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)

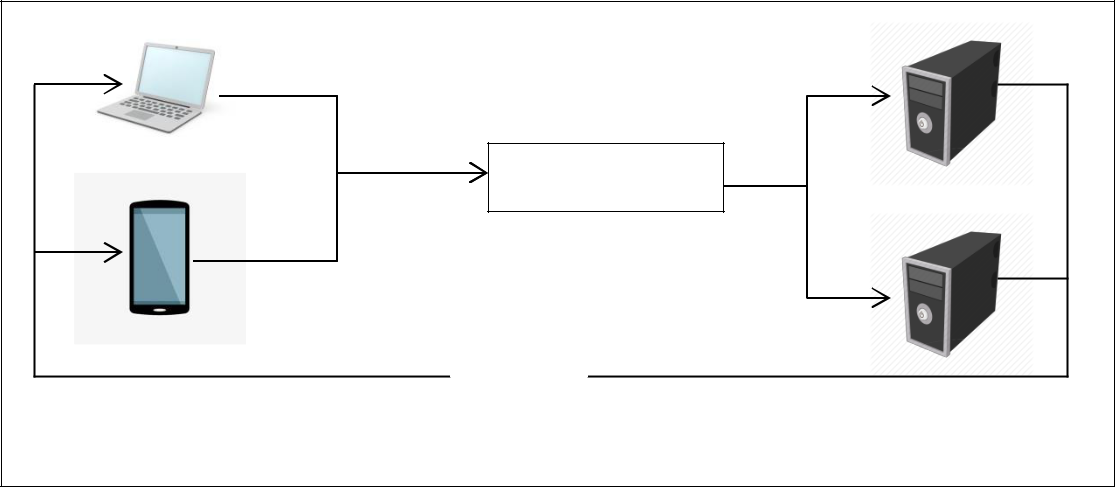
# Introduction

## 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.

# Getting Started

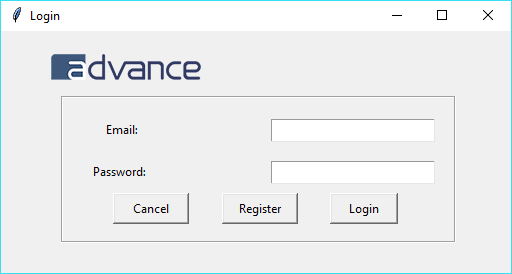
1. The entire Defendr package can be found on <https://github.com/cos301-2019-se/Defendr.git>
2. Navigate into the root Defendr Folder
3. Open the terminal
4. Run the command: “chmod +x installcommands.sh”
5. Run the command: “./installcommands.sh”
6. Follow instructions on the screen

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

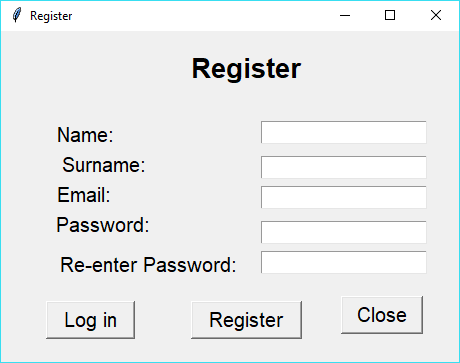
# Using the System

* 1. Sign in window

****

This is the first window that the client will see. The client has to enter an e-mail address and password, which will then be checked against a Mongo database by retrieving the salted and hashed password for the specific e-mail address. If the user’s login was successful, l they will proceed to the home window of Defendr. The user will be able to close the application by clicking on the close button. If there are no users currently registered, the user can click the register button, which will take them to the register window.

* 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, e-mail address, password and will also be requested to retype their password. Please note that the password must contain an upper- and lowercase character, as well as 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. 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.

* 1. 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, user management window or they will have the option to Log out. Note that only admin users can access the user management window.

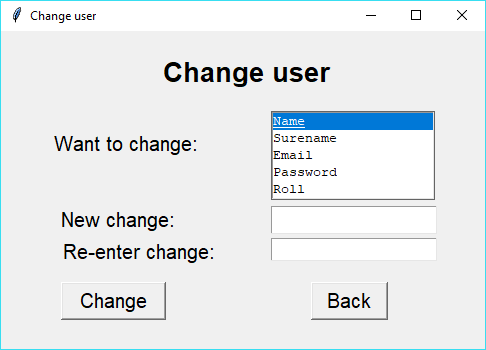
* 1. User Management window

This window has four main functions, namely adding a user, removing a user, changing a user 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 his/her name, surname, e-mail address, password and will also be requested to retype their password. Please note that the password must contain an upper- and lowercase character, as well as a symbol and a number. 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, which will direct them to the change user window. 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. It achieved these functions by using three different queries to the database, namely find, insert and delete respectively.

* 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).

# 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.