Jurnal Mantik Penusa

Volume 3, No.1, Juni 2019

e-ISSN 2580-9741
p-ISSN2088-3943

IMPLEMENTASI IDS MENGGUNAKAN SNORT PADA SISTEM OPERASI UBUNTU

I Putu Agus Eka Pratama[1], Ni Kade Mega Handayani[2]

[1,2] Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana
Denpasar, Bali

E-mail: eka.pratama@unud.ac.id[1], megahandayani95@gmail.com[2]

Abstract

Network security can be improved by implementing the Intrusion Detection System (IDS). Snort is an Intrusion Detection System program, which is a program that can detect an intrusion attempt on a computer network system. Implementation of an Open Source intrusion based Snort detection system is a cost advantage with reliable performance in detecting attacks. Snort can be implemented on various operating systems including Ubuntu Linux. An attack can be detected or not by Snort IDS, depending on the rules / rules in Snort. Snort testing is done with several attack patterns such as Ping, Port Scanning, Ping of Deatch with several tools such as NMAP, SQLMAP and others. Based on the results of testing Snort can detect and provide warnings about attacks that threaten a computer network of a server. The test results are expected to be used as a alternative in server network security..

Keywords: *Security, Snort, Intrusion Detection System, Linux, Ping*

Abstrak

Keamanan jaringan dapat ditingkatkan dengan mengimplementasikan Intrusion Detection System (IDS). Snort merupakan salah satu program Intrusion Detection System, yaitu program yang dapat mendeteksi suatu usaha penyusupan pada sistem jaringan komputer. Implementasi system deteksi intrusi berbasis Snort yangt Open Source menjadi keuntungan dari segi biayadengan performa yang handal dalam mendeteksi serangan. Snort bisa diimplementasikan pada berbagai sistem operasi termasuk Linux Ubuntu. Suatu serangan dapat dideteksi atau tidak oleh Snort IDS, tergantung pada aturan/rule dalam Snort. Pengujian Snort dilakukan dengan dengan beberapa pola serangan misalnya Ping, Port Scanning, Ping of Deatch dengan beberapa tool seperti NMAP, SQLMAP dan lainnya. Berdasarkan hasil pengujian Snort dapat mendeteksi dan memberikan peringatan tentang serangan yang mengancam suatu jaringan komputer suatu server. Hasil pengujian diharapkan bisa digunakan sebagai alternatif dalam keamanan jaringan server.

Kata Kunci:*Keamanan, Snort, Intrusion Detection System, Linux, Ping*

1. Pendahuluan

Keamanan jaringan pada server merupakan faktor penting dalam jaringan. Keamanan yang baik dapat memberikan rasa percaya pada suatu server yang digunakan dan mengurangi kerugian dari serangan yang terjadi pada jaringan suatu server [1].

Aspek keamanan suatu jaringan menerukan stabilitas, integritas dan validasi data. Snort merupakan salah satu program Network-Base Intrusion Detection System, yaitu program yang dapat mendeteksi suatu usaha penyusupan pada sistem jaringan komputer [2].

Implementasi Aplikasi pendeteksi intrusi/ Intrusion Detection System berbasis Snort dapat menghemat biaya pengadaan software karena bersifat open source dan cukup handal dalam mendeteksi suatu serangan terhadap keamanan jaringan suatu server. Snort sebagai IDS bisa diimplementasikan pada berbagai sistem operasi termasuk Linux Ubuntu.

Suatu serangan dapat dideteksi atau tidak oleh Snort dikonfigurasi pada pengaturan jaringan dan rule Snort yang ada. Pengujian Snort IDS dilakukan dengan beberapa pola serangan untuk menguji kehandalan Snort dalam mendeteksi sebuah serangan terhadap sistem keamanan. Berdasarkan hasil pengujian sistem Snort IDS dengan ping, nmap, eksploitasi, dan Ping of Deacth, Snort dapat memberikan peringatan adanya serangan keamanan terhadap sistem jaringan. Hasil peringatan tersebut dapat digunakan sebagai acuan untuk menentukan kebijakan keamanan jaringan.

Salah satu cara untuk meningkatkan keamanan dalam jaringan adalah dengan mengimplementasikan Intrusion Detection System (IDS). Intrusion Detection System adalah sebuah sistem yang digunakan untuk melakukan deteksi

adanya usaha-usaha penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik secara *real-time*. Beberapa keunggulan Snort dibandingkan software IDS lain adalah kode sumber berukuran kecil, dapat digunakan pada banyak sistem operasi, cepat dan mampu mendeteksi serangan pada jaringan, mudah dikonfigurasi dan terutama Snort ini bersifat gratis [3].

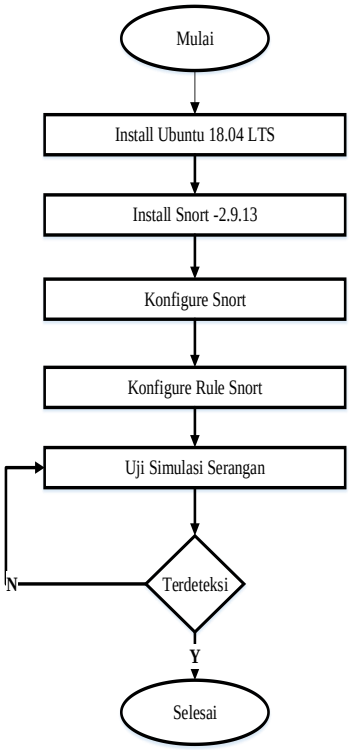
Hasil implementasi Snort sebagai Intrusion Detection System dapat digunakan untuk meningkatkan keamanan server pada Ubuntu. Meningkatkan keamanan server dengan Snort IDS melalui beberapa pengujian, sehingga, manfaat yang didapat dari hasil penelitian ini adalah meningkatnya keamanan dalam jaringan, dapat digunakan pada banyak sistem operasi, cepat dan mampu mendeteksi serangan pada jaringan, mudah dikonfigurasi dan *open source*.

2. Metode Penelitian

Metode peneliian yang digunakan yaitumetode eksperimen dimana dilakukan percobaan menggunakan sistem operasi Ubuntu.

a. Tahapan Penelitian

Flowchat dibawa ini merupakan tahapan dari proses penelitian.

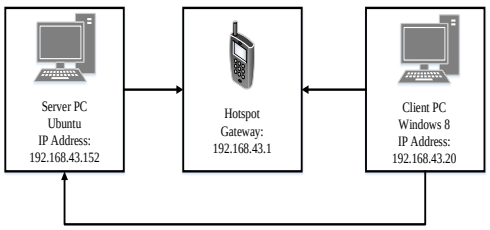


Gambar 1. Diagram Alir Perancangan dan Pengujian

Gambar 1 merupakan tahapan penelitian yang dijabarkan dalam flowchart penelitian, tahapahan dimulai dengan instalasi sistem operasi, lalu instalasi Snort, dan dilanjutkan dengan pengujian dengan teknik serangan.

b. Desain

Pemodelan yang digunakan pada penelitian ini adalah model jaringan *Client/Server*. Jaringan yang digunakan dalan penelitian ini adalah jaringan hostspot. Yang diimplementasikan dengan konsep *Snort Network – Based Intrusion Detection System.*



Gambar 2. Skema Jaringan Penelitian

Gambar 2 merupakan desain dari pemodelan jaringan dengan menggunakan model client/server. Menggunakan dua komputer dimana PC satu sebagai server dan PC lainnya sebagai client yang akan mengakses server untuk melakukan serangan.

3. Hasil dan Pembahasan

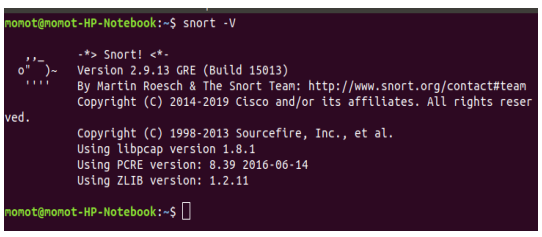
Berdasarkan diagram alir pada Gambar 1. dapat diuraikan langkah – langkah yang dilakukan selama perancangan, konfigurasi dan pengujian. Penjabaran dari langkah – langkah tersebut.

a. Instal Ubuntu 18.04 LTS OS

Lakukan instalasi Ubuntu pada komputer server atau dapat menggunakan live CD juga bisa menggunakan *virtual machine*. Penelitian ini melakukan install langsung pada sebagi komputer server. Spesifikasi komputer server Ubuntu 18.04 LTS, Ram 8 GB, HDD 500 GB dan Intel Core i3

b. Instalasi Snort

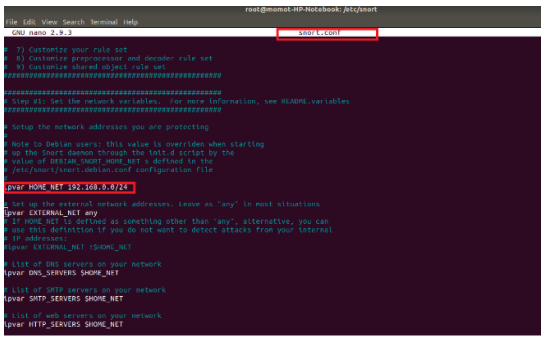
Langkah installsi Snort dapat dilakukan dapat dengan apt-get install atau mengunduh program secara langsung pada situs resmi Snort (www.snort.org). pada penelitian ini menggunakan Snort *versi* 2.9.13 dan *rule* Snort dengan versi yang sama.



Gambar 3. Snort Versi

c. Konfigurasi Snort

File konfigurasi Snort terdapat pada file snort.conf yang terletak pada direktori /etc/snort/snort.conf. Pengaturan utama yang diperlukan adalah konfigurasi pada jaringan. Pengaturan jaringan pada Snort seperti ditunjukkan pada Gambar 4.



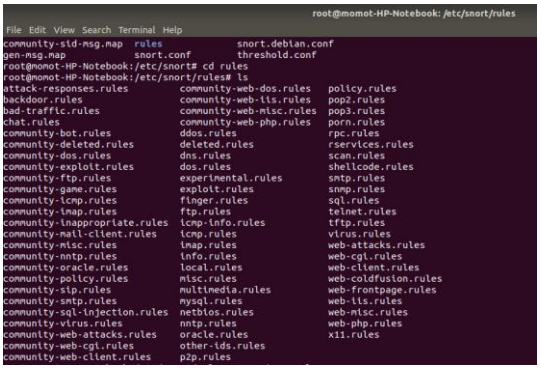
Gambar 4. Snort.conf

d. Konfigurasi Rules Snort

Konfigurasi rules snort dapat dilakukan secara manual atau dengan men-dowload package rules Snort. Konfigurasi pada penelitian inimenggunakan rules Snort package versi Snort 3 yang diinstal dengan langkah sebagai berikut.

```
# wget
https://www.snort.org/downloads/community/sn
ort3-community-rules.tar.gz
# tar -xvzf snort3-community-rules.tar.gz
# cd snort3-community-rules
#sudo mkdir /usr/local/etc/snort/rules
#sudo mkdir /usr/local/etc/snort/builtin_rules
#sudo mkdir /usr/local/etc/snort/so_rules
#sudo mkdir /usr/local/etc/snort/lists
#sudo cp snort3-community.rules
/usr/local/etc/snort/rules/
#sudo cp sid-msg.map /usr/local/etc/snort/rules/
```

Melihat rules yang sudah dikonfigurasi pada /etc/snort/rules/. Pengaturan utama yang diperlukan adalah konfigurasi rules Snort ditunjukkan pada Gambar 5**.**



Gambar 5. Rules Snort

e. Skenario Pengujian IDS Snort

Jenis serangan yang sering terjadi sebagai bagian untuk melakukan intrusi terhadap suatu sistem dapat berupa NMAP *port*, scan, eksploitasi, SQL Injection dan pengaksesan *database*. Oleh karena itu, langkah pengujian system Snort IDS dalam penelitian ini dilakukan melalui 5 macam skenario pengujian sebagai berikut.

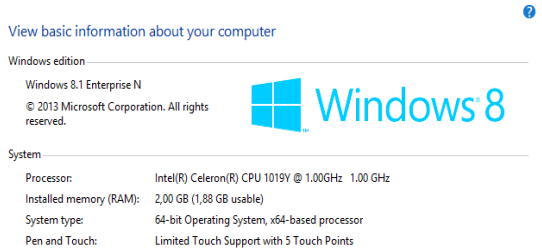
1) *Ping*

Ping adalah sebuah program yang digunakan untuk memeriksa indukivitas jaringan berbasis teknologi (TCP/IP). Dengan menggunakan program ini, dapat diuji apakah sebuah komputer terhubung dengan komputer lainnya. Hal ini dilakukan dengan mengirimkan sebuah paket kepada alamat IP yang hendak diujicoba konektivitasnya dan menunggu respon darinya. *Client* akan melakukan ping pada komputer server.

2) Skenario Uji coba 2: NMAP *portscan*

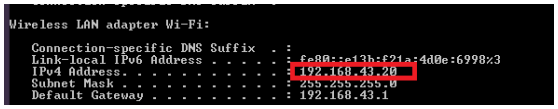
Pengujian 2 dilakukan dengan melakukan NMAP *port scan* dengan menggunakan aplikasi NMAP. Informasi yang diinginkan adalah port-port yang terbuka pada server, sistem operasi, dan versi sistem operasi dari server. Proses *port scan* dilakukan dengan teknik nmaping, dimana server hanya akan memberikan *reply* terhadap paket data yang dikirimkan *client*. Pihak penyerang dalam simulasi ini adalah komputer *client* dengan spesifikasi komputer sistem operasi Windows 8, Intel Celeron, RAM 2 GB yang mendapatkan IP dari hotspot.

e-ISSN 2580-9741
p-ISSN2088-3943



Gambar 6. Spesifikasi PC Client

PC client yang digunakan sebagai penyerang mempunyai IP konfigurasi seperti ditunjukan Gambar 7.



Gambar 7. IP Konfigurasi

3) Skenario Uji coba 4: SQL Injection

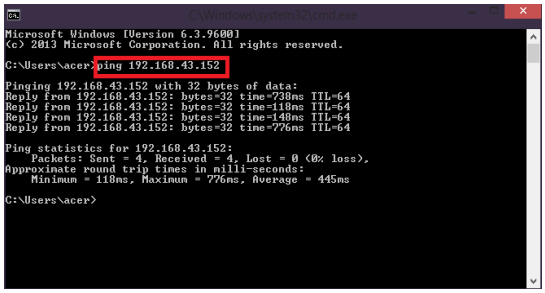
Teknik SQL Injection saat ini sering dilakukan dalam serangan keamanan untuk mendapatkan akses *root*, terutama pada web berbasis php-MySQL. Teknik ini dilakukan dengan memberikan kode-kode khusus dalam bahasa MySQL terhadap masukan yang dimana oleh sebuak halaman web, agar server memberikan informasi yang seharusnya. Pengujian simulasi ini dilakukan terhadap halaman web DVWA yang telah terinstall pada server. Pada komputer *client* digunakan aplikasi SQLMAP untuk melakukan teknik SQL-Injection.

f. Hasil Analisis Pengujian IDS Snort

Hasil analisa dari pengujian yang dilakukan terhadap PC server pada skenario penyerangan yang dilakukan sebagai berikut.

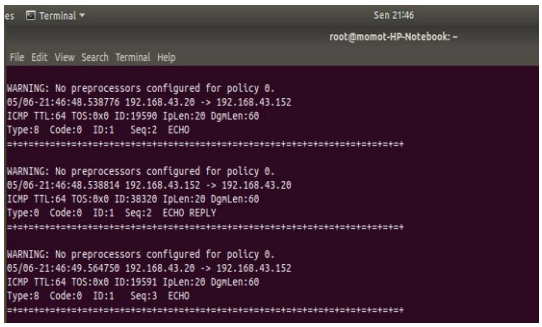
1) Ping

Ping bekerja dengan mengirimkan sebuah paket data yang disebut dengan *Internet Control Message Protocol* (ICMP) *Echo Request.* Mekanisme kerjanya yaitu ketika melakukan ping terhadap situs target (objek) maka akan tampil pada layar hasil respon berupa informasi nomor IP dari mana ping memperoleh *Echo Reply*, waktu (dalam milisekon) yang diperlukan program ping mendapatkan balasan dan yang terakhir adalah *Time To Live* (TTL). Pengujian ping dengan perintah ping IP server 192.168.43.152 pada CMD dari komputer client dengan IP Address 192.168.43.20 seperti ditunjukkan pada Gambar 8.



Gambar 8. Perintah CMD Ping Server

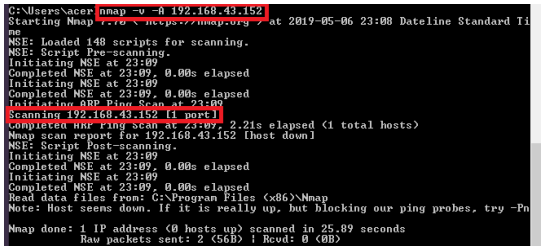
Hasil pengujian ping dengan perintah `ping 192.168.43.152` dari komputer client dengan IP Address 192.168.43.20 menghasilkan hasil seperti ditunjukkan pada Gambar 9.



Gambar 9. Respon Ping pada CLI IDS

2) Nmap Port Scan

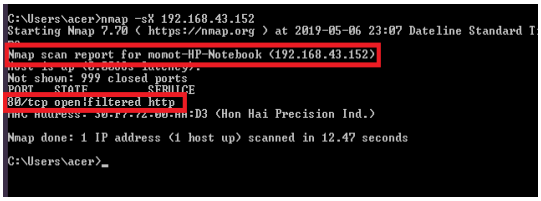
Pengujian yang dilakukan melalui PC client dengan menggunakan tool bantuan NMAP dengan menggunakan perintah perintah `nmap -v 192.168.43.152` seperti ditunjukan pada Gambar 10.



Gambar 10. Nmap Scanning

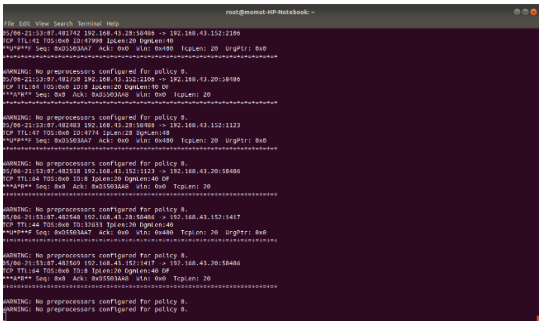
Pengujian yang dilakukan melalui PC client dengan menggunakan tool bantuan NMAP dengan menggunakan perintah perintah `nmap -sX 192.168.43.152` seperti ditunjukan pada Gambar 11.

Jurnal Mantik Penusa
Volume 3, No.1, Juni 2019
e-ISSN 2580-9741
p-ISSN2088-3943



Gambar 11. Nmap Scanning

Hasil pengujian ping dengan perintah port scanning dengan tool NMAP dari komputer client dengan IP Address 192.168.43.20 menghasilkan hasil seperti ditunjukkan pada Gambar 12.

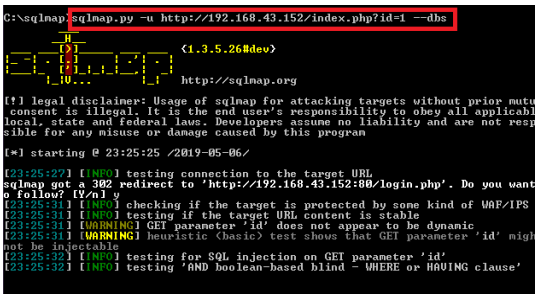


Gambar 12. Respon Port Scanning pada CLI IDS

Pengertian dari perintah scan pada pengujian ini adalah memeritahkan nmap untuk melakukan port scan dengan opsi –sX untuk mode XMAS scan. –O untuk deteksi sistem operasi target, -v untuk menampilkan versi dari system operasi target dengan IP Address target adalah 192.168.43.152. Hasil peringatan Snort menunjukkan bahwa decoder Snort mendeteksi serangan nmap XMAS scan terhadap server oleh client dengan IP Address 192.168.43.20. Simulasi serangan ini dapat terdeteksi Snort karena paket data yang dikirimkan client ke server memenuhi kriteria *rule*.

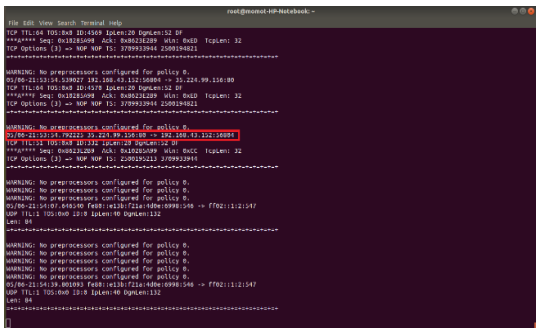
3) SQL Injection

Pengujian SQL Injection dilakukan dengan menggunakan tool SQLMAP yang digunakan untuk melakukan serangan SQL Injection melalui *client* dengan IP address 192.168.43.20 dengan perintah seperti ditunjukan Gambar 13.



Gambar 13. Perintah SQLMAP

Pengujian juga dilakukan dengan secara langsung mengakses web server melalui port 80 dan memberi input terhadap halaman web DVWA pada form *input* SQL *Injection*.Hasil deteksi Snort terhadap pengujian SQL *Injection* yang dilakukan menghasilkan peringatan dalam CLI yang ditunjukkan pada Gambar 14.

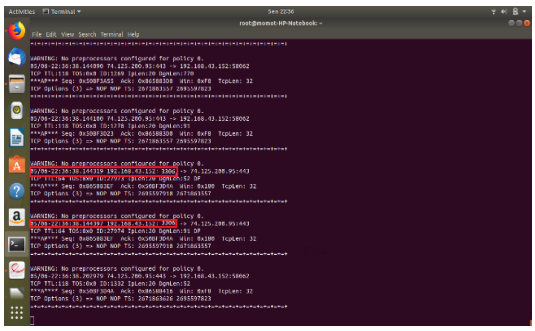


Gambar 14. Hasil pengujian SQL Injection pada CLI IDS

Peringatan Snort IDS sebagaimana ditunjukkan pada gambar 12 menunjukkan bahwa telah terjadi serangan SQL Injection melalui protocol TCP pada layanan HTTP *port*.Peringatan Snort ini mengacu pada rule sebagaimana ditunjukkan pada gambar 12 yang membandingkan paket data ke server pada *port-port* layanan HTTP.

4) Pengaksesan Database

Hasil pengujian pengaksesan database server dengan melakukan *login* MySQL. *Root* dan perintah untuk menampilkan *database* dari *client* dengan hasil tampilan informasi pada Gambar 15.



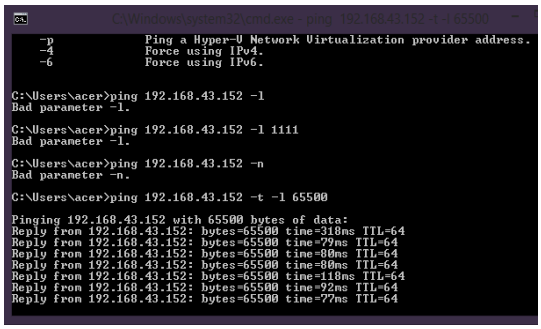
Gambar 15. Hasil pengujian Mysql Login pada CLI IDS

Hasil peringatan Snort pada Gambar 15 menunjukkan bahwa terjadi serangan pengasksesan *database* melalui protocol TCP pada layanan MySQL. Penyerang melakukan *login* sebagai MySQL *root* dan melakukan pengaksesan terhadap database dengan

menampilkan seluruh *database* yang ada. Serangan ini terdeteksi oleh mesin Snort.

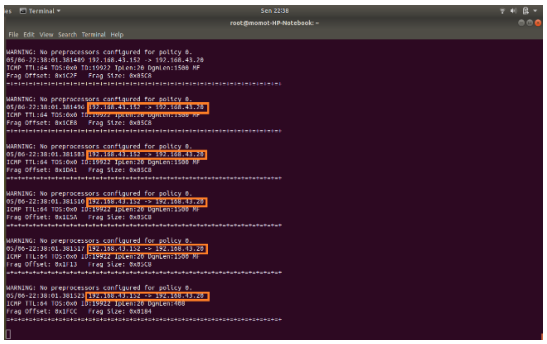
a) Ping of Death

Pengujian Ping of Death dilakukan dengan menggunakan CMD pada PC client dengan perintah `ping 192.168.43.152 -t -l 65500` seperti ditunjukan Gambar 16.



Gambar 16. Perintah Ping of Death PC Server

Hasil pengujian DOS dengan menggunakan perintah ping pada CMD client ditunjukan pada Gambar 17.



Gambar 17. Hasil Dos Server pada IDS CLI

4. Kesimpulan

Kesimpulan yang dapat diambil berdasarkan hasil penelitian ini adalah sebagai berikut :

1) Berdasarkan hasil pengujian yang dilakukan pada penelitian diatas dapat disimpulkan bahwa Snort dapat diimplementasikan sebagai *Intrusion Detection System*(IDS) pada sistem operasi Ubuntu 18.04 LTS Linux untuk mendeteksi serangan berupa ping, NMAP *portscan*, SQL Injection, pengaksesan *database* dan *Ping of Deacth*
2) Hasil Analisis yang didapat dalam proses pengujian ping, didapat berupa informasi dari *client* yang melakukan ping pada server IDS. Nmap port scan yang dilakukan juga dideteksi oleh Snort IDS. Pengujian dengan ekspoitasi yang dilakukan juga sudah diberikan pendeteksian intrusi berupa peringatan, begitu juga dengan SQL Injection, *database* dan *Ping of Deacth*.
3) Snort dapat memberikan peringatan adanya sebuah serangan keamanan, sehingga dapat meningkatkan keamanan jaringan. Dapat atau tidaknya sebuah serangan terdeteksi oleh Snort IDS tergantung dari ada tidaknya *rule* dengan jenis *signature* pada sebuah pola serangan.
4) Snort dapat dengan mudah diinstal dab dikonfigurasi pada sistem operasi apa saja, termasuk Linux yang digunakan pada penelitian ini.

5. References

[1] Affandi, Mohammad & Setyowibowo, Sigit. "Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux", Jurnal Teknologi Informasi, Vol 4 No 2 . 2013

[2] Beale, Jay. 2003. *Snort 2.0 Intrusion Detection*, Masachusset : Syngress Publishing, Inc

[3] Rafiudin, Rahmat.. *Mengganyang Hacker dengan SNORT*, Andi Offset, Surabaya, 2010

[4] Roesch, Martin,& Green, Chris.*SNORT1#1 Users Manual 2.9.13*, http://manual-snort-org.s3-website-us-east-1.amazonaws.com/, 29 April 2019 07.12

[5] Fathoni, Walid, dkk,. "Deteksi Penyusupan Pada Jaringan Komputer Menggunakan IDS*"*, e-Proceeding of Engineering, Vol 3 No 1, p. 1169, 2016.

[6] Junoto G., *"Sistem Untuk Mendeteksi Penyusup (IDS: Intrusion Detection System",* Universitas AKI Semarang, 2011, pp. 46-54