Note: This tool is meant to be used in conjunction with at least one honeypot from which you are gathering your data from. The data input cannot be simply data collected from a normal network, since the tool does not differentiate between attacks and regular connections. It treats every IP in the input data file as an attacker.

In this document, I will describe how to use the AIP algorithm tool. Since it is written in python, it is quite simple to set up for your system.

Requirements

1. A Linux based OS. I have used it on Ubuntu, Kali, Mint, PopOS, and Elementary.
2. Python 3.7+….. I have never tested it on an older version, so I am not sure. If you test it on an older version and it works, please let me know.
3. Python modules: **csv**, **operator**, **time**, **datetime** and **os** (all these are default so it should not be a problem).
4. An input data file collected from your honeypots in a format described below.

Steps

1. Download or git, and unzip the **AIP.tar.xz** file. This is the only file you need. It contains a copy of this document in PDF.
2. Copy the unzipped **AIP** folder to a directory of your choosing. This will be the directory where all the files will be stored, the network data will need to be imported to, and the blacklist files will be stored. In this example, I will use the directory **/home/awesome/AIP.**
3. You now need to go through the different files in the **AIP** folder and anywhere you see ‘**{something}**’ you need to replace the **‘something’** with the full path to the AIP directory. In our case, that means **/home/awesome/AIP.** For this, I usually use nano or vi, but any text editor will work. The files that need to be changed are as follows:
    - **AIP.py** - change the AIP-directory variable on line 22.
    - **Run-AIP.sh** - there should be only five lines in the file, and you need to change things on lines 2-5.
4. Everything should be ready to run for the first time.

The Input Data

In terms of file format for the input data, the program accepts a .csv file that has one IP per line, with each of the following data inputs for each IP on that line, separated by commas:

1. The IP address
2. Number of events - Meaning the total connections to your honeypots originating from the given IP
3. Total Duration - How long did this IP connect for the total of its events
4. Average duration - The average length in seconds of all the connections by this IP
5. Amount of Bytes - Total bytes sent and received by this IP
6. Average number of bytes - For bytes transferred in each connection by this IP
7. Total packets - Of all the connections by this IP
8. Average packets - Average packets sent per connection by this IP
9. Last event time - UNIX time of the last time this IP tried to connect to something in the last 24 hours

10. First event time - UNIX time of the first time the IP tried to connect in the last 24 hour

For example, a single line in the file could look like this:

"IPv4-Address", ”26049”, "7415310", "284.6", "41808957", "1605.0", ”284577”, "10.92", "157899154", "1578968762.519"

Copy your data file to the directory **/AIP/Input-Data/**, move to the **/AIP/** directory and then run the **Run-AIP** bash script:

```
./Run-AIP
```

Your blacklists will be in the **/AIP/Todays-Blacklists/** directory.

Useful Information

The tool is designed to be run once a day at a time of your choosing after copying the .csv file that contains the data from the last 24 hours to the Input-Data directory. If it is not run once a day, the rating system will be thrown off, but it will still work.

The Run-AIP script is designed to simply run the python script for AIP, and then copy the generated blacklist files to another location to be saved.