Manual for

SDN Based Threat Vector and Security Solutions

Contents

[1. Pre-Requirements for the experiment setup , Links and Manual to install. 2](#_Toc436860652)

[a. Mac OS, Windows with Ubuntu Operating System. 2](#_Toc436860653)

[b. Virtual Box or VMware virtual player 2](#_Toc436860654)

[c. Mininet network Emulator 2](#_Toc436860655)

[d. Installation of Python 3](#_Toc436860656)

[e. Installation of Scapy 3](#_Toc436860657)

[2. Creating the Test Environment. 4](#_Toc436860658)

[3. Steps to perform the experiment. 5](#_Toc436860659)

[I. Find the Threshold for usual Traffic(normal) 5](#_Toc436860660)

[II. Detection of DDoS threat using the value of Entropy 8](#_Toc436860661)

[4. Appendix 11](#_Toc436860662)

**List of Figures**

[Figure 1: Virtual machine 3](#_Toc436860681)

[Figure 2 : Scapy installation 4](#_Toc436860682)

[Figure 3:ssh the mininet 6](file:///C:\Users\amogh\Documents\my%20220%20doc.docx#_Toc436860683)

[Figure 4: Installing Pox controller 6](file:///C:\Users\amogh\Documents\my%20220%20doc.docx#_Toc436860684)

[Figure 5:Creating the topology 7](#_Toc436860685)

[Figure 6:Generating the traffic 8](#_Toc436860686)

[Figure 7: Entropy value 9](#_Toc436860687)

[Figure 8: Launching the attack 10](#_Toc436860688)

[Figure 9:Change in entropy value of controller 11](#_Toc436860689)

# 1. Pre-Requirements for the experiment setup , Links and Manual to install.

## a. Mac OS, Windows with Ubuntu Operating System.

The following experiment setup works better for almost all kinds of operating systems.

## b. Virtual Box or VMware virtual player

* Virtual box can be downloaded using the following link: <https://www.virtualbox.org/wiki/Downloads>

## c. Mininet network Emulator

* Ensure suitable version of Virtual Box is installed into your system.
* Download suitable version of mininet using the following link:

http://mininet.org/download/

* Open the virtual Box and click on import Appliance.
* Search for a ‘.ovf ’ extension of mininet and click on Ok.
* This process should install Mininet on the Virtual Box
* The following YouTube link should be useful for guiding one through the process of installing Virtual Box and Mininet:

https://www.youtube.com/watch?v=yNmv7GiHI KE

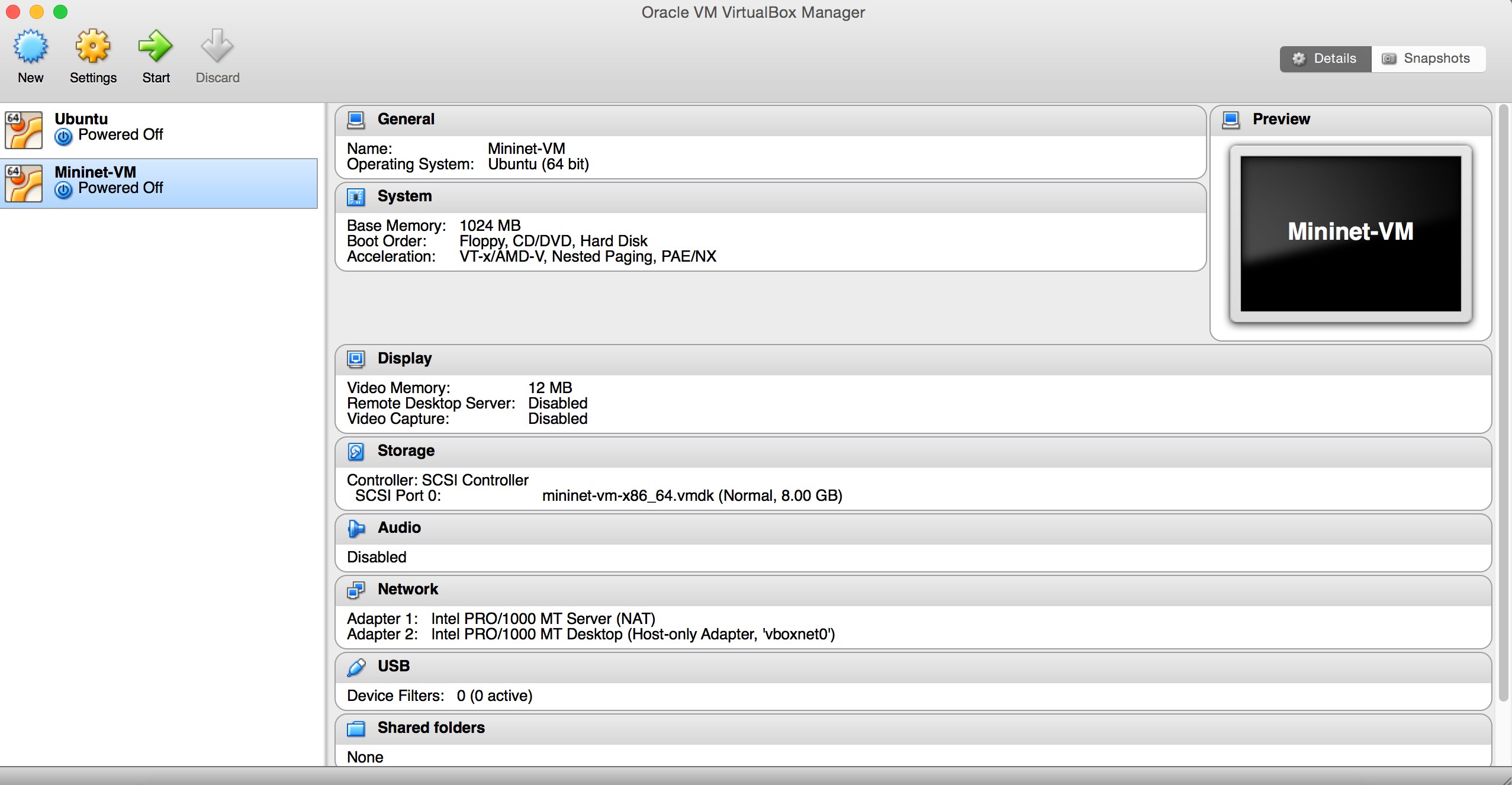
* On successful installation one can able to see the mininet on the virtual box as shown in the Figure-­‐ 1 below: 

Figure : Virtual machine

## d. Installation of Python

* Type the following command to check if python is installed on mininet:

$ python –V

* The above command should display the version of python.
* If python is not installed on the mininet, type in the following command to install it manually:

$ sudo apt-get install python

## e. Installation of Scapy

* Most recent versions of mininet comes with pre-­‐ installed versions of python and scapy
* To verify whether scapy is installed type the following command logging into mininet:

$ sudo scapy

You should be able to see an output as shown in the figure below:

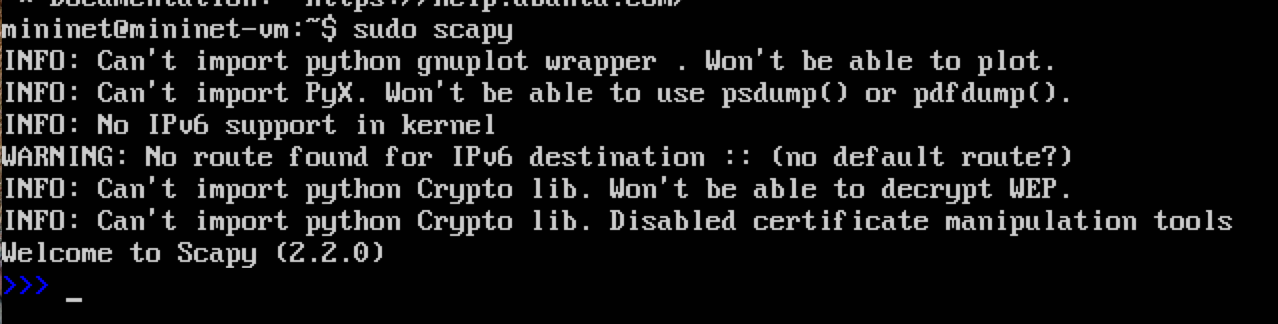


Figure : Scapy installation

* The above figure shows that the scapy has been pre-­‐ installed. If an error pops up, scapy has to be pre-­‐ installed manually.
* Type quit() to exit from scapy
* To install scapy manually type in the following command:

sudo apt-get install python-scapy

# 2. Creating the Test Environment.

a. Do a ssh to mininet from your local host giving the command:

$ ssh –X mininet@IPAddress

b. Create a new python script for normal traffic generation in the folder mininet/custom

$ cd mininet/custom

$ vim launchTraffic.py

c. Copy the contents of script traffic.py provided in the appendix of the manual and save the file.

d. Similarly repeat Step b and c to create an attack traffic file

$ vim launchAttack.py

e. Now go to the mininet in the virtual box and run the following commands:

$ cd pox/pox/forwarding

$ vim detection.py

f. Copy the contents of the detection.py script provided in the appendix into above file and save it.

g. now make copy of the l3\_forwarding module using the following command:

$ cp l3\_forwarding.py l3\_edited

Note: The above step can omitted if you prefer to edit the already existing pre-­‐installed l3\_forwarding module.

h. Once a copy is made, you must be able to see the same contents of l3\_forwading.py file in your newly created file. Now modify the file as shown in appendix and save it.

# 3. Steps to perform the experiment.

## I. Find the Threshold for usual Traffic(normal)

a. On successful setting up of the testbed, you should able to see a ssh window of mininet and mininet running on the virtual box as shown in the figure below:

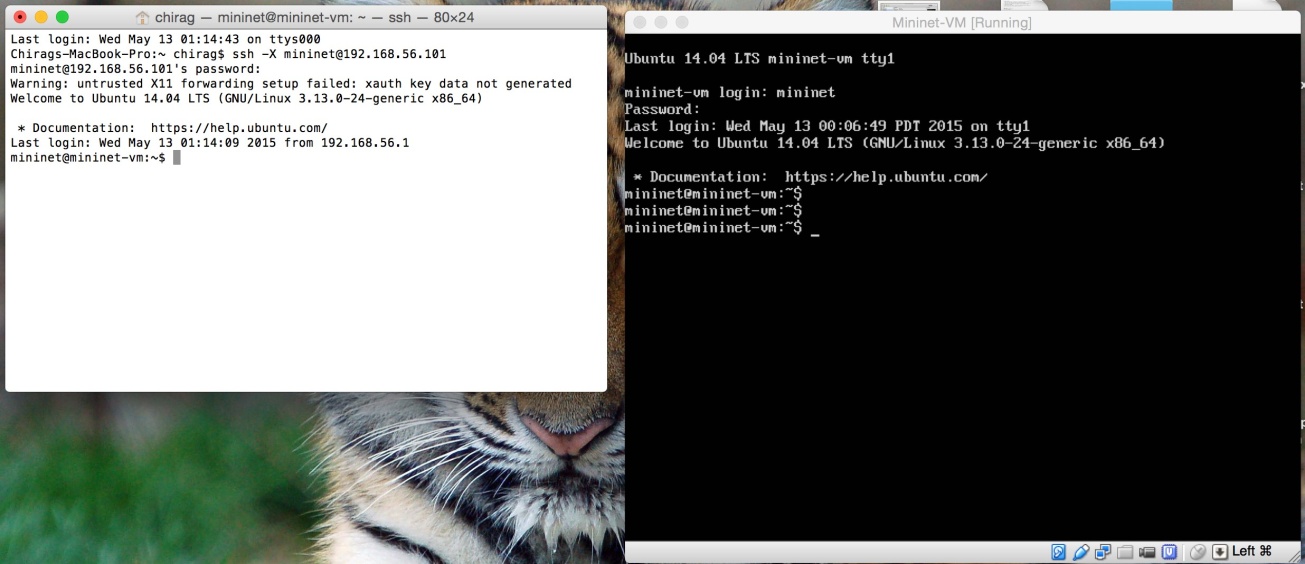
Change the image

Figure :ssh the mininet

b. In the mininet terminal of virtual box enter the following command to run the pox controller:

$ cd pox

$ python ./pox.py forwarding.l3\_edited

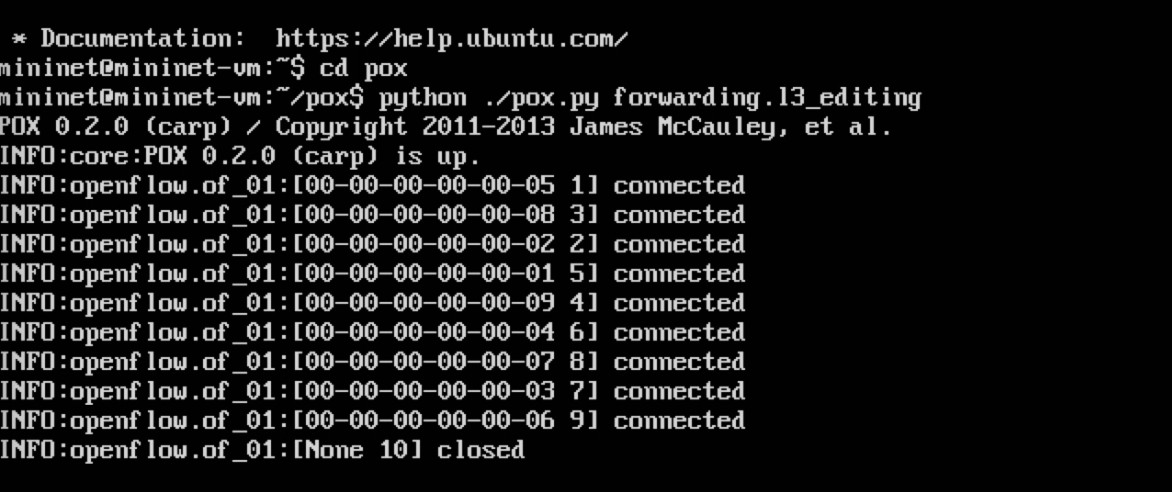


Figure : Installing Pox controller

c. Now create a mininet topology by entering the following command in the ssh window:

$ sudo mn --switch ovsk --topo tree,depth=2,fanout=8 -- controller=remote,ip=127.0.0.1,port=6633

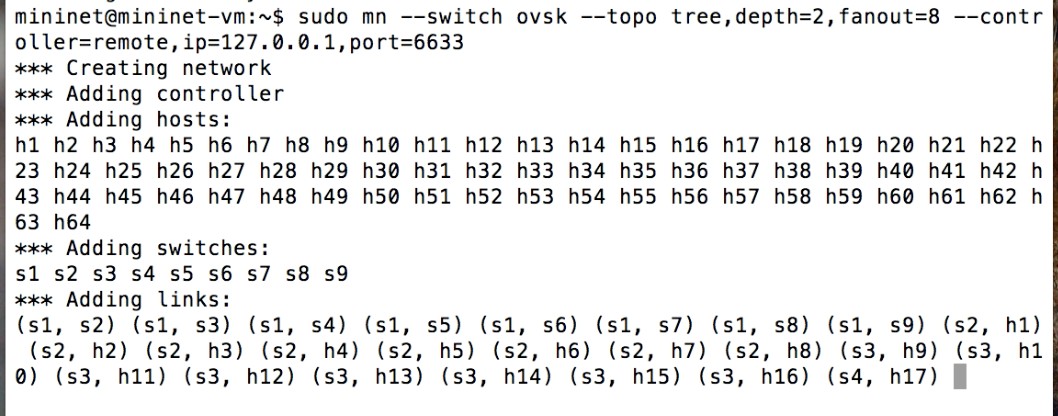


Figure :Creating the topology

Note: To determine the IP address of your pox controller

Enter the following command in the mininet of your virtual box:

$ ifconfig

The loopback address is your IPaddress in the above command.

d. Now open xterm for an host by typing the following command:

mininet>xterm h1 h2 h3 h64

e. In the xterm window of h1 run the following command:

# python traffic.py –s 2 –e 65

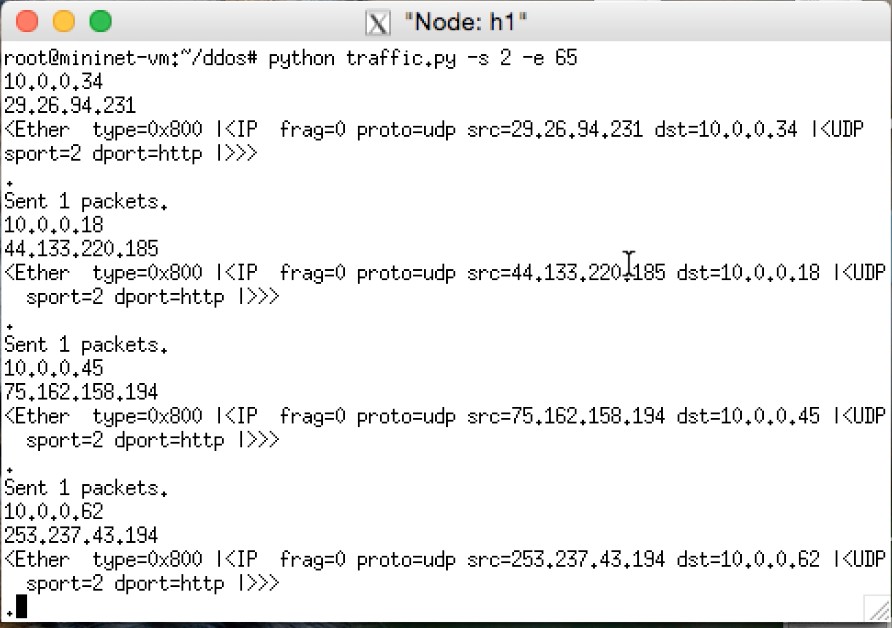


Figure :Generating the traffic

f. Now you should be able to see the pox controller generating a list of values for entropy as shown in the figure below. The least value obtained is the threshold entropy for normal traffic. To avoid false positives and negatives due to loss of a switch we choose an entropy value as 1.00 instead of 1.14. This implies 10% fault tolerance.

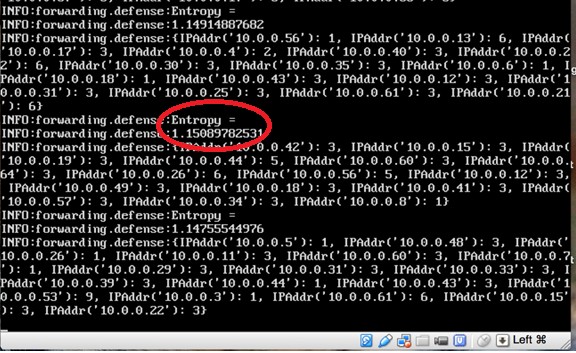


Figure : Entropy value

## II. Detection of DDoS threat using the value of Entropy

g. Now on xterm window of h64 enter the following commands:

# script h64.txt

# tcpdump –v

h. Now repeat step e on h1 and parallelly enter the following commands to run the attack traffic on h2 and h3 xterm windows:

# python attack.py 10.0.0.64

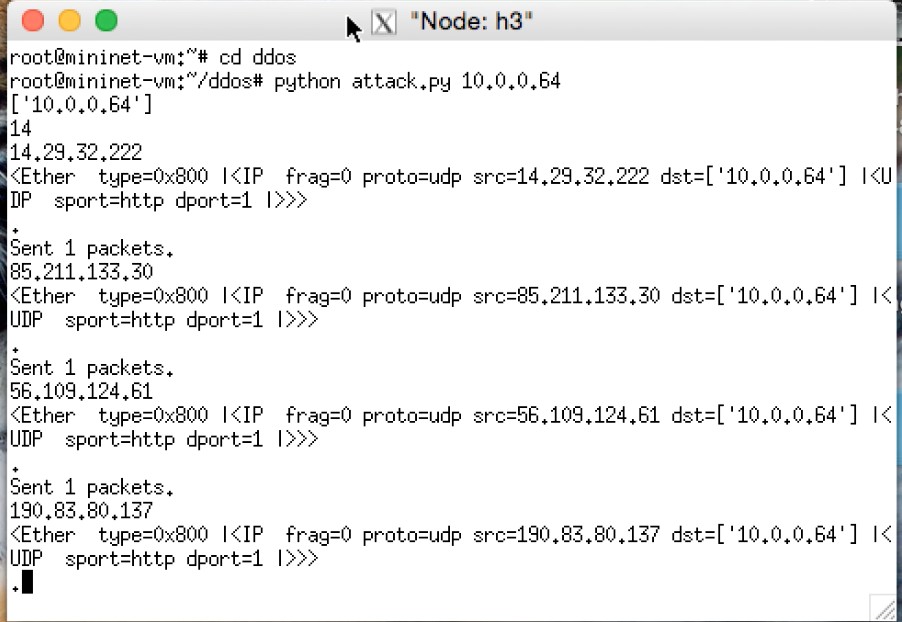


Figure : Launching the attack

i. Observe the entropy values in the pox controller. The value decreases below the threshold value for normal traffic as determined in step f (shown in the figure below). Thus we can detect the attack within the first 250 packets of malicious traffic attacking a particular host in the SDN network.

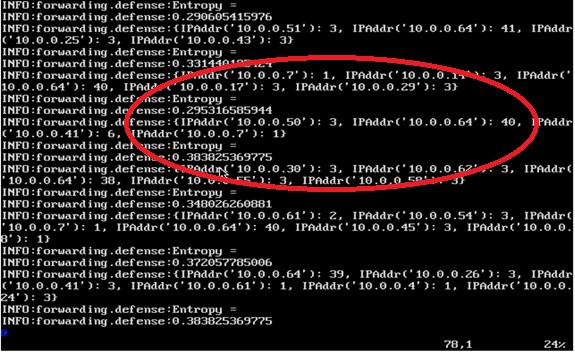


Figure :Change in entropy value of controller

j. On successful completion of experiment, terminate tcpdump on h64 by entering ‘control/command + c’

k. Stop running mininet topology by entering the following command:

mininet>exit

# 4. Appendix