

Project/Lab 3

Submitted by : Nandini Krupa Krishnamurthy

Task:

To launch man-in-the-middle attack in SDN and understand how attackers can steal information and to understand the importance of a secure communication between the controller and switch.

Experiment:

All the steps are explained along with the screenshots.

Step1 : Starting the experiment by creating a profile.

Step 1.1: Creating controller profile.

Figures starting from Fig1 to Fig12 show the steps needed to create a profile for controller and also for starting it.

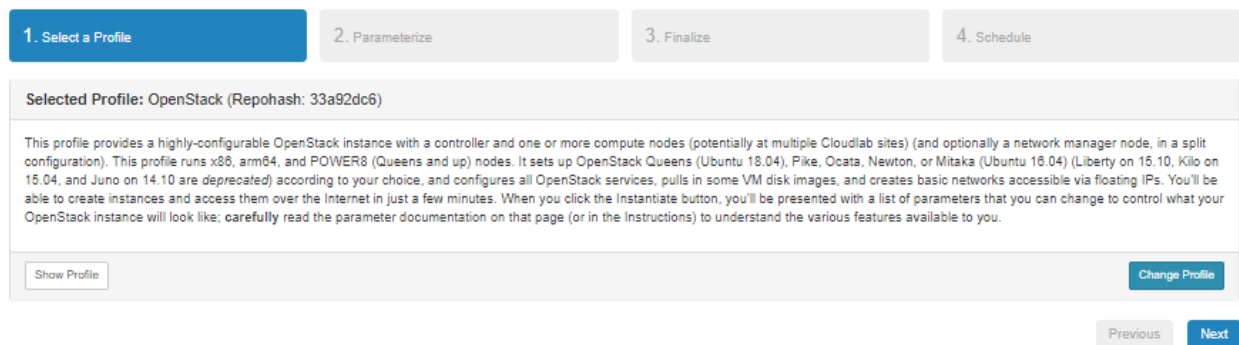


Fig 1 : Changing a profile for the experiment.

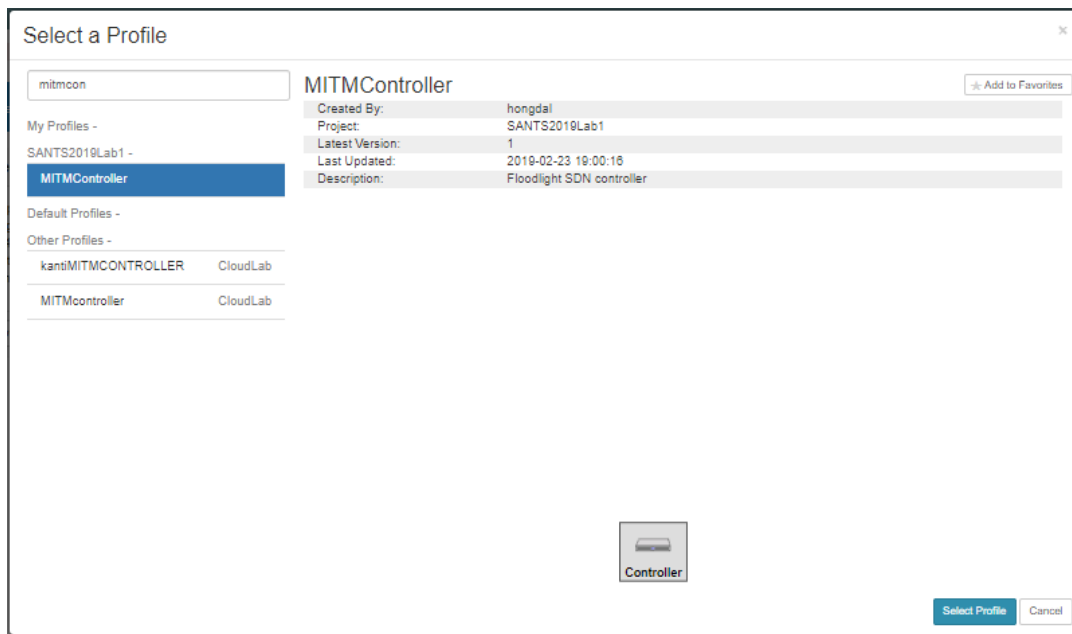


Fig 2: MITMController is necessary for this experiment.

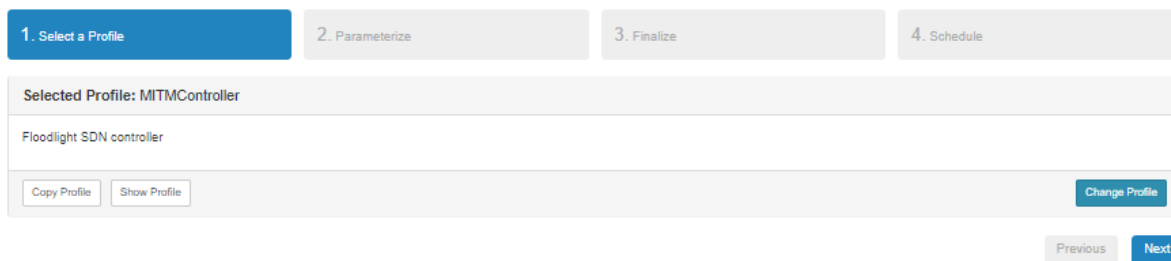


Fig 3: Selecting and changing a profile.

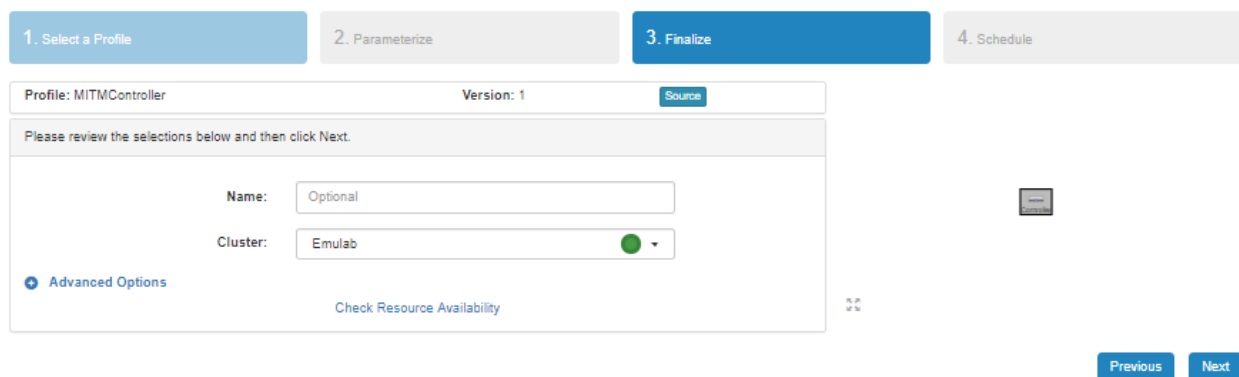


Fig 4: Selecting a Cluster (the one chosen here is Emulab).

1. Select a Profile

2. Parameterize

3. Finalize

4. Schedule

Please select when you would like to start this experiment and then click Finish.

Start immediately

or

Start on date/time

MM/DD/YYYY

Time

Experiment Duration

16 hours

Previous

Finish

Fig 5: Selecting the duration of the experiment.

Your experiment is ready!

Name: Krupa-QV49112

State: ready

Profile: MITMAttacks_kk

Started: Mar 25, 2019 4:23 PM

Expires: Mar 26, 2019 8:23 AM (in 16 hours)

Logs

Create Disk Image

Copy

Extend

Terminate

Profile Instructions

Topology View

List View

Manifest

Graphs

Controller

Controller

Controller

Click on a node for more options. Click and drag to move things around.

Reload Topo

Refresh Status

Fig 6: The controller is running successfully.

Topology View

List View

Manifest

Graphs

Controller

Controller

Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Mar 25 14:26:21 2019 from 155.98.33.74

```

controller:~> ifconfig
eth0      Link encap:Ethernet  HWaddr 02:49:5c:9b:ae:d2
          inet addr:155.98.37.82  Bcast:155.98.39.255  Mask:255.255.252.0
          inet6 addr: fe80::49:5cff:fe9b:aed2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:384 errors:0 dropped:0 overruns:0 frame:0
          TX packets:436 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:77607 (77.6 KB)  TX bytes:49737 (49.7 KB)

lo        Link encap:Local Loopback

          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1

          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          collisions:0 txqueuelen:1  pped:0 overruns:0 carrier:0

```

Fig 7: Finding IP of the controller using “ipconfig”.

```
Topology View List View Manifest Graphs Controller X Controller X
COLLISIONS:0 txqueuelen:1 pped:0 overruns:0 carrier:0
RX bytes:1560 (1.5 KB) TX bytes:1560 (1.5 KB)
controller:~> sudo su -
root@controller:~# wget 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.
Length: 310 [text/x-sh]ting response... 200 OK
Saving to: 'set_floodlight.sh'
set_floodlight.sh                               100%[=====] 310  --KB/s  in 0s

2019-03-25 14:28:28 (3.59 MB/s) - 'set_floodlight.sh' saved [310/310]
--2019-03-25 14:28:28-- http://./
wget: unable to resolve host address '.'sociated with hostname.
FINISHED --2019-03-25 14:28:28--
```

Fig 8: Switching to “root” using “sudo su –”.

```
Topology View List View Manifest Graphs Controller X
RX packets:24 errors:0 dropped:0 overruns:0 frame:0
collisions:0 txqueuelen:1 pped:0 overruns:0 carrier:0
RX bytes:1560 (1.5 KB) TX bytes:1560 (1.5 KB)
controller:~> sudo su -
root@controller:~# wget https://people.cs.clemson.edu/~hongdal/set_floodlight.sh .
```

Fig 9: Downloading floodlight using
“wget https://people.cs.clemson.edu/~hongdal/set_floodlight.sh .”

```
Topology View List View Manifest Graphs Controller X
set_floodlight.sh 100%[=====]

2019-03-25 14:28:28 (3.59 MB/s) - 'set_floodlight.sh' saved [310/310]
--2019-03-25 14:28:28-- http://./
wget: unable to resolve host address '.'sociated with hostname.
FINISHED --2019-03-25 14:28:28--

Downloaded: 1 files, 310 in 0s (3.59 MB/s)
root@controller:~# chmod +x set_floodlight.sh

Get:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:2 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]

Get:4 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1,201 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial/main i386 Packages [1,196 kB]

Get:7 http://us.archive.ubuntu.com/ubuntu xenial/restricted amd64 Packages [8,344 B]
Get:8 http://us.archive.ubuntu.com/ubuntu xenial/restricted i386 Packages [8,684 B]
```

Fig 10: Using “chmod +x set_floodlight.sh” to change permission and then using “./set_floodlight.sh” to set it.

```
Topology View List View Manifest Graphs Controller x Controller x
[javac] NOTE: Recompile with -Xlint:unchecked for details.
[javac] 1 warning
[copy] Copying 54 files to /root/floodlight/target/bin

compile-test:
[javac] Compiling 91 source files to /root/floodlight/target/bin-test
[javac] warning: [options] bootstrap class path not set in conjunction with -source 1.7
[javac] 1 warning

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

BUILD SUCCESSFUL
Total time: 55 seconds
root@controller:~# cd floodlight
root@controller:~/floodlight# java -jar target/floodlight.jar
```

Fig 11: Changing directory to floodlight using “cd floodlight” and starting floodlight using “java -jar target/floodlight.jar”.

```
Topology View List View Manifest Graphs Controller x Controller x
14:42:47.558 INFO [n.f.f.Forwarding:main] Default idle timeout not configured. Using 5.
14:42:47.558 INFO [n.f.f.Forwarding:main] Default priority not configured. Using 1.
14:42:47.560 INFO [n.f.f.Forwarding:main] Default flags will be empty.
14:42:47.560 INFO [n.f.f.Forwarding:main] Default flow matches set to: VLAN=true, MAC=true, IP=true, TPPT=true
14:42:47.561 INFO [n.f.f.Forwarding:main] Not flooding ARP packets. ARP flows will be inserted for known destinations
14:42:47.563 INFO [n.f.s.StatisticsCollector:main] Statistics collection disabled
14:42:47.564 INFO [n.f.s.StatisticsCollector:main] Port statistics collection interval set to 10s
14:42:48.587 INFO [o.s.s.i.c.FallbackCCProvider:main] Cluster not yet configured; using fallback local configuration
14:42:48.588 INFO [o.s.s.i.SyncManager:main] [32767] Updating sync configuration ClusterConfig [allNodes={32767=Node [ho:
torePath=/etc/floodlight/auth_credentials.jceks, keyStorePassword is unset]
14:42:49.137 INFO [o.s.s.i.r.RPCService:main] Listening for internal floodlight RPC on localhost/127.0.0.1:6642
14:42:49.187 INFO [n.f.c.i.OFSwitchManager:main] Listening for switch connections on /0.0.0.0:6653
14:42:49.210 INFO [n.f.l.i.LinkDiscoveryManager:main] Setting autoportfast feature to OFF
14:42:56.930 INFO [n.f.j.JythonServer:debugserver-main] Starting DebugServer on :6655
14:43:04.217 INFO [n.f.l.i.LinkDiscoveryManager:Scheduled-3] Sending LLDP packets out of all the enabled ports
14:43:19.222 INFO [n.f.l.i.LinkDiscoveryManager:Scheduled-0] Sending LLDP packets out of all the enabled ports
14:43:34.229 INFO [n.f.l.i.LinkDiscoveryManager:Scheduled-3] Sending LLDP packets out of all the enabled ports
14:43:49.235 INFO [n.f.l.i.LinkDiscoveryManager:Scheduled-4] Sending LLDP packets out of all the enabled ports
```

Fig 12: Controller has successfully started to send packets.

Step 1.2 – Creating profile for nodes needed for experiment.

Figures from Fig 13 to Fig 18 show the steps needed to create a profile for nodes and for configuring it with the controller.

Modify Profile

Name: MITMAttack
Version: 1
Project: SANTS2019Lab1
Creator: Knapa
Updated by: Knapa
Updated: Mar 24, 2019 9:46 AM
[Activity](#)

Modify Profile SANTS2019Lab1/MITMAttack

Source code [Edit Topology](#) [Edit Code](#) [Convert to gen-rl](#) [New](#)

Description [?](#)
Man in the middle attack lab. Add routable IPs to user1 and user2

Instructions [?](#)
Man in the middle attack lab

[Show/Hide Tour](#)

Who can instantiate your profile?
☐ Anyone
☒ Only members of your project
☐ Allow members of your project to modify this profile [?](#)

[Delete](#) [Copy](#) [Share](#) [Instantiate](#)

[Save](#) [Cancel](#)

Fig 13: Adding the topology downloaded from <https://people.cs.clemson.edu/~hongdal/mitm-attack.xml> into the new profile here by using “Edit Topology” button.

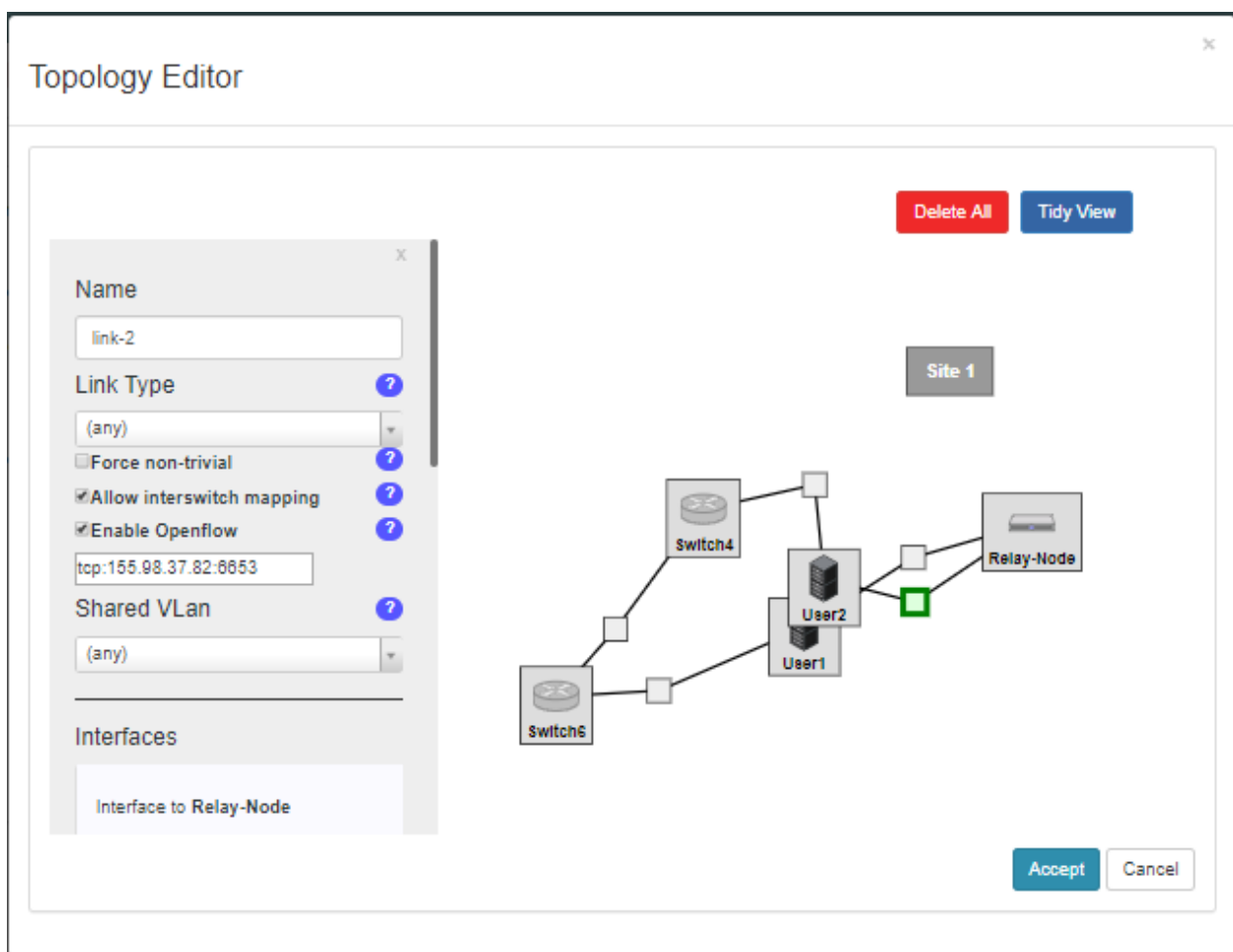


Fig 14: IP address of the controller is added to link2. Here IP of the controller is : 155.98.37.82.

Modify Profile

Name: MITMAttack
Version: 2
Project: SANTS2019Lab1
Creator: Krupa
Updated by: Krupa
Updated: Mar 25, 2019 12:43 PM
[Activity](#)

Modify Profile SANTS2019Lab1/MITMAttack

Source code

[Edit Topology](#)
[Edit Code](#)
[Convert to genesis](#)

Description

Man in the middle attack lab. Add routable IPs to user1 and user2

Instructions

Man in the middle attack lab

[Show/Edit Tour](#)

Who can instantiate your profile?

☐ Anyone
☒ Only members of your project
☐ Allow members of your project to modify this profile.

[Delete](#)
[Copy](#)
[Share](#)
[Instantiate](#)

[Save](#)
[Cancel](#)

Version History

Vers	Description	Created	From
2	Man in the middle attack lab. Add routable IPs to user1 and user2	2019-03-25	1
1	Man in the middle attack lab. Add routable IPs to user1 and user2	2019-03-24	0
0	Man in the middle attack lab. Add routable IPs to user1 and user2	2019-03-24	

Fig 15: Saving the profile and instantiating it.

1. Select a Profile

2. Parameterize

3. Finalize

4. Schedule

Profile: MITMAttack Version: 2 [Source](#)

Please review the selections below and then click Next.

Name: Optional

Cluster: Emulab

[Advanced Options](#)

[Check Resource Availability](#)

[Previous](#)
[Next](#)

Fig16: Selecting a Cluster (the one chosen here is Emulab).

1. Select a Profile

2. Parameterize

3. Finalize

4. Schedule

Please select when you would like to start this experiment and then click Finish.

Start immediately

☒

or

Start on date/time

MM/DD/YYYY

Time

Experiment Duration

18 hours

[Previous](#)
[Finish](#)

Fig17: Selecting the duration of the experiment.

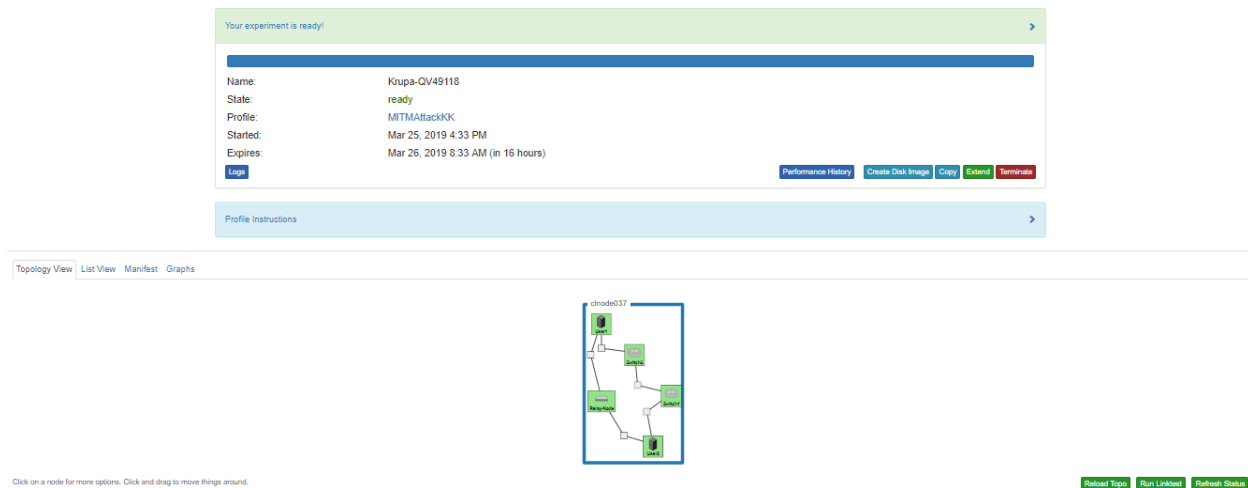


Fig 18: Profile is successfully created.

Step 2: Starting the Experiment.

Figures starting from Fig 19 to Fig 34 shows the steps needed to start this experiment.

Step 2.1: Setting up OVS for User1.

```

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@user1:~$ sudo su -
root@user1:~# get https://people.cs.clemson.edu/~hongdal/set_ovs.sh

```

Fig 19: Switching to root using “sudo su -” and downloading script - set_ovs.sh using “wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh” for User1.


```
Topology View List View Manifest Graphs User1 User2 Switch4 Switch6 Relay-Node
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@user1:~$ sudo su -
root@user1:~# get https://people.cs.clemson.edu/~hongdal/set_ovs.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.
Length: 374 [text/x-sh]ting response... 200 OK

Saving to: 'set_ovs.sh'
set_ovs.sh                               100%[=====] 374 --KB/s in 0s

2019-03-25 16:51:05 (7.82 MB/s) - 'set_ovs.sh' saved [374/374]

root@user1:~#
```

Fig 20: Script is downloaded successfully.

```
Topology View List View Manifest Graphs User1 User2 Switch4 Switch6 Relay-Node
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@user1:~$ sudo su -
root@user1:~# get https://people.cs.clemson.edu/~hongdal/set_ovs.sh
Resolving people.cs.clemson.edu (people.cs.clemson.edu)... 130.127.201.228, 2620:103:a004:
Connecting to people.cs.clemson.edu (people.cs.clemson.edu)[130.127.201.228]:443... connec
Length: 374 [text/x-sh]ting response... 200 OK

Saving to: 'set_ovs.sh'
set_ovs.sh                               100%[=====]

2019-03-25 16:51:05 (7.82 MB/s) - 'set_ovs.sh' saved [374/374]

root@user1:~# chmod +x set_ovs.sh
root@user1:~# ./set_ovs.sh eth1 eth2 155.98.37.82 10.10.10.1
```

Fig 21: Changing permissions using “chmod +x set_ovs.sh” and setting the User1 with the controller using “./set_ovs.sh eth1 eth2 155.98.37.82 10.10.10.1”. Here 10.10.10.1 is the experimental IP we have provided for User1.

```
Topology View List View Manifest Graphs User1 User2 Switch4 Switch6 Relay-Node
Selecting previously unselected package openvswitch-switch.

Unpacking openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...16.04.2_amd64.deb ...
Processing triggers for man-db (2.7.5-1) ...

ureadahead will be reprofiled on next reboot19) ...
Processing triggers for systemd (229-4ubuntu21.15) ...

Setting up openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...
update-alternatives: using /usr/lib/openvswitch-switch/ovs-vswitchd to provide /usr/sbin/ovs-vswitchd (ovs-vswitchd) in auto mode

inserv: can not symlink(/.init.d/pubsubd, ../rc2.d/S01pubsubd): File exists
inserv: can not symlink(/.init.d/pubsubd, ../rc3.d/S01pubsubd): File exists

openvswitch-nonetwork.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (229-4ubuntu21.15) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@user1:~#
```

Fig 22: openswitch network is successfully established.

Step 2.2: Setting up OVS for User1.

```
Topology View List View Manifest Graphs User1 User2 Switch4 Switch6 Relay-Node
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '16.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@user2:~$ sudo su -
root@user2:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh
```

Fig 23: Switching to root using “sudo su –” and downloading script - set_ovs.sh using “wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh” for User2.

```
Topology View List View Manifest Graphs User1 User2 Switch4 Switch6 Relay-Node
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@user2:~$ sudo su -
root@user2:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.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.
Length: 374 [text/x-sh]ting response... 200 OK

Saving to: 'set_ovs.sh'
set_ovs.sh                               100%[=====] 374 --.-KB/s  in 0s

2019-03-25 16:53:20 (8.18 MB/s) - 'set_ovs.sh' saved [374/374]

root@user2:~#
```

Fig 24: Script is downloaded successfully.

```
Topology View List View Manifest Graphs User1 User2 Switch4 Switch6 Relay-Node
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@user2:~$ sudo su -
root@user2:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.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.
Length: 374 [text/x-sh]ting response... 200 OK

Saving to: 'set_ovs.sh'
set_ovs.sh                               100%[=====] 374 --.-KB/s  in 0s

2019-03-25 16:53:20 (8.18 MB/s) - 'set_ovs.sh' saved [374/374]

root@user2:~# chmod +x set_ovs.sh
root@user2:~# ./set_ovs.sh eth1 eth2 155.98.37.82 10.10.10.2
```

Fig 25: Changing permissions using “chmod +x set_ovs.sh” and setting the User1 with the controller using “./set_ovs.sh eth1 eth2 155.98.37.82 10.10.10.2”. Here 10.10.10.2 is the experimental IP we have provided for User2.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
Selecting previously unselected package openvswitch-switch.
Unpacking openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...16.04.2_amd64.deb ...
Processing triggers for man-db (2.7.5-1) ...

ureadahead will be reprofiled on next reboot19) ...
Processing triggers for systemd (229-4ubuntu21.15) ...

Setting up openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...
update-alternatives: using /usr/lib/openvswitch-switch/ovs-vswitchd to provide /usr/sbin/ovs-vswitchd (ovs-vswitchd) in auto mode

insserv: can not symlink(/usr/lib/openvswitch-switch/ovs-vswitchd) to provide /usr/sbin/ovs-vswitchd (ovs-vswitchd) in auto mode
insserv: can not symlink(/usr/lib/openvswitch-switch/ovs-vswitchd) to provide /usr/sbin/ovs-vswitchd (ovs-vswitchd) in auto mode

openvswitch-nonetwork.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (229-4ubuntu21.15) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@user2:~#
```

Fig 26: openswitch network is successfully established.

Step 2.3: Setting up OVS for Switch4

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@switch4:~$ sudo su -
root@switch4:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh
```

Fig 27: Switching to root using “sudo su –” and downloading script - set_ovs.sh using “wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh” for Switch4.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@switch4:~$ sudo su -
root@switch4:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh
Resolving people.cs.clemson.edu (people.cs.clemson.edu)... 130.127.201.228, 2620:103:0004:e::228
Connecting to people.cs.clemson.edu (people.cs.clemson.edu)[130.127.201.228]:443... connected.
Length: 374 [text/x-sh]ting response... 200 OK
Saving to: 'set_ovs.sh'
set_ovs.sh                               100%[=====] 374 ---KB/s  in 0s

2019-03-25 16:55:03 (8.05 MB/s) - 'set_ovs.sh' saved [374/374]
root@switch4:~#
```

Fig 28: Script is downloaded successfully.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@switch4:~$ sudo su -
root@switch4:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.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.
Length: 374 [text/x-sh]ting response... 200 OK

Saving to: 'set_ovs.sh'
set_ovs.sh                               100%[=====

2019-03-25 16:55:03 (8.05 MB/s) - 'set_ovs.sh' saved [374/374]

root@switch4:~# chmod +x set_ovs.sh
root@switch4:~# ./set_ovs.sh eth1 eth2 155.98.37.82 10.10.10.3
```

Fig 29: Changing permissions using “chmod +x set_ovs.sh” and setting the User1 with the controller using “./set_ovs.sh eth1 eth2 155.98.37.82 10.10.10.3”. Here 10.10.10.3 is the experimental IP we have provided for Switch4.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

Selecting previously unselected package openvswitch-switch.
Unpacking openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ....16.04.2_amd64.deb ...
Processing triggers for man-db (2.7.5-1) ...

ureadahead will be reprofiled on next reboot19) ...
Processing triggers for systemd (229-4ubuntu21.15) ...

Setting up openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...
update-alternatives: using /usr/lib/openvswitch-switch/ovs-vswitchd to provide /usr/sbin/o

insserv: can not symlink(../init.d/pubsubd, ../rc2.d/S01pubsubd): File exists
insserv: can not symlink(../init.d/pubsubd, ../rc3.d/S01pubsubd): File exists

openvswitch-nonetwork.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (229-4ubuntu21.15) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@switch4:~#
```

Fig 30: openswitch network is successfully established.

Step 2.4: Setting up OVS for Switch 6

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '16.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@switch6:~$ sudo su -
root@switch6:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh
```

Fig 31: Switching to root using “sudo su -” and downloading script - set_ovs.sh using “wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh” for Switch6.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@switch6:~$ sudo su -
root@switch6:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.sh
Resolving people.cs.clemson.edu (people.cs.clemson.edu)... 130.127.201.228, 2620:103:8004:e::228
Connecting to people.cs.clemson.edu (people.cs.clemson.edu)[130.127.201.228]:443... connected.
Length: 374 [text/x-sh]ting response... 200 OK

Saving to: 'set_ovs.sh'
set_ovs.sh                               100%[=====] 374  --KB/s  in 0s

2019-03-25 16:56:52 (8.16 MB/s) - 'set_ovs.sh' saved [374/374]

root@switch6:~#
```

Fig 32: Script is downloaded successfully.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Krupa@switch6:~$ sudo su -
root@switch6:~# wget https://people.cs.clemson.edu/~hongdal/set_ovs.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.
Length: 374 [text/x-sh]ting response... 200 OK

Saving to: 'set_ovs.sh'
set_ovs.sh                               100%[=====]

2019-03-25 16:56:52 (8.16 MB/s) - 'set_ovs.sh' saved [374/374]

root@switch6:~# chmod +x set_ovs.sh
root@switch6:~# ./set_ovs.sh eth1 eth2 155.98.37.82 10.10.10.4
```

Fig 33: Changing permissions using “chmod +x set_ovs.sh” and setting the User1 with the controller using “./set_ovs.sh eth1 eth2 155.98.37.82 10.10.10.4”. Here 10.10.10.4 is the experimental IP we have provided for Switch6.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

Selecting previously unselected package openvswitch-switch.
Unpacking openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...16.04.2_amd64.deb ...
Processing triggers for man-db (2.7.5-1) ...

ureadahead will be reprofiled on next reboot19) ...
Processing triggers for systemd (229-4ubuntu21.15) ...

Setting up openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...
update-alternatives: using /usr/lib/openvswitch-switch/ovs-vswitchd to provide /usr/sbin/ovs-vswitchd (ovs-vswitchd) in auto mode

insserv: can not symlink(/etc/passwd, /etc/passwd): File exists
insserv: can not symlink(/etc/passwd, /etc/passwd): File exists

openvswitch-nonetwork.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (229-4ubuntu21.15) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@switch6:~#
```

Fig 34: openvswitch network is successfully established.

Step 3: Conducting the Experiment (Normal Flow)

Figures starting from Fig 35 to Fig 43 show the normal flow of packets when there is no attack.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

10      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:24 errors:0 dropped:0 overruns:0 frame:0
        TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)

ovs-lan Link encap:Ethernet  HWaddr 2e:ea:a4:76:03:4f
        inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.0
        inet6 addr: fe80::2cea:a4ff:fe76:34f/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:4 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:224 (224.0 B)  TX bytes:648 (648.0 B)

root@user1:~#
```

Fig 35: Experimental IP address of the User1: 10.10.10.1 using “ipconfig”.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

10      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:24 errors:0 dropped:0 overruns:0 frame:0
        TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)

ovs-lan Link encap:Ethernet  HWaddr c2:88:09:57:77:4b
        inet addr:10.10.10.2  Bcast:10.10.10.255  Mask:255.255.255.0
        inet6 addr: fe80::c088:9ff:fe57:774b/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:7 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:392 (392.0 B)  TX bytes:648 (648.0 B)

root@user2:~#
```

Fig 36: Experimental IP address of the User1: 10.10.10.2 using “ipconfig”.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:24 errors:0 dropped:0 overruns:0 frame:0
        TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:1560 (1.5 KB)  TX bytes:1560 (1.5 KB)

ovs-lan Link encap:Ethernet  HWaddr 2e:ea:a4:76:03:4f
        inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.0
        inet6 addr: fe80::2cea:a4ff:fe76:34f/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:4 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:224 (224.0 B)  TX bytes:648 (648.0 B)

root@user1:~# ping 10.10.10.2

```

Fig 37: Pinging from User1 to User2 using “ping 10.10.10.2”.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

        inet6 addr: fe80::2cea:a4ff:fe76:34f/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:4 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:224 (224.0 B)  TX bytes:648 (648.0 B)

root@user1:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data:
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=711 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=1.06 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.956 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=64 time=0.600 ms
64 bytes from 10.10.10.2: icmp_seq=5 ttl=64 time=0.598 ms
64 bytes from 10.10.10.2: icmp_seq=6 ttl=64 time=0.593 ms
64 bytes from 10.10.10.2: icmp_seq=7 ttl=64 time=0.571 ms
64 bytes from 10.10.10.2: icmp_seq=8 ttl=64 time=0.640 ms
64 bytes from 10.10.10.2: icmp_seq=9 ttl=64 time=0.612 ms

```

Fig 38: Ping successful.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

Unpacking openvswitch-common (2.5.5-0ubuntu0.16.04.2) ...16.04.2_amd64.deb ...
Selecting previously unselected package openvswitch-switch.

Unpacking openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...16.04.2_amd64.deb ...
Processing triggers for man-db (2.7.5-1) ...

ureadahead will be reprofiled on next reboot19) ...
Processing triggers for systemd (229-4ubuntu21.15) ...

Setting up openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...
update-alternatives: using /usr/lib/openvswitch-switch/ovs-vswitchd to provide /usr/sbin/ovs-vswitchd (ovs-vswitchd) in auto mode

inserv: can not symlink(/init.d/pubsubd, ../rc2.d/S01pubsubd): File exists
inserv: can not symlink(/init.d/pubsubd, ../rc3.d/S01pubsubd): File exists

openvswitch-nonetwork.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (229-4ubuntu21.15) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@switch4:~# tcpdump -i eth1 -nq icmp

```

Fig 39: Using “tcpdump -i eth1 -nq icmp” to view the packets through Switch4.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

inserv: can not symlink(/init.d/pubsubd, ../rc2.d/S01pubsubd): File exists
inserv: can not symlink(/init.d/pubsubd, ../rc3.d/S01pubsubd): File exists

openvswitch-nonetwork.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (229-4ubuntu21.15) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@switch4:~# tcpdump -i eth1 -nq icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:01:38.522386 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 68, length 64
17:01:38.522565 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 68, length 64
17:01:39.522386 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 69, length 64
17:01:39.522566 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 69, length 64
17:01:40.522366 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 70, length 64
17:01:40.522595 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 70, length 64
17:01:41.522382 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 71, length 64
17:01:41.522557 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 71, length 64

```

Fig 40: Packets are flowing through Switch4.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

Unpacking openvswitch-common (2.5.5-0ubuntu0.16.04.2) ....16.04.2_amd64.deb ...
Selecting previously unselected package openvswitch-switch.

Unpacking openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ....16.04.2_amd64.deb ...
Processing triggers for man-db (2.7.5-1) ...

ureadahead will be reprofiled on next reboot19) ...
Processing triggers for systemd (229-4ubuntu21.15) ...

Setting up openvswitch-switch (2.5.5-0ubuntu0.16.04.2) ...
update-alternatives: using /usr/lib/openvswitch-switch/ovs-vswitchd to provide /usr/sbin/ovs-vswitchd

inserv: can not symlink(/init.d/pubsubd, /rc2.d/S01pubsubd): File exists
inserv: can not symlink(/init.d/pubsubd, /rc3.d/S01pubsubd): File exists

openvswitch-nonetwork.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (229-4ubuntu21.15) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@switch6:~# tcpdump -i eth1 -nq icmp

```

Fig 41: Using “tcpdump -i eth1 -nq icmp” to view the packets through Switch6.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

inserv: can not symlink(/init.d/pubsubd, /rc3.d/S01pubsubd): File exists

openvswitch-nonetwork.service is a disabled or a static unit, not starting it.
Processing triggers for systemd (229-4ubuntu21.15) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@switch6:~# tcpdump -i eth1 -nq icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:02:13.524566 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 103, length 64
17:02:13.524907 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 103, length 64
17:02:14.524524 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 104, length 64
17:02:14.524951 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 104, length 64
17:02:15.524567 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 105, length 64
17:02:15.524894 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 105, length 64
17:02:16.524569 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 106, length 64
17:02:16.524907 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 106, length 64
17:02:17.524570 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 107, length 64
17:02:17.525028 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 107, length 64

```

Fig 42: Packets are flowing through Switch6.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
root@relay-node:~# tcpdump -i eth1 -nq icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Fig 43: When “tcpdump -i eth1 -nq icmp” is used for Relay_Node, it is observed that no packet is flowing through it.

Step 4 – Conduct Man-In-Middle-Attack.

Figures starting from Fig 44 to Fig 53 show the flow of traffic in case of an MITM attack.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
root@relay-node:~# tcpdump -i eth1 -nq icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@relay-node:~# wget https://people.cs.clemson.edu/~hongdal/attack.sh
```

Fig 44: Downloading attack script using “wget https://people.cs.clemson.edu/~hongdal/attack.sh”.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
root@relay-node:~# tcpdump -i eth1 -nq icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@relay-node:~# wget https://people.cs.clemson.edu/~hongdal/attack.sh
--2019-03-25 17:05:34-- https://people.cs.clemson.edu/~hongdal/attack.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: 374 [text/x-sh]
Saving to: 'attack.sh'

attack.sh                               100%[=====] 374 --KB/s in 0s

2019-03-25 17:05:35 (7.99 MB/s) - 'attack.sh' saved [374/374]
root@relay-node:~#
```

Fig 45: Script is successfully downloaded.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@relay-node:~# wget https://people.cs.clemson.edu/~hongdal/attack.sh
--2019-03-25 17:05:34-- https://people.cs.clemson.edu/~hongdal/attack.sh
Resolving people.cs.clemson.edu (people.cs.clemson.edu)... 130.127.201.228, 2620:103:a004:
Connecting to people.cs.clemson.edu (people.cs.clemson.edu)|130.127.201.228|:443... connec
HTTP request sent, awaiting response... 200 OK
Length: 374 [text/x-sh]
Saving to: 'attack.sh'

attack.sh                               100%[=====]

2019-03-25 17:05:35 (7.99 MB/s) - 'attack.sh' saved [374/374]
root@relay-node:~# chmod +x attack.sh

root@relay-node:~# ./attack.sh eth1 eth2 155.98.37.82 10.10.10.5

```

Fig 46: Changing the permissions using “chmod +x attack.sh” and starting the attack by running the command “./ attack.sh eth1 eth2 155.98.37.82 10.10.10.5”. Here 155.98.37.82 denotes the controller IP and 10.10.10.5 denotes the Relay-Node IP.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

Selecting previously unselected package openvswitch-switch.
Preparing to unpack .../openvswitch-switch_2.5.5-0ubuntu0.16.04.2_amd64.deb ...
Processing triggers for man-db (2.7.5-1) ...16.04.2) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for systemd (229-4ubuntu21.15) ...
Setting up openvswitch-common (2.5.5-0ubuntu0.16.04.2) ...

update-alternatives: using /usr/lib/openvswitch-switch/ovs-vswitchd to provide /usr/sbin/ovs-vswitchd (ovs-vswitchd) in auto mode
insserv: can not symlink(/init.d/pubsubd, ../rc1.d/K01pubsubd): File exists
insserv: can not symlink(/init.d/pubsubd, ../rc3.d/S01pubsubd): File exists
insserv: can not symlink(/init.d/pubsubd, ../rc6.d/K01pubsubd): File exists

Processing triggers for systemd (229-4ubuntu21.15) ...c unit, not starting it.
Processing triggers for ureadahead (0.100.0-19) ...

root@relay-node:~#

```

Fig 47: Attack is initiated.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

64 bytes from 10.10.10.2: icmp_seq=213 ttl=64 time=0.595 ms
64 bytes from 10.10.10.2: icmp_seq=214 ttl=64 time=0.676 ms
64 bytes from 10.10.10.2: icmp_seq=215 ttl=64 time=0.608 ms
64 bytes from 10.10.10.2: icmp_seq=216 ttl=64 time=0.596 ms
64 bytes from 10.10.10.2: icmp_seq=217 ttl=64 time=0.626 ms
64 bytes from 10.10.10.2: icmp_seq=218 ttl=64 time=0.588 ms
64 bytes from 10.10.10.2: icmp_seq=219 ttl=64 time=0.579 ms
64 bytes from 10.10.10.2: icmp_seq=220 ttl=64 time=0.625 ms
64 bytes from 10.10.10.2: icmp_seq=221 ttl=64 time=0.742 ms
64 bytes from 10.10.10.2: icmp_seq=222 ttl=64 time=0.712 ms
64 bytes from 10.10.10.2: icmp_seq=223 ttl=64 time=0.638 ms
64 bytes from 10.10.10.2: icmp_seq=224 ttl=64 time=0.637 ms
64 bytes from 10.10.10.2: icmp_seq=225 ttl=64 time=0.656 ms
64 bytes from 10.10.10.2: icmp_seq=226 ttl=64 time=0.797 ms
^C
--- 10.10.10.2 ping statistics ---
226 packets transmitted, 226 received, 0% packet loss, time 225001ms
rtt min/avg/max/mdev = 0.503/3.775/711.876/47.206 ms
root@user1:~# ping 10.10.10.2

```

Fig 48: User2 is pinged again from User1.

Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x

```

64 bytes from 10.10.10.2: icmp_seq=222 ttl=64 time=0.712 ms
64 bytes from 10.10.10.2: icmp_seq=223 ttl=64 time=0.638 ms
64 bytes from 10.10.10.2: icmp_seq=224 ttl=64 time=0.637 ms
64 bytes from 10.10.10.2: icmp_seq=225 ttl=64 time=0.656 ms
64 bytes from 10.10.10.2: icmp_seq=226 ttl=64 time=0.797 ms
^C
--- 10.10.10.2 ping statistics ---
226 packets transmitted, 226 received, 0% packet loss, time 225001ms
rtt min/avg/max/mdev = 0.503/3.775/711.876/47.206 ms
root@user1:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=113 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.729 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.397 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=64 time=0.402 ms
64 bytes from 10.10.10.2: icmp_seq=5 ttl=64 time=0.407 ms
64 bytes from 10.10.10.2: icmp_seq=6 ttl=64 time=0.406 ms
64 bytes from 10.10.10.2: icmp_seq=7 ttl=64 time=0.406 ms

```

Fig 49: Ping is successful.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
Selecting previously unselected package openvswitch-switch.
Preparing to unpack .../openvswitch-switch_2.5.5-0ubuntu0.16.04.2_amd64.deb ...

Processing triggers for man-db (2.7.5-1) ....16.04.2) ...
Processing triggers for ureadahead (0.100.0-19) ...

Processing triggers for systemd (229-4ubuntu21.15) ...
Setting up openvswitch-common (2.5.5-0ubuntu0.16.04.2) ...

update-alternatives: using /usr/lib/openvswitch-switch/ovs-vswitchd to provide /usr/sbin/ovs-vswitchd (ovs-vswitchd) in auto mode
insserv: can not symlink(/../init.d/pubsubd, ../rc1.d/K01pubsubd): File exists

insserv: can not symlink(/../init.d/pubsubd, ../rc3.d/S01pubsubd): File exists
insserv: can not symlink(/../init.d/pubsubd, ../rc6.d/K01pubsubd): File exists

Processing triggers for systemd (229-4ubuntu21.15) ...c unit, not starting it.
Processing triggers for ureadahead (0.100.0-19) ...

root@relay-node:~# tcpdump -i eth1 -nq icmp
```

Fig 50: “tcpdump -i eth1 -nq icmp” is the command used to observe the flow of packets in Relay-Node.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
insserv: can not symlink(/../init.d/pubsubd, ../rc1.d/K01pubsubd): File exists

insserv: can not symlink(/../init.d/pubsubd, ../rc3.d/S01pubsubd): File exists
insserv: can not symlink(/../init.d/pubsubd, ../rc6.d/K01pubsubd): File exists

Processing triggers for systemd (229-4ubuntu21.15) ...c unit, not starting it.
Processing triggers for ureadahead (0.100.0-19) ...

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes

17:13:07.761640 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2962, seq 91, length 6464
17:13:08.761437 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2962, seq 92, length 64

17:13:09.761431 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2962, seq 93, length 64
17:13:09.761577 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2962, seq 93, length 64
17:13:10.761445 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2962, seq 94, length 64
17:13:10.761615 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2962, seq 94, length 64
```

Fig 51: We see that the packets, unlike the previous case, have started flowing now.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
17:04:11.522720 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 221, length 64
17:04:12.522379 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 222, length 64
17:04:12.522610 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 222, length 64
17:04:13.522355 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 223, length 64
17:04:13.522544 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 223, length 64
17:04:14.522387 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 224, length 64
17:04:14.522596 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 224, length 64
17:04:15.522403 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 225, length 64
17:04:15.522597 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 225, length 64
17:04:16.522399 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 226, length 64
17:04:16.522606 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 226, length 64
^C
318 packets captured
318 packets received by filter
0 packets dropped by kernel
root@switch4:~# tcpdump -i eth1 -nq icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
█
```

Fig 52: To see packet flow in Switch4 “tcpdump -i eth1 -nq icmp” is used. We see that no packet is flowing through this.

```
Topology View List View Manifest Graphs User1 x User2 x Switch4 x Switch6 x Relay-Node x
17:04:11.525089 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 221, length 64
17:04:12.524578 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 222, length 64
17:04:12.524979 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 222, length 64
17:04:13.524559 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 223, length 64
17:04:13.524909 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 223, length 64
17:04:14.524592 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 224, length 64
17:04:14.524965 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 224, length 64
17:04:15.524569 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 225, length 64
17:04:15.524960 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 225, length 64
17:04:16.524562 IP 10.10.10.1 > 10.10.10.2: ICMP echo request, id 2931, seq 226, length 64
17:04:16.524975 IP 10.10.10.2 > 10.10.10.1: ICMP echo reply, id 2931, seq 226, length 64
^C
248 packets captured
248 packets received by filter
0 packets dropped by kernel
root@switch6:~# tcpdump -i eth1 -nq icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
█
```

Fig 53: To see packet flow in Switch6 “tcpdump -i eth1 -nq icmp” is used. We see that no packet is flowing through this.

The above screenshots successfully demonstrate the Man-In-Middle-Attack process. In the first scenario, before the initiation of attack, we see that packets are flowing in Switch4 and Switch6 but not in Relay-Node. But, when there is attack happening, we see that there is no flow of packets in Switch4 and Switch6 whereas they are flowing in Relay-Node. We can successfully demonstrate the Man-In-Middle-Attack in the Relay-Node. Thus, the data gets stolen using this process by an attacker.