PENGARUH PENEMPATAN *SNORT* TERHADAP KEAMANAN JARINGAN (STUDI KASUS LABORATORIUM VI JARINGAN KAMPUS 3 IST AKPRIND YOGYAKARTA)

Yusuf Abdulloh[1], Joko Triyono[2], Uning Lestari[3]
[1, 2, 3] Jurusan Informatika, FTI, IST AKPRIND
[1]yusuf.77.abdulloh@gmail.com, [2]jack@akprind.ac.id, [3]uning@akprind.ac.id

ABSTRACT

Snort is an application or security tool that serves to detect attacks while also preventing them. In the network, Snort can be placed in several positions, where the Snort placement is adjusted to the needs or criteria of the desired network security by the network administrator. In the development of the current network security system, the correct and appropriate Snort system placement will make the network more secure and difficult for intrusion by irresponsible parties.

This research implements a network security system using the Snort IDS (Intrusion Detection System) application, with two Snort placement positions on the network under the Router (Snort inside) and above the Router (Snort outside), both positions will be tested with three attack activities that is Port Scanning, SSH, and DoS. With the different position of Snort placement on the network, it will certainly make a difference in the results of network traffic analysis on Snort, then from these results can be considered in terms of Snort placement by the network administrator.

In testing the network security system using the Snort IDS application with two Snort placement positions on the local network Laboratory VI Campus IST AKPRIND Yogyakarta, the results obtained by testing the Port Scanning attack, SSH, and DoS, Snort placement inside are better than placing Snort outside.

Keywords: *IDS, Snort, Network Security*

INTISARI

Snort merupakan aplikasi atau *security tools* yang berfungsi untuk mendeteksi serangan sekaligus juga melakukan pencegahan. Di dalam jaringan, *Snort* dapat ditempatkan di beberapa posisi, yang mana penempatan *Snort* tersebut disesuaikan dengan kebutuhan atau kriteria keamana jaringan yang di inginkan oleh pengelola suatu jaringan. Dalam perkembangan sistem keamanan jaringan saat ini, penempatan sistem *Snort* yang benar dan sesuai akan dapat menjadikan jaringan yang lebih aman dan sulit untuk di intrusi oleh pihak tidak bertanggung jawab.

Penelitian ini mengimplementasikan sistem keamanan jaringan menggunakan aplikasi *IDS (Intrusion Detection System) Snort*, dengan dua posisi penempatan *Snort* pada jaringan yaitu di bawah *Router* (*Snort* dalam) dan di atas *Router* (*Snort* lsuar), kedua posisi tersebut akan diuji dengan tiga aktivitas serangan yaitu *Port Scanning*, *SSH*, dan *DoS*. Dengan perbedaan posisi penempatan *Snort* pada jaringan, hal tersebut tentu akan membuat perbedaan dalam hasil analisis trafik jaringan pada *Snort*, kemudian dari hasil tersebut dapat menjadi pertimbangan dalam hal penempatan *Snort* oleh pengelola jaringan.

Pada pengujian sistem keamanan jaringan menggunakan aplikasi *IDS Snort* dengan dua posisi penempatan *Snort* pada jaringan lokal Laboratorium VI Jaringan Kampus 3 IST AKPRIND Yogyakarta, didapatkan hasil dengan pengujian serangan *Port Scanning*, *SSH*, dan *DoS,* penempatan *Snort* dalam lebih baik dibandingkan penempatan *Snort* luar.

Kata Kunci : IDS, Snort, Keamanan Jaringan

PENDAHULUAN

Dalam mengamankan suatu jaringan, ada banyak metode dan aplikasi yang bisa digunakan. Salah satunya yaitu dengan menggunakan aplikasi *Intrusion Detection System (IDS)* yaitu *Snort*. *IDS* sendiri merupakan aplikasi yang bekerjasama dengan *firewall* dalam mendeteksi intrusi dan memberikan respon secara *real time* serta mengatasi intrusi yang dilakukan oleh pihak tidak bertanggung jawab.

Aplikasi *Snort* itu sendiri merupakan aplikasi *IDS* yang berfungsi sebagai *alert* atau peringatan dalam bentuk *file* yang berisikan informasi penyusup yang melakukan intrusi kemudian nantinya akan diteruskan ke administrator jaringan. Dalam penempatannya dalam suatu jaringan, Sistem *Snort* dapat ditempakan di beberapa tempat dalam jaringan, bisa melalui client ataupun di atasnya antara *switch* dengan *router* dan beberapa penempatan lainnya sesuai dengan spesifikasi jaringan. Dari penempatan tersebut tentu saja terdapat perbedaan yang dapat mempengaruhi keamanan jaringan.

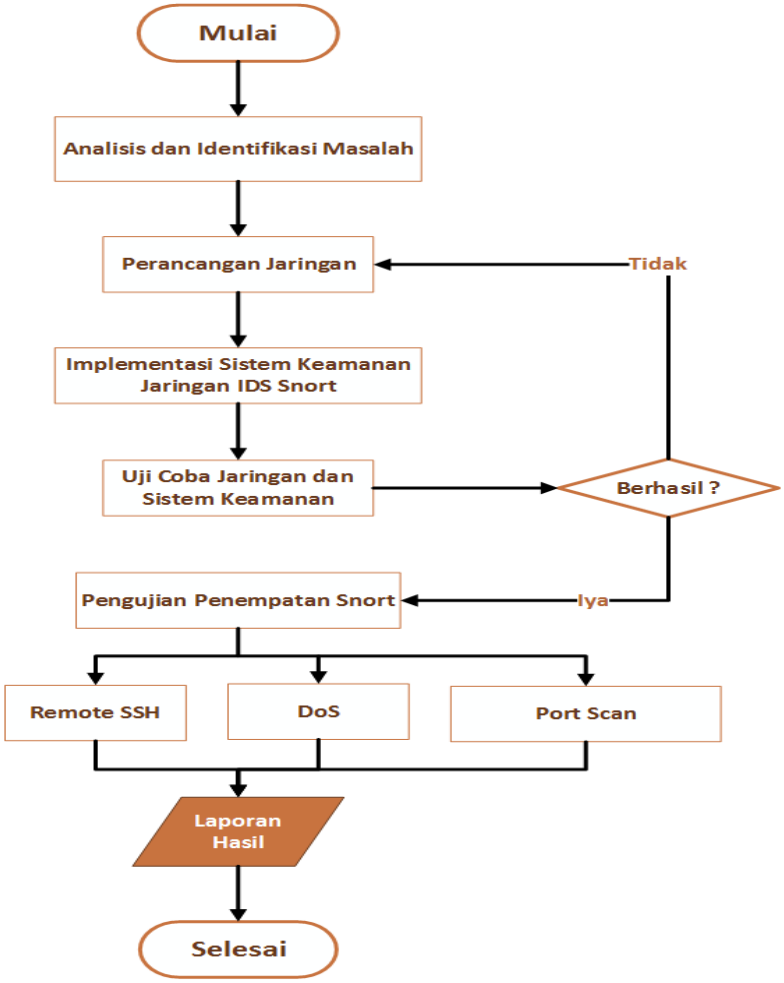
Dalam perkembangan sistem keamanan jaringan saat ini, maka diharapkan penempatan sistem *Snort* yang benar dan sesuai akan dapat menjadikan jaringan yang lebih aman dan sulit untuk di intrusi oleh pihak tidak bertanggung jawab.

Pada penelitian yang penulis lakukan, penelitian akan dilaksanakan di Laboratorium Jaringan Kampus III Institut Sains & Teknologi AKPRIND Yogyakarta. Pada Laboratorium tersebut saat ini menggunakan jaringan *internet* untuk bisa menunjang aktivitas ataupun kegiatan yang ada pada Laboratorium. Dengan adanya jaringan komputer pada suatu tempat terutama jaringan kampus, tentunya pada jaringan tersebut terdapat data penting yang perlu dijaga agar tidak bisa diakses ataupun diunduh oleh pengguna yang tidak dikenal. Saat ini pada jaringan komputer Laboratorium masih belum ada aplikasi keamanan jaringan seperti *IDS* yang dipasang secara langsung pada *server* Laboratorium. Dengan adanya sistem keamanan jaringan, tentunya akan lebih menjaga dan membuat jaringan lebih aman dari ancaman-ancaman keamanan jaringan serta dapat mengetahui sumber serangan, jenis serangan dan tujuan serangan yang akan dilakukan. Dengan belum ada penerapan sistem keamanan jaringan tersebut, penulis memilih aplikasi *IDS Snort* untuk diterapkan pada sistem keamanan Laboratorium.

Dengan latar belakang tersebut munculah gagasan penelitian untuk menganalisa pengaruh penempatan sistem *Snort* terhadap keamanan jaringan. Dengan adanya hasil analisa dari sistem ini, diharapkan dapat menjadi rujukan dalam penempatan sistem *Snort* yang sesuai pada penerapan sistem keamanan jaringan lainnya.

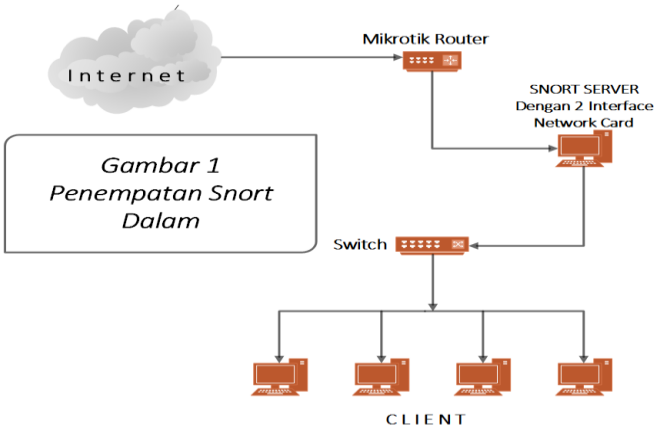
Berikut adalah diagram alir langkah penelitian yang penulis gunakan pada penelitian ini, seperti terlihat pada gambar 1. Dimulai dengan analisis dan identifikasi masalah yang akan dijadikan pembahasan pada penelitian ini. Setelah didapatkan hasil analisis dan identifikasi masalah pada langkah pertama, dilanjutkan pada tahap perancangan jaringan sesuai dengan spesifikasi jaringan yang dibutuhkan. Setelah perancangan jaringan dibuat, alur setelahnya yaitu implementasi sistem keamanan jaringan menggunakan IDS Snort, dengan memasang Snort pada server di jaringan laboratorium. Alur selanjutnya yaitu uji coba jaringan beserta sistem keamanan jaringan yang sudah dipasang aplikasi IDS Snort, apabila masih ada kegagalan sistem, maka kembali ke alur perancangan jaringan untuk dilakukan perbaikan. Namun sebaliknya apabila sistem jaringan beserta keamanan jaringan dapat berjalan sebagaimana mestinya maka dapat dilanjutkan ke alur penelitian selanjutnya. Alur selanjutnya yaitu pengujian sistem keamanan jaringan, dengan diberikan penetration testing ataupun serangan jaringan berupa Port Scan, SSH dan DoS terhadap server.

Setelah diberikan pengujian berupa penyerangan terhadap sistem jaringan dari dua penempatan sistem Snort, didapatkan data hasil pengujian yang dapat dijadikan tolak ukur kerentanan pada sistem keamanan jaringan berdasarkan dua penempatan Snort.



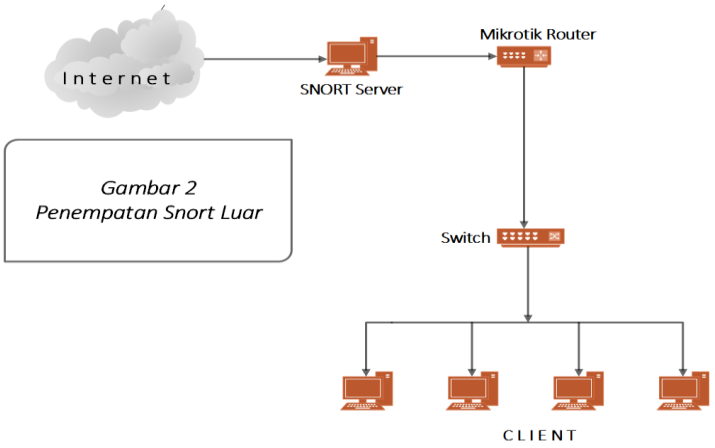
Gambar 1. Diagaram Alir Langkah Penelitian

Rancangan penempatan sistem Snort yang akan diimplementasikan pada jaringan ditunjukkan pada gambar 2 dan 3, dengan istilah yang penulis sebut dengan sebutan Snort Dalam dan Snort Luar.



Gambar 1 Penempatan Snort Dalam

Gambar 2. Snort Dalam



Gambar 2
Penempatan Snort Luar

Gambar 3. Snort Luar

Pada Snort Dalam seperti ditunjukkan oleh gambar 2, sistem Snort pada jaringan ditempatkan antara Router dengan Switch atau dapat dikatakan posisinya tepat dibawah Router. Sedangkan Snort Luar seperti ditunjukkan oleh gambar 3, sistem Snort ditempatkan diatas Router, sehingga letaknya diantara Router dengan ISP/Internet. Dari kedua penempatan sistem Snort tersebut akan dianalisis dari segi kerentanan keamanan jaringan setelah diberikan pengujian serangan terhadap keamanan jaringan IDS Snort.

TINJAUAN PUSTAKA

Penelitian ini menggunakan pustaka hasil-hasil penelitian sebelumnya yang relevan, yaitu penelitian (Sutarti, Pancaro, & Saputra, 2018), (Khairil & Kalsum, 2014), (Masse, Hidayat, & Badrianto, 2015), dan Buku karya dari (Rafiudin, 2010) berjudul *Mengganyang Hacker Dengan Snort*.

Penelitian yang dilakukan oleh (Sutarti, Pancaro, & Saputra, 2018) bertujuan untuk mewujudkan sistem keamanan jaringan dengan menggunakan aplikasi *Intrusion Detection System (IDS)* yaitu *Snort* dan *PfSense (Router OS)* guna mengurangi penyalahgunaan jaringan atau ancaman intrusi pada SMAN 1 Cikeusal.

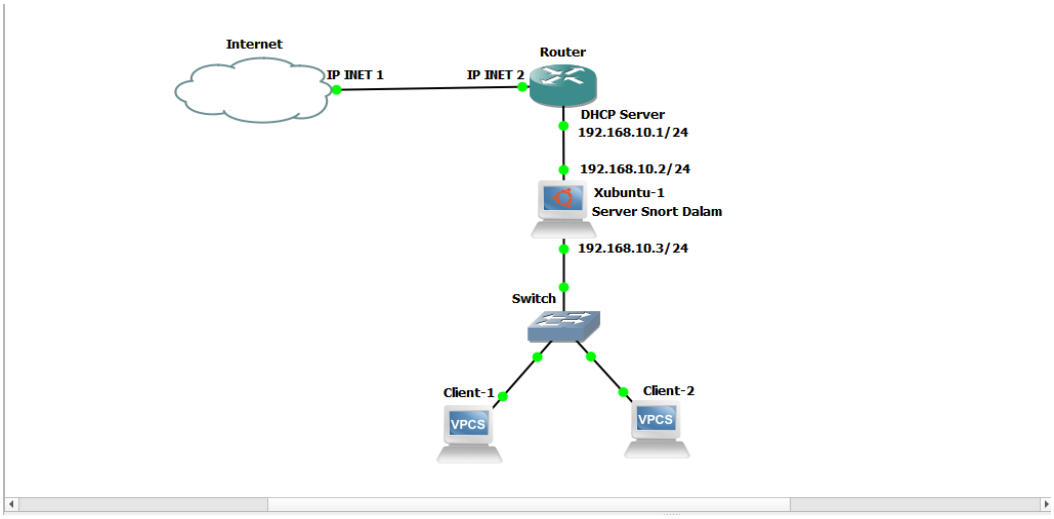
Penelitian yang dilakukan oleh (Khairil & Kalsum, 2014) bertujuan untuk mengetahui secara *real-time* ataupun *log-file* aktifitas paket-paket data pada jaringan yang terkoneksi dengan *web server* Universitas Dehasen Bengkulu. Terutama paket data yang mengancam terhadap keamanan *web server* seperti penyusupan atau penyerangan.

Penelitian yang dilakukan oleh (Masse, Hidayat, & Badrianto, 2015) bertujuan untuk merancang dan membuat sistem keamanan jaringan menggunakan *database MySql* pada *hotspot* kota. Sistem keamanan jaringan pada penelitian ini menggunakan aplikasi *IDS Snort*, yang mana dengan aplikasi ini diharapkan mampu mendeteksi paket-paket berbahaya pada jaringan dan langsung memberikan *alert* atau peringatan kepada administrator jaringan tentang kondisi jaringan pada saat itu sehingga dapat melakukan pencegahan atau tindakan dengan cepat.

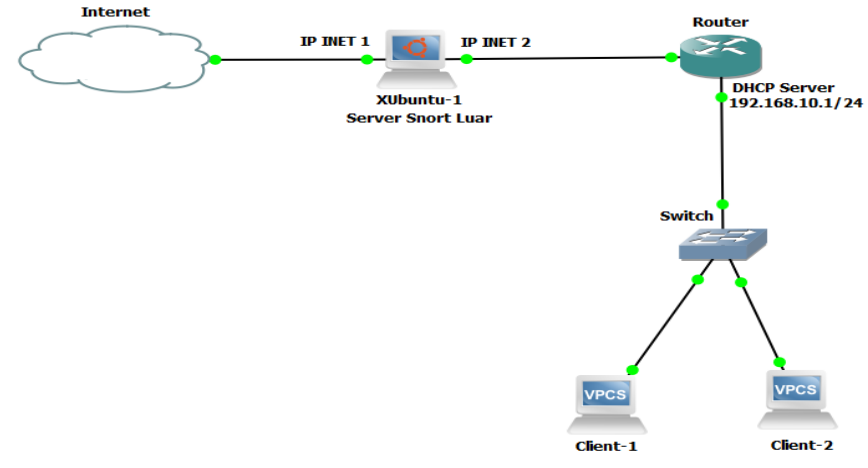
PEMBAHASAN

Perancangan dimulai dengan pembuatan skema jaringan berdsarkan dari hasil analisis dan identifikasi masalah yang sudah dilakukan sebelumnya dengan spesifikasi dan kebutuhan sesuai dari pengelola jaringan. Berikut topologi fisik yang

sudah dirancang melalui simulasi jaringan menggunakan aplikasi simulator GNS3 seperti ditunjukkan oleh gambar 4 dan 5.



Gambar 4. Rancangan Topologi Fisik Snort Dalam



Gambar 5. Rancangan Topologi Fisik Snort Luar

Tahapan selanjutnya setelah perancangan jaringan yaitu mengimplementasikan sistem keamanan jaringan dengan aplikasi IDS Snort. Pada tahap ini, langkah-langkah yang dilakukan yaitu instalasi IDS Snort beserta syarat-syarat beserta library yang perlu dipenuhi sebelum memasang IDS Snort pada server jaringan. Pada gambar 6, merupakan hasil instalasi Snort yang berhasil dengan memeriksa versi Snort yang sudah terpasang.

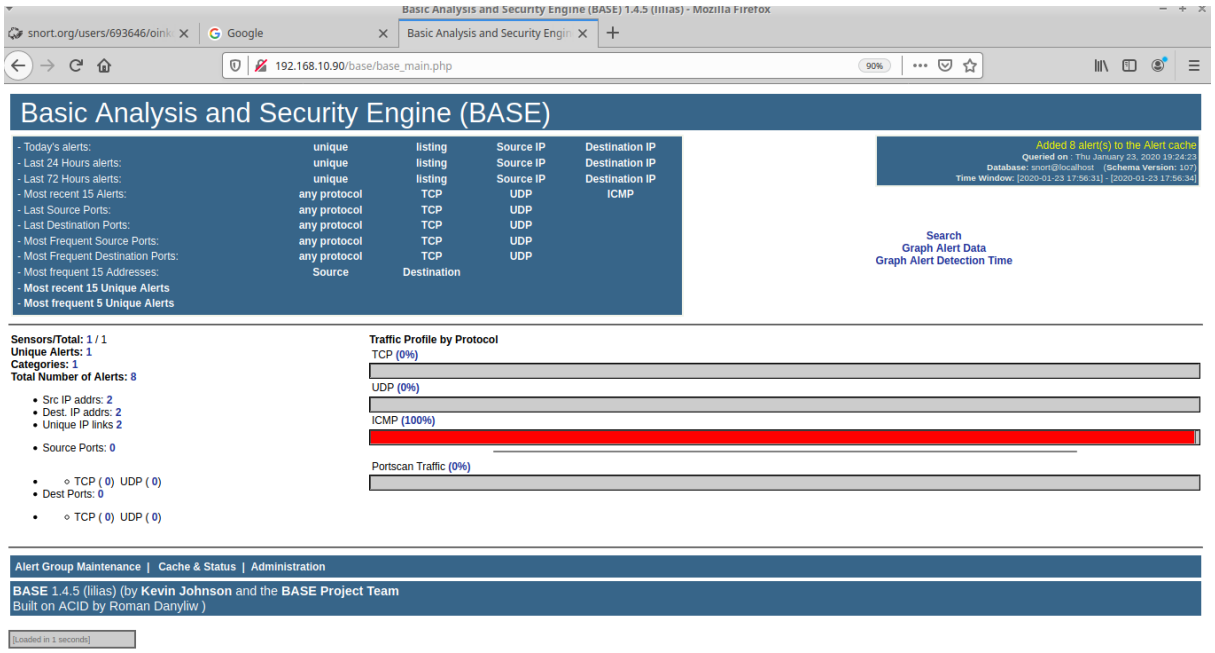
```
root@lab6-desktop:~/snort_src# snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

root@lab6-desktop:~/snort_src#
```

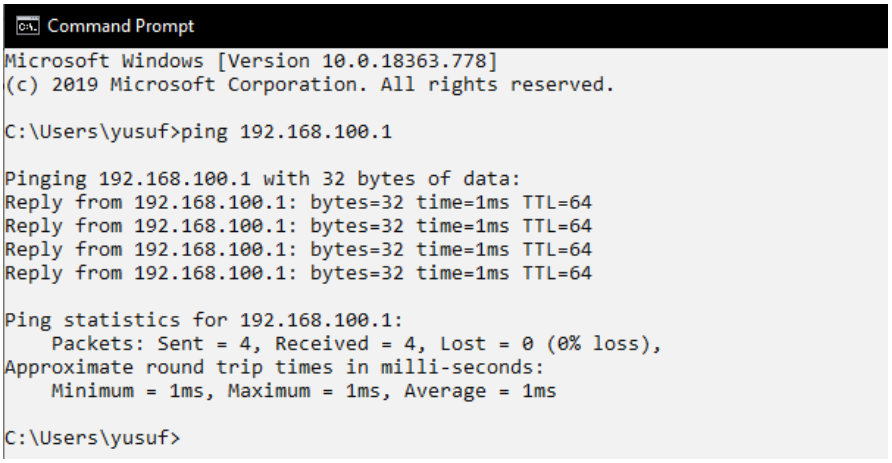
Gambar 6. Versi Snort

Selain IDS Snort yang dipasang pada server jaringan, terdapat langkah tambahan yang perlu dilakukan untuk bisa menggunakan IDS Snort menjadi lebih user friendly, yaitu memasang aplikasi-aplikasi pendukung Snort guna menjadikan IDS Snort lebih mudah dikelola dan monitoring seperti Barnyard2, Apache pada linux, BASE, yang mana aplikasi pendukung tersebut untuk menerjemahkan data hasil IDS Snort untuk kemudian ditampilkan menggunakan web server sehingga menjadikan Snort lebih mudah dibaca serta dikelola oleh pengelola jaringan. Pada gambar 7, merupakan hasil pemasangan salah satu aplikasi pendukung Snort sebagai web server data Snort yaitu BASE.



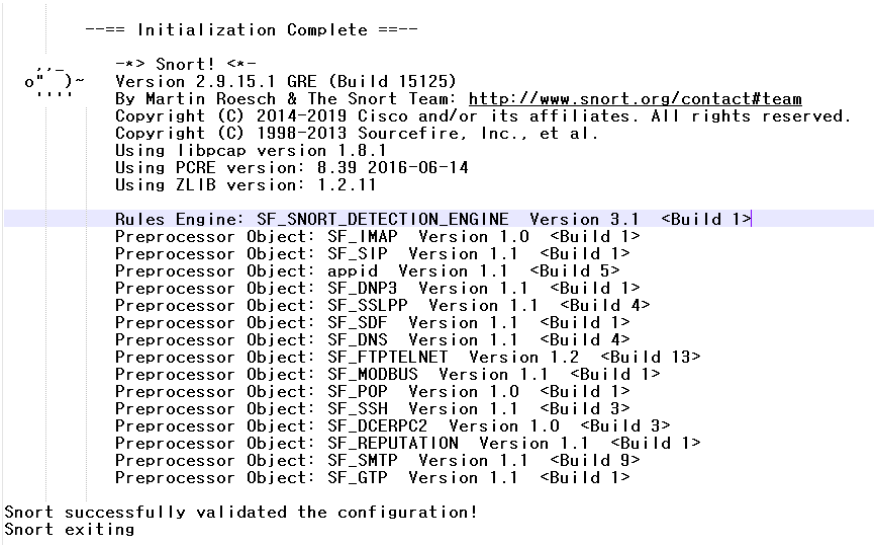
Gambar 7. BASE Web Server Snort

Tahapan selanjutnya setelah implementasi sistem keamanan jaringan IDS Snort, yaitu pengujian penggunaan jaringan beserta sistem keamanan jaringan IDS Snort. Pada tahap ini langkah yang dilakukan yaitu melakukan simulasi konektivitas antar perangkat yang terhubung dan juga antar jaringan. Pada pengujian jaringan, dilakukan tes ping antar perangkat seperti ditunjukkan pada gambar 8.



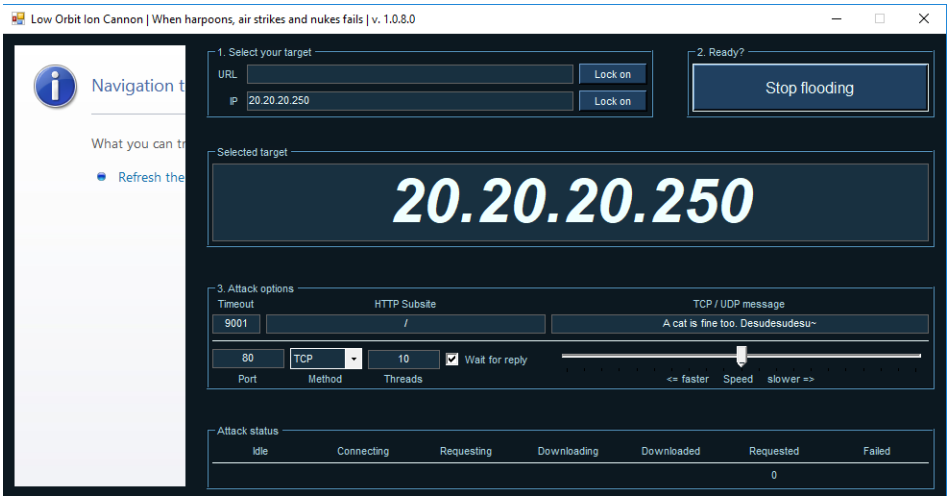
Gambar 8. Uji Konektivitas Jaringan

Untuk pengujian IDS Snort, dilakukan uji validitas konfigurasi Snort guna mengetahui apakah IDS Snort sudah siap dan bisa untuk digunakan. Pada gambar 9, merupakan hasil pemeriksaan validitas konfigurasi IDS Snort pada server.



Gambar 9. Cek Validitas Konfigurasi Snort

Langkah berikutnya yaitu pengujian penempatan Snort sesuai pada desain rancangan penempatan Snort pada dua posisi. Kemudian pada setiap penempatan Snort tersebut akan diberikan pengujian serangan terhadap Snort. Pengujian yang diberikan antara lain Port Scanning, SSH, dan DoS. Pada setiap penempatan Snort di kedua posisi pada jaringan akan diberikan tiga macam pengujian tersebut. Pada gambar 10, merupakan salah satu proses pengujian yang diberikan dengan pengujian serangan DoS terhadap server Snort.



Gambar 10. Proses Serangan DoS Terhadap Snort

Pada IDS Snort, ketika aktivitas serangan DoS tersebut dilakukan, Snort dapat mendeteksi aktivitas tersebut untuk kemudian dapat menjadi peringatan kepada selaku pengelola jaringan sehingga dapat segera diberikan tindakan pencegahan untuk mengamankan jaringan yang dikelola. Pada keterangan dibawah merupakan hasil pendeteksian aktivitas DoS terhadap Snort yang tampil pada terminal.

```
02/06-23:22:18.841434  [**] [1:2019348:2] ET DOS Terse HTTP GET Likely AnonMafiaIC DDoS tool [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 20.20.20.251:53463 -> 20.20.20.1:80
```

Dari dua pengujian penempatan *Snort* dalam jaringan yang sudah penulis eksplorasi, penulis menyimpulkan bahwa penempatan *Snort* dalam, lebih baik dan lebih aman dibandingkan dengan penempatan *Snort* luar. Sesuai dengan hasil pengujian yang sudah penulis lakukan, *Snort* dalam berhasil berfungsi sebagimana fungsi dari *IDS* maupun *IPS*. Sedangkan pada penempatan *Snort* luar, dikarenakan perbedaan segmen jaringan, *Snort* tidak dapat bekerja dengan maksimal sebagaimana mestinya fungsi *IDS* maupun *IPS*. Pada penempatan *Snort* luar, *Snort* hanya dapat mendeteksi sumber *ip* dari *ip Router* saja, tanpa bisa mendeteksi sumber *ip* penyerang secara langsung sehingga tidak dapat terhubung langsung dengan segmen jaringan yang berbeda walaupun sudah dikonfigurasi bagian *Routing* pada *Router*.

Kemudian pengaruh keamanan jaringan pada Laboratorium setelah dipasang sistem *IDS Snort*, dapat membuat keamanan pada jaringan Laboratorium yang sebelumnya belum ada sistem keamanan seperti *IDS*, melainkan hanya melalui *monitoring* dan langsung melalui *Router*. Dengan adanya layanan *Snort* pada jaringan, pengelola akan mudah dalam membuat konfigurasi keamanan, dengan konfigurasi melalui *rules Snort*. Pada *rules* tersebut, dapat dibuat dan dirubah sesuai dengan keinginan ataupun kebutuhan pengelola jaringan, sehingga ketika ada aktivitas yang tidak sesuai atau ada aktivitas serangan, akan otomatis terdeteksi sesuai konfigurasi pada *rules* yang telah dibuat, kemudian dapat langsung diberikan tindakan.

No	Jenis Serangan	Sumber & Destinasi Serangan	Keterangan	Penempatan Snort	
		IP Sumber - IP Destinasi		Dalam	Luar
1	Port Scanning	20.20.20.251/24 – 20.20.20.1/24	*IP Client* ke *IP Router*	Terdeteksi	---
		20.20.20.251/24 – 20.20.20.250/24	*IP Client* ke *IP Server Snort*	Terdeteksi	---
		192.168.10.248/24 – 20.20.20.1/24	*IP Client* ke *IP Gateway Inet*	---	Terdeteksi, kurang maksimal
		192.168.10.248/24 – 20.20.20.250/24	*IP Client* ke *IP Server Snort*	---	Terdeteksi, kurang maksimal
2	SSH	20.20.20.251/24 – 20.20.20.1/24	*IP Client* ke *IP Router*	Terdeteksi	---
		20.20.20.251/24 – 20.20.20.250/24	*IP Client* ke *IP Server Snort*	Terdeteksi	---
		192.168.10.248/24 – 20.20.20.1/24	*IP Client* ke *IP Gateway Inet*	---	Terdeteksi, kurang maksimal
		192.168.10.248/24 – 20.20.20.250/24	*IP Client* ke *IP Server Snort*	---	Terdeteksi, kurang maksimal
3	DoS	20.20.20.251/24 – 20.20.20.1/24	*IP Client* ke *IP Router*	Terdeteksi	---
		20.20.20.251/24 – 20.20.20.250/24	*IP Client* ke *IP Server Snort*	Terdeteksi	---
		192.168.10.248/24 – 20.20.20.1/24	*IP Client* ke *IP Gateway Inet*	---	Terdeteksi, kurang maksimal
		192.168.10.248/24 – 20.20.20.250/24	*IP Client* ke *IP Server Snort*	---	Terdeteksi, kurang maksimal

Tabel 1. Data Rangkuman Hasil Penelitian

Dari tabel 1, merupakan data hasil pengujian penempatan *Snort* dari dua posisi penempatan, di atas *Router* dan di bawah *Router*, dengan diberikan tiga macam aktivitas pengujian. Dari tabel tersebut, dapat disimpulkan bahwa dengan penempatan *Snort* pada jaringan, *Snort* akan bekerja dengan baik ketika *Snort* ditempatkan pada satu segmen jaringan, sehingga untuk menjalankan layanan *Snort* pada jaringan, diperlukan jaringan pada masing-masing *Snort*. Penempatan *Snort* dalam dapat disimpulkan lebih baik dikarenakan dapat memenuhi unsur fungsi kinerja dari pada *IDS* sendiri.

KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan, dapat diperoleh beberapa kesimpulan sebagai berikut:

1. Setiap penempatan *Snort*, agar *Snort* dapat berfungsi sebagaimana fungsinya sebagai *IDS* maupun *IPS* dan lebih *safety* dalam mengelola jaringan, pada setiap penempatan *Snort* diberikan jaringan tersendiri sesuai kebutuhan masing-masing jaringan, sehingga pengelola jaringan pun juga akan lebih mudah dalam mengelola dan mengamankan jaringan.
2. Penempatan *Snort* dalam lebih baik dari segi fungsi kineja IDS dibandingkan dengan penempatan *Snort* luar.
3. Agar *Snort* bisa lebih mudah untuk di*monitoring* serta dibaca datanya, perlu untuk memasang aplikasi pendukung *Snort* seperti *BASE* ataupun *Snorby* sebagai *monitoring GUI Snort* dengan *web server*, *Barnyard2* sebagai penerjemah *output file Snort* agar dapat lebih mudah dibaca dan dapat dikelola melalui *database MySQL*, maupun aplikasi pendukung lainnya yang dapat menjadikan *Snort* mudah untuk dikelola oleh pengelola jaringan.
4. Pada Laboratorium setelah dibuatkan sistem keamanan jaringan, lebih aman dan terpantau akses trafik jaringan.

DAFTAR PUSTAKA

Dordal, P. L. (2019). *An Introduction to Computer Networks.* Chicago: Loyola University Chicago.

K, Y. (2018, 5 1). *Pengertian DDOS Dan Bagaimana Menaggulanginya*. Dipetik 2 20, 2020, dari Niagahoster: https://www.niagahoster.co.id/blog/ddos-adalah/

K, Y. (2019, 7 31). *Apa itu SSH*. Dipetik 2 20, 2020, dari Niagahoster: https://www.niagahoster.co.id/blog/apa-itu-ssh/

Khairil, & Kalsum, T. U. (2014). IMPLEMENTASI INTRUSION DETECTION SYSTEM SEBAGAI KEAMANAN WEB SERVER UNIVERSITAS DEHASEN BENGKULU. *Pseudocode, Volume 2 Nomor 1*, 155-169.

Kizza, J. M. (2014). *Guide to Computer Network Security (3th Edition).* Chattanooga: Springer.

Lowe, D. (2011). *Networking All-in-One For Dummies 4th Edition.* Indianapolis: Wiley Publishing, Inc.

M. R.-O. (2013). *The Complete Reference; Information Security (2th Edition).* New York: McGraw-Hill Education.

Masse, F. A., Hidayat, A. N., & Badrianto. (2015). PENERAPAN NETWORK INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT BERBASIS DATABASE MYSQL PADA HOTSPOT KOTA. *Elektronik Sistem Informasi Dan Komputer, Vol 1 No.2*, 1-16.

Mikrotik. (2018). *Port Scan Detection*. Dipetik 2 20, 2020, dari mikrotik.id: http://mikrotik.co.id/artikel_lihat.php?id=284

Rafiudin, R. (2010). *Mengganyang Hacker dengan SNORT.* Yogyakarta: Andi.

Rehman, R. U. (2003). *Intrusion Detection Systems With Snort.* New Jersey: Pearson Education, Inc.

Sutarti, Pancaro, A. P., & Saputra, F. I. (2018). IMPLEMENTASI IDS (INTRUSION DETECTION SYSTEM) PADA SISTEM KEAMANAN JARINGAN SMAN 1 CIKEUSAL. *Jurnal PROSISKO Vol.5 No.1*, 1-8.

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks (5th Edition).* Boston: Pearson Education, Inc.

Taringan, A. (2009). *Bikin Gateway Murah Pakai MikroTik.*