

Configuration Manual

MSc Internship
Cyber-Security

Tanmay Nitin Shinde
Student ID: X18175830

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Tanmay Nitin Shinde
Student ID: X18175830
Programme: MSc in Cybersecurity **Year:** 2019-20
Module: Internship
Lecturer: Michael Pantridge
Submission Due Date: 17/08/2020
Project Title: Honeypots to detect malware and mitigate network traffic attacks using a Game Theory based approach

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.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: Tanmay Nitin Shinde

Date: 16/08/2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

| | |
|---|--------------------------|
| Attach a completed copy of this sheet to each project (including multiple copies) | <input type="checkbox"/> |
| Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies). | <input type="checkbox"/> |
| 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. | <input type="checkbox"/> |

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

Tanmay Nitin Shinde
Student ID: X18175830

1 Overview

The system is designed to detect, mitigate, and prevent DDOS attacks as well as detect any malicious file downloaded by the user. The implemented system does not have a graphical user interface and can be run using the command prompt on Ubuntu operating system. The output of the system is displayed on the same whenever the system detects an attack or whenever it detects a malicious file. The detection and mitigation of the DDOS attack is done by the game theory script and the prevention of it is done by the Iptables script. The malware detection part is done by the LaikaBoss Framework. This LaikaBoss Framework was integrated into our honeypot to scan the malicious files dynamically whenever the user downloads a file. Zeek IDS was also integrated into our honeypot to add another layer of protection for the system. When the honeypot is deployed Zeek IDS automatically starts monitoring the system. All the Zeek logs are stored for the admin to analyse them later.

2 Environment Setup:

The system has been designed and developed on the Ubuntu 18.04 LTS. It is developed in Python, shell scripts and MySQL.

OS Requirements: Ubuntu 18.04 or similar.

Python: Version 2 installed and version 3.6 or above installed.

MySQL: MySQL 8.0 installed.

Workbench : Version 8 installed.

2.1. Python Variables for Game Theory Script:

- I. Install pip3 variable of python.
- II. Download requirements.txt file and run the following command with sudo or root privileges.

```
pip3 install -r requirements.txt
```

2.2. LaikaBoss Setup:

For Installing LaikaBoss on Ubuntu, Run the following commands:

- I. **Install framework dependencies:**
apt-get install yara python-yara python-progressbar python-pip

```
pip install interruptingcow
```

II. Install network client and server dependencies:

```
apt-get install libzmq3 python-zmq python-gevent python-pexpect
```

III. Install module dependencies:

```
apt-get install python-ipy python-m2crypto python-pyclamd liblzma5 libimage-  
exiftool-perl python-msgpack libfuzzy-dev python-cffi python-dev unrar  
pip install fluent-logger olefile ssdeep py-unrar2 pylzma javatools  
wget https://github.com/smarnach/pyexiftool/archive/master.zip  
unzip master.zip  
cd pyexiftool-master  
python setup.py build  
python setup.py install  
wget https://github.com/erocarrera/pefile/archive/pefile-1.2.10-139.tar.gz  
tar vxzf pefile-1.2.10-139.tar.gz  
cd pefile-1.2.10-139  
python setup.py build  
python setup.py install
```

2.3. MySQL:

Install MySQL 8 Server and Workbench on the system from the following sites and setup the connection.

<https://dev.mysql.com/downloads/>

<https://www.mysql.com/products/workbench/>

2.4. Installation:

- I. Download and extract all the files from the zip and save them into a folder.
- II. Setup the connection between MySQL and python3.
- III. Edit the connection details in files attack.py, capture.py and gt.py.

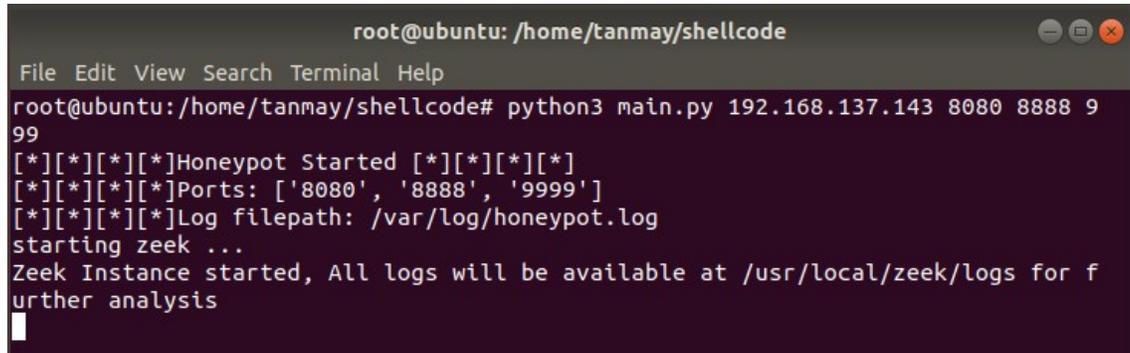
```
try:  
    mydb = mysql.connector.connect(  
        host="192.168.137.143",  
        user="tanmay",  
        passwd="██████████",  
        database="test_db"  
    )
```

- IV. Open MySQL WorkBench, copy and paste the queries from dbs.sql file and run it on WorkBench. The required tables and fields would be automatically created.

- V. For LaikaBoss, add or edit the required Yara rules, dispatch logic and the disposition file.

3 Using the System:

- I. Open the terminal where the system is setup.
- II. Run the main.py script with the parameters as ip address of the system and the ports to open for fake services to run on the honeypot. The honeypot will be deployed and will start monitoring the network activity to detect a DDOS attack and will also detect whenever a malicious file is downloaded.

A terminal window titled 'root@ubuntu: /home/tanmay/shellcode' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'python3 main.py 192.168.137.143 8080 8888 9999' and its output: '[*][*][*][*]Honeypot Started [*][*][*][*]', '[*][*][*][*]Ports: ['8080', '8888', '9999']', '[*][*][*][*]Log filepath: /var/log/honeypot.log', 'starting zeek ...', and 'Zeek Instance started, All logs will be available at /usr/local/zeek/logs for further analysis'.

```
root@ubuntu: /home/tanmay/shellcode
File Edit View Search Terminal Help
root@ubuntu:/home/tanmay/shellcode# python3 main.py 192.168.137.143 8080 8888 9999
[*][*][*][*]Honeypot Started [*][*][*][*]
[*][*][*][*]Ports: ['8080', '8888', '9999']
[*][*][*][*]Log filepath: /var/log/honeypot.log
starting zeek ...
Zeek Instance started, All logs will be available at /usr/local/zeek/logs for further analysis
```

Whenever a DDOS is detected, a popup window will appear which will display a warning of a DDOS attack, and the mitigation will take place. Also, when a user downloads a malware, that file will be automatically scanned by LaikaBoss and its output will be displayed on the honeypot's output terminal.

3.1. Evaluation:

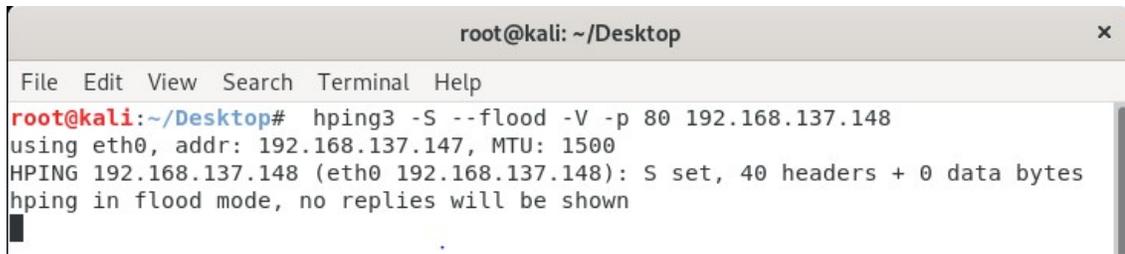
The system is evaluated by conducting various experiments on the system. The experiments were conducted by simulating a ddos attack to test the ddos detection and mitigation functionality as well as by downloading a malware to test the malware detection capability of the system.

We use two separate Kali Machines to attack. The DDOS attack was simulated by using the hping tool which is prebuilt in Kali.

Hping is the tool which allows us to set the size, quantity, fragmentation of packets which can be used to conduct a DOS attack. To conduct a DDOS, we use multiple attacking machines and attack a single target.

The following command was used to conduct the DOS attack. Just open the terminal and run the following command with root or sudo privileges.

sudo hping3 -S --flood -V -p 80 [ip_address]

A terminal window titled "root@kali: ~/Desktop" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command "hping3 -S --flood -V -p 80 192.168.137.148" being executed. The output indicates it is using eth0, address 192.168.137.147, MTU: 1500, and is in flood mode with 40 headers and 0 data bytes. The output ends with a period and a cursor.

```
root@kali:~/Desktop# hping3 -S --flood -V -p 80 192.168.137.148
using eth0, addr: 192.168.137.147, MTU: 1500
HPING 192.168.137.148 (eth0 192.168.137.148): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
.
```

For malware detection we pass a few malicious files and malware samples hidden inside zip files to our system. These malicious files will be hosted from the Apache server of the Kali Machine.

When a DDOS attack or a malicious file is detected, the output will appear on the honeypot's output screen.

References

- [1] lmco/laikaboss. Lockheed Martin, 2020 [Online]. Available: <https://github.com/lmco/laikaboss>. [Accessed: 10-Aug-2020]
- [2] Beloglazov and R. Buyya, "Openstack neat: a framework for dynamic and energy-efficient consolidation of virtual machines in openstack clouds," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 5, pp. 1310–1333, 2015.
- [3] D. G. Gomes, R. N. Calheiros, and R. Tolosana-Calasanç, "Introduction to the special issue on cloud computing: Recent developments and challenging issues," *Computers & Electrical Engineering*, vol. 42, pp. 31–32, 2015.