|  |  |
| --- | --- |
| Logo  Description automatically generated | SOFTWARE DEFINED NETWORKING  Sử dụng ONOS và mô phỏng tấn công mạng |

Nhóm học phần:

1) Mã SV, Họ và tên

3)

MỤC LỤC

[1. ONOS with Mininet 1](#_Toc175651539)

[2. Excercise 2](#_Toc175651540)

[3. References 2](#_Toc175651541)

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

# View SDN topology network on Web ONOS

* Build a simple topology in Mininet in another terminal

$ sudo mn --topo tree,2,3 --mac --switch ovsk --controller=remote,ip=127.0.0.1

\*\*\* Creating network

\*\*\* Adding controller

Connecting to remote controller at 127.0.0.1:6653

\*\*\* Adding hosts:

h1 h2 h3 h4 h5 h6 h7 h8 h9

\*\*\* Adding switches:

s1 s2 s3 s4

\*\*\* Adding links:

(s1, s2) (s1, s3) (s1, s4) (s2, h1) (s2, h2) (s2, h3) (s3, h4) (s3, h5) (s3, h6) (s4, h7) (s4, h8) (s4, h9)

\*\*\* Configuring hosts

h1 h2 h3 h4 h5 h6 h7 h8 h9

\*\*\* Starting controller

c0

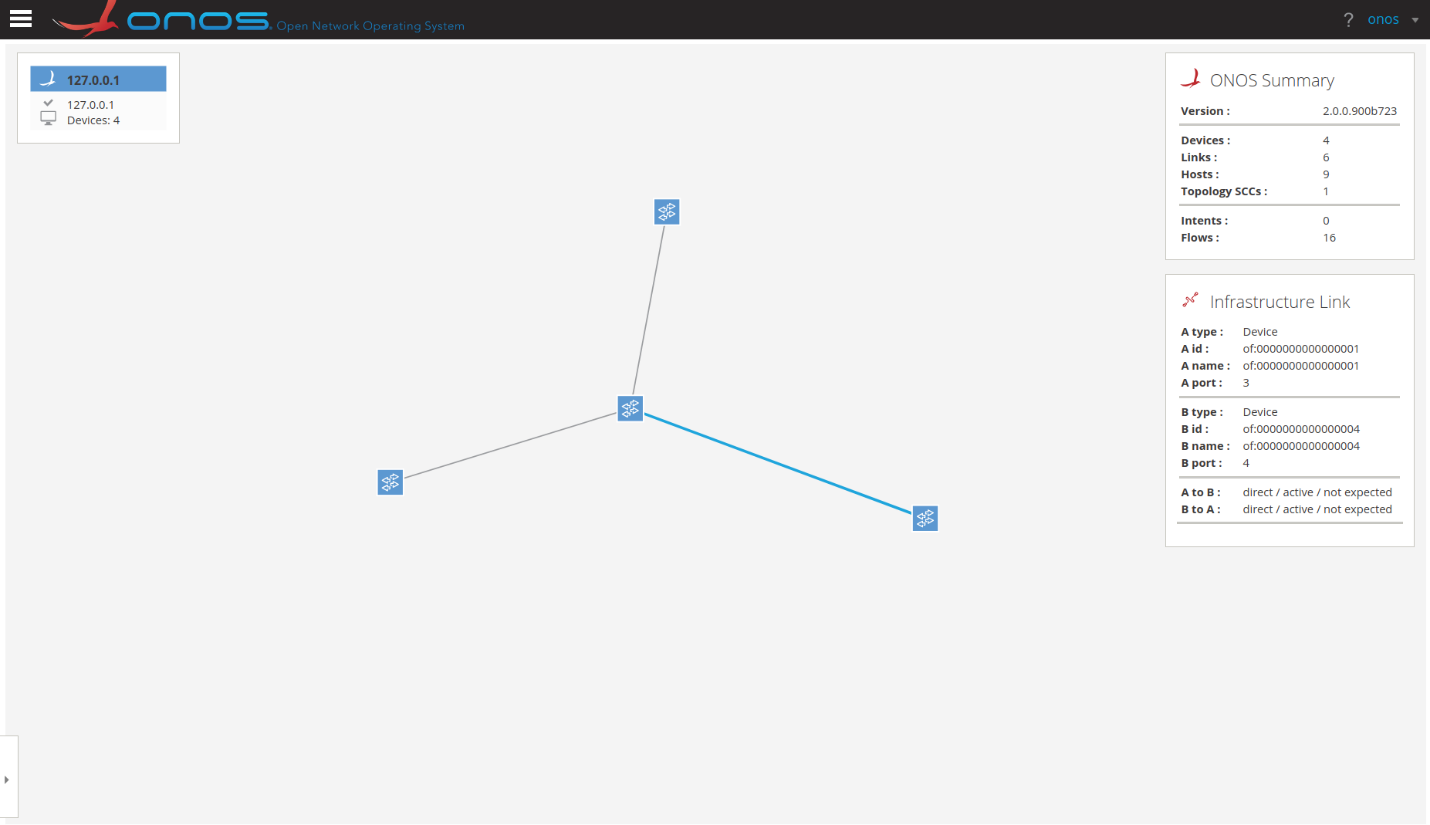
\*\*\* Starting 4 switches

s1 s2 s3 s4 ...

\*\*\* Starting CLI:

mininet>

* View the topology on *http://wandertour.ddns.net:8181/onos/ui/*



You will only see switches in the toplogy!

* Because the Open vSwitch has not know the hosts, we are going to ping all hosts in the Mininet

# Ping all hosts in the Mininet topology

mininet> pingall

\*\*\* Ping: testing ping reachability

h1 -> h2 h3 h4 h5 h6 h7 h8 h9

h2 -> h1 h3 h4 h5 h6 h7 h8 h9

h3 -> h1 h2 h4 h5 h6 h7 h8 h9

h4 -> h1 h2 h3 h5 h6 h7 h8 h9

h5 -> h1 h2 h3 h4 h6 h7 h8 h9

h6 -> h1 h2 h3 h4 h5 h7 h8 h9

h7 -> h1 h2 h3 h4 h5 h6 h8 h9

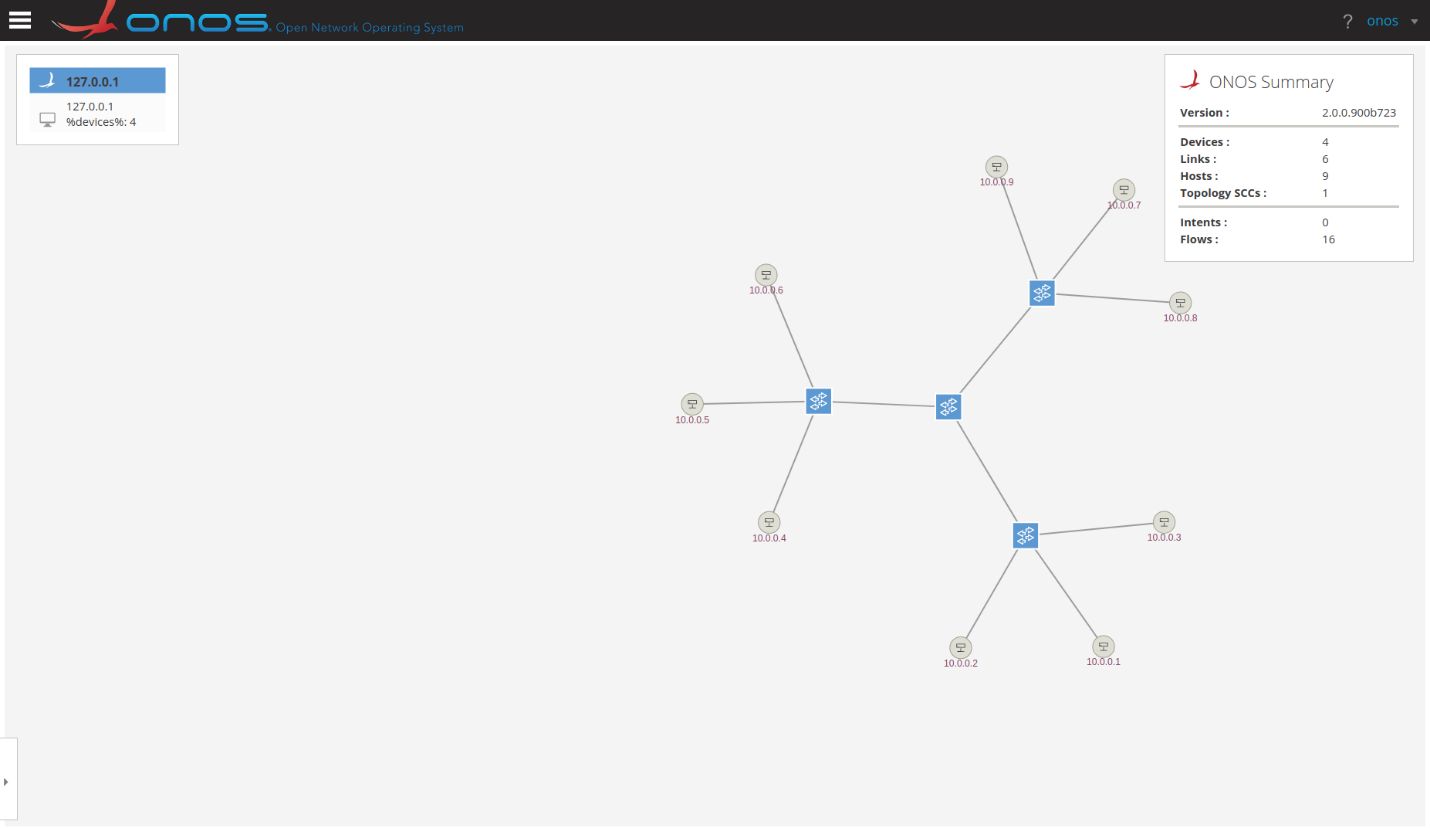
h8 -> h1 h2 h3 h4 h5 h6 h7 h9

h9 -> h1 h2 h3 h4 h5 h6 h7 h8

\*\*\* Results: 0% dropped (72/72 received)

mininet>

* View the topology on http://wandertour.ddns.net:8181/onos/ui



* Press H to show all hosts in topology
* Press P to highlight the port of each link
* Press T to change into night mode

1. https://github.com/yungshenglu/onos-practice/blob/master/src/tutorials/1\_install/README.md

# DoS attack the SDN network

This tutorial will focus on attacking the ONOS SDN controller. We will use the following attacks:

* Slow HTTP Headers (Slowloris)
* Slow HTTP Post (R-U-Dead-Yet or RUDY)
* Slow Read Attack
* Apache Killer (Range) Attack.

As you may notice this attacks are all based on application level using HTTP to attack a server. This tutorial will focus on running and understanding the attacks, but not on the implementation of the attacks. We will use a denial of service attack simulator called slowhttptest it is a CLI that already has implemented this attacks so we can run them with ease.

To verify if the installation was successful run:

$ slowhttptest –h

As you can see this command allow us to run attacks in 4 modes, each of those with the 4 attacks that we will test. Below is the list of the attacks following with its proper flag that need to be passed to the CLI.

* Slowloris (default): -H
* R-U-Dead-Yet or Rudy: -B
* Apache killer: -R
* Slow Read: -X

## Setting up an attack

**2. Run topology**

Before running our topology, double check if you have the ONOS website running .

In order to run an attack we need to setup our topology with a http server to attack. To do that please run the following commands:

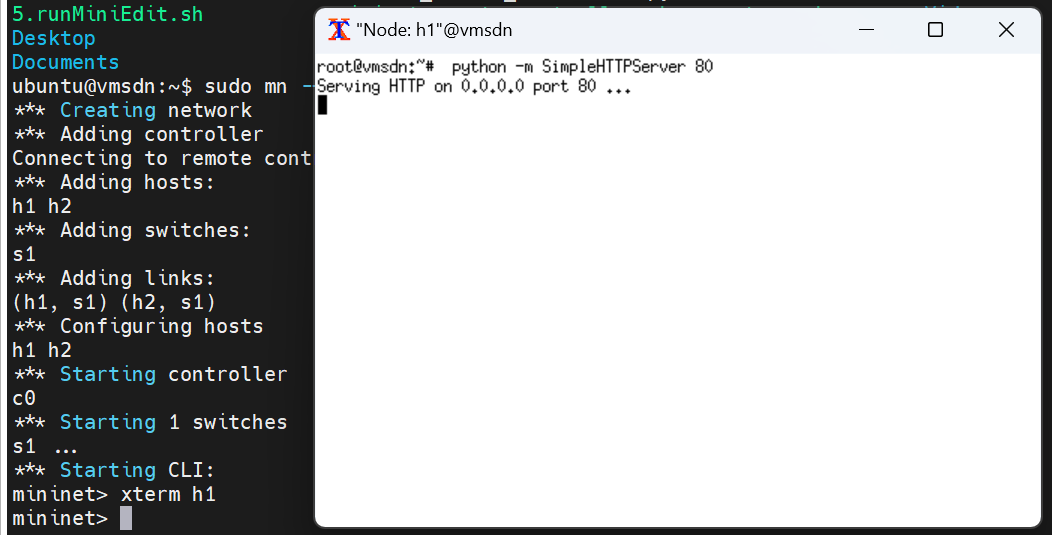
$ sudo mn --topo single,5 --controller=remote,ip=127.0.0.1,port=6653

* Above command  this will run a simple topology with 5 hosts, 1 switch and it will connect to the ONOS controller with the ONOS\_IP. You can get the ONOS controller ip from the ONOS UI.

mininet> xterm h1

* Above command  this will open an emulated terminal for the host 1, which will be our http server.
* On the h1 terminal run coomd to setup a simple http server on the host 1 that will listen on the port 80.

root@vmsdm:~# python -m SimpleHTTPServer 80



Then you can do a request to that server by running the following command:

mininet> h2 wget -O - h1

--2024-08-28 15:32:09-- http://10.0.0.1/

Connecting to 10.0.0.1:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 2646 (2.6K) [text/html]

Saving to: ‘STDOUT’

- 0%[ ] 0 --.-KB/s <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>

<title>Directory listing for /</title>

<body>

<h2>Directory listing for /</h2>

<hr>

<ul>

<li><a href=".bash\_history">.bash\_history</a>

<li><a href=".bash\_logout">.bash\_logout</a>

<li><a href=".bashrc">.bashrc</a>

...

...

<li><a href="Videos/">Videos/</a>

</ul>

<hr>

</body>

</html>

- 100%[===================>] 2.58K --.-KB/s in 0s

2024-08-28 15:32:09 (107 MB/s) - written to stdout [2646/2646]

mininet>

And we are ready to do some attacks!

## Running an attack

In order to start the attack from host 2 we need to open a new emulated terminal by running xterm h2, on this new terminal we will run the default attack (Slowloris) using the slowhttptest CLI we previously installed.

mininet> xterm h2

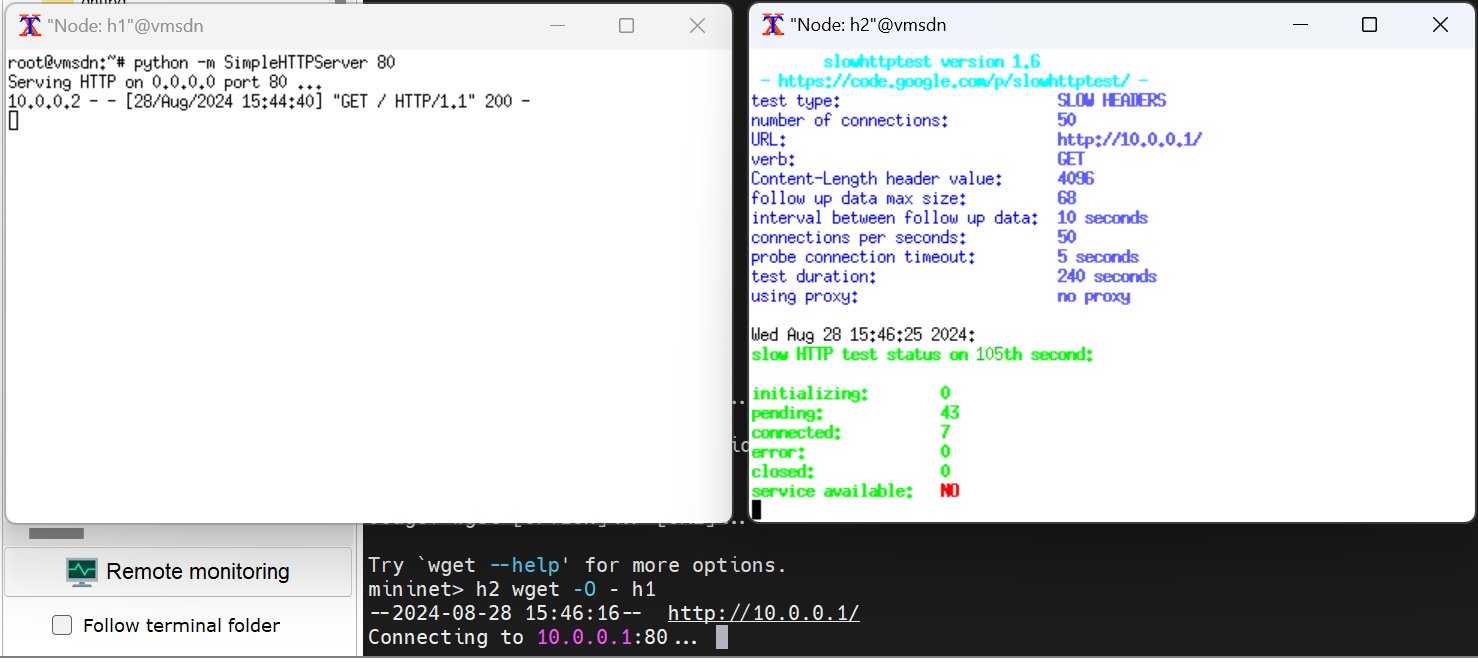
On windows h2, you can run the Slowloris attack by running:

root@vmsdm:~# slowhttptest -u  http://10.0.0.1

After running the attack we can try a request to host 1 http server by running the following command on the mininet terminal

mininet> h2 wget -O - h1

The request will be blocked because the attack was successful.



To run the other attacks you just add the respective flags that were explained on the Install slowhttptest section. Below is the list with the full commands.

* Slowloris (default):

root@vmsdm:~# slowhttptest -H -u http://10.0.0.1

* R-U-Dead-Yet or Rudy:

root@vmsdm:~# slowhttptest -B -u http://10.0.0.1

* Apache killer:

root@vmsdm:~# slowhttptest -R -u http://10.0.0.1

* Slow Read:

root@vmsdm:~# slowhttptest -X -u http://10.0.0.1

# Excercise

* Build other attack scenarios on networks with different topologies (routers, switches, servers, ...)

# References

1. .

(Tài liệu lưu hành nội bộ)

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