COS 301 CAPSTONE PROJECT

Denendr User Manual

Advance & Dark nITes

Ruslynn Appana
Jeandre Botha
Muhammed Carrim
Sisa Khoza
Christiaan Opperman

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

advance

Table of Contents

1. Introduction 2
  1.1. System Overview 2
  1.2. System Configuration 2
  1.3. Installation 2
    1.3.1 Dependencies 2
    1.3.2 Dowload 3
2. Getting started 3
3. Using the System 3
  3.1. Sign in window 3
  3.2. Home window 3
  3.3. IP list window 3
  3.4. Log window 4
4. Troubleshooting 4

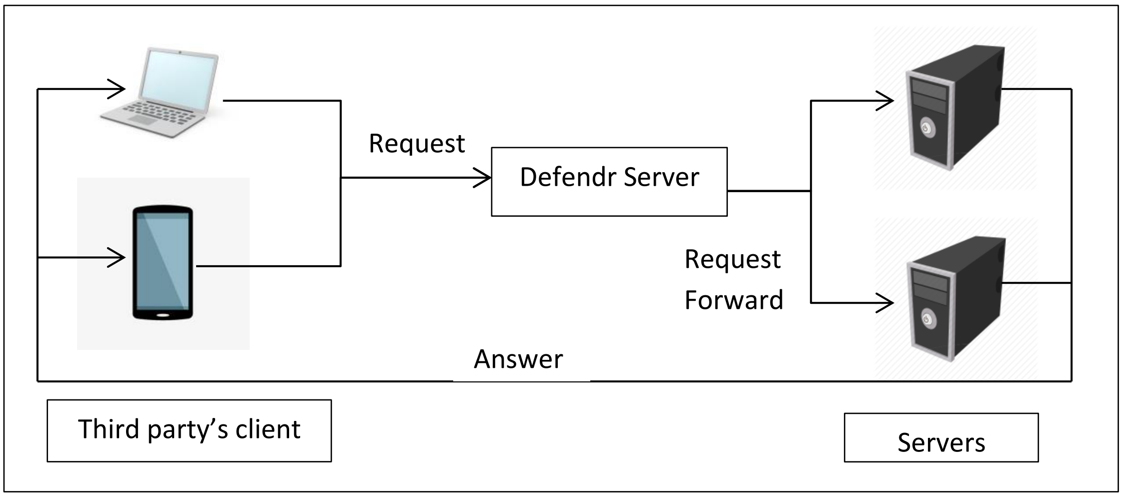
1. Introduction

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



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

1.3.1 Dependencies

If Installing Defendr on a new system for the first time follow the instructions below else go on to section 1.3.2.

Open the command line terminal anywhere on the system and enter and run the following commands to install all the necessary dependencies.

1. sudo apt install clang llvm libelf-dev
2. sudo apt install linux-tools-$(uname -r)
3. sudo apt install linux-headers-$(uname -r)

1.3.2 Dowload

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

The user can simply download the .zip file and extract in the directory of their choosing. That's it, you are done and Defendr is ready to defend your clients against ant attack. All that is left is to start up the application and log in with your issued credentials. In the event that you have lost or forgotten your supplied credentials please contact us at info@darknites.co.za

2. Getting started

The system's main point of entry for (graphical) use is via a front-fracing Python compiled user interface, as such it will be necessary to have Python installed on the machine.

To install Python, execute the following command as an (eleveated user):

sudo apt-get install python -y

To access the user interface, the following assumes that the you have downloaded "Defendr". In a termial, navigate to "Defendr/src/Interfaces" and executed the following py command:

python Home.pyc

The system makes use of networked resources as well, so the machine will need to have some networking interface (a network card) as well as an active internet connection.

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

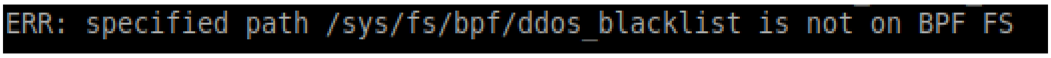
This window enables the user to see blacklisted IP addresses and add or remove blacklisted IP addresses from the list. It achieved these functions by using three different queries to the database, namely find, insert and delete respectively.

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,



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

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.