|  |  |
| --- | --- |
| Logo  Description automatically generated | SDN Lab  Detect DoS attacks using Snort |

Nhóm học phần:

1) Mã Sinh viên, Họ và Tên:

2)

3)

MỤC LỤC

[1. Introduction 1](#_Toc175896891)

[2. Example 1](#_Toc175896892)

[3. Excersices 2](#_Toc175896893)

[4. Reference 2](#_Toc175896894)

*>> Yêu cầu chụp hình ảnh là kết quả thực hành của SV. Không sử dụng lại hình ảnh của bài lab.*

# Introduction

Setup an SDN network with 5 hosts, with host 5 sniffing traffic on host 4 using Snort.

This project will have 3 malicious actors *(h1, h2, h3)*, a victim machine (h4) and an IDS using Snort sniffer *(h5)*

We will configure the network such that the 5 hosts are connected to the a switch, and the switch is connected to Floodlight SDN Controller. *h1, h2* and *h3* will attack h4 with a DoS attack, and *h5* will be able to pick it up using Snort rules.

# Example

* Test Snort is up and running

$ snort -V

,,\_ -\*> Snort! <\*-

o" )~ Version 2.9.8.3 GRE (Build 383)

'''' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team

Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.

Using libpcap version 1.7.4

Using PCRE version: 8.38 2015-11-23

Using ZLIB version: 1.2.8

$ ifconfig

View information of network interfaces.

$ sudo snort -vd

* Run snort to show the layer 2 headers run:

$ sudo snort -vde

* Run snort with file snort.conf

$ sudo snort -v -c /etc/snort/snort.conf

* Getting started with Snort’s Packet Logger mode. Snort to show only headers and log the traffic on the disk type:

$ mkdir log

$ sudo snort -d -c /etc/snort/snort.conf -l ./log

Nhấn Ctrl + C để dừng

$ ls ./log

alert snort.log.1699083554 snort.log.1699083926

$ sudo cat ./log/snort.log.1699083926

* Read the log files type:

$ sudo snort -d -v -r ./log/snort.log.1699083926

$ snort -T -i ens33 -c /etc/snort/snort.conf -l ./log

* Run snort to alert in the terminal with the parameter “-A console”

$ sudo snort -A console -i ens33 -q

Explain the command & display result.

$ sudo snort -A console -i ens33 -c /etc/snort/snort.conf

Explain the command & display result.

$ sudo snort -A console -i ens33 -c snort.conf -q

Explain the command & display result.

$ sudo snort -A console -i ens33 -c snort.conf -d -l ./log

Explain the command & display result.

* Adding a rule in *mylocal.rules*

alert icmp any any -> any any (threshold: type both, track by\_dst, count 70, seconds 10; msg: "DoS by ICMP detected"; sid:1001;)

* Spawn your network with the command:

$ sudo mn --topo single,5 --controller=remote,ip=127.0.0.1,port=6653

* Spawns a single layer network, with 5 hosts connected to a switch.
* The switch is connected to a remote controller, which is the floodlight service you setup earlier. Port number of 6653 is used for communicating with your switch.
* Mirroring port h4 to h5 and sniff using Snort. Command to mirror h4 traffic to h5

mininet> s1 ovs-vsctl -- set Bridge "s1" mirrors=@m -- --id=@s1-eth4 get Port s1-eth4 -- --id=@s1-eth5 get Port s1-eth5 -- --id=@m create Mirror name=e4toe5 select-dst-port=@s1-eth4 output-port=@s1-eth5

* Now all traffic that is flowing into h4 will be mirrored onto h5, where Snort is running.

mininet> xterm h5

* In the new terminal spawned for h5, run:

h5> ifconfig

h5> snort -i h5 -eth0 -v -c $HOME/snort/snort.conf &

h5 is now sniffing traffic on h4

* Starting the attack

mininet> h1 ping -f h4

You should see in your /var/log/snort/alert the message "DoS by ICMP detected"

# Excersices

# Reference

1. ..

(Tài liệu lưu hành nội bộ)

-----------------------------------------------