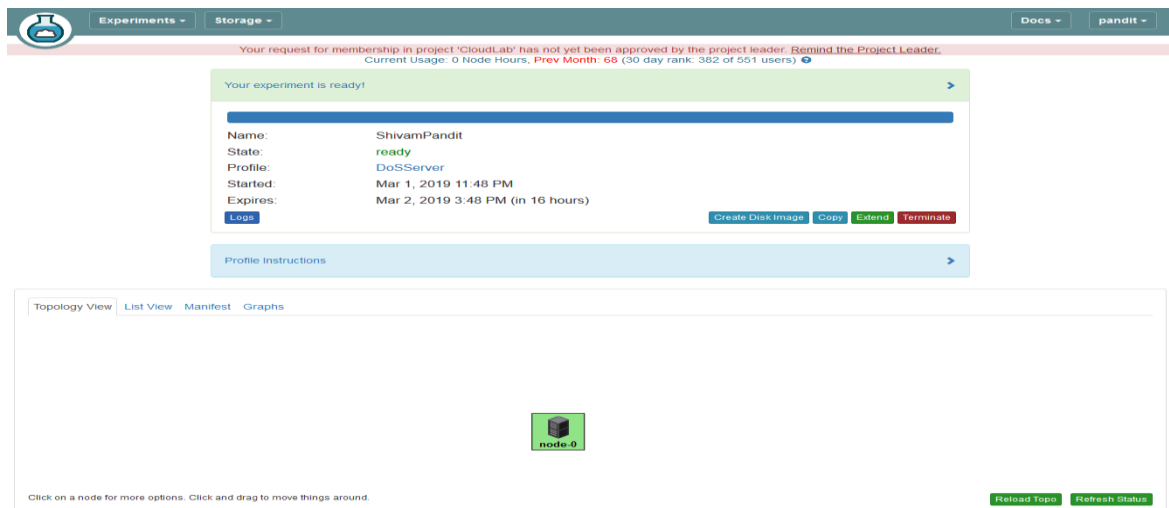


Denial-of-Service (DoS) Attacks in SDN - Lab2

BY: SHIVAM PANDIT

1. First we will start the experiment as shown below in screen dumps.



2. Then, after starting experiment next step is to conduct experiments. So, to conduct experiments we will install floodlight, mininet and hping3.
 - a. First, we will install floodlight by using shell commands as shown below.

```
Topology View List View Manifest Graphs node-0 x
pandit@node-0:~$ sudo apt-get install default-jdk -y; sudo apt-get install default-jre -y'
Reading package lists... Done
Building dependency tree
Reading state information... Done
default-jdk is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 136 not upgraded.
E: Command line option '-' [from -y'] is not known.
pandit@node-0:~$ sudo apt-get install default-jdk -y; sudo apt-get install default-jre -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
default-jdk is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 136 not upgraded.
Reading package lists... Done
Building dependency tree
Reading state information... Done
default-jre is already the newest version.
default-jre set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 136 not upgraded.
pandit@node-0:~$
```

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

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

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

BUILD SUCCESSFUL
Total time: 18 seconds
pandit@node-0:~/floodlight$ sudo mkdir /var/lib/floodlight
pandit@node-0:~/floodlight$ sudo chmod 777 /var/lib/floodlight
pandit@node-0:~/floodlight$
```

```
Topology View List View Manifest Graphs node-0 X
[jar] Building jar: /users/pandit/floodlight/target/floodlight.jar
[jar] Building jar: /users/pandit/floodlight/target/floodlight-test.jar

BUILD SUCCESSFUL
Total time: 18 seconds
pandit@node-0:~/floodlight$ sudo mkdir /var/lib/floodlight
pandit@node-0:~/floodlight$ sudo chmod 777 /var/lib/floodlight
pandit@node-0:~/floodlight$ wget https://people.cs.clemson.edu/~hongdal/set_floodlight.sh
--2019-03-01 22:44:17-- https://people.cs.clemson.edu/~hongdal/set_floodlight.sh
Resolving people.cs.clemson.edu (people.cs.clemson.edu)... 130.127.201.228, 2620:103:a004:e::228
Connecting to people.cs.clemson.edu (people.cs.clemson.edu)[130.127.201.228]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 310 [text/x-sh]
Saving to: 'set_floodlight.sh'

100%[=====>] 310 --.-K/s in 0s

2019-03-01 22:44:18 (29.2 MB/s) - 'set_floodlight.sh' saved [310/310]

pandit@node-0:~/floodlight$ sudo /bin/sh set_floodlight.sh; cd floodlight
```

b. Now after installing floodlight next step is to install mininet as shown below

```
Topology View List View Manifest Graphs node-0 X
remote: Enumerating objects: 1, done.
remote: Counting objects: 100% (1/1), done.
remote: Total 9618 (delta 0), reused 0 (delta 0), pack-reused 9617
Receiving objects: 100% (9618/9618), 2.96 MiB | 0 bytes/s, done.
Resolving deltas: 100% (6386/6386), done.
Checking connectivity... done.
pandit@node-0:~$ cd mininet
pandit@node-0:~/mininet$ git tag
1.0.0
2.0.0
2.1.0
2.1.0p1
2.1.0p2
2.2.0
2.2.1
2.2.2
2.3.0d3
2.3.0d4
cs244-spring-2012-final
pandit@node-0:~/mininet$
```

```
Topology View List View Manifest Graphs node-0 x
Receiving objects: 100% (9618/9618), 2.96 MiB | 0 bytes/s, done.
Resolving deltas: 100% (6386/6386), done.
Checking connectivity... done.
pandit@node-0:~$ cd mininet
pandit@node-0:~/mininet$ git tag
1.0.0
2.0.0
2.1.0
2.1.0p1
2.1.0p2
2.2.0
2.2.1
2.2.2
2.3.0d3
2.3.0d4
cs244-spring-2012-final
pandit@node-0:~/mininet$ git checkout -b 2.2.1 2.2.1
Switched to a new branch '2.2.1'
pandit@node-0:~/mininet$ cd ..
pandit@node-0:~$
```

```
Topology View List View Manifest Graphs node-0 x
0 upgraded, 0 newly installed, 0 to remove and 130 not upgraded.
fatal: destination path 'openflow' already exists and is not an empty directory.
pandit@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 (256 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) ...
pandit@node-0:~$
```

c. Now, we will install hping3 using **sudo apt-get install hping3** as shown below

```
Topology View List View Manifest Graphs node-0 x
0 upgraded, 0 newly installed, 0 to remove and 130 not upgraded.
fatal: destination path 'openflow' already exists and is not an empty directory.
pandit@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 (256 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) ...
pandit@node-0:~$
```

- d. Now we will run floodlight using `java -jar target/floodlight.jar` as shown below in new terminal shell window.

```
Topology View List View Manifest Graphs node-0 X node-0 X
* Documentation: https://help.ubuntu.com/
Last login: Fri Mar 1 23:11:10 2019 from ops.emulab.net
pandit@node-0:~$ cd floodlight/
pandit@node-0:~/floodlight$ java -jar target/floodlight.jar
23:18:15.760 INFO [n.f.c.m.FloodlightModuleLoader:main] Loading modules from src/main/resources/floodlightdefault.properties
23:18:15.874 WARN [n.f.r.RestApiServer:main] HTTPS disabled; HTTPS will not be used to connect to the REST API.
23:18:15.874 WARN [n.f.r.RestApiServer:main] HTTP enabled; Allowing unsecure access to REST API on port 8080.
23:18:16.952 WARN [n.f.c.i.OFSwitchManager:main] SSL disabled. Using unsecure connections between Floodlight and switches.
23:18:16.952 INFO [n.f.c.i.OFSwitchManager:main] Clear switch flow tables on initial handshake as master: TRUE
23:18:16.952 INFO [n.f.c.i.OFSwitchManager:main] Clear switch flow tables on each transition to master: TRUE
23:18:16.952 INFO [n.f.c.i.OFSwitchManager:main] Setting 0x1 as the default max tables to receive table-miss flow
23:18:16.957 INFO [n.f.c.i.OFSwitchManager:main] Setting max tables to receive table-miss flow to 0x1 for DPID 00:00:00:00:00:00:01
23:18:16.957 INFO [n.f.c.i.OFSwitchManager:main] Setting max tables to receive table-miss flow to 0x1 for DPID 00:00:00:00:00:00:02
23:18:17.006 INFO [n.f.c.i.OFSwitchManager:main] Computed OpenFlow version bitmap as [62]
23:18:17.007 INFO [n.f.c.i.Controller:main] OpenFlow port set to 6653
23:18:17.008 INFO [n.f.c.i.Controller:main] Number of worker threads set to 16
23:18:17.008 INFO [n.f.c.i.Controller:main] Controller role set to ACTIVE
23:18:17.033 INFO [n.f.l.i.LinkDiscoveryManager:main] Link latency history set to 10 LLDP data points
23:18:17.033 INFO [n.f.l.i.LinkDiscoveryManager:main] Latency update threshold set to +/-0.5 (50.0%) of rolling historical average
23:18:17.041 INFO [n.f.f.Forwarding:main] Default hard timeout not configured. Using 0.
```

3. Now we will use `sudo mn --controller=remote,ip=127.0.0.1,port=6653 -`
`-switch ovsk, protocols=OpenFlow13` to run mininet topology in new terminal
window as shown below.

```
Topology View List View Manifest Graphs node-0 X node-0 X node-0 X
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
pandit@node-0:~$ sudo mn --controller=remote,--switch=ovsk,ip=127.0.0.1,port=6653,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> 
```

4. We will use **pingall** on **mininet** to check hosts are reachable as shown below.

```
Topology View List View Manifest Graphs node-0 x node-0 x node-0 x
*** 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> pingall
*** Ping: testing ping reachability
h1 -> h2
h2 -> h1
*** Results: 0% dropped (2/2 received)
mininet> 
```

5. Now, we see flow rules at switch s1 using **sudo ovs-ofctl dump-flows s1 -O OpenFlow13** on a new terminal as shown below and observe that flow rules are empty as we didn't start ping yet.

```
Topology View List View Manifest Graphs node-0 x node-0 x node-0 x node-0 x
node-0:~> sudo ovs-ofctl dump-flows s1
NXST_FLOW reply (xid=0x4):
node-0:~> 
```

6. Now we will use **h1 hping3 h2 -c 10000 -S -flood -rand-source -v** to flood a lot of packets to h2 on the mininet terminal and observe that there are lot of flow rules added to switch s1 since packets are from random source since after receiving a packet controller sends message to switch to add new rule using OFPT_FLOW_MOD in response to OFPT_FLOW_IN

```
Topology View List View Manifest Graphs node-0 x node-0 x node-0 x node-0 x
s1
*** Adding links:
(h1, s1) (h2, s1)
*** Configuring hosts
h1 h2
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2
h2 -> h1
*** Results: 0% dropped (2/2 received)
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

```

```

Topology View List View Manifest Graphs node-0 node-0 node-0 node-0 node-0
cookie=0x20000000000000, duration=0.909s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=0, priority=1,tcp,in_port=1,d1_src=a2:8
0:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=110.214.14.101,nw_dst=10.0.0.2,tp_src=24357,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=1.222s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=1, priority=1,tcp,in_port=1,d1_src=a2:8
0:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=19.238.36.241,nw_dst=10.0.0.2,tp_src=23271,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=0.284s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=0, priority=1,tcp,in_port=1,d1_src=a2:8
0:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=125.140.112.237,nw_dst=10.0.0.2,tp_src=31001,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=1.468s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=1, priority=1,tcp,in_port=1,d1_src=a2:8
0:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=107.42.228.246,nw_dst=10.0.0.2,tp_src=23041,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=1.298s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=1, priority=1,tcp,in_port=1,d1_src=a2:8
0:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=55.174.76.234,nw_dst=10.0.0.2,tp_src=23210,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=0.2s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=0, priority=1,tcp,in_port=1,d1_src=a2:80:
ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=235.32.242.157,nw_dst=10.0.0.2,tp_src=31446,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=0.629s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=0, priority=1,tcp,in_port=1,d1_src=a2:8
0:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=212.222.246.5,nw_dst=10.0.0.2,tp_src=29151,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=4.77s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=4, priority=1,tcp,in_port=1,d1_src=a2:80
:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=1.13.21.222,nw_dst=10.0.0.2,tp_src=11704,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=0.584s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=0, priority=1,tcp,in_port=1,d1_src=a2:8
0:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=232.247.123.253,nw_dst=10.0.0.2,tp_src=29462,tp_dst=0 actions=output:2
cookie=0x20000000000000, duration=0.999s, table=0, n_packets=0, n_bytes=0, idle_timeout=5, idle_age=0, priority=1,tcp,in_port=1,d1_src=a2:8
0:ac:82:16:2d,d1_dst=2e:be:9a:2c:fc:a8,nw_src=46.216.67.73,nw_dst=10.0.0.2,tp_src=2404

```

- Now, we will stop **hping3** using **ctrl + C** on mininet terminal that was flooding packets and ping h1 from h2 and notice that time to fetch packet increased substantially which slowly decreases with time as shown below showing DoS Attack made service inaccessible.

```

Topology View List View Manifest Graphs node-0 node-0 node-0 node-0
--- 10.0.0.2 hping statistic ---
550069 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
mininet> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=25711 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=23695 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=22688 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=21680 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=20673 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=19669 ms
64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=18662 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=17655 ms
64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=16647 ms
64 bytes from 10.0.0.2: icmp_seq=11 ttl=64 time=15640 ms
64 bytes from 10.0.0.2: icmp_seq=12 ttl=64 time=14632 ms
64 bytes from 10.0.0.2: icmp_seq=13 ttl=64 time=13625 ms
64 bytes from 10.0.0.2: icmp_seq=14 ttl=64 time=12617 ms
64 bytes from 10.0.0.2: icmp_seq=17 ttl=64 time=9594 ms
64 bytes from 10.0.0.2: icmp_seq=18 ttl=64 time=8591 ms
64 bytes from 10.0.0.2: icmp_seq=20 ttl=64 time=6575 ms

```

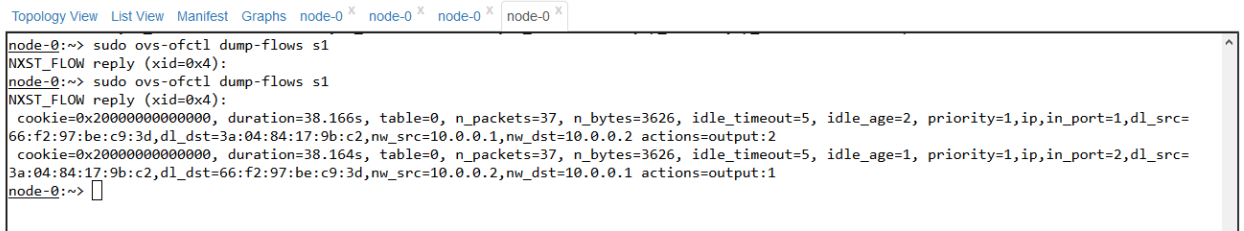
- Now, we wait for 2-3 mins and repeat **h1 ping h2** and observe the traffic flows and flow rules at switch s1 set by controller shows time got substantially decreased as shown below time=9.16ms against earlier 25711ms.

```

mininet> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=9.16 ms

```

9. Now, if we check flow table at **ovs switch s1** after attack is over the flow rules are back to normal against abnormally high shown in step 6 as shown below.



```
node-0:~> sudo ovs-ofctl dump-flows s1
NXST_FLOW reply (xid=0x4):
node-0:~> sudo ovs-ofctl dump-flows s1
NXST_FLOW reply (xid=0x4):
  cookie=0x2000000000000000, duration=38.166s, table=0, n_packets=37, n_bytes=3626, idle_timeout=5, idle_age=2, priority=1,ip,in_port=1,d1_src=
66:f2:97:be:c9:3d,d1_dst=3a:04:84:17:9b:c2,nw_src=10.0.0.1,nw_dst=10.0.0.2 actions=output:2
  cookie=0x2000000000000000, duration=38.164s, table=0, n_packets=37, n_bytes=3626, idle_timeout=5, idle_age=1, priority=1,ip,in_port=2,d1_src=
3a:04:84:17:9b:c2,d1_dst=66:f2:97:be:c9:3d,nw_src=10.0.0.2,nw_dst=10.0.0.1 actions=output:1
node-0:~>
```

CONCLUSION:

So, we successfully showed how DoS attack resulted in resource exhaustion and making services inaccessible as shown from state of switch and time to ping hosts. This happens as switch starts to drop packets since it doesn't receive instructions to add flow-entry due to resource exhaustion.