Student Name: Marco Ermini  
Email: mermini@asu.edu  
Submission Date: 28th Jun, 2021  
Class Name and Term: CSE548 Summer 2021

Project Report 3: SDN-Based DoS Attacks and Mitigation

# Project Overview

In this lab I am emulating Denial of Service (DoS) attacks in an SDN networking environment. DDoS Attacks can target various components in the SDN infrastructure. I am setting up an SDN-based firewall environment based on containernet, POX controller, and Over Virtual Switch (OVS). To mitigate DoS attacks, I have developed a “port security” solution to counter the implemented DoS attacks.

In the lab I am implementing firewall filtering rules in order to implement the required firewall security policies, along with a sequence of screenshots and corresponding illustrations to demonstrate how I have fulfilled the firewall’s packet filtering requirements.

All the files and configurations used for this lab have been uploaded on GitHub; references are provided throughout the text and in the Appendix A at the bottom of the file.

# Network Setup

Since I have experienced some issues with connecting the VM to my lab through my host PC running Windows 10, I have chosen to set up the VM in VirtualBox in a bridged network configuration.

In this way, I could avoid configuring a static IP address to the VM and simply opted to fetch an IP for the VM via DHCP; this IP is then assigned directly to my router, which can be useful to troubleshoot eventual connectivity issues. On the Ubuntu/Linux side this has brought no issues whatsoever once the configuration commands are adjusted (e.g. use “dhclient br0” rather than assigning an IP address with “ifconfig br0”).

Because of the use of DHCP, depending on the lab run and when I restarted the VM, it may have assumed a different address in the 192.168.1/24 network. This does not affect the outcome of the lab exercises, but it may look inconsistent in the screenshots. Apologies about that.

Please find below the initial set-up of the virtual infrastructure as I have configured it in VirtualBox.

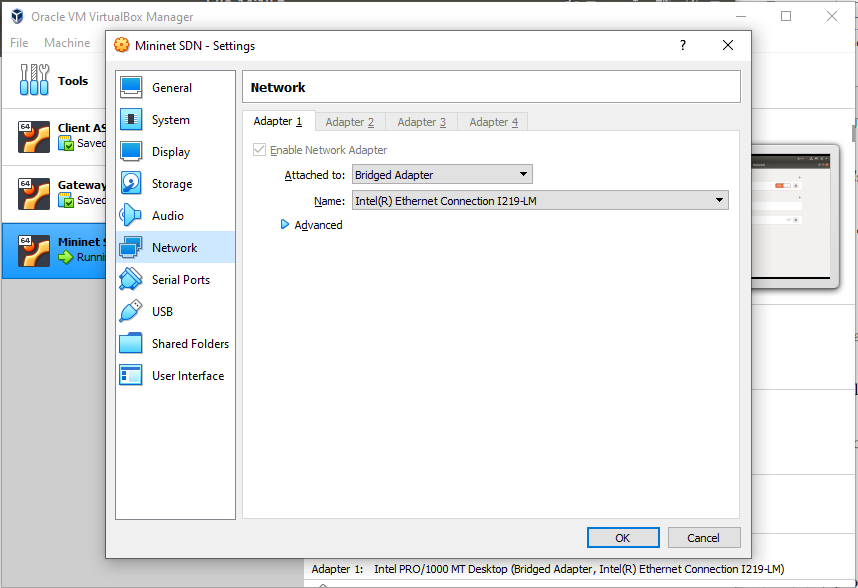


Figure - Bridged network setup in VirtualBox

# Software

For this first lab, the following software has been used:

* Various network tools (specifically: ping, hping3, and nping)
* POX (GitHub link: <https://noxrepo.github.io/pox-doc/html/>
* Open vSwitch: <http://www.openvswitch.org/>
* Open vSwitch Cheat Sheet: <https://therandomsecurityguy.com/openvswitch-cheatsheet/>
* Containernet: <https://containernet.github.io/>
* Containernet tutorial: <https://github.com/containernet/containernet/wiki/Tutorial:-Getting-Started>

# Project Description

In this assignment, I have executed the various labs assignments, obtaining the proofs that they have been successfully completed.

.

## Setting up mininet and Running mininet topology

I have created a script to execute the mininet command line, since I need to restart it several times for troubleshooting purposes. The script “*runlab3.sh*” is produced in GitHub and reported here:

mn --topo=single,4 \

--controller=remote,port=6655 \

-i 192.168.2.10 \

--switch=ovsk --mac

mn -c

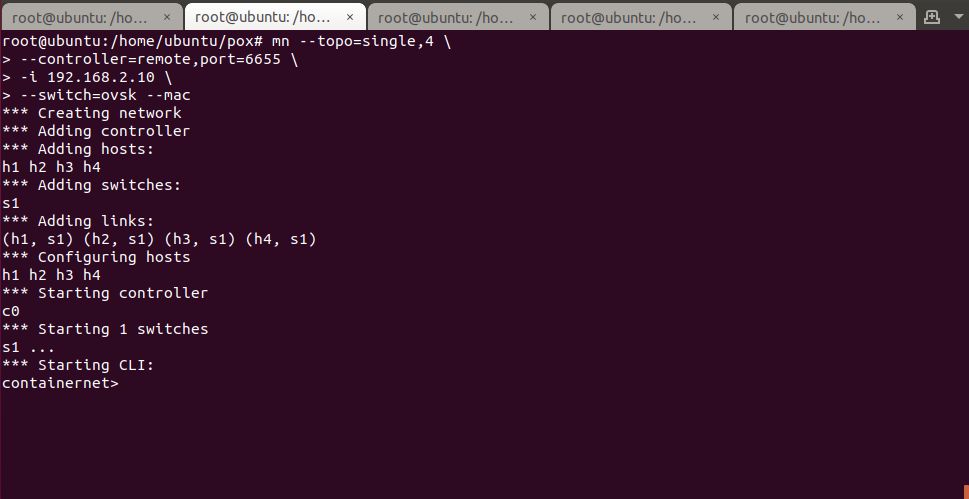


Figure – Running mininet

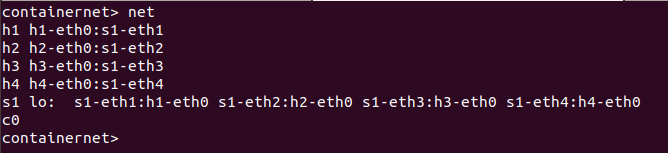


Figure - Mininet network

## Should assign IP addresses to hosts.

I have executed this again using a very simple source script called “lab3ips.sh” and executed from the mininet CLI with the command “*source lab3ips.sh*”. The script is referenced in GitHub and reproduced here:

py h1.setIP('192.168.2.10/24')

py h2.setIP('192.168.2.20/24')

py h3.setIP('192.168.2.30/24')

py h4.setIP('192.168.2.40/24')

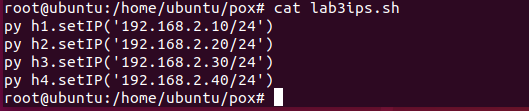


Figure - Setting IP addresses for the lab

Screenshot showing the IP addresses changed:

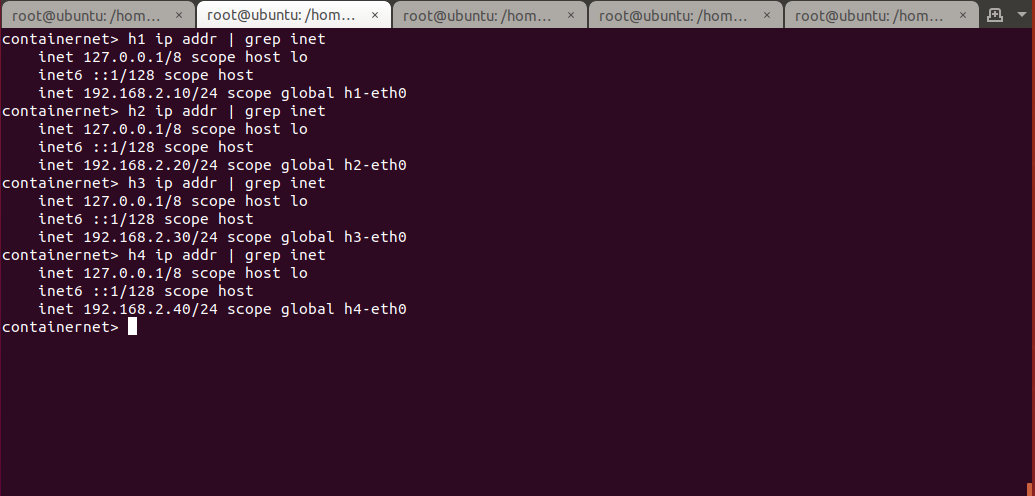


Figure - Checking IP addresses for the containers in the lab

## Perform Flood attack on SDN controller following a suggested procedure:

### Run l3 learning application in POX controller.

I have again used a simple script to allow executing multiple times as needed in an easier manner. The script “*run\_pox3.sh*” is on GitHub and reported below.

Please notice that I set the log level to “DEBUG” in order to work more effectively on the software by inserting debug comments in the code.

set -x

sudo ./pox.py openflow.of\_01 \

--port=6655 pox.forwarding.l3\_learning \

pox.forwarding.Lab3Firewall \

--l2config="l2firewall.config" \

--l3config="l3firewall.config" \

log.level –DEBUG

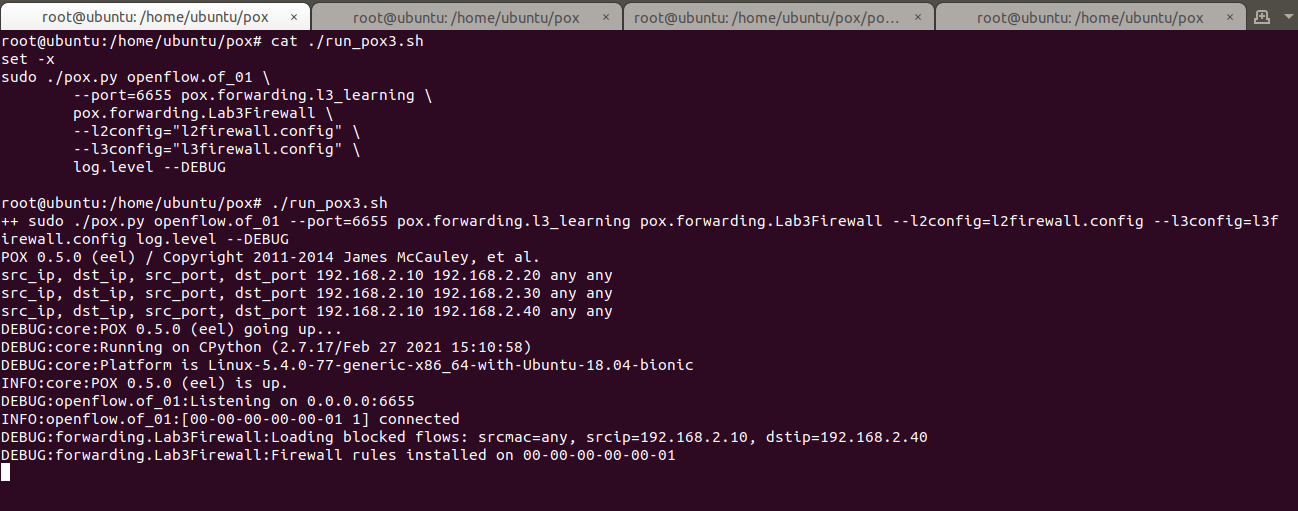


Figure - Running POX

### Check openflow flow-entries on switch 1.

### Start flooding from any container host to container host #2

### Check Openflow flow entries at switch 1

In the next sequence of screenshots, I will illustrate the Denial of Service happening on OVS because of the flood attack.

I have aligned the four X terminals of the four containers of the mininet, and used one to produce the flood, one to show the OVS flows, and another to try to ping another container.

In the first image, I am showing that the command “*ovs-ofctl dump-flows s1*” (used to dump the OVS flows) does not show anything – this is correct because there is no traffic yet.

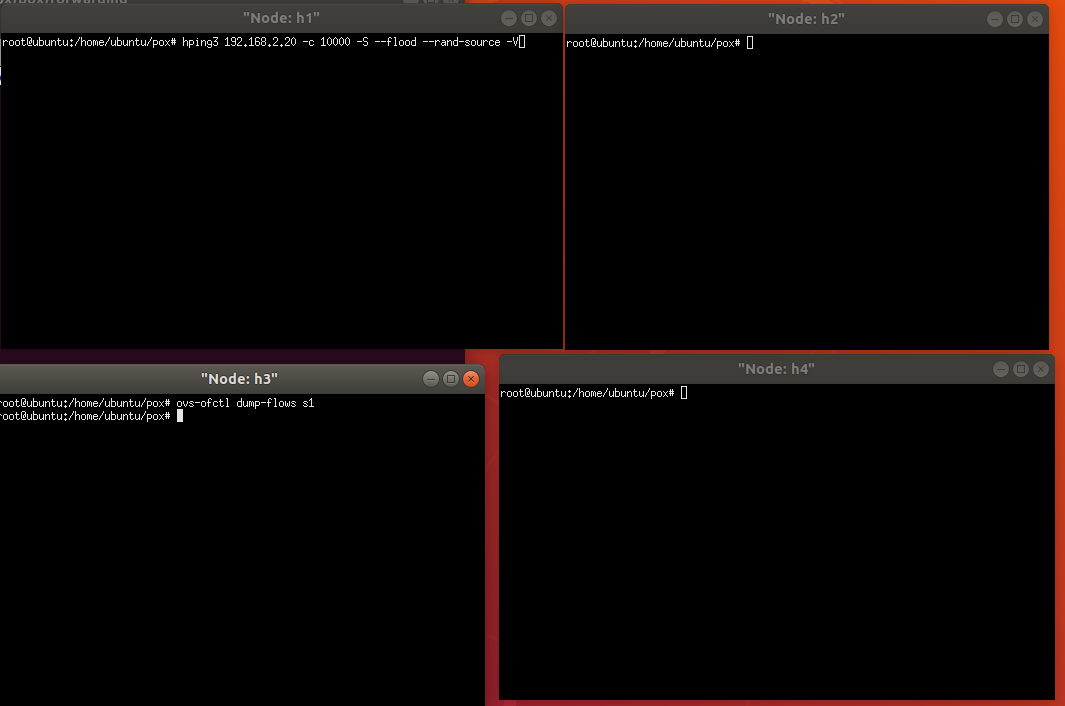


Figure - Check openflow flow-entries on switch 1

In the next screenshot, I have started the flood attack from the container h1 against h2. On container h2 I am trying to ping container 4, but with no success – the OVS controller is effectively under stress and does not forward the flows. Conversely, the containers are quite responsive – it’s just their networking that is affected.

On the container 3 I am dumping the OVS flows – they are hundreds, and do not stop increase even after I have stopped the flood.

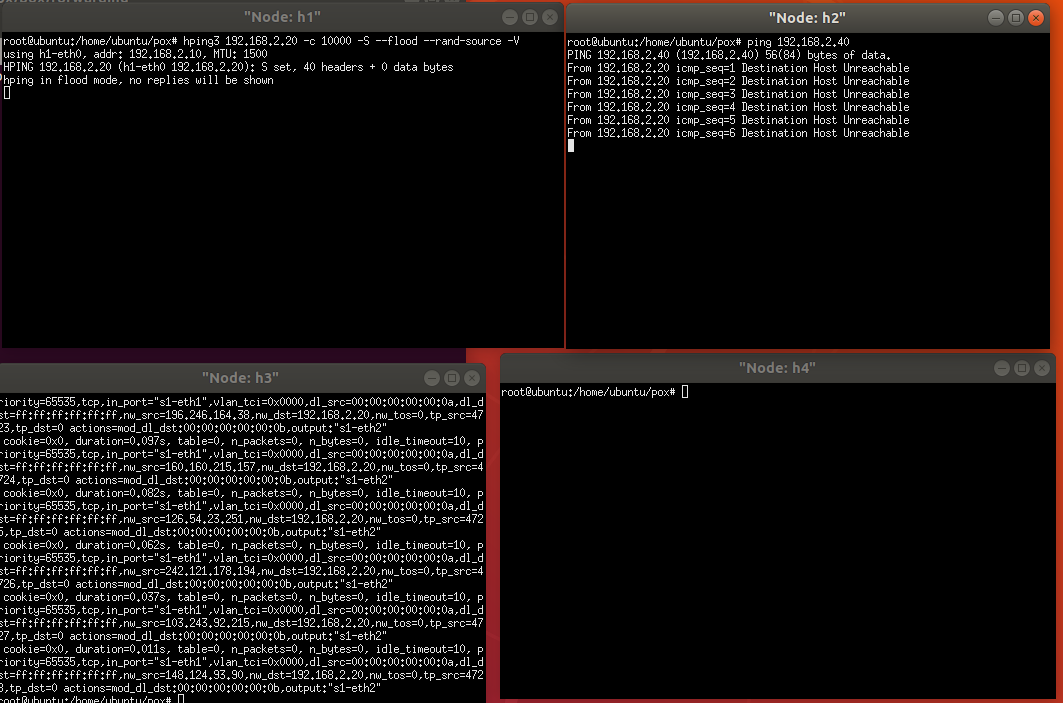


Figure - Start flooding from any container host to container host #2

After the flood is concluded, the OVS comes back to normal slowly. From the next screenshot, it is possible to appreciate that it needs at least five minutes after the attack is terminated, to start resume the network.

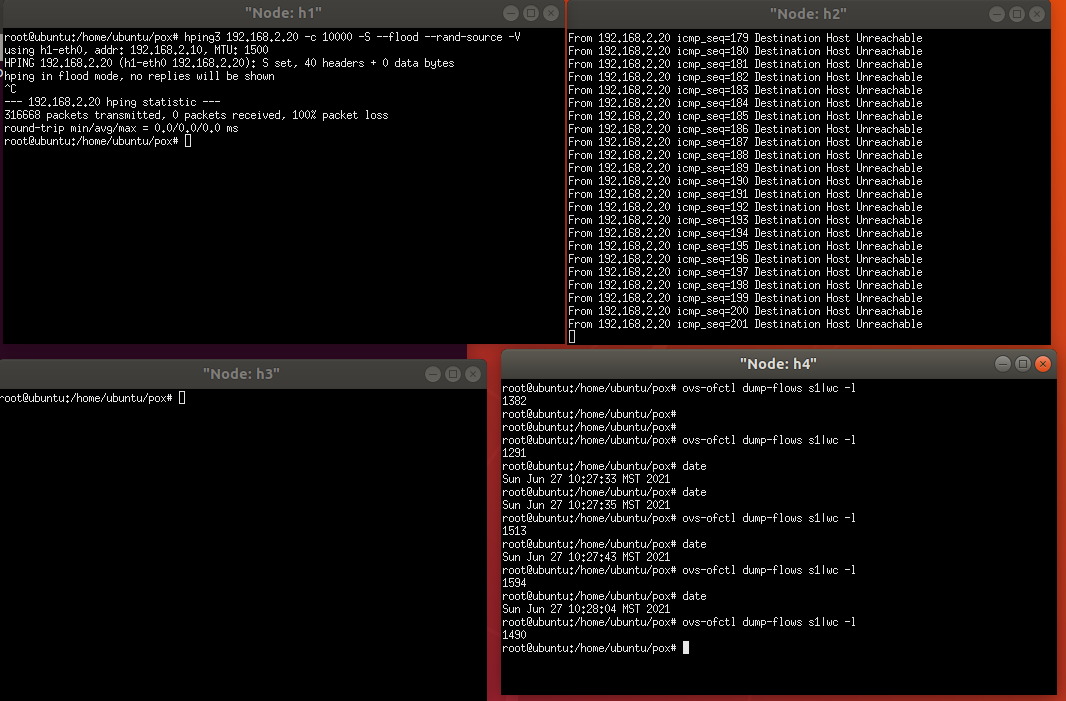


Figure d. - OVS Slowly resuming operation

I have used “*wc -l*” to count the number of flows present on the switch, and they do not necessarily start diminishing after the flood is terminated.

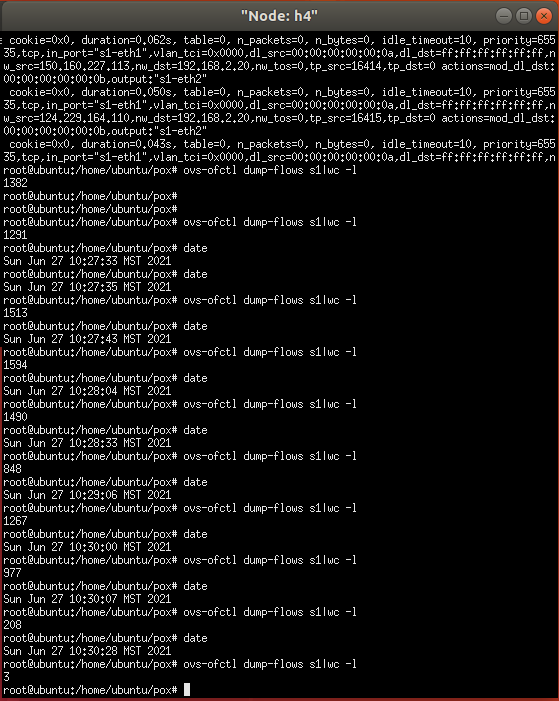


Figure - Counting the flows on OVS

## Mitigate DoS attack by implementing port security and using OpenFlow based firewall.

### You should illustrate (through screenshots and descriptions) your implemented program codes.

### You should demo how your implementation can mitigate the DoS through a sequence of screenshots with explanation.

### You should submit the source codes of your implementation.

In this lab, I have modified the provided L3Firewall.py implementing “Lab3Firewall.py”. The complete code is presented on GitHub; however, I will highlight here the most noticeable points.

The logic for spoofing and DoS detection is implemented through a Python Dict() object. Every time a new flow is observed by the OVS, the source MAC address of the processed packets is stored as the key; the source and destination IP addresses, as well as the OVS switchport, are stored as Dict values. For instance:

SpoofingTable = {

# src MAC address src IP dst IP src OVS port

"00:00:00:00:00:0a": ["192.168.2.10", "192.168.2.30", "1"],

"00:00:00:00:00:0b": ["192.168.2.20", "192.168.2.10", "2"],

"00:00:00:00:00:0c": ["192.168.2.30", "192.168.2.40", "3"]

}

I have also implemented an algorithm that implements both the two spoofing attacks (spoofing of IP and spoofing of the MAC address), as required by the “Bonus Points” section.

I have extensively commented the source code in order to understand the program as it is being red.

The main principles for are the following:

* In the case of **IP address spoofing** (“base” case for the Lab):

The packet from the attacker arrives with a certain MAC address and source IP, destined against the victim:

Source MAC Source IP Victim’s IP OVS switchport

"00:00:00:00:00:0a": ["192.168.2.10", "192.168.2.30", "1"]

The subsequent spoofed packets change their IP addresses, but keep the Source MAC and Victim’s IP the same:

Source MAC Source IP Victim’s IP OVS switchport

"00:00:00:00:00:0a": ["192.168.2.11", "192.168.2.30", "1"]

"00:00:00:00:00:0a": ["192.168.2.12", "192.168.2.30", "1"]

The pattern for this attack is the following:

Source MAC Source IP Victim’s IP OVS switchport

Constant Changing Constant Constant

* In the case of **MAC address spoofing** (“Bonus” case for the Lab):

The packet from the attacker arrives with a certain MAC address and source IP, destined against the victim:

Source MAC Source IP Victim’s IP OVS switchport

"00:00:00:00:00:0a": ["192.168.2.10", "192.168.2.30", "1"]

The subsequent spoofed packets change their IP addresses, but keep the Source MAC and Victim’s IP the same:

Source MAC Source IP Victim’s IP OVS switchport

"00:00:00:00:01:0a": ["192.168.2.10", "192.168.2.30", "1"]

"00:00:00:00:02:0a": ["192.168.2.10", "192.168.2.30", "1"]

The pattern for this attack is the following:

Source MAC Source IP Victim’s IP OVS switchport

Changing Constant Constant Constant

It is to be noticed, that the best way to block a Denial of Service attack is always by indicating a tuple of attack source + destination and not just blocking the attack source, as this can be a too wide rule which will end up also blocking legitimate users. In any case, in this Lab considerations over Distributed Denial of Services (and therefore, multiple attack sources against multiple targets) are not considered, and we are only resorting to relatively simple cases.

Please find below the pseudo-algorithm and the implementation for the function “verifyPortSecurity” which detects both floods:

if packet.source.MAC not in the SpoofingTable

iterates through the SpoofingTable

if packet.source.IP is present in the SpoofingTable = **MAC spoofing detected**

block packet.source.IP + packet.destination.IP

add packet.source.MAC, packet.source.IP, packet.destination.IP in the SpoofingTable

else

if both packet.source.IP & packet.destination.IP are the same as saved in the SpoofingTable for packet.source.MAC

the packet has been already observed, nothing to be done

if packet.source.IP is different than source.IP in the SpoofingTable = **IP spoofing detected**

block packet.source.MAC + packet.destination.IP

end-if





Figure - Function "verifyPortSecurity"

Please find below the screenshots that demonstrate the mitigation of the two attacks.

### IP Spoofing Attack Mitigation

I have done my best to illustrate the software working properly, I hope this comes through as clear enough.

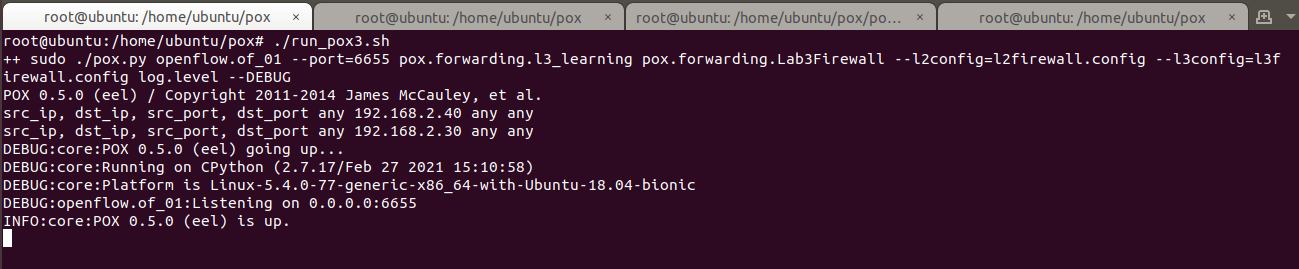


Figure - IP Spoofing - Running POX

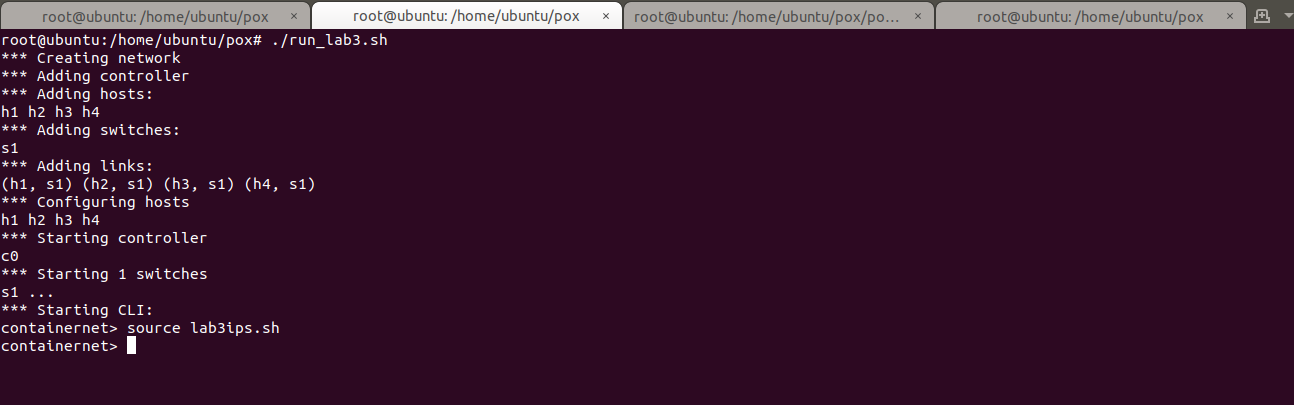


Figure - IP Spoofing - Running mininet

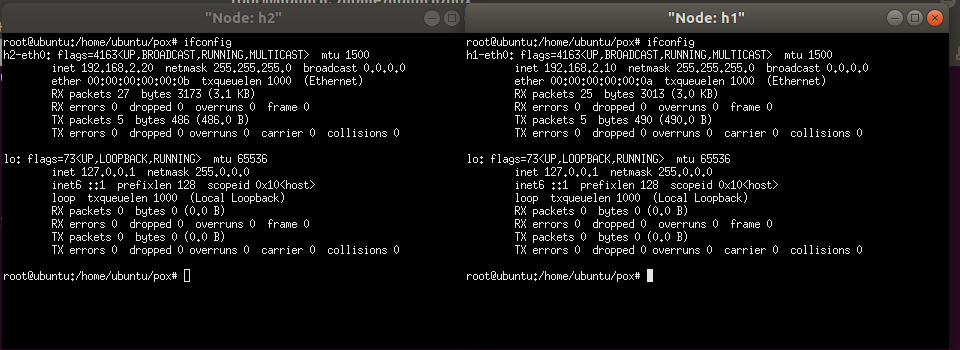


Figure - IP Spoofing - h1 and h2 with their starting IPs and MAC addresses

As visible from the next two screenshots, hping3 is running a flood on one container, while the other is able to ping without issues, meaning that the OVS is not flooded.

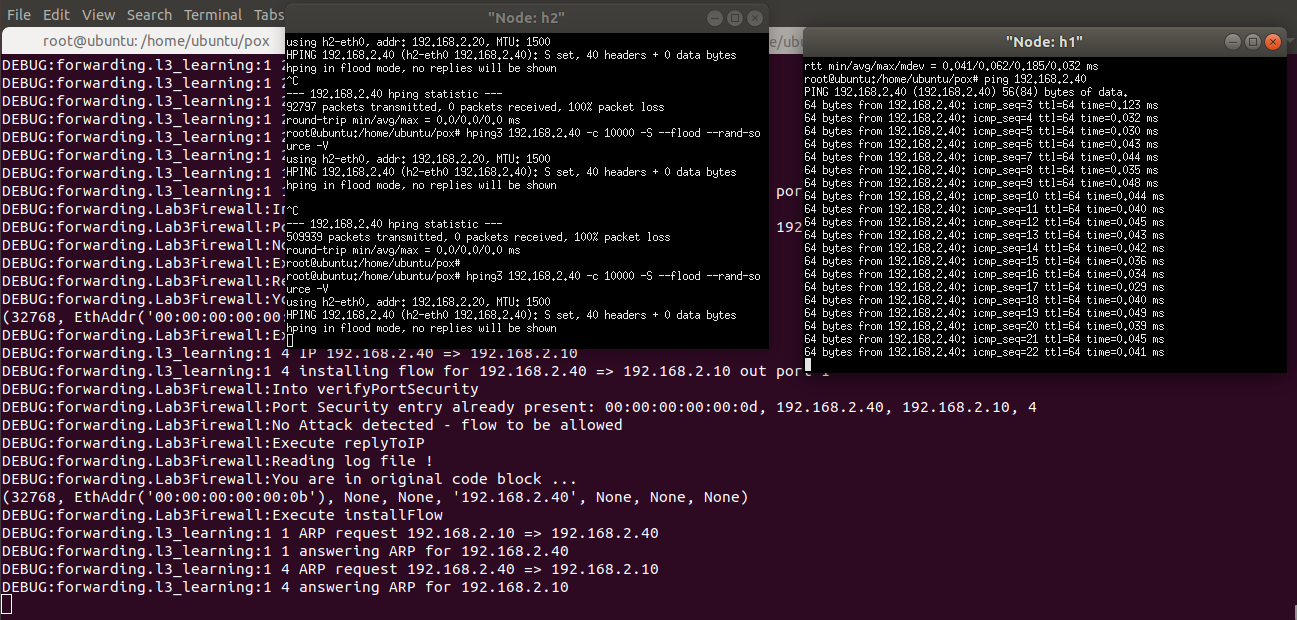


Figure - IP Spoofing - Running hping3 on h2 and running ping on h1

I have minimized the two xterm in order to see the debug messages more clearly. It is possible to appreciate the fact that the attack is noticed at the second packet and the flow is blocked. The algorithm obviously requires two packets with the same MAC and two different IPs as a minimum, which will block the source MAC + victim’s IP. After blocking, the next attack packets do not require further action, as they are automatically dropped by the OVS.

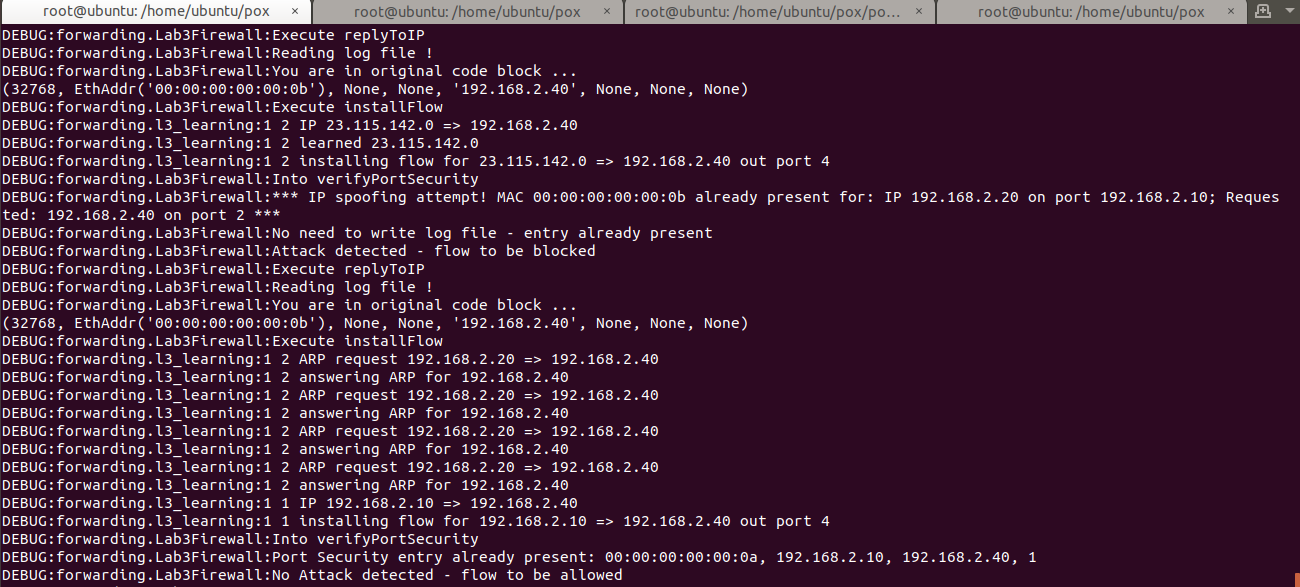


Figure - IP Spoofing - debug messages showing malicious packets being blocked

Debug messages:

DEBUG:forwarding.Lab3Firewall:Execute replyToIP

DEBUG:forwarding.Lab3Firewall:Reading log file !

DEBUG:forwarding.Lab3Firewall:You are in original code block ...

(32768, EthAddr('00:00:00:00:00:0b'), None, None, '192.168.2.40', None, None, None)

DEBUG:forwarding.Lab3Firewall:Execute installFlow

DEBUG:forwarding.l3\_learning:1 2 IP 23.115.142.0 => 192.168.2.40

DEBUG:forwarding.l3\_learning:1 2 learned 23.115.142.0

DEBUG:forwarding.l3\_learning:1 2 installing flow for 23.115.142.0 => 192.168.2.40 out port 4

DEBUG:forwarding.Lab3Firewall:Into verifyPortSecurity

DEBUG:forwarding.Lab3Firewall:\*\*\* IP spoofing attempt! MAC 00:00:00:00:00:0b already present for: IP 192.168.2.20 on port 192.168.2.10; Requested: 192.168.2.40 on port 2 \*\*\*

DEBUG:forwarding.Lab3Firewall:No need to write log file - entry already present

DEBUG:forwarding.Lab3Firewall:Attack detected - flow to be blocked

DEBUG:forwarding.Lab3Firewall:Execute replyToIP

DEBUG:forwarding.Lab3Firewall:Reading log file !

DEBUG:forwarding.Lab3Firewall:You are in original code block ...

### MAC Spoofing Attack Mitigation

I have performed two kind of attacks: one to simply show that the mitigation is conceptually working, by simply manually changing the MAC address of the attacker container; the second by running a tool called *nping*.

At the beginning, the environment is readied, and pings are executed to be sure that networking is functioning, and the Lab firewall is processing the packets – and therefore registering the flow in the SpoofingTable.

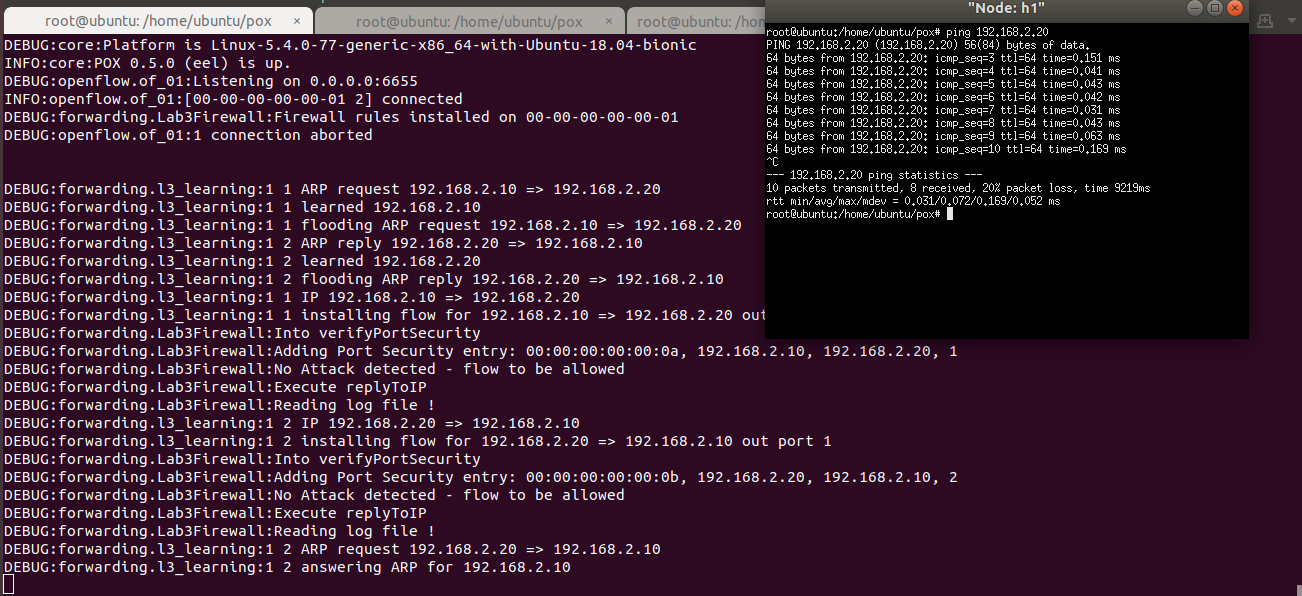


Figure - MAC spoofing - initial setup



Figure - MAC spoofing - changing MAC manually

From here, I manually change the MAC address of the contained with a Python-one-liner using the mininet API. The command is “*py h1.setMAC('00:00:00:00:02:0b')*”

We can see from the xterm’s screenshot that the container has changed its MAC address to the value we have chosen.

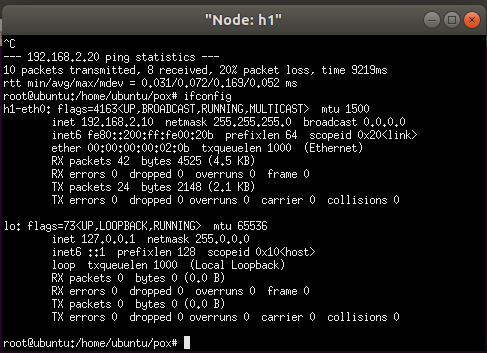


Figure - MAC spoofing - confirmation of MAC change

From the next screenshot the whole picture is presented.

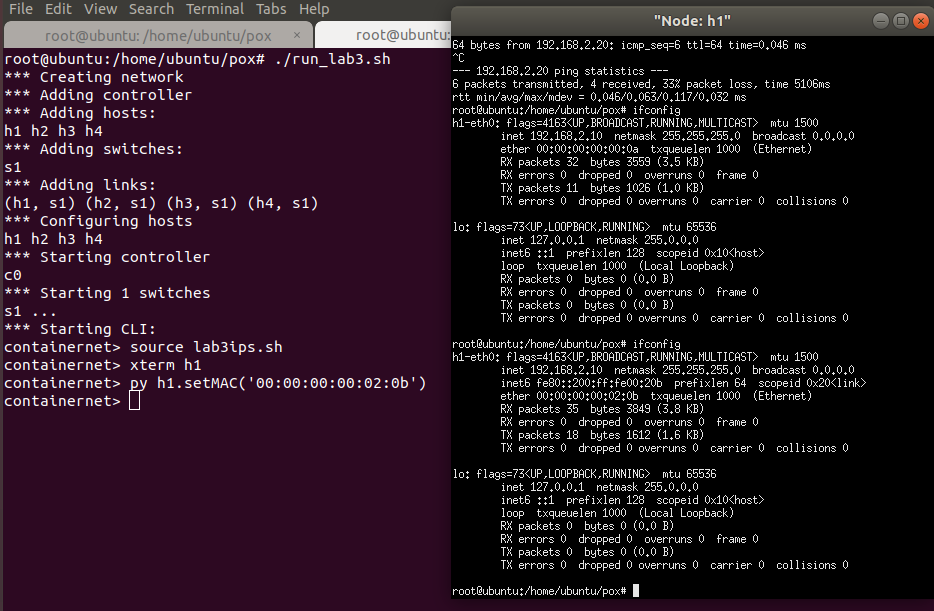


Figure - MAC spoofing - Before and after MAC change

After the MAC address has changed, the networking takes a bit of time to “reconverge” – in my system, it has taken 9 echo-request cycles, but it will vary depending on the case. Basically, the switch needs time to re-adjust to the fact that the topology has changed, and only after this has been reflected in the OVS, we can effectively catch the offending packets. This is because our software is executed after the basic switch functionalities – included in *l3\_learning.py* – are executed.

The only way to improve and have a faster detection for MAC address spoofing, would be to work directly on the l3\_learning.py or *l2\_learning.py* Python programs in order to access the packets “on the (virtual) wire”.

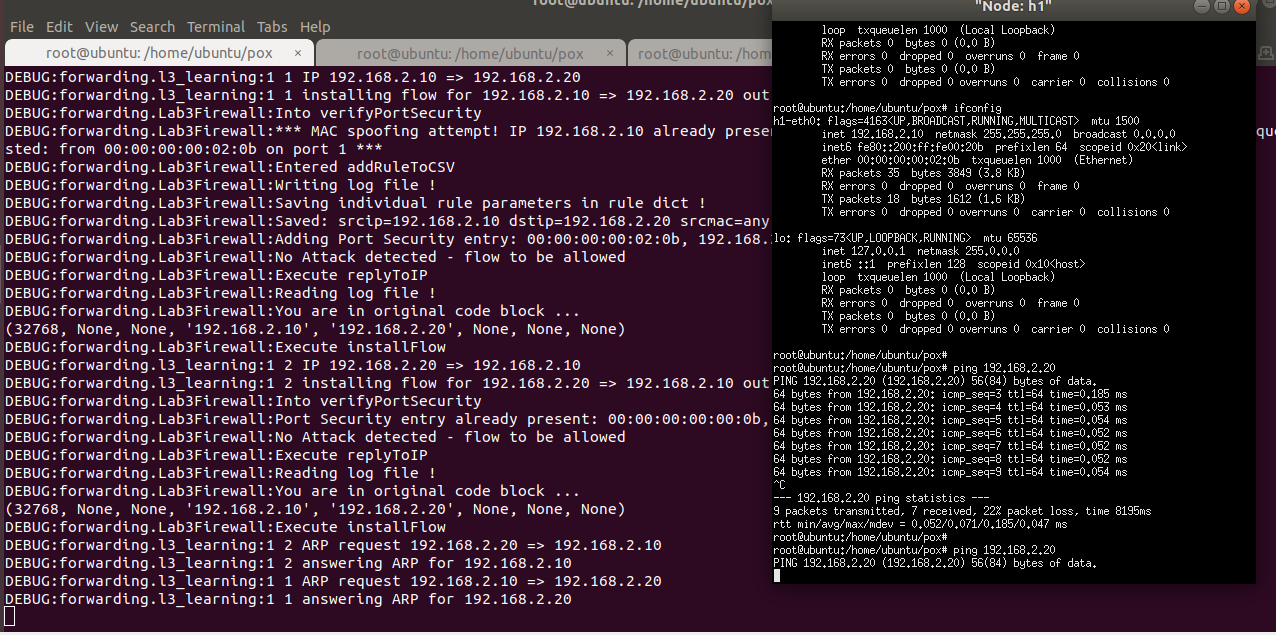


Figure - MAC spoofing - detection after a certain number of packets

Zooming into the xterm to show that after a while, packets are effectively blocked.

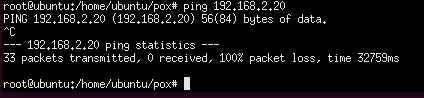


Figure - MAC spoofing - xterm showing all dropped ICMP packets

The next attack is performed using *nping*, which allows generating random IP addresses for an attack. The command I used is the following:

nping -c 10 --icmp --source-mac rand 192.168.2.20

As it is possible to see, here as well some packet comes through in the first attack, but nothing comes through in the second as the switch has “learned”.

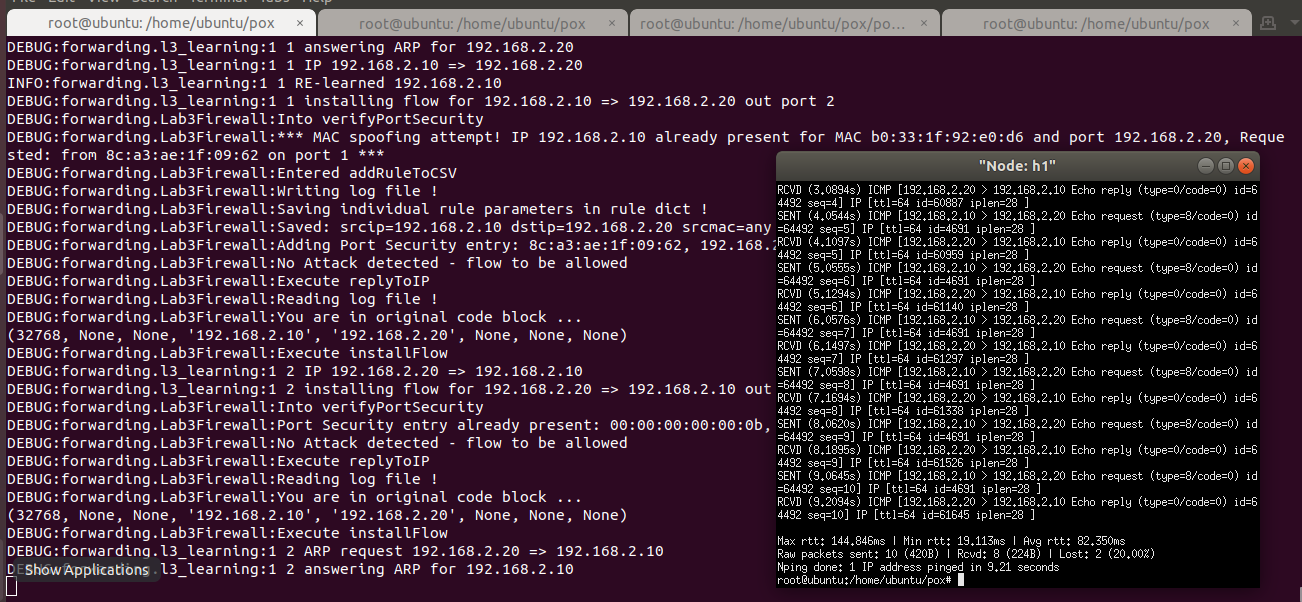


Figure - MAC spoofing – nping – first attack

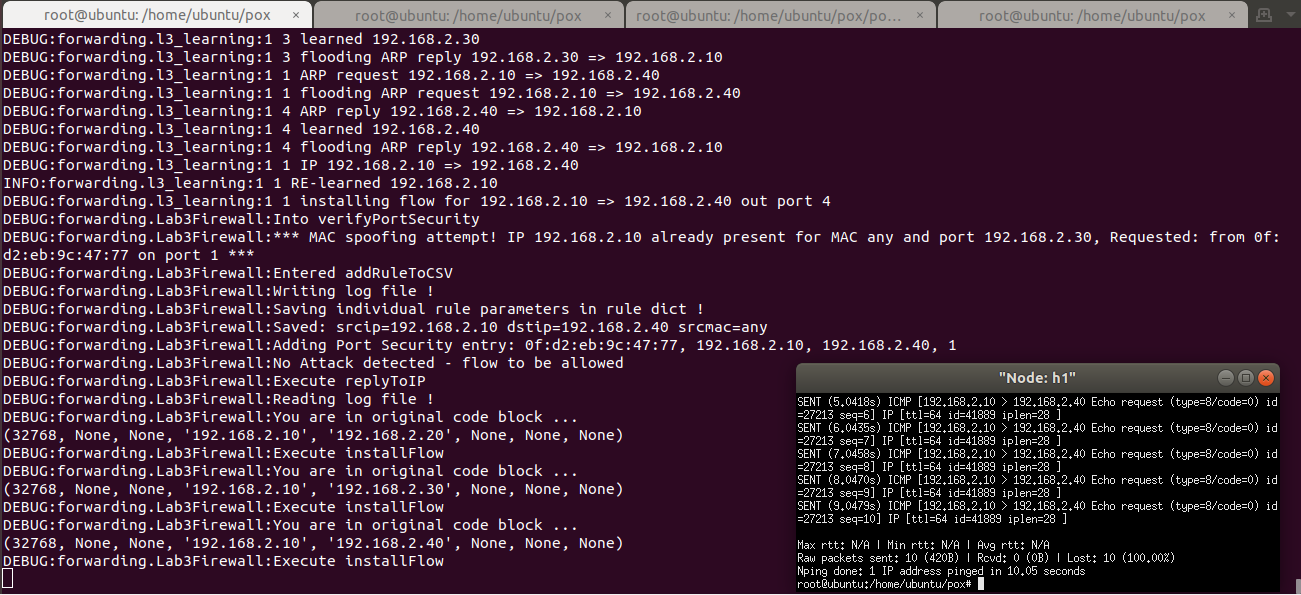


Figure - MAC spoofing – nping – second attack

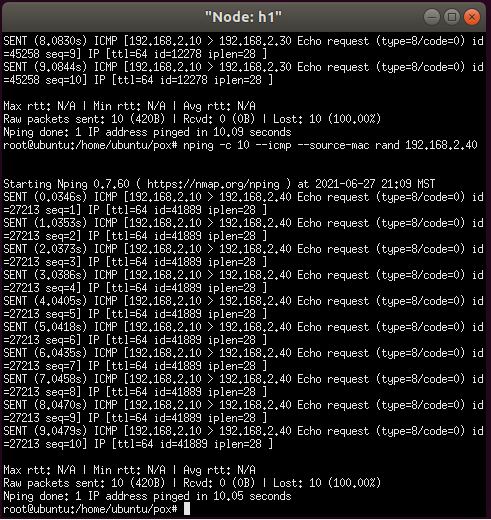


Figure - MAC spoofing – nping – second attack, zoom in

It is worth noticing that detected malicious flows are both blocked immediately – by issuing a message to OVS – and also saved into the l3firewall.config configuration file, to be resumed later.

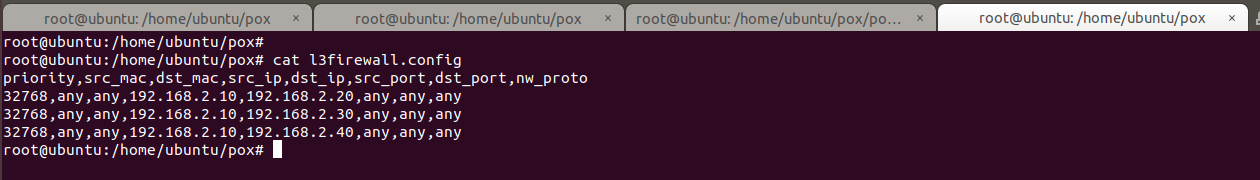


Figure – MAC spoofing – flows captured in l3firewall.config

To be able to restart the Lab without being affected by flows detected in a previous run, I have created an empty l3firewall.config (*l3firewall.config.empty*) file with just the row headers, and I am copying it over the l3firewall.config file generated by the mitigation software in the previous run.

# Appendix A: Files for the Lab

Please find the list of files created for this lab and mentioned throughout this document, plus their GitHub link for download.

The overall GitHub directory for the project is: <https://github.com/markoer73/CSE-548/tree/main/Project%202%20-%20SDN-Based%20Stateless%20Firewall>

|  |  |
| --- | --- |
| Project-Report-3 SDN-Based DoS Attacks and Mitigation.docx | <https://github.com/markoer73/CSE-548/blob/b44720f56fb7d262a8fb80d8077dc88e96812c74/Project%203%20-%20SDN-Based%20DoS%20Attacks%20and%20Mitigation/Project-Report-3%20SDN-Based%20Stateless%20Firewall.docx> |
| Lab3Firewall.py | <https://github.com/markoer73/CSE-548/blob/b44720f56fb7d262a8fb80d8077dc88e96812c74/Project%203%20-%20SDN-Based%20DoS%20Attacks%20and%20Mitigation/Lab3Firewall.py> |
| l3firewall.config.empty | <https://github.com/markoer73/CSE-548/blob/b44720f56fb7d262a8fb80d8077dc88e96812c74/Project%203%20-%20SDN-Based%20DoS%20Attacks%20and%20Mitigation/l3firewall.config.empty> |
| l3firewall.config | <https://github.com/markoer73/CSE-548/blob/main/Project%202%20-%20SDN-Based%20Stateless%20Firewall/l3firewall.config> |
| lab3ips.sh | <https://github.com/markoer73/CSE-548/blob/b44720f56fb7d262a8fb80d8077dc88e96812c74/Project%203%20-%20SDN-Based%20DoS%20Attacks%20and%20Mitigation/lab3ips.sh> |
| run\_lab3.sh | <https://github.com/markoer73/CSE-548/blob/b44720f56fb7d262a8fb80d8077dc88e96812c74/Project%203%20-%20SDN-Based%20DoS%20Attacks%20and%20Mitigation/run_lab3.sh> |
| run\_pox3.sh | <https://github.com/markoer73/CSE-548/blob/b44720f56fb7d262a8fb80d8077dc88e96812c74/Project%203%20-%20SDN-Based%20DoS%20Attacks%20and%20Mitigation/run_pox3.sh> |

# File Content

The file content has been reported inline with the text where applicable.

# References

* POX Github: <https://noxrepo.github.io/pox-doc/html/>
* POX Controller Tutorial: <http://sdnhub.org/tutorials/pox/>
* Open vSwitch Cheat Sheet: <https://therandomsecurityguy.com/openvswitch-cheat-sheet/>
* Containernet: <https://containernet.github.io/>
* Containernet tutorial: <https://github.com/containernet/containernet/wiki/Tutorial:-Getting-Started>
* Port security: <https://packetlife.net/blog/2010/may/3/port-security/>

VIII. Table of Figures

[Figure 1 - Bridged network setup in VirtualBox 1](#_Toc75762346)

[Figure 2 – Running mininet 2](#_Toc75762347)

[Figure 3 - Mininet network 3](#_Toc75762348)

[Figure 4 - Setting IP addresses for the lab 3](#_Toc75762349)

[Figure 5 - Checking IP addresses for the containers in the lab 3](#_Toc75762350)

[Figure 6 - Running POX 4](#_Toc75762351)

[Figure 7 - Check openflow flow-entries on switch 1 5](#_Toc75762352)

[Figure 8 - Start flooding from any container host to container host #2 6](#_Toc75762353)

[Figure 9d. - OVS Slowly resuming operation 7](#_Toc75762354)

[Figure 10 - Counting the flows on OVS 8](#_Toc75762355)

[Figure 11 - Function "verifyPortSecurity" 10](#_Toc75762356)

[Figure 12 - IP Spoofing - Running POX 11](#_Toc75762357)

[Figure 13 - IP Spoofing - Running mininet 11](#_Toc75762358)

[Figure 14 - IP Spoofing - h1 and h2 with their starting IPs and MAC addresses 11](#_Toc75762359)

[Figure 15 - IP Spoofing - Running hping3 on h2 and running ping on h1 12](#_Toc75762360)

[Figure 16 - IP Spoofing - debug messages showing malicious packets being blocked 12](#_Toc75762361)

[Figure 17 - MAC spoofing - initial setup 14](#_Toc75762362)

[Figure 18 - MAC spoofing - changing MAC manually 14](#_Toc75762363)

[Figure 19 - MAC spoofing - confirmation of MAC change 14](#_Toc75762364)

[Figure 20 - MAC spoofing - Before and after MAC change 15](#_Toc75762365)

[Figure 21 - MAC spoofing - detection after a certain number of packets 15](#_Toc75762366)

[Figure 22 - MAC spoofing - xterm showing all dropped ICMP packets 16](#_Toc75762367)

[Figure 23 - MAC spoofing – nping – first attack 16](#_Toc75762368)

[Figure 24 - MAC spoofing – nping – second attack 17](#_Toc75762369)

[Figure 25 - MAC spoofing – nping – second attack, zoom in 17](#_Toc75762370)

[Figure 26 – MAC spoofing – flows captured in l3firewall.config 18](#_Toc75762371)

Contents

[I. Project Overview 1](#_Toc75762393)

[II. Network Setup 1](#_Toc75762394)

[III. Software 2](#_Toc75762395)

[IV. Project Description 2](#_Toc75762396)

[1. Setting up mininet and Running mininet topology 2](#_Toc75762397)

[2. Should assign IP addresses to hosts. 3](#_Toc75762398)

[3. Perform Flood attack on SDN controller following a suggested procedure: 4](#_Toc75762399)

[a. Run l3 learning application in POX controller. 4](#_Toc75762400)

[b. Check openflow flow-entries on switch 1. 4](#_Toc75762401)

[c. Start flooding from any container host to container host #2 4](#_Toc75762402)

[d. Check Openflow flow entries at switch 1 4](#_Toc75762403)

[4. Mitigate DoS attack by implementing port security and using OpenFlow based firewall. 8](#_Toc75762404)

[a. You should illustrate (through screenshots and descriptions) your implemented program codes. 8](#_Toc75762405)

[b. You should demo how your implementation can mitigate the DoS through a sequence of screenshots with explanation. 8](#_Toc75762406)

[c. You should submit the source codes of your implementation. 8](#_Toc75762407)

[d. IP Spoofing Attack Mitigation 11](#_Toc75762408)

[a. MAC Spoofing Attack Mitigation 14](#_Toc75762409)

[V. Appendix A: Files for the Lab 19](#_Toc75762410)

[VI. File Content 19](#_Toc75762411)

[VII. References 19](#_Toc75762412)

[VIII. Table of Figures 19](#_Toc75762413)