Security Test of Indonesian E-health Community Cloud Model Test Bed on Pragma Cloud

Arie Surachman
Sri Chusri Haryanti
Ummi Azizah Rachmawati
Sri Puji Atmoko U.
Rosini

Pragma 36
April 24th, 2019
Jeju, Korea

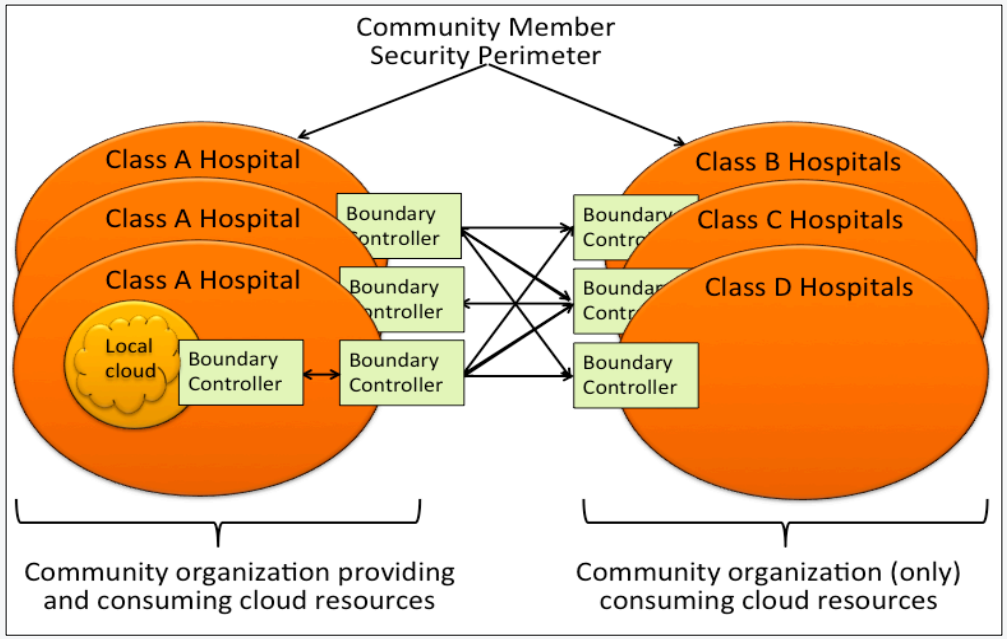
“The Expert in anything was once a Beginner”

Introduction & Aim

Introduction & Aim

- Indonesian e-Health community cloud model
- Virtual firewall for securing Indonesian e-Health cloud from DDoS attacks
- Previous work: simulation
- Recent research: test bed on PRAGMA Cloud

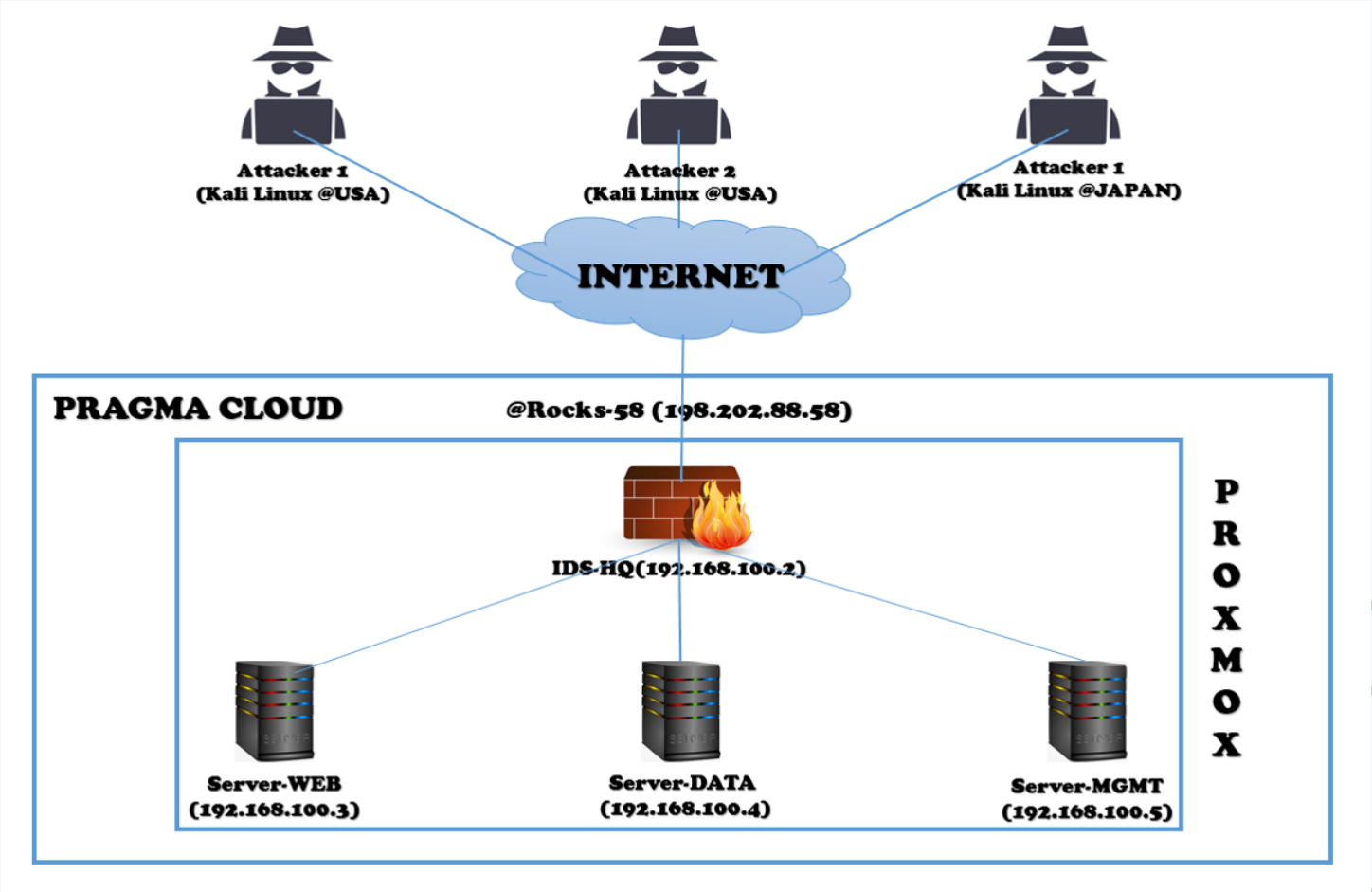
Indonesian E-Health Community Cloud Model



Experiment Overview

- Proxmox VE for the virtualization environment of Indonesian e-Health cloud model.
- Modification of Snort & netfilter Iptables is used to detect & block IP from Attackers.
- The Indonesian e-Health community cloud model is implemented on PRAGMA Cloud in Indiana University site, and the attackers are on San Diego Supercomputer Center (SDSC), the United States and Nara Institute of Science and Technology (NAIST), Japan.
- Two scenarios of test: the cloud, with and without Snort & netfilter Iptables

Topology

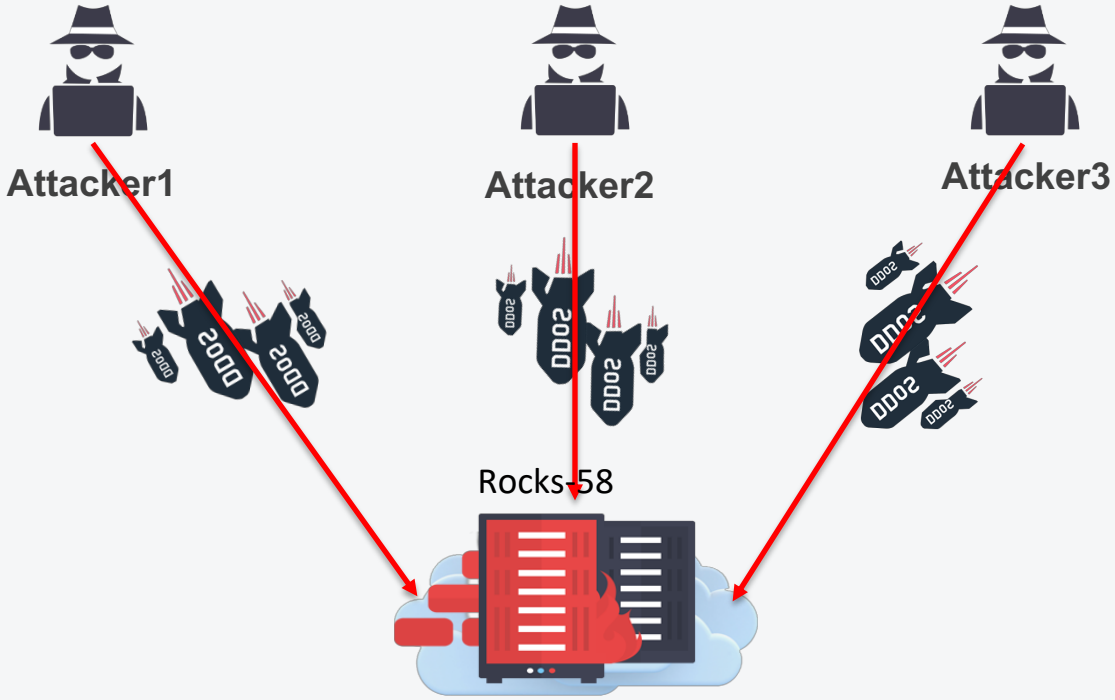

Attacker 1
(Kali Linux @USA)
Attacker 2
(Kali Linux @USA)
Attacker 1
(Kali Linux @JAPAN)
INTERNET
PRAGMA CLOUD
@Rocks-58 (198.202.88.58)
IDS-HQ(192.168.100.2)
PROXMOX
Server-WEB
(192.168.100.3)
Server-DATA
(192.168.100.4)
Server-MGMT
(192.168.100.5)

Hardware & Software Specification

Unit	CPU	RAM	HDD	OS
Rocks-58 ProxmoxVE (198.202.88.58)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	1Gb Ram 2133 Mhz	60 Gb	Debian 8 Jessie Integrated With Proxmox VE 4.4
IDS-HQ (192.168.100.2)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	512 Mb Ram 2133 Mhz	20 Gb	Ubuntu Server 14.04 Trusty Tahr
Server-WEB (192.168.100.3)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	512 Mb Ram 2133 Mhz	8 Gb	Ubuntu Server 14.04 Trusty Tahr
Server-DATA (192.168.100.4)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	512 Mb Ram 2133 Mhz	8 Gb	Ubuntu Server 14.04 Trusty Tahr
Server-MGMT (192.168.100.5)	1 x Intel(R) Xeon(R) CPU E5520 @ 2.27 Ghz (1 Socket)	512 Mb Ram 2133 Mhz	8 Gb	Ubuntu Server 14.04 Trusty Tahr

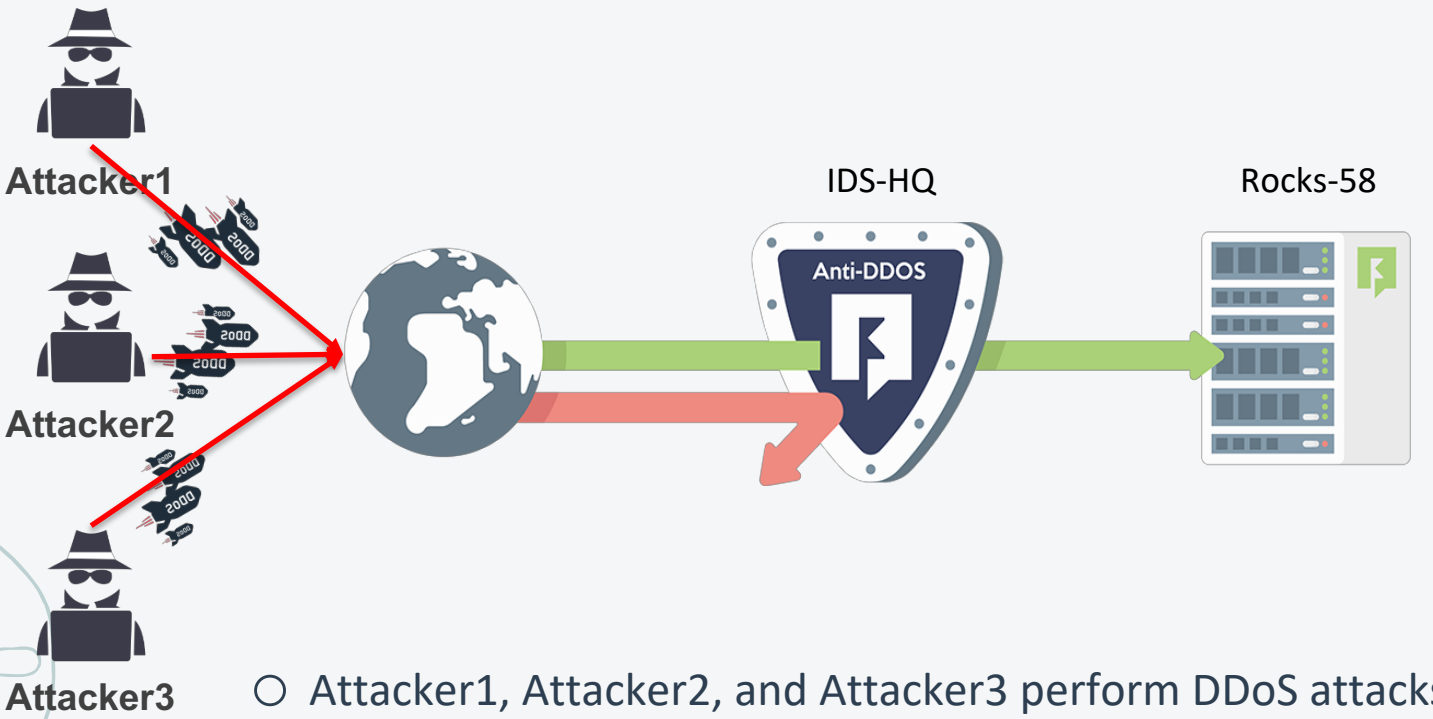
There are four virtual server inside Proxmox server: IDS-HQ as a firewall, Server-Web as a webserver, Server-Data and Server-MGMT

The first scenario



- Attacker1, Attacker2, and Attacker3 perform DDoS attacks with Slowloris.pl script in 300 seconds until the server is inaccessible.
- Performance: the average number of packets received and the average time before the server is down

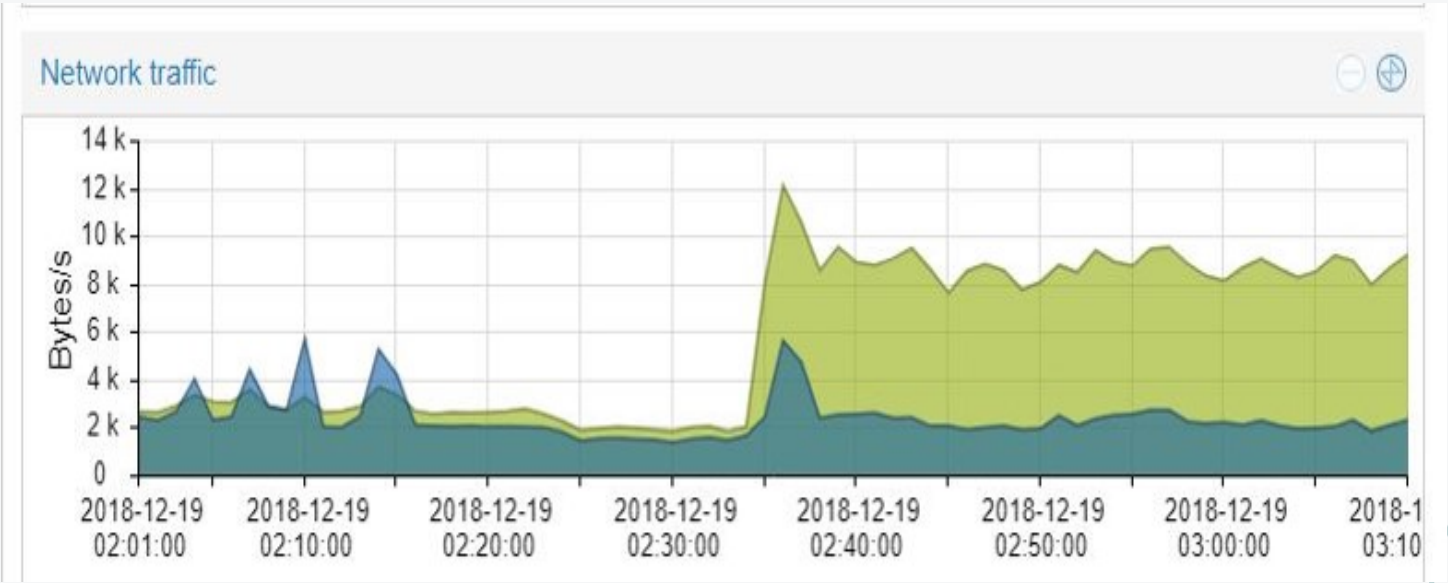
The second scenario



- Attacker1, Attacker2, and Attacker3 perform DDoS attacks with Slowloris.pl script
- On IDS-HQ, we added Snort to gives an alert of DDoS attempt
- Attacker IP addresses are blocked using netfilter IPtables

Result of the first scenario….(1)

Result of the first scenario….(2)



Result of the second scenario….(1)

Snort shows ip address from outside the networks

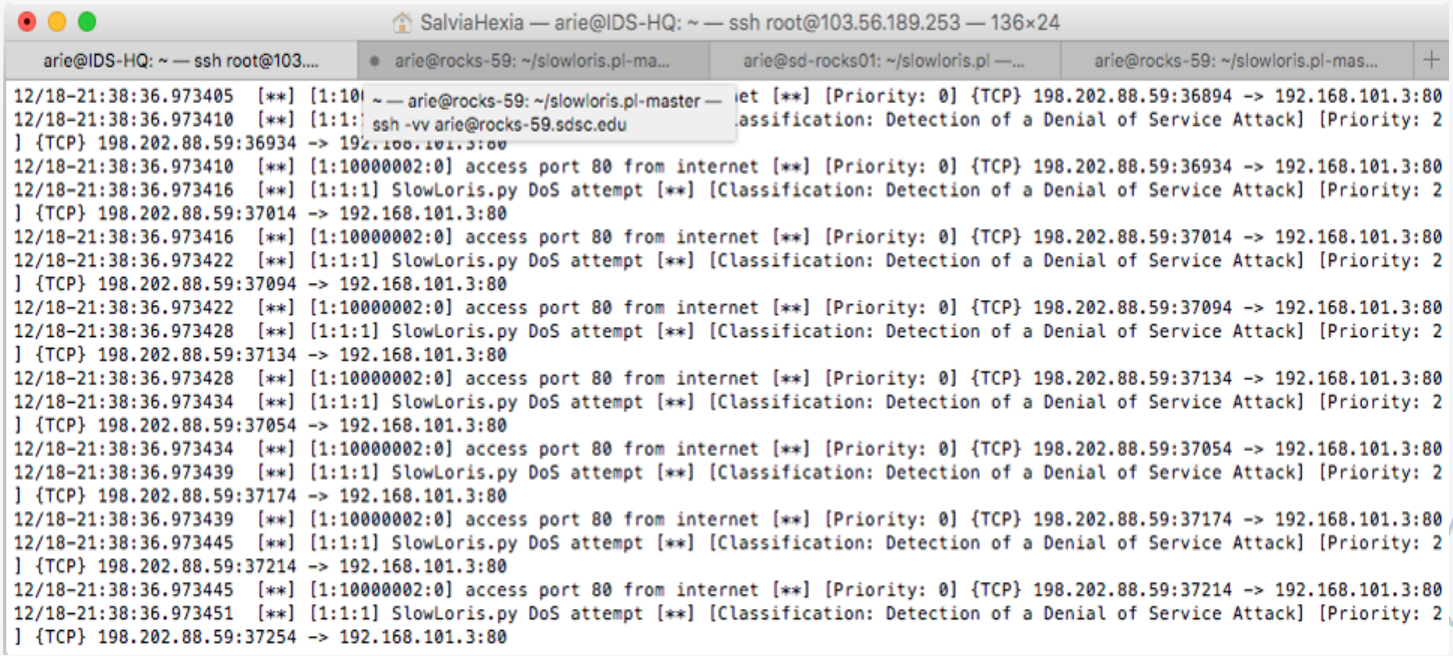
SalviaHexia — arie@IDS-HQ: ~ — ssh root@103.56.189.253 — 136×24

arie@IDS-HQ: ~ — ssh root@103.... | arie@rocks-59: ~/slowloris.pl-ma... | arie@sd-rocks01: ~/slowloris.pl —... | arie@rocks-59: ~/slowloris.pl-mas...

```
12/18-21:32:29.602677  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60302 -> 192.168.101.3:80
12/18-21:32:29.604743  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60302 -> 192.168.101.3:80
12/18-21:32:29.604764  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60342 -> 192.168.101.3:80
12/18-21:32:29.606787  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60304 -> 192.168.101.3:80
12/18-21:32:29.606800  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60304 -> 192.168.101.3:80
12/18-21:32:29.608827  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60344 -> 192.168.101.3:80
12/18-21:32:29.619158  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60346 -> 192.168.101.3:80
12/18-21:32:29.621191  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60306 -> 192.168.101.3:80
12/18-21:32:29.621204  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60306 -> 192.168.101.3:80
12/18-21:32:29.621215  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 198.202.88.59:35214 -> 192.168.101.3:80
12/18-21:32:29.621225  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 198.202.88.59:35214 -> 192.168.101.3:80
12/18-21:32:29.621240  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 198.202.88.59:35254 -> 192.168.101.3:80
12/18-21:32:29.627814  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60308 -> 192.168.101.3:80
12/18-21:32:29.629865  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60308 -> 192.168.101.3:80
12/18-21:32:29.629885  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60348 -> 192.168.101.3:80
12/18-21:32:29.635643  [**] [1:10000002:0] access port 80 from internet [**] [Priority: 0] {TCP} 163.221.11.97:60310 -> 192.168.101.3:80
```

Result of the second scenario….(2)

Snort gives an alert when there is DDoS attempt



Discussion

- ✓ Virtual firewall by modifying Snort on Ubuntu Server 14.04 for Indonesian e-Health cloud model is working successfully
- ✓ The result obtained from the first scenario is the average downtime is 197.5 seconds with the deviation standard is 49.38 seconds before the server was down because of DDoS attacks.
- ✓ The result of the second scenario show that the Snort and IPtables on IDS-HQ manage to block the attacker ip address and survive from DDoS attacks.

Future Work

In the future, a security system that has more complex rules for Snort originating from outside and inside the network will be formulated. Other methods for IDS also will be exercised to improve the security of the cloud.

References

1. Deshmukh, R. V. and Devadkar. K. K. (2015). Understanding DDoS Attack & Its Effect in Cloud Environment. Procedia Computer Science, 49, pp.202-210.

2. Haryanti, S. C., Pradipta, A., Atmoko, S. P. U., Rachmawati, U. A., Suhartanto, H. (2017). Indonesian E-Health Community Cloud. Poster, SEAIP 4-8 Desember 2017, Taiwan.

3. Modi, C., dkk. (2013). A survey of instrusion detection techniques in Cloud. Journal of Network and Computer Applications, 42-57(36).

4. Munir. (2016). Statistik Pendidikan Pengantar Analisis Data untuk Penulisan Skripsi & Tesis, Jember.

5. Simon, M.C. Cheng. (2014). Proxmox High Availability. Packt Publishing Ltd. Pp. 41 – ISBN 978-1-78398-089-5.

6. Somani, G., Gaur, M.S., Sanghi, D., Conti, M. And Buyya, R. (2017). DDoS attacks in cloud computing : Issues, taxonomy, and future directions. Computer Communications, 107, pp.30-48.

THANK YOU!

You can find me at:

@localhost.id

abiegailz@outlook.com