User Manual

For an Intrusion Detection System using a Neural Network

Version 1.0

Submitted in partial fulfillment of the requirements of the degree of MSE

Blake Knedler

CIS 895 – MSE Project

Kansas State University

Table of Contents

1 Introduction 3
2 Installation 3
2.1 System Requirements 3
2.2 Starting the IDS 3
3 Usage 4
3.1 Save Log 4
3.2 Load Weights 4
3.3 Save Weights 4
3.4 Set Accuracy 4
3.5 Toggle Notifications 4
3.6 Toggle Detailed Log 4
3.7 Train 4
3.8 Start 5
3.9 Stop 5
3.10 Print Packet 5
3.11 Clear Log 5
3.12 PyIDS GitHub 5
3.13 About 5
4 Output Messages 6
4.1 Training 6
4.2 Malicious Attack 6
5 Figures 7
5.1 Home Screen 7
5.2 File Menu 7
5.3 Settings Menu 9
5.4 Commands Menu 11
5.5 Help Menu 12
5.6 Outputs 13

1 Introduction

This document will be a user guide for the Intrusion Detection System (IDS). The IDS is a host-based system that will monitor network traffic aimed at detecting malicious intrusions. This means that the IDS is only responsible for aiding in the detection and notification of malicious attacks on the system of which it is being used. The IDS will not prevent attacks in any way nor will it aid in the detection on other systems. This document will explain the requirements for the system and how to use the system. It will also explain the basic usages and notifications of the system.

2 Installation

The IDS has a few requirements to be able to properly work on a host system. This section will explain the requirements for the IDS to work properly and how to start the system. The IDS may work with environments not described, but those environments are untested and are therefore not supported.

2.1 System Requirements

- Operating System
  - Windows 10
- Language
  - Python 3.5
- Drivers
  - WinPCAP
- Libraries
  - PyQt4
  - Numpy
  - Sklearn
  - Scapy

2.2 Starting the IDS

The IDS does not need to be compiled. This is because the language being used for the IDS is Python. The main reasons for using this language are the quick development speed of Python and the ease of portability to other operating systems if needed. This means that the application can be taken to other operating systems without much difficulty to get it to work. In order to start the application, the requirements need to be met by installing them. The libraries can be obtained using the pip method for python 3.5. Then to run the application the user only needs to run the PyIDS.py file in a python command prompt to start the application. The system may also be executed through an IDE such as Visual Studio and using the PyIDS project file.

3 Usage

3.1 Save Log

The save log option will save the detailed version of the log output to a specified file. To perform the save log option, the user should press the "Save Log" button to be prompted where to save and with what filename.

3.2 Load Weights

The load weights option is a viable option if the user has previously trained the system and saved the weights for that training. This option will allow the user to save time from having to always continually retrain the system every time it is started. To load the weights, the user must select the "Load Weights" option on the GUI. This will load the last set of saved weights and allow the user to bypass the training step.

3.3 Save Weights

The save weights option will save the current training weight information. This allows the user to save the current information to avoid continually training in the future. To save the weights, the user must select the "Save Weights" option on the GUI.

3.4 Set Accuracy

The set accuracy settings option will allow the user to change the minimum accuracy requirement when training the system. To change the accuracy, the user should go to the set accuracy option in the settings menu and increase or decrease the value.

3.5 Toggle Notifications

The toggle notifications setting option will allow the user to turn off/on the notifications in the system tray. To change this setting, the user should go to the toggle notifications option in the settings menu and select the option on/off.

3.6 Toggle Detailed Log

The toggle detailed log setting option will allow the user to turn off/on the detailed log output when the system is running. To change this setting, the user should go to the toggle detailed log option in the settings menu and select the option on/off.

3.7 Train

To begin using the IDS the user must first train the system. This is done by pressing the "Train" button on the Graphical User Interface (GUI). This may take some to train the system to meet the minimum level of accuracy. If the system is for some reason unable to meet the accuracy requirement after a given amount of time it will stop attempting to train and notify the user of the current accuracy. The user can then decide to accept that accuracy or attempt to train again.

3.8 Start

Once the system has been train either through loading weights or training, the user may then start the system. Starting the system will tell the system to begin monitoring network traffic and to attempt to determine if there are any malicious attacks. To start the system, the user must have previously trained the and press the "Start" button on the GUI.

3.9 Stop

If the system is running there will be an option to stop the system. This will essentially pause the system until the user chooses to start again. To stop the user must have previously started the system and then press the "Stop" button on the GUI.

3.10 Print Packet

The user has the option to print a single packet that was received. This option will print detailed information about the packet in the log output as well as creating a notification if the notification setting is turned on. To print a packet, the user should press the "Print Packet" button.

3.11 Clear Log

The user has the option to clear the current log screen. To perform this operation, the user should press the "Clear Log" button.

3.12 PyIDS GitHub

The user can directly go to the PyIDS GitHub page from the application. This will open the PyIDS GitHub webpage with the default web browser. To perform this action, the user should press the "PyIDS GitHub" button.

3.13 About

The user can request to see the about help option for the application. This about window shows the name of the application and the developer's name. To perform this operation, the user should press the "About" button.

4 Output Messages

There are several messages that the system will give to the user during different scenarios.

4.1 Training

When the system is training on the data, there will be a series of messages presented to notify the user of the current status of the training. These messages include:

- Reading Data Files
- Getting small dataset
- Getting large dataset
- Finished Initializing
- Beginning Training
- Computing dataset
- Calculating correctness
- Data Correct/Total: …

These will indicate the different steps within the training process. If the training is poor on the dataset, the user will notice this when the system gives the accuracy of the training performed in the last message.

4.2 Malicious Attack

The malicious attack messages are the one way a user can receive system notifications along with messages through the typical message notification system. These malicious attack notifications will alert the user that a suspicious packet has been noted and that the user should look into the packet. Information about the packet will also be displayed to the user. Since this system is using a Neural Network and these are known to not be 100% accurate. That is why it is on the user to investigate the packet data and take measures that they seem fit.

5 Figures

5.1 Home Screen

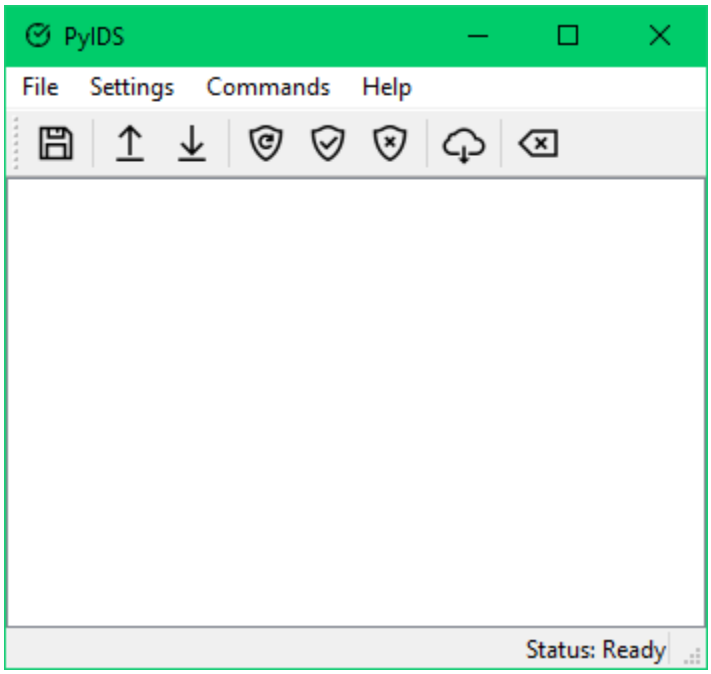

Figure 1. Startup Screen

5.2 File Menu

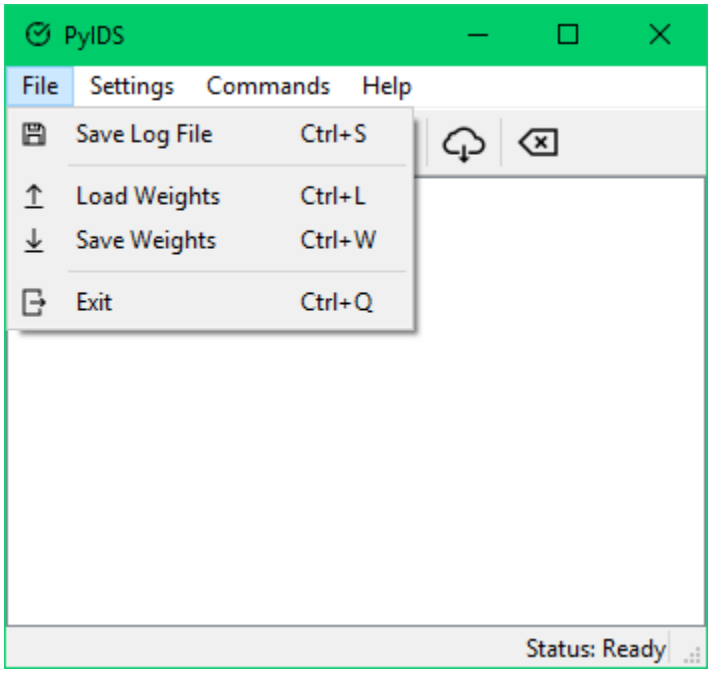

Figure 2. File Menu

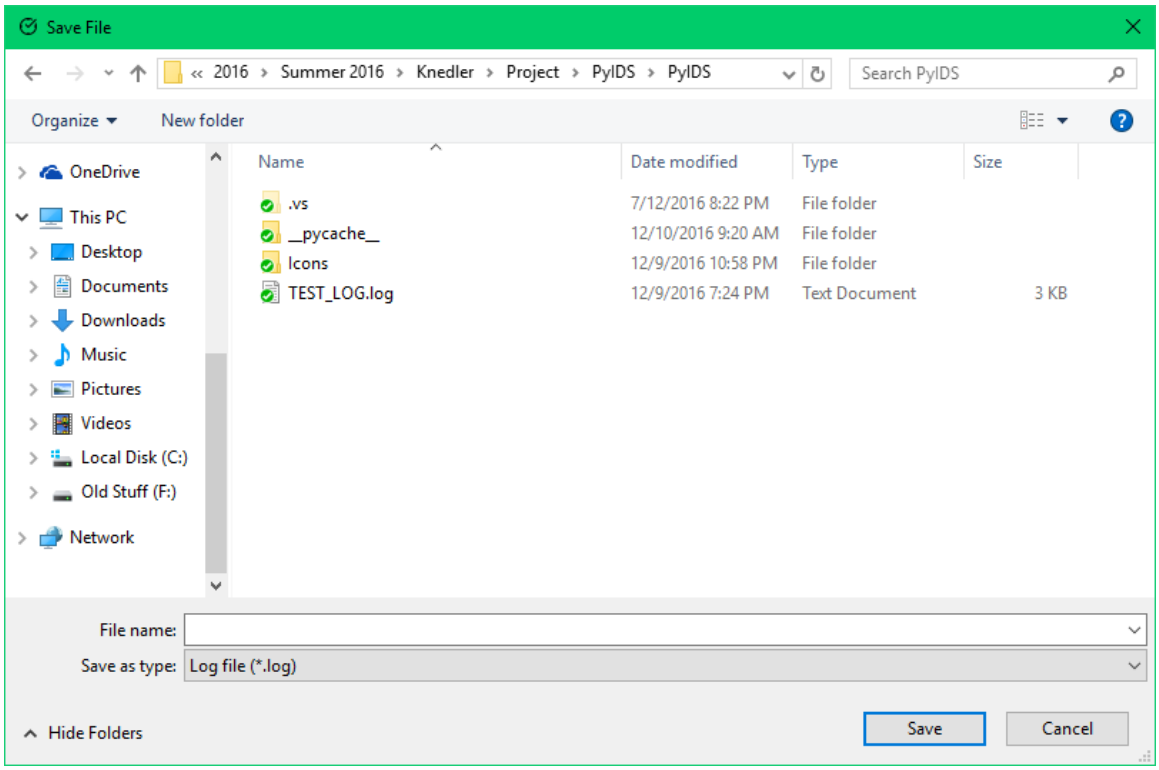

Figure 3. Save Log File Menu

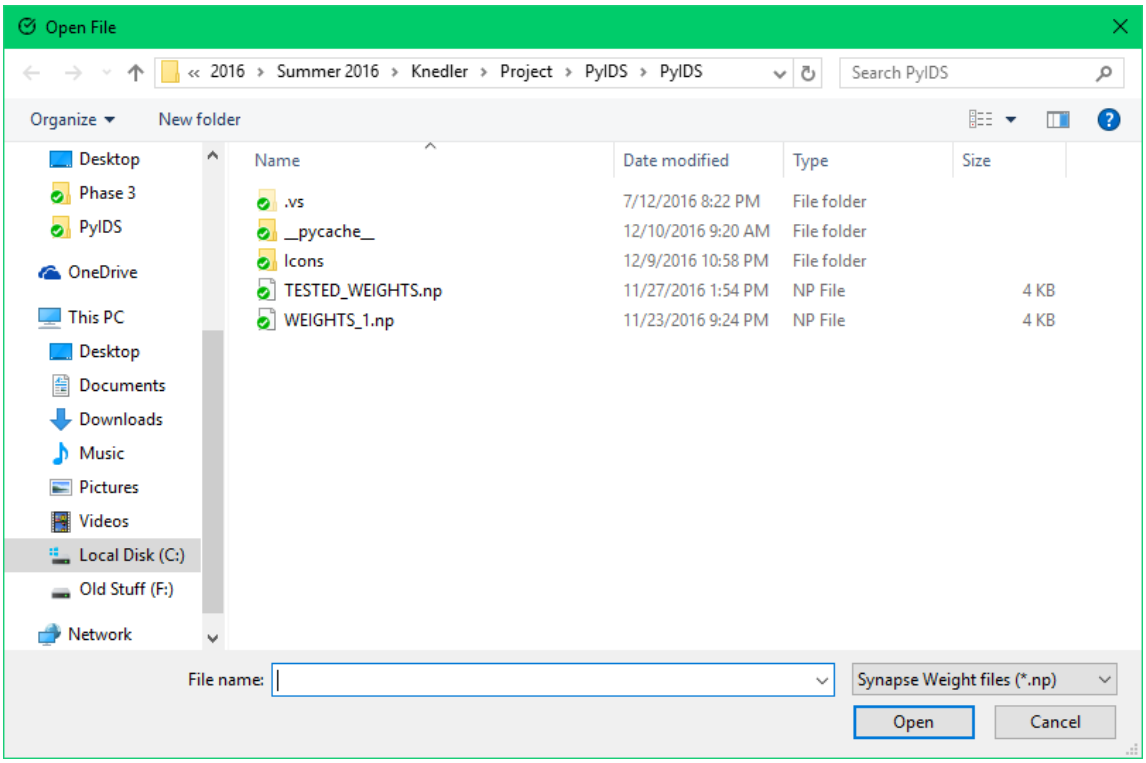

Figure 4. Load Weights Menu

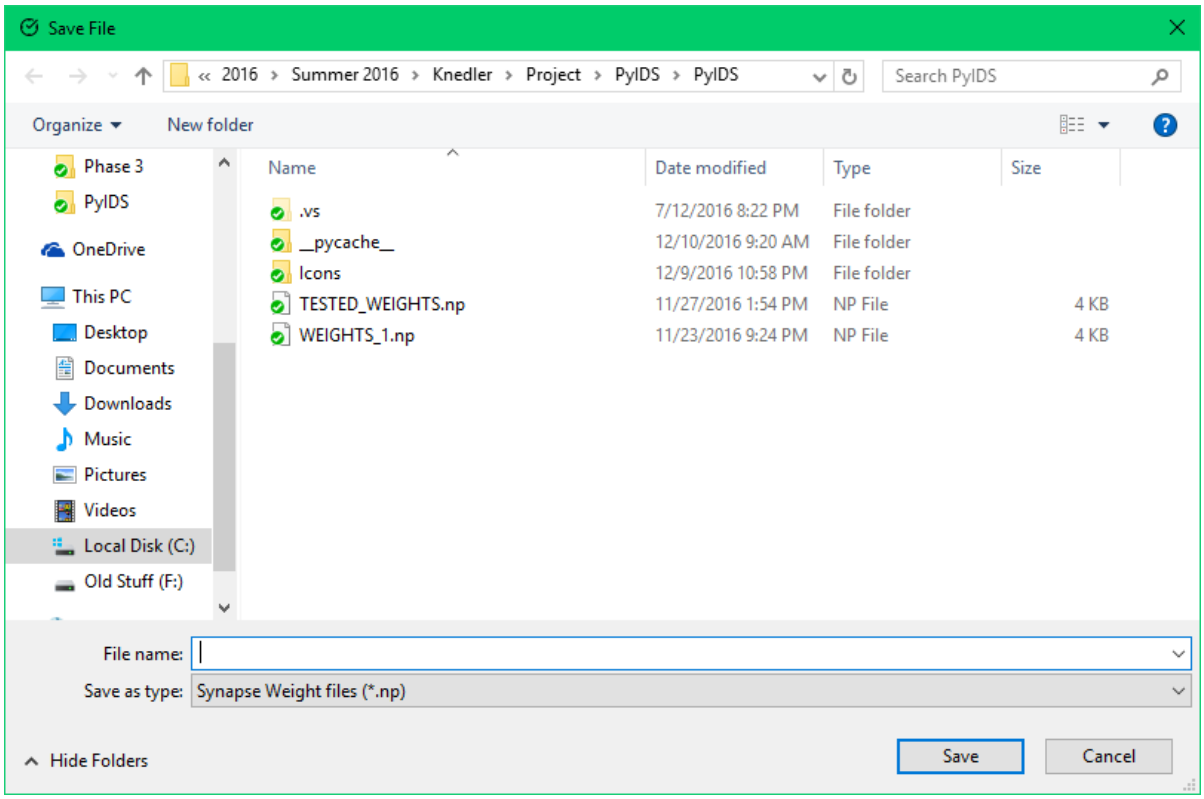

Figure 5. Save Weights Menu

5.3 Settings Menu

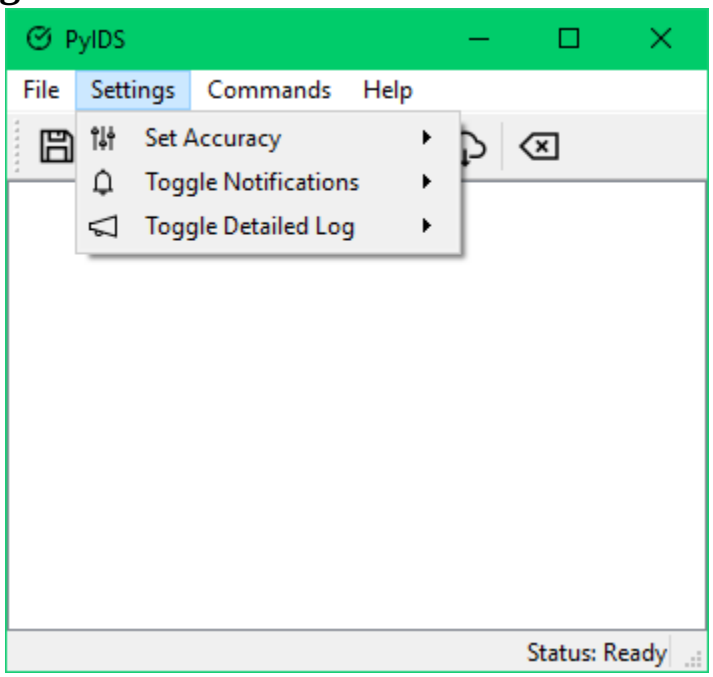

Figure 6. Settings Menu

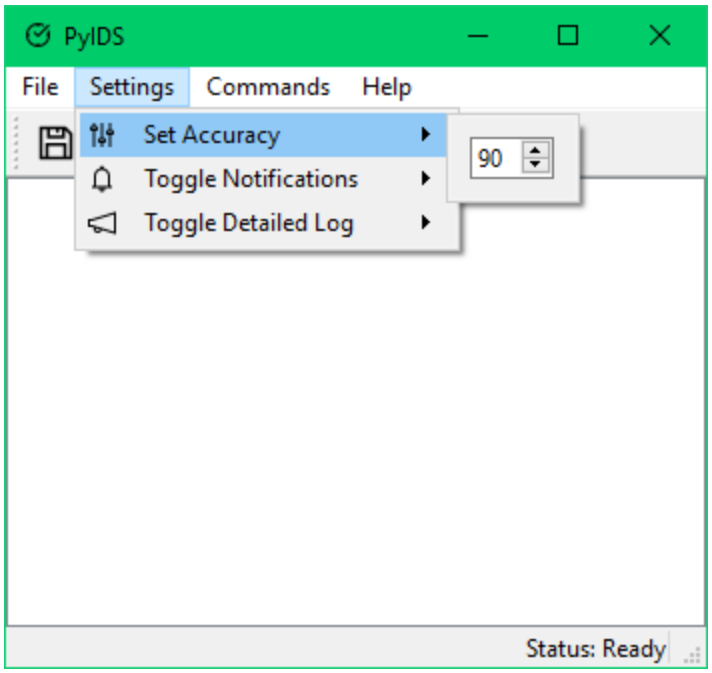

Figure 7. Accuracy Setting

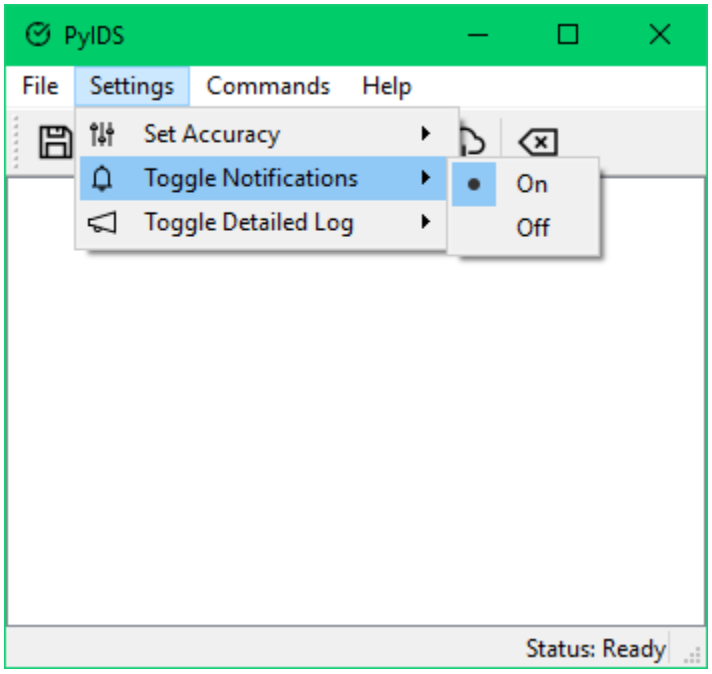

Figure 8. Toggle Notifications Setting

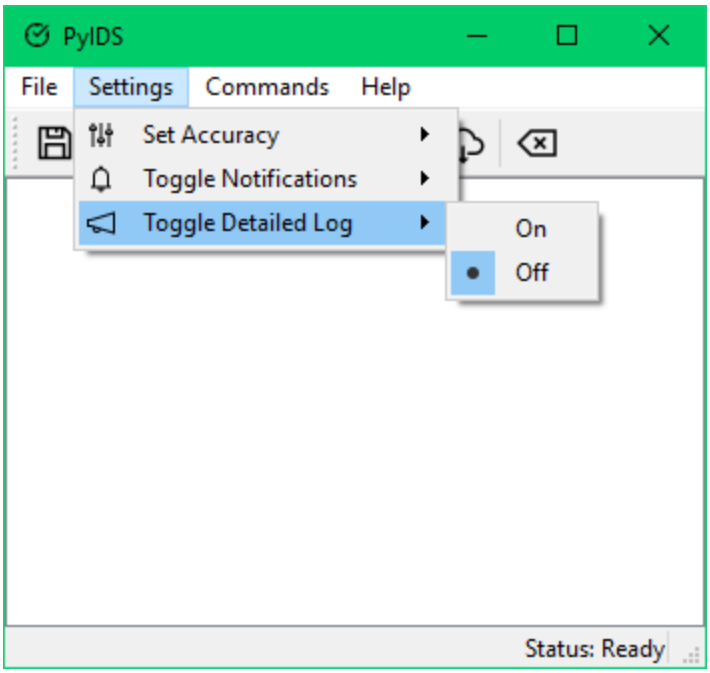

Figure 9. Toggle Detailed Log Setting

5.4 Commands Menu

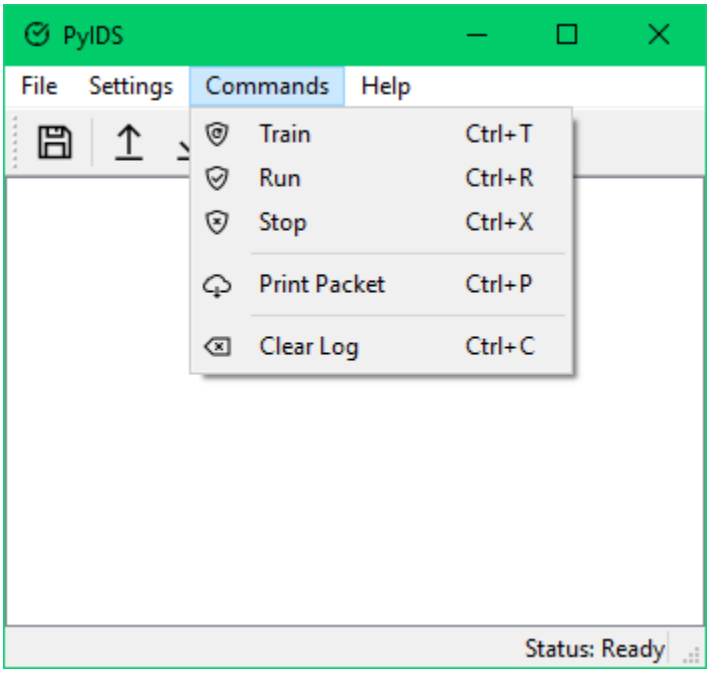

Figure 10. Commands Menu

5.5 Help Menu

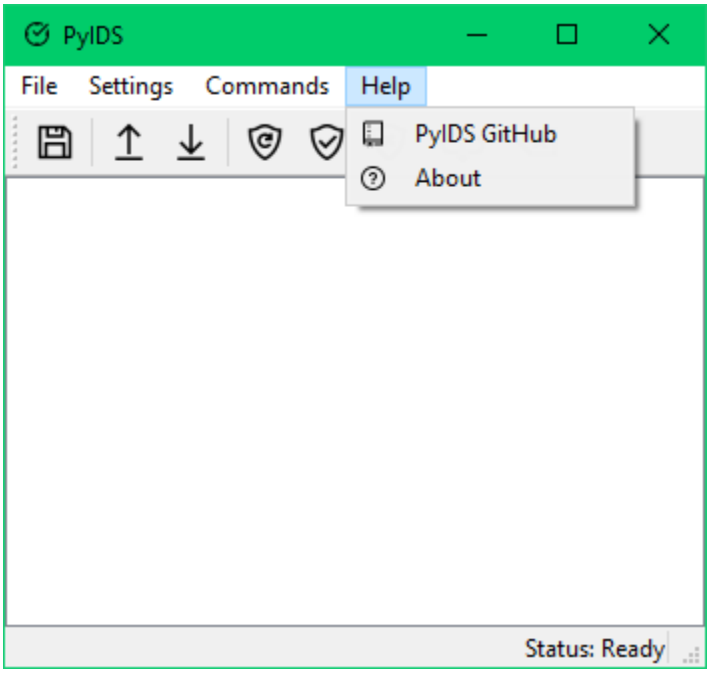

Figure 11. Help Menu

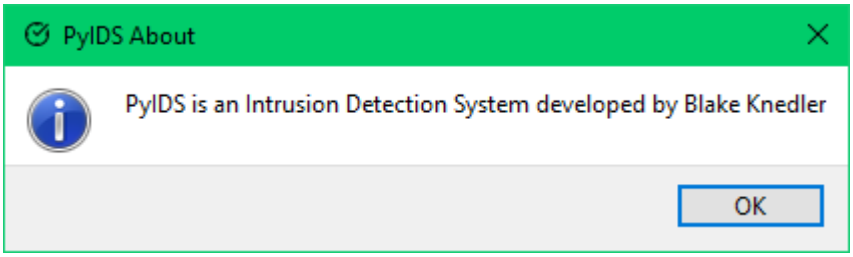

Figure 12. About Window

5.6 Outputs

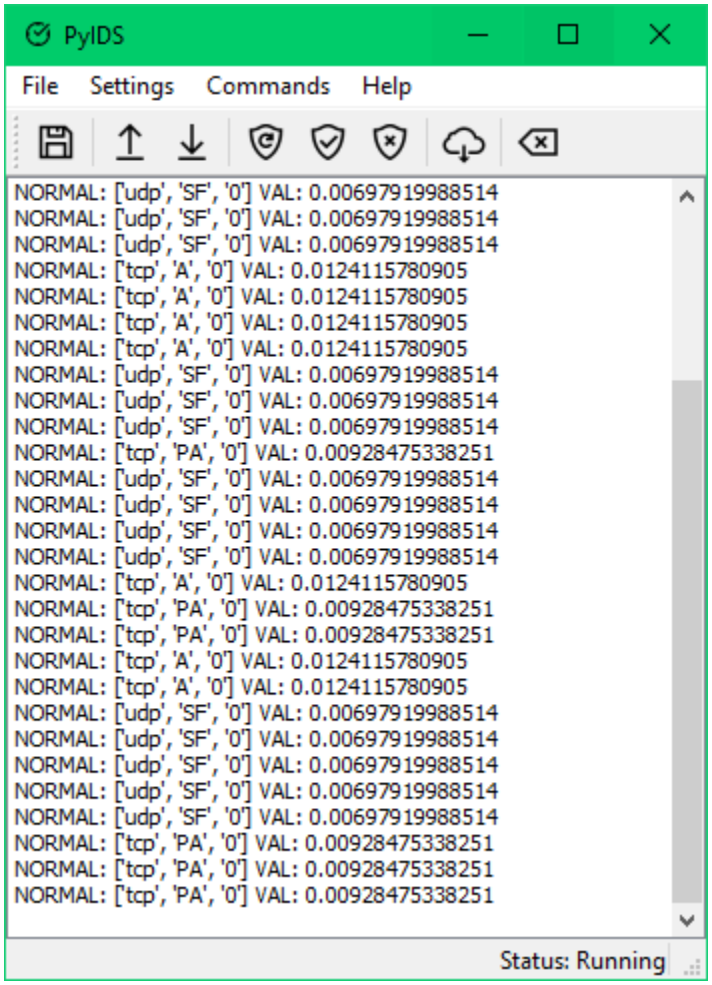

Figure 13. Home Screen Log Output Example

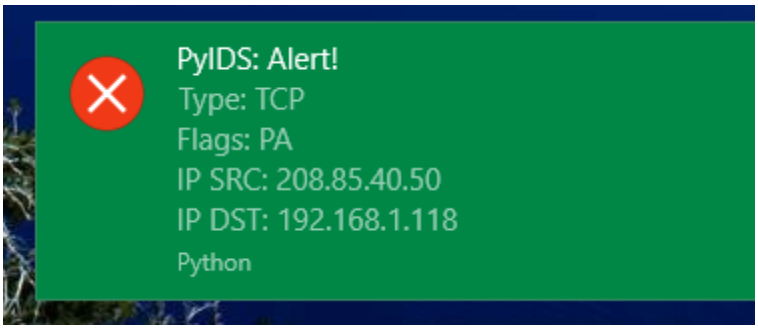

Figure 14. Notification Output