National College of Ireland

# Configuration Manual

MSc Research Project
Programme Name

Jasmine Killedar
Student ID: x19204663

School of Computing
National College of Ireland

Supervisor: Liam McCabe

**National College of Ireland**

**MSc Project Submission Sheet**

**School of Computing**

**Student Name:** ……Jasmine Killedar.
……

**Student ID:** ……x19204663……
……..……

**Programme:** …… **Year:** ……2021-2022
…

**Module:** …Cybersecurity……..……

**Lecturer:** ……
……..……

**Submission Due Date:** ……
……..……

**Project Title:** ……
……..……

**Word Count:** …… **Page Count:**
……..……..……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** ……Jasmine Killedar
……
……

**Date:** ……
……
……

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

| | |
|---|---|
| Attach a completed copy of this sheet to each project (including multiple | □ |

| | |
|---|---|
| copies) | |
| **Attach a Moodle submission receipt of the online project submission,** to each project (including multiple copies). | □ |
| **You must ensure that you retain a HARD COPY of the project**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | □ |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| **Office Use Only** | |
|---|---|
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

Configuration Manual

Jasmine Killedar
Student ID: x19204663

# 1 Introduction

In the given paper, application refers to unsupervised anomaly detection that is used to detect vulnerability in BGP. This Configuration Manual explains how to set up an application, including pre-requisites, installation instructions, and files for evaluating operations. It also includes any screenshots that are required.

# 2 Section 2

Following the installation of the software prerequisite, the programme will be ready to execute locally on the PC.

## 2.1 Software configuration

Following the installation of the software prerequisite, the programme will be ready to execute locally on the PC.

- Google Chrome
- Python 2.7.6
- Visual Studio Code
- GNS3 2.2.24
- VM version 0.11.1
- Wireshark

# 3 Section 3

Below is the source of Legitimate URL and network anomaly detection link

| Type of Dataset | Dataset | Source |
|---|---|---|
| Legitimate URL Links | https://github.com/kaggle/docker-python | Internet |
| Network anomaly detection link | Kaggle/input/network-anomaly-detection/Train.txt | Internet |

Unstructured dataset

# 4 Configuration steps

This section explains how to install and configure the programme on the computer to run the recommended solution:

### 4.1 Installing python and setting class path

- Python2.7 is used in the proposed solution. It is available for download at https://www.python.org/download/releases/2.7/ Once the Python version is installed, we must manually change the CLASS PATH on Windows.

- Python is installed by default on C Drive, therefore the CLASS PATH may be changed to C: python27, C:python27Scripts.

### 4.2 Installing IDE

- To run the python files, use Anaconda (Spyder/Visual Studio Code). ANACONDA includes both the applications Spyder and Visual Studio Code.

  To install anaconda: *https://docs.anaconda.com/anaconda/install/*

### 4.3 Installing GNS3

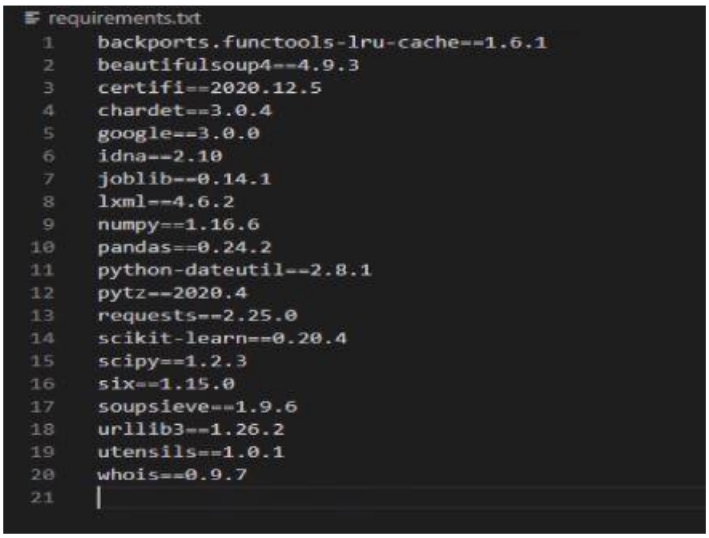
- To run network topology with router and switches use GNS3 2.2.24 https://gns3.com/software

### 4.4 Installing VM

- To install VM in order to run python in GNS3 https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

### 4.5 Installing project dependencies

- We're ready to install Python requirements to execute the application now that we've set up the necessary software and server. The steps for doing so are as follows:



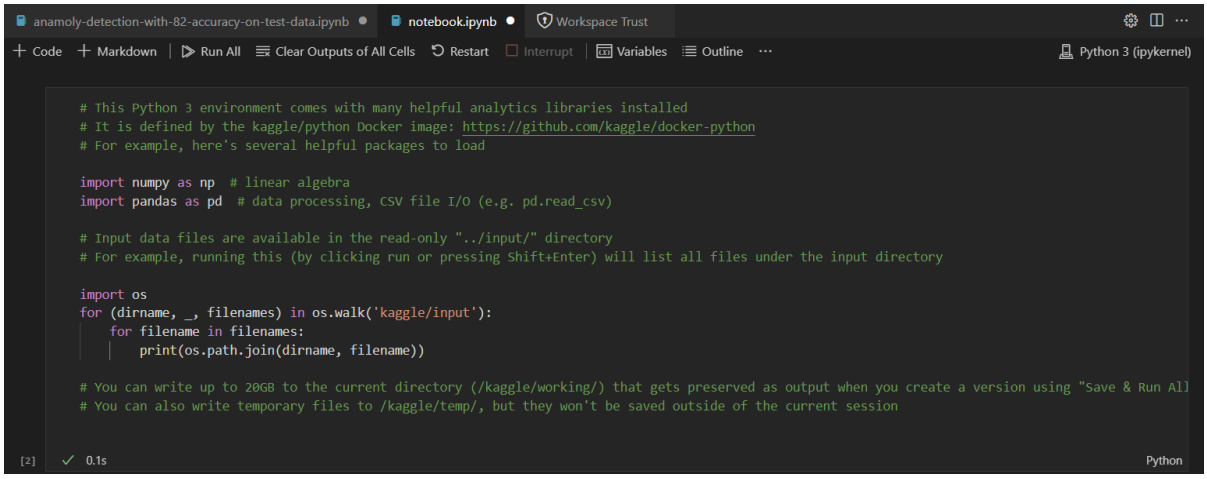
Python extensions

- Install all packages indicated in the ".txt" necessary to run the Python code using the console/cmd command pip install -r requirements.txt.
- By entering pip -V, you can keep pip up to date with Python27.

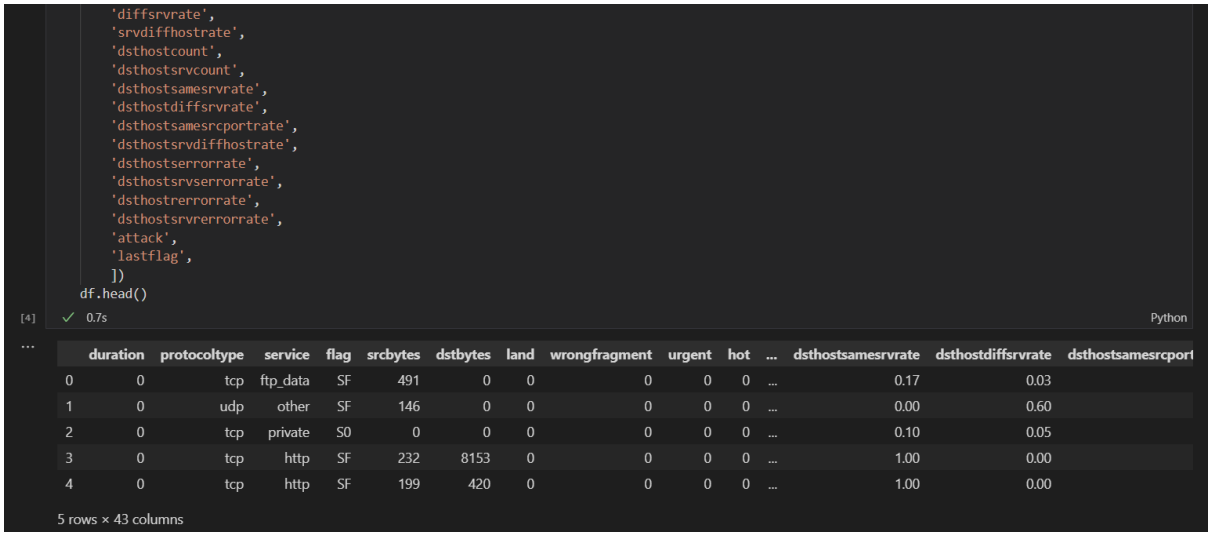
## 5. Setting up detection method on visual studio code

To detect the attacks in a BGP network follow the steps below.

- Load the code in the test file and train file in C drive on the system C:\Users\jasmi\kaggle\input\network-anamoly-detection
- Open the test folder in visual studio code and connect the jupyter-server in the CMD using the command jupyter-server , install python extensions and execute individual cells according the output will be displayed below the cells .



Network anomaly detection in visual studio



Output of a specific cell

```
df.select_dtypes(exclude=[np.number])
```

✓ 0.4s Python

| | protocoltype | service | flag | attack |
|---|---|---|---|---|
| 0 | tcp | ftp_data | SF | normal |
| 1 | udp | other | SF | normal |
| 2 | tcp | private | S0 | neptune |
| 3 | tcp | http | SF | normal |
| 4 | tcp | http | SF | normal |
| ... | ... | ... | ... | ... |
| 125968 | tcp | private | S0 | neptune |
| 125969 | udp | private | SF | normal |
| 125970 | tcp | smtp | SF | normal |
| 125971 | tcp | klogin | S0 | neptune |
| 125972 | tcp | ftp_data | SF | normal |

125973 rows × 4 columns

As we are focussing on Binomial Classification for this dataset, we can make all other classes other than normal as 'attack'

Output with protocol type and number of attacks occurred

## 6. Preventing attacks in BGP using GNS3

- Download GNS3 software and install VM inorder to configure devices using python

R3 R2 NetworkAutomation-1

```
  GNU nano 4.8


import getpass
import telnetlib


user = input("Enter your username:  ")
password = getpass.getpass()

for n in the range(72,77)
        HOST = "192.168.122." + str(n)
        tn = telnetlib.Telnet(HOST)

        tn.read_until(b"Username: ")
        tn.write(user.encode('ascii') + b"\n")
        if password:
                tn.read_until(b"Password: ")
                tn.write(password.encode('ascii') + b"\n")


        tn.write(b"end\n")
        tn.write(b"exit\n")



        print(tn.read_all().decode('ascii'))
```

Configuration of device using python

- Border gateway protocol is configured in each of the network devices in order to establish connectivity , to avoid Ddos attack and bgp prefix hijack attack MD5 and TTL-security configuration is configured so that any malicious activity or any hacker claiming trying to establish connectivity can be prevented or avoided

```
R2#sh bgp summ
BGP router identifier 10.10.14.4, local AS number 2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.12.5      4            3      27      27        1    0    0 00:22:38        0
```

BGP neighbour before TTL-Security command (up and running)

```
R2#sh bgp summ
BGP router identifier 10.10.14.4, local AS number 2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.12.5      4            3       0       0        1    0    0 00:00:16 Idle
```

BGP neighbour after TTL-Security command ( in an Idle state)

## 5 References


Dai, X. & Wang, N., 2019. *Application of machine learning*, s.l.: Journal of Physics: Conference Series 1176, 3.

H. K. Thakkar,, 2020. *Machine Learning Techniques for detecting BGP anomalies*, s.l.: School of Engineering Science faculty of applied science.

https://support.huawei.com/enterprise/en/doc/EDOC1, 2019. *NE40E V800R010C10SPC500 Configuration Guide - Security 01*, s.l.: HUAWEI.