OntarioTech Business & IT

Final Project - Manual

MITS5200 G ADVANCED COMMUNICATION NETWORKS
(Prof: Shahram Heydari)

Network Denial of Service Detection Using SDN

Team:

Bimal Bhattarai (100796733)

Himangshu Das (100805968)

Samin Yasar (100796755)

Ranjeet Singh (100806699)

OntarioTech Business & IT

1. Prerequisites

I. Install Python
II. Install Mininet along with pox controller
    a) Mininet installation : http://mininet.org/download/
    b) pox controller
        a. Clone the repository : http://github.com/noxrepo/pox

Or

```
$ git clone git://github.com/mininet/mininet
$ cd mininet
$ git tag  # list available versions
$ git checkout -b mininet-2.3.0 2.3.0  # or whatever version you wish to install
$ cd ..
$ mininet/util/install.sh -a
```

2. Creating Test Environment

I. Download 100796733_100805968_100796755_100806699.zip
II. Copy the contents from custom folder to mininet/custom/*
III. Copy the content from forwarding folder to pox/pox/forwarding/*
IV. Enter the following command to run the pox controller:

```
$ cd ~pox
$ python3 ./pox.py forwarding.l3_edit
```

V. Now create a Mininet topology by entering the following command in another terminal: #This will launch a topology with 64 hosts and 9 switches

```
$ sudo mn --switch ovsk --topo tree,depth=2,fanout=8 --controller=remote,ip=127.0.0.1
```

VI. Now open Xterm for an host by typing the following command:

```
$ mininet>xterm h1
```

VII. In the xterm window of h1, run the following commands:

```
$ cd ~mininet/custom
$ python trafficLauncher.py –s 2 –e 65
```

VIII. Analyse the pox controller window in step IV
IX. Now open another Xterm window from h2

```
$ mininet>xterm h2
```

X. In the xterm window of h2 launch the attack using following commands

```
$ cd ~mininet/custom
$ python3 attackLauncher.py 10.0.0.7  # this will attack host h7
```

XI. Once the entropy value reached less than or equal to .5, the application will block the port.

Source Code used for reference: https://github.com/Anandkumar26/DDOSAttack_SDN