DUBLIN CITY UNIVERSITY

ELECTRONIC AND COMPUTER ENGINEERING

EEXXX - Module Title

Assignment Subtitle

Author

Michael Lenehan   michael.lenehan4@mail.dcu.ie

Student Number: 15410402

XX/XX/20XX

Declaration

I declare that this material, which I now submit for assessment, is entirely my own work and has not been taken from the work of others, save and to the extent that such work has been cited and acknowledged within the text of my work. I understand that plagiarism, collusion, and copying are grave and serious offences in the university and accept the penalties that would be imposed should I engage in plagiarism, collusion or copying. I have read and understood the Assignment Regulations set out in the module documentation. I have identified and included the source of all facts, ideas, opinions, and viewpoints of others in the assignment references. Direct quotations from books, journal articles, internet sources, module text, or any other source whatsoever are acknowledged and the source cited are identified in the assignment references. This assignment, or any part of it, has not been previously submitted by me or any other person for assessment on this or any other course of study.

I have read and understood the DCU Academic Integrity and Plagiarism at `https://www4.dcu.ie/sites/default/files/policy/1%20-%20integrity_and_plagiarism_ovpaa_v3.pdf` and IEEE referencing guidelines found at `https://loop.dcu.ie/mod/url/view.php?id=448779`.

Signed: _____   Date: <u>XX/XX/20XX</u>

Michael Lenehan

Contents

Listings

1 Introduction

In order to extensively evaluate the impact of Distributed Denial of Service attacks, and the role which IoT devices play in modern DDoS attacks, simulations can be used. For the purpose of simulation, the "Mininet" network emulator is utilised. Mininet utilises the advantages offered by Linux containers. This allows for many hosts, running Linux kernel code and application code, to connect over a virtualized network.

2 Resources

The following resources were utilised in the completion of these simulations:

2.1 Hardware:

- HP Envy 17
    - Intel Core i7-6500U
    - 12GB RAM

2.2 Software:

2.2.1 Operating System:

- Manjaro Linux
    - Kernel Version 5.4.52-1-MANJARO
    - OS Type: 64-bit

2.2.2 Simulation Software:

- Mininet

– Version: 2.3.0d6

- Floodlight Controller

  – Version: 1.2

3 Denial of Service Simulation

For the initial Denial of Service simulation, the network topology is as shown in Figure 1. This network consists of an attacking traffic source (shown on the left), a legitimate user traffic source (shown on the right), and a server (shown on the bottom).
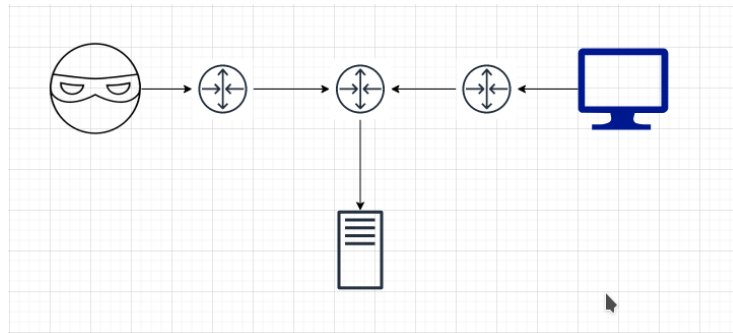

Figure 1: Denial of Service Network Topology

The initial attack type simulated is a Low-Rate TCP attack.

4 Distributed Denial of Service Simulation

For the Distributed Denial of Service simulation, an expanded version of the topology used in Figure 1, consisting of a significantly larger number of attacking sources is used. This reflects the increase in attackers, which is common in DDoS attacks involving IoT botnets.

5 Results

6 Reproduction

The following steps must be performed in order to reproduce the achieved simulations. As the Manjaro Linux distribution was used for these simulations, all package manager instructions will be given for Manjaro.

6.1 Mininet

Mininet must first be installed. This can be done according to the Mininet documentation **??**. For Debian based systems, Mininet can be installed via the "apt" package manager, using the command:

```
$ apt-get install mininet
```

Listing 1: Debian-based Distro Mininet Install

For Arch based distributions, Mininet may be installed using the Arch User Repository using the following command:

```
$ yay -S mininet-git
```

Listing 2: Arch-based Distro Mininet Install

To test the installation, execute the command:

```
$ sudo mn --test pingall
```

Listing 3: Mininet installation test

If the error "ovs-vsctl: unix:/run/openvswitch/db.sock database connection failed" occurs, the Open vSwitch must be started using the command:

```
$ sudo /usr/share/openvswitch/scripts/ovs-ctl
    start
```

Listing 4: Open vSwitch service start command

6.2 Floodlight OpenFlow Controller

The Floodlight OpenFlow Controller can be installed via GitHub**??**. For version 1.2
(as used for these simulation), the Java 8 development kit must be installed:

```
$ sudo pacman -S openjdk8-src
```

Listing 5: openjdk8 installation

Floodlight has a number of dependencies which can be installed via the following com-
mand:

```
sudo pacman -S git ant maven python-dev
```

Listing 6: Floodlight Dependencies

To download and build Floodlight, execute the following commands:

```
$ git clone git://github.com/floodlight/
    floodlight.git
$ cd floodlight
$ git submodule init
$ git submodule update
$ ant
# If the ant build fails, Floodlight can be built
    using Maven
$ sudo mvn package
```

Listing 7: Floodlight installation commands

6.3   Source Code

The source code for the simulations can be found on GitHub, and can be downloaded using the following command:

```
$ git clone git://github.com/
```

Listing 8: Source code download

7   Conclusion

A   Appendix