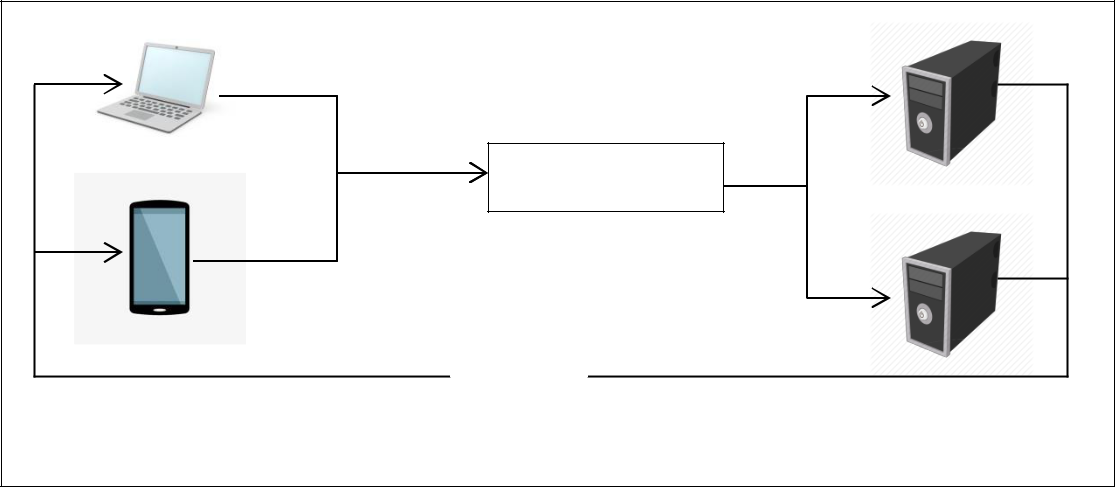
**1. Introduction**

**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**



|  |  |  |
| --- | --- | --- |
|  | 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.

**1.3. Getting Started**

1. The entire Defendr package can be found on <https://github.com/cos301-2019-se/Defendr.git>
2. Navigate into the root Defendr Folder
3. Open the terminal
4. Run the command: “chmod +x installcommands.sh”
5. Run the command: “./installcommands.sh”
6. Follow instructions on the screen

All that is left is to register as a user after the application starts up. After you register; Login and begin using the interface system.

In the unfortunate event that you have lost or forgotten your supplied credentials, please contact us at info@darknites.co.za

**3. Using the System**

**3.1. Sign in window**

This is the first window that the client will see. The client has to enter a username and password, which will then be checked against a Mongo database by retrieving the salted and hashed password for the specific username. If the user’s login was successful they will proceed to the home window of Defendr. The user will be able to close the application by clicking on the close button.

**3.2.** **Home window**

This is the main hub of the application, from here a user can navigate to the IP list window, logs window, matrix window or they will have the option to Log out.

**3.3.** **IP list window**

This window enables the user to see blacklisted IP addresses and add or remove blacklisted IP addresses from the list. It achieved these functions by using three different queries to the database, namely find, insert and delete respectively.

**3.4. 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).

**4. 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.