Final Presentation/ Demo

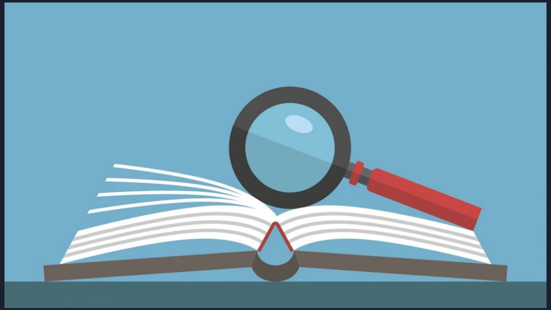
https://images.app.goo.gl/DAuBVjhPK8brsJHp8

Team A

Exploring Suricata and DOS Protection in an SDN Context

Project Definition

- Goal: to evaluate Suricata’s feasibility as an IDS integrated within an SDN environment, through investigating its ability to detect and prevent common forms of DOS attacks.
- Scope: implementation using mininet with a common tree network topology to best reflect University networks.
- Motivation: the need for network security on large enterprise networks; a common victim of both internal and external DOS attacks due to their servicing of a large number of users.



https://images.app.goo.gl/g8c1oobut3CDWYyQ6

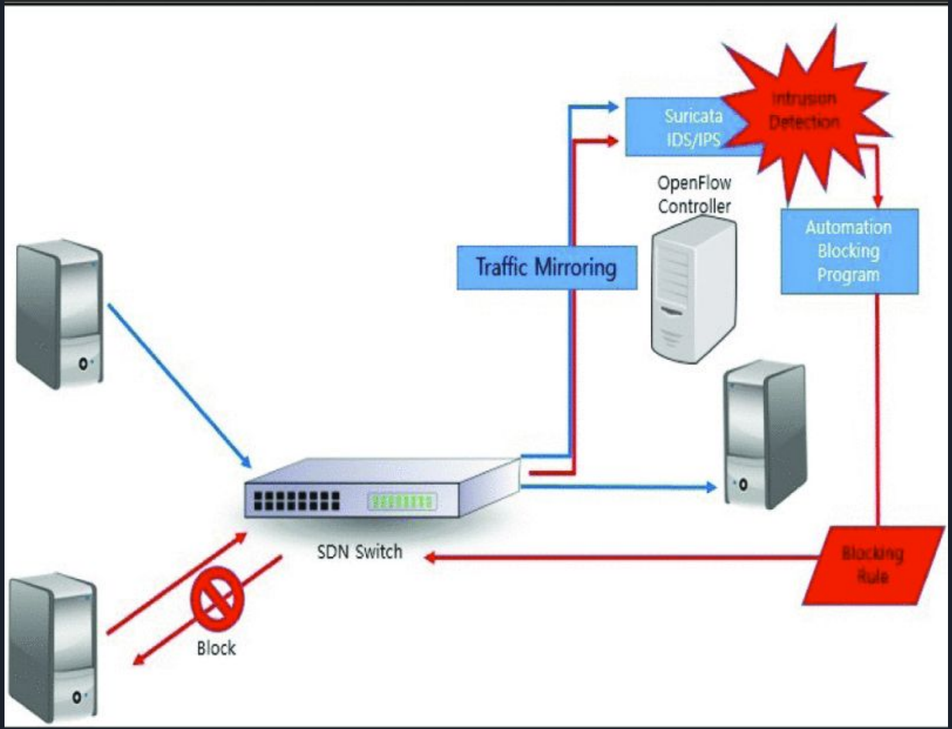
Background

- SDN
- Network Security
- DOS Attacks
  - ICMP Flooding
  - SYN Packet Flooding
- Anomaly Based Detection

https://images.app.goo.gl/SNfiHkeHzKh5w7FN7

Methodology - Tools

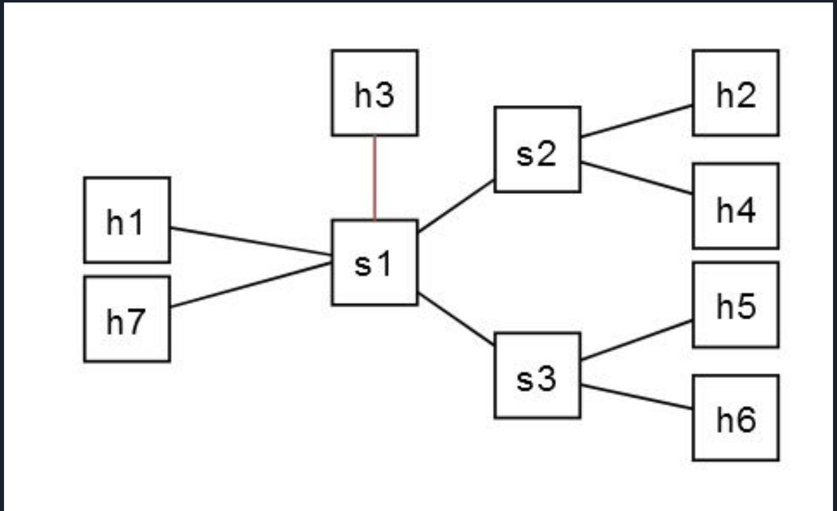
- Mininet
- Suricata
- ONOS
- Python
- HPing3
- Nmap
- Ovs-ofctl



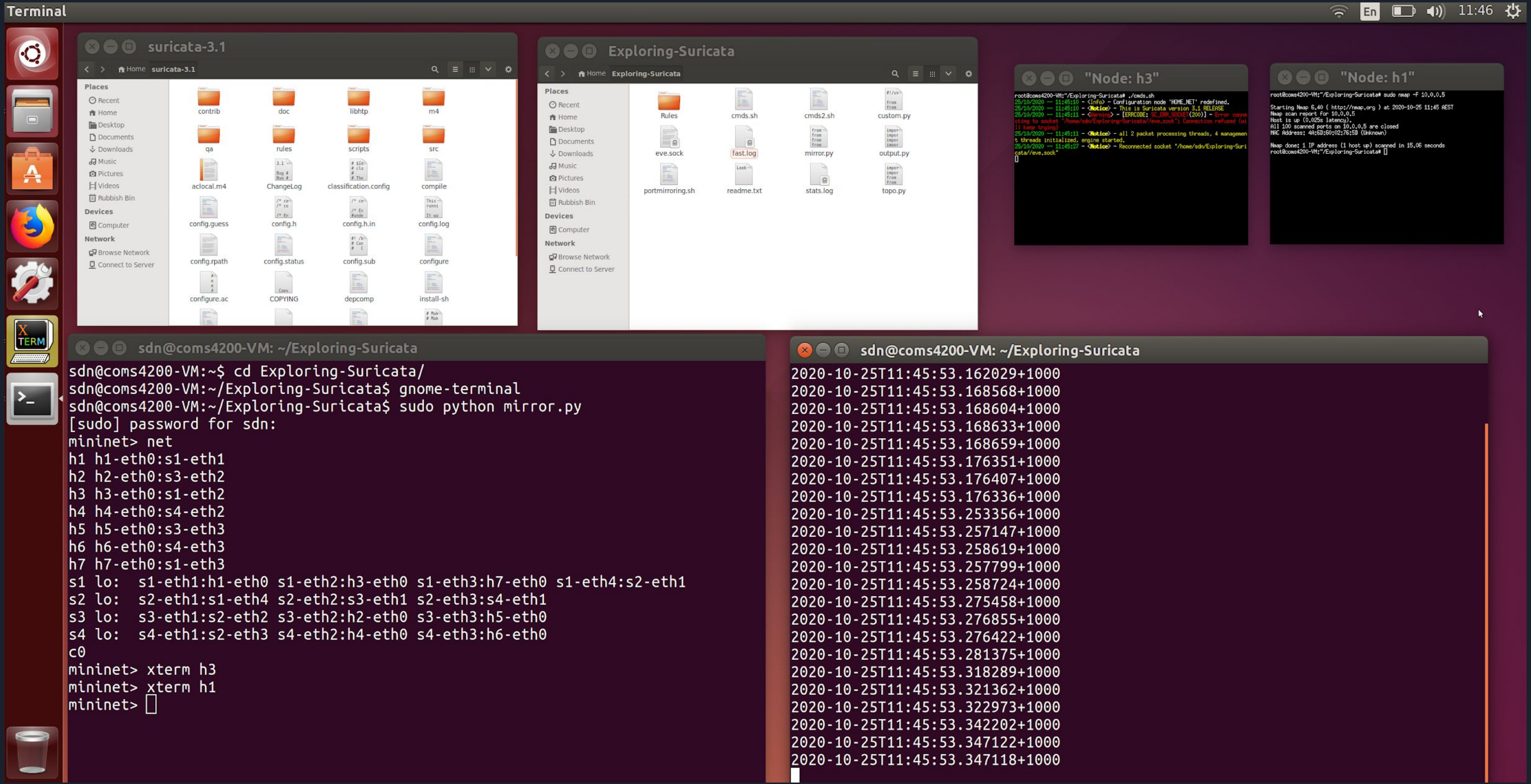
K. Nam and K. Kim, "A study on sdn security enhancement using open source ids/ips suricata," in 2018 International Conference on Information and Communication Technology Convergence (ICTC), 2018: IEEE, pp. 1124-1126.

Methodology - Approach

1. Setup and Connect Tools Together
2. Implement Topology
3. Implement Attack Technique
4. Implement Defense Technique/ Improve Integrability
5. Testing / Running Experiments and Collecting Result



Live Demo



```
root@coms4200-VM:~/Exploring-Suricata# ./cmds.sh
25/10/2020 -- 11:45:10 - <Info> - Configuration node 'HOME_NET' redefined.
25/10/2020 -- 11:45:10 - <Notice> - This is Suricata version 3.1 RELEASE
25/10/2020 -- 11:45:11 - <Warning> - [ERRCODE: SC_ERR_SOCKET(200)] - Error conne
cting to socket "/home/sdn/Exploring-Suricata//eve.sock": Connection refused (wi
ll keep trying)
25/10/2020 -- 11:45:11 - <Notice> - all 2 packet processing threads, 4 managemen
t threads initialized, engine started.
25/10/2020 -- 11:45:27 - <Notice> - Reconnected socket "/home/sdn/Exploring-Suri
cata//eve.sock"
```

```
root@coms4200-VM:~/Exploring-Suricata# sudo nmap -F 10.0.0.5

Starting Nmap 6.40 ( http://nmap.org ) at 2020-10-25 11:45 AEST
Nmap scan report for 10.0.0.5
Host is up (0.025s latency).
All 100 scanned ports on 10.0.0.5 are closed
MAC Address: 4A:6D:60:02:76:5D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 15.06 seconds
root@coms4200-VM:~/Exploring-Suricata# 
```

```
sdn@coms4200-VM:~$ cd Exploring-Suricata/
sdn@coms4200-VM:~/Exploring-Suricata$ gnome-terminal
sdn@coms4200-VM:~/Exploring-Suricata$ sudo python mirror.py
[sudo] password for sdn:
mininet> net
h1 h1-eth0:s1-eth1
h2 h2-eth0:s3-eth2
h3 h3-eth0:s1-eth2
h4 h4-eth0:s4-eth2
h5 h5-eth0:s3-eth3
h6 h6-eth0:s4-eth3
h7 h7-eth0:s1-eth3
s1 lo:  s1-eth1:h1-eth0 s1-eth2:h3-eth0 s1-eth3:h7-eth0 s1-eth4:s2-eth1
s2 lo:  s2-eth1:s1-eth4 s2-eth2:s3-eth1 s2-eth3:s4-eth1
s3 lo:  s3-eth1:s2-eth2 s3-eth2:h2-eth0 s3-eth3:h5-eth0
s4 lo:  s4-eth1:s2-eth3 s4-eth2:h4-eth0 s4-eth3:h6-eth0
c0
mininet> xterm h3
mininet> xterm h1
mininet> 
```

```
2020-10-25T11:45:53.162029+1000
2020-10-25T11:45:53.168568+1000
2020-10-25T11:45:53.168604+1000
2020-10-25T11:45:53.168633+1000
2020-10-25T11:45:53.168659+1000
2020-10-25T11:45:53.176351+1000
2020-10-25T11:45:53.176407+1000
2020-10-25T11:45:53.176336+1000
2020-10-25T11:45:53.253356+1000
2020-10-25T11:45:53.257147+1000
2020-10-25T11:45:53.258619+1000
2020-10-25T11:45:53.257799+1000
2020-10-25T11:45:53.258724+1000
2020-10-25T11:45:53.275458+1000
2020-10-25T11:45:53.276855+1000
2020-10-25T11:45:53.276422+1000
2020-10-25T11:45:53.281375+1000
2020-10-25T11:45:53.318289+1000
2020-10-25T11:45:53.321362+1000
2020-10-25T11:45:53.322973+1000
2020-10-25T11:45:53.342202+1000
2020-10-25T11:45:53.347122+1000
2020-10-25T11:45:53.347118+1000
```

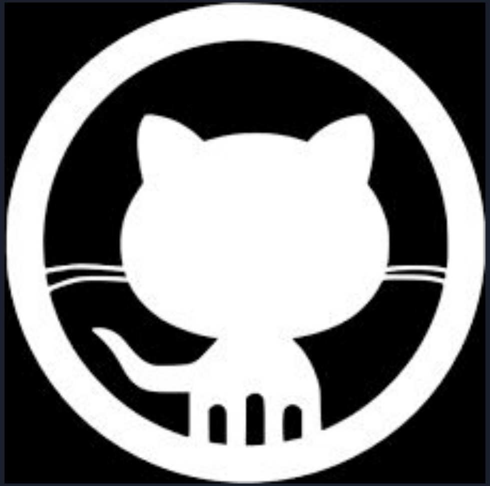
https://github.com/jhhuang7/Exploring-Suricata

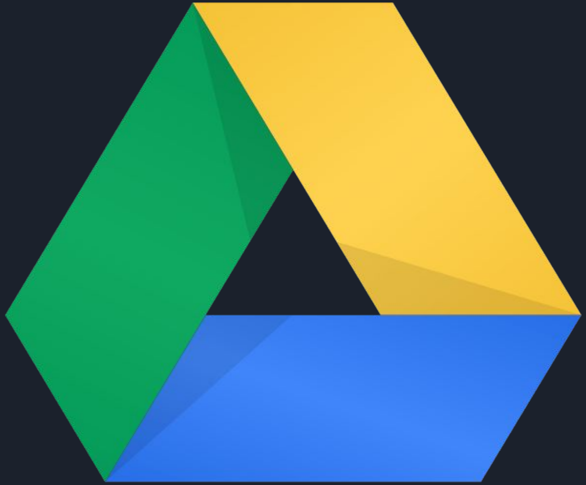
Conclusion

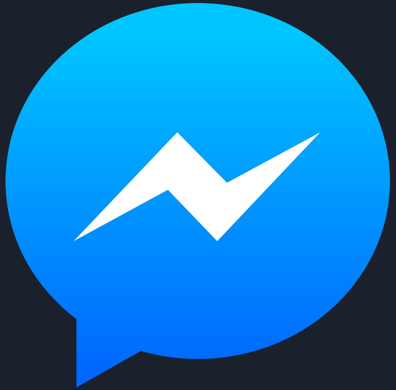
- Easy applications to real-world context with SDN being able to be easily configured and programmed.
- Project Limitations:
  - The architecture that we used was quite low level and required high proficiency in Python programming.
  - False-positive detection.
- Future work:
  - Running Suricata in IPS mode.
  - Scalability of system on large scale networks.

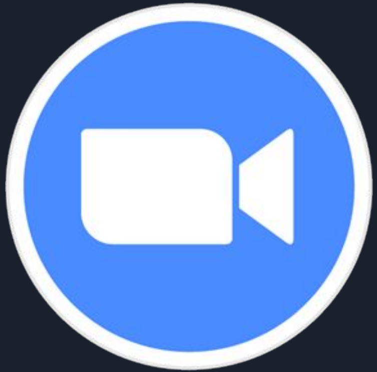
https://images.app.goo.gl/V3b1fXGEDmEz51pc8

Team Collaboration









https://images.app.goo.gl/56zw59QJpHjqNpwP6
https://images.app.goo.gl/wayacTJWHK9TBVyG9
https://images.app.goo.gl/g1meaX1K6gQWs1sN9
https://images.app.goo.gl/Ex3FbiT1ArPP8iiY6

Thank you for listening!

Q&A