National College of Ireland

Configuration Manual

MSc Research Project
Cybersecurity

Kar Chun Goh
Student ID: 20102062

School of Computing
National College of Ireland

Supervisor: Niall Heffernan

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Kar Chun Goh
Student ID:	20102062
Programme:	Cybersecurity
Year:	2018
Module:	MSc Research Project
Supervisor:	Niall Heffernan
Submission Due Date:	20/12/2018
Project Title:	Configuration Manual
Word Count:	XXX
Page Count:	5

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:	
Date:	16th August 2021

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

Kar Chun Goh
20102062

1 Introduction

This configuration manual provides the detail of configuration regarding the research of Toward Automated Penetration Testing Intelligently with Reinforcement Learning. The configuration manual provides the detail about setting experiment environment, experiment environment configuration and any other relevant information. Since the experiment was conducted under Docker containerisation, hence the experiment should work with other platforms.

2 System specification

2.1 Hardware and Platform

The following list providing information about the platform and hardware that this research is using.

- Processor: 2.9 GHz Quad-Core Intel Core i7
- Memory: 16 GB 2133 MHz LPDDR3
- GPU: Radeon Pro 560 4 GB & Intel HD Graphics 630 1536 MB
- OS: MacOS 11.5.1

2.2 Relevant Technology

The following list provides information about the relevant technology that used in this research. It provides a reference while others redo or further investigate the research.

- Docker Desktop 3.5.2
- Docker Engine 20.6.4
- Nmap 7.7
- Python3-Nmap 1.5
- Kali 2021.06.08
- Msf 6.0.49
- Mini Conda 4.10.3
- Python 3.8.5
- Jupyter notebook 6.4
- numpy 1.20.2
- Pandas 1.2.4
- pymetasploit3 1.0.3
- Tensorflow 2.4.1

3 Environment Setup

3.1 Step 1

Since this research was conducted on Docker, hence Docker will require to install in advance. The information of installation show following link.

Link to install Docker in Window: Link

Link to install Docker in Mac: Link

3.2 Step 2

The following command was used to set up the docker environment for the research. Open terminal or command line and input the following command.

Listing 1: Container configuration

```
Create of subnet name msf
# docker network create --subnet=172.18.0.0/16 msf

Create a container for anaconda environment
# docker run -i -t --rm --network msf --name conda
-v "/Users/karl/Documents/research/notebook:/opt/notebooks"
-p 8888:8888 continuumio/miniconda3 /bin/bash \
-c "/opt/conda/bin/conda install jupyter -y --quiet && mkdir -p \
/opt/notebooks && /opt/conda/bin/jupyter notebook \
--notebook-dir=/opt/notebooks --ip='*' --port=8888 \
--no-browser --allow-root"

Create a conatiner for Kali Linux
# docker run --network msf --name kali --ip 172.18.0.7 --expose=5432
--expose=55553 --tty --interactive kalilinux/kali-rolling /bin/bash

Create a container for Metasploitatble
# docker run --network msf --name metaploitable --ip 172.18.0.9 -it
tleemcjr/metasploitable2:latest sh -c "/bin/services.sh && bash"
```

3.3 Step 3

Once the Kali Linux container is successful deployed, the following command could be used to install Metasploit Framework. In addition, the command used to deploy the Metasploit RPC daemon is shown below. After deployment, the daemon should similar to Figure 1.

Listing 2: Kali Linux Container configuration

```
Update Kali Linux environment
# apt update
# apt dist-upgrade -y
```

```
Install Metasploit Framework
# apt install metasploit-framework -y

Deploy Msfrpc Deamon on Kali Linux container with password 1234
# msfrpcd -S -P 1234 -n -f
```

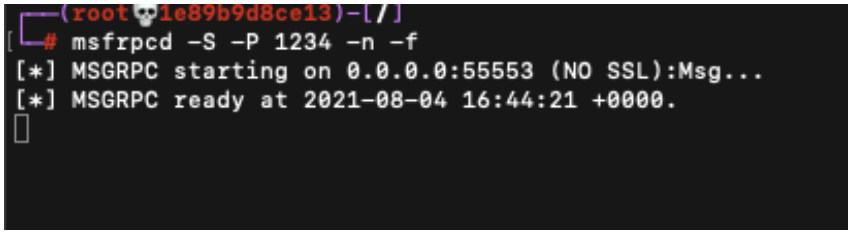

Figure 1: Msfrpc Deamon

3.4 Step 4

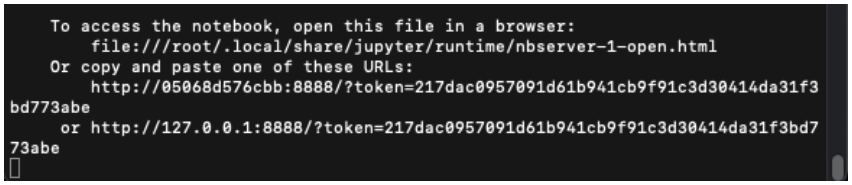

Figure 2: Terminal for access Anaconda interface

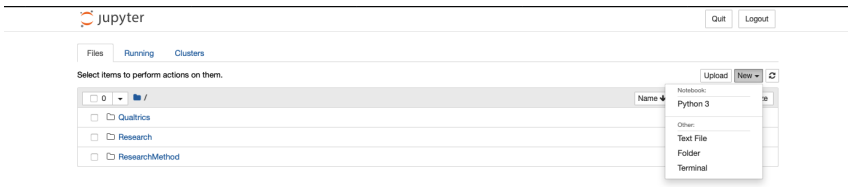

Figure 3: Anaconda interface

Figure 2 shows the Anaconda container was successful deploy and provide the URL to access the anaconda interface. If success to access anaconda interface, It should look similar to Figure 3. The next is to click the terminal to open a terminal window and install the following library and technology.

Listing 3: Anaconda container configuration

```
Pip may need to install in advance
apt install python3-pip

Install Nmap, Nmap3 Library, and pymetasploit3
# git clone https://github.com/wangoloj/python3-nmap.git
# pip3 install -r requirements.txt
```

```
# apt-get install nmap
# pip3 install --user pymetasploit3
```

Install other machine learning library

```
# conda install numpy
# conda install pandas
# conda install tensorflow
```

4 Execution

After all the containers have been successful deploy and configured, this section describes the execution of the research. The research will require installing Git in advance. Users require to download the necessary file from the Git repository of this research. Open Anaconda terminal (detail under Section 3 Step 4), input the following command:

Listing 4: Container configuration

Clone code from repository

```
# cd /opt/notebooks
# git clone https://github.com/KarChun0227/Master-research.git
```

After success to clone the files from the research repository. Navigate to the main interface of the Anaconda, and navigate to the "MasterResearch" folder. The folder should look similar to the Figure 4. The folder contains few files for various purposes. The filename "QTableNone" is a file for the experiment of testing without any algorithm assistance. The files name "QtableTraining" and "QtableTesting" for the experiment of training and testing the Q-learning algorithm, the file name "Qtable.pkl" storing the Q-table of this research. The files name "DeepQLearningTraining" and "DeepQLearningTest" for train and test the Deep Q-learning model. The files start will "DeepQmodel" storing the Deep Q-learning model data and parameter.

Figure 4: Master Research Folder

To execute any of the files, the user can open the file and navigate to kenal choose Restart and Run All, it shows in Figure 5. User may need to change the client's IP address (which IP address connect to Msfrpcd) and target machine's IP address (Metasploitable2 in this research), shown in Figure 6. The result will shows at end of the file after fully compile.

Figure 5: Master Research Folder

Q-learning Testing Enviroment

```
client = MsfRpcClient('1234', port=55553, server='172.18.0.7')
```

```
target = '172.18.0.9'
all_action = load_all_exploit()# + load_all_auxiliary()
console_cid = client.consoles.console().cid

```

Figure 6: Master Research Folder

5 Tips

- Make sure every containers are deployed under a same subnet.
- Make sure every containers able to connect each others.
- Make sure target's IP address are correct.
- Make sure every Libraries are installed.
- If problem of versioning, Section 2 has reference.
- Make sure Msfrpcd client's password, IP address and port is correct