Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 8-12
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Penerapan Snort Sebagai Sistem Pendeteksi Serangan Keamanan Jaringan

Rahmat Novrianda Dasmen[1], Cendri Ariyanto[2], Muhammad Haris Surya[3], Hafiizh Ramadhan[4]
[1,2,3,4]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma.
[1]rahmat.novrianda.d@gmail.com, [2]zidansaputracool@gmail.com, [3]haris.surya02@yahoo.com.ac.id,
[4]hafiizhrmd0112@gmail.com

Abstract

Network security is very important in an effort to prevent abuse on a network.Our research aims to detect networks using snort where this application has sensor that can indentify abuse on the network besides snort also funcitions to detect intrusions. Detection is carried out according to the rules contained in the configuration file,snort can perform analysis on rule based systems,adaptive system.Snort can operate sniffer mode, packet logger mode and intrusion detection mode.

Keywords : *Network security, SMS Gateway, Snort*

Abstrak

Keamanan jaringan adalah hal yang sangat penting dalam upaya menangkal penyalahgunaan pada sebuah jaringan. Penelitian kami bertujuan untuk mendeteksi jaringan menggunakan snort dimana aplikasi ini memiliki sensor yang dapat mengindentifikasi penyalahgunaan pada jaringan tersebut, selain itu snort juga berfungsi mendeteksi intrusi. Deteksi yang dilakukan sesuai dengan aturan yang ada pada file konfigurasi, Snort dapat melakukan analisa terhadap rule based systems, adaptive systems. Snort dapat mengoperasikan sniffer mode, packet logger mode dan Intrusion Detection mode.

Kata kunci: *keamanan jaringan, SMS gateway, snort*

1. PENDAHULUAN

Dengan berkembangnya teknologi dibidang Networking saat ini telah membuat berbagai macam teknologi, tools dan fitur berkembang secara pesat. Teknologi jaringan dan komputer telah menyediakan berbagai macam kemudahan untuk masyarakat terutama internet, namun demikian alangkah baiknya kita menjaga data kita agar tetap terjaga dari serangan pihak lainnya dimana hal tersebut dapat mengganggu aktifitas dan kerja yang kita lakukan. Keamanan data sangatlah penting bagi pribadi maupun institusi atau lembaga, dimana institusi tersebut haruslah memiliki pencegah dari keterbukaan akses dari pihak lain yang tidak memiliki hak. Adapun peran terpenting dari sebuah sistem keamanan terletak pada seorang administrator sebagai pemegang akses penuh terhadap infrastruktur jaringan yang dirancangnya. Jaringan komputer haruslah memberikan rasa aman terhadap user atau pemakainya, adapun salah satu caranya yakni dengan memberikan notifikasi kepada administrator saat jaringan diserang ataupun bermasalah.

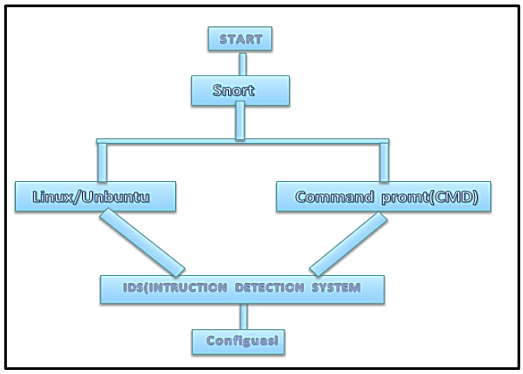
2. METODOLOGI PENELITIAN

Snort adalah sebuah aplikasi yang memiliki fungsi dapat mencegah intruksi dan serangan jaringan. Snort dapat membentuk analis trafik-trafik dan logging paket-paket secara real time dalam jaringan berbasis TCP/IP. Adapun orang yang pertama kali menulis snort adalah Martin Roesch dan saat ini dikelola oleh

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 8-12
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Sourcefire, yang mana *Roesch* sebagai pendiri dan CTO (*Chief of Technical Officer*). Snort adalah penggabungan dari system analisis protocol dan system pendeteksi penyusupan, hal ini sangatlah bermanfaat untuk mendeteksi serangan terhadap host dalam jaringan [2].

Flowchart atau sering disebut dengan diagram alir merupakan suatu jenis diagram yang merepresentasikan algoritma atau langkah-langkah instruksi yang berurutan dalam sistem [3].



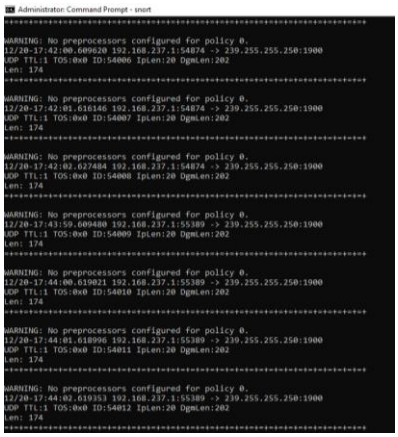
Gambar 1. Struktur Jaringan Snort

Pada gambar diatas perancangan akan dimulai dari aplikasi snort, yang dapat didowload di berbagai media google,internet dan lainnya.Selanjutnya gunakan linux/unbuntu di *virtual box* dan *command prompt* untuk menghubungkan snort.Kemudian lakukan cara mengkonfigurasi IDS (*Instruction Detection System*) di *linux* maupun di *Command prompt* agar dapat terhubung ke dalam jaringan.

3. HASIL DAN PEMBAHASAN

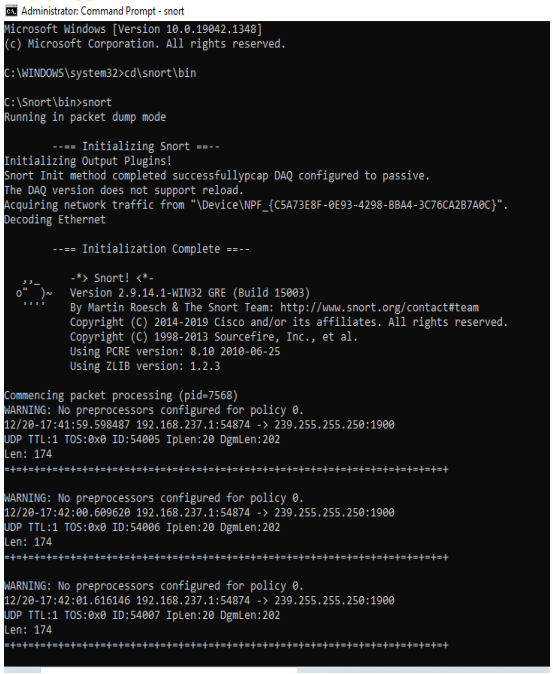
3.1. Konfigurasi Snort di *Command prompt*

Dalam menentukan perancangan ini,melakukan konfigurasi snort IDS (*Instruction Detection System*) dengan mengunakan linux dan *commad prompt*. Kemudian melakukan penginputan data di Snort IDS mengunakan linux dan *commad prompt* [4]. Berikut adalah tampilan snort di CMD:



Gambar 2. Snort

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 8-12
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 3. Snort

Pada gambar yang ditampilkan disamping adalah cara kerja snort menggunakan *command prompt*. Kemudian akan di tampilkan versi snort yang di gunakan yaitu snort versi 2.9.14.1 win 32 bit. Cara mengkonfigurasi snort di *command* sebagai berikut :

a) Klik *Command prompt* di pengaturan;
b) Next, klik enter dan jalankan program *command prompt* di windows 10;
c) Lakukan konfigurasi snort dengan cara ketik, CD\SNORT\BIN, kemudian ;
d) Ketik SNORT.

Program keseluruhan nya akan ditampilkan semua di *command prompt* yang terdapat pada gambar diatas.

3.2. Perancangan skema jaringan snort menggunakan cisco packet tracer

Tahap ini penelitian kami menggunakan skema jaringan snort menggunakan *cisco packet tracer* untuk menganalisa sebuah *client* yang masuk atau keluar pada suatu jaringan [5]. Adapun jumlah – jumlah *sever, PC, router* dan *switch* yang digunakan sebagai berikut;

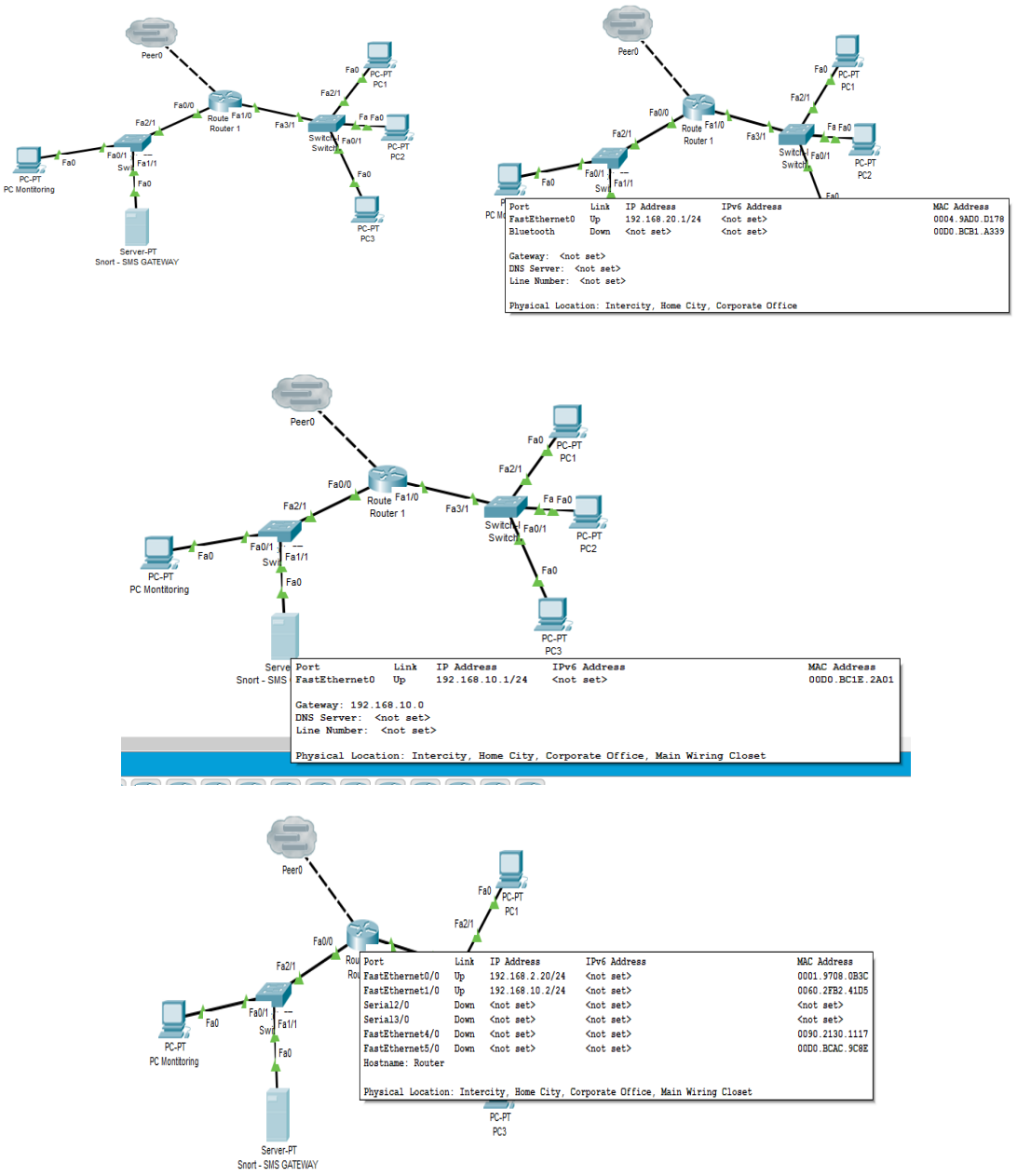
Tabel 1. Adapun jumlah – jumlah *sever, PC, router* dan *switch* yang digunakan

Device	Interface	IP address	Subnet mask	Default Gateway
Router	Fa0/0	192.168.2.20	255.255.255.0	N/A
	Fa1/0	192.168.10.2	255.255.255.0	N/A
Server	NIC	192.168.10.1	255.255.255.0	192.168.10.0
Pc Monitering	NIC	192.168.20.1	255.255.255.0	192.168.20.0
PC 1	NIC	192.168.20.2	255.255.255.0	N/A

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 7 Nomor 1 Februari 2022, pp 8-12
ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Device	Interface	IP address	Subnet mask	Default Gateway
PC 2	NIC	192.168.20.3	255.255.255.0	N/A
PC 3	NIC	192.168.10.4	255.255.255.0	N/A

Beberapa gambar yang kami implementasikan jaringan snort di cisco antara lain sebagai berikut:



Gambar 4. Beberapa implementasikan jaringan snort di cisco

```
Konfigurasi Jaringan snort di cisco ;
Konfigurasi di Router:
Router#enable
Router#configure terminal
```

```
Router(config)#interface Fa0/0
Router(config-if)#ip address 192.168.2.20 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface Fa1/0
Router(config-if)#ip address 192.168.10.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Selanjutnya untuk memasukan alamat *ip address* dan *subnet mask* di *PC* monitoring, PC1, PC2 dan PC3. Dengan melakukan *double klik* pada PC yang ingin dimasukan IP *Address*, *subnet mask*, dan *default gateway*. Selanjutnya akan muncul dekstop. Kemudian klik pada dekstop akan muncul beberapa pilihan seperti *command prompt* dan IP *configuration*. Lalu klik pada IP *configuration*, Isilah IP *address*, *Subnet mask* dan *Default gateway*. *Finish*.

4. SIMPULAN

Berdasarkan hasil Penerapan pendeteksi jaringan di snort menggunakan IDS (*Instruction Detection System*) dapat disimpulkan bahwa penggunaan sistem ini dapat mempermudah mendeteksi jaringan yang termasuk illegal (berbahaya untuk sebuah sistem operasi), mencegah kehilangan data dan informasi. Dengan adanya snort IDS (*Instruction Detection System*) dapat mengetahui jaringan apa saja yang masuk ke dalam system operasi.

DAFTAR PUSTAKA

[1] T. Keamanan and J. Komputer, "Keamanan Jaringan Komputer," *Scanning Keamanaan Jaringan Komputer*. 2021.

[2] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *AITI*, vol. 17, no. 2, 2021, doi: 10.24246/aiti.v17i2.143-158.

[3] R. Rosaly and A. Prasetyo, "Pengertian Flowchart Beserta Fungsi dan Simbol-simbol Flowchart yang Paling Umum Digunakan," *Https://Www.Nesabamedia.Com*, vol. 2, 2019.

[4] | Harjono and A. P. Wicaksono, "Sistem Deteksi Intrusi dengan Snort (Intrusion Detection System with Snort)," 2014.

[5] Zulkipli, M. Efendi, and Sihkabuden, "Pengembangan Modul Sistem Keamanan Jaringan Berbasis Simulasi CISCO," *Jurnal Pendidikan: Teori, Penelitian, dan Pengembangan*, vol. 1, no. 3, 2016.