IMPLEMENTASI DAN ANALISIS KEMANAN JARINGAN VIRTUAL HIPS SNORT PADA LAYANAN WEB SERVER DENGAN PENYERANGAN DOS DAN DDOS

IMPLEMENTATION AND ANALYSIS VIRTUAL NETWORK SECUTIRY WITH HIPS SNORT ON WEB SERVER SERVICE AGAINTS DOS AND DDOS ATTACK

Riyo Surya Putra[1], Ratna Mayasari[2], Nyoman Bogi Aditya Karna[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]**riyosuryaa@students.telkomuniversity.ac.id**
[2]**ratnamayasari@telkomuniversity.ac.id**, [3]**aditya@telkomuniversity.ac.id**

Abstrak

Web server adalah perangkat yang memberikan layanan berbasis paket data kepada klien melalui protokol HyperText Transfer Protocol (HTTP). Protokol ini memberikan layanan berbagi informasi melalui World Wide Web (WWW) dimana klien akan meminta informasi dari suatu website dan web server akan memberikan informasi yang diminta. Berdasarkan data pengukuran yang dikeluarkan oleh McAfee Labs, selama tahun 2016 36% dari serangan di jaringan menyerang Web Server. Salah satu serangan yang digunakan adalah Denial of Service (DOS) yaitu serangan dengan satu *Attacker* dan Distributed Denial of Service (DDOS) yaitu serangan dengan lebih dari satu *Attacker* yang bertujuan untuk membuat layanan Server terganggu bahkan dapat merusak *Hardware* dari Server tersebut. Oleh karenanya banyak metode ditawarkan untuk menjaga layanan suatu web server agar tetap stabil, salah satunya adalah Host Intrusion Prevention System (HIPS).

Kata kunci : Web Server, HIPS, DOS, DDOS, Snort dan TCP SYN Flood.

Abstract

Web server is a device that provides services based on packet data to the client via the HyperText Transfer Protocol (HTTP) protocol. This protocol provides information sharing services through the World Wide Web (WWW) where the client will request information from the website and the web server will provide the requested information. Based on measurement data released by McAfee Labs, during 2016 36% of attacks on the network invade Web Server. One of the attacks is a Denial of Service (DOS) attacking with one Attacker and Distributed Denial of Service (DDOS) attacking with more than one Attacker which aims to make Server services remain compromised and can even damage the Hardware from the Server. Because of the many ways offered to keep the web server stable, one of them is Host Intrusion Prevention System (HIPS).

Keywords: Web Server, HIPS, DOS, DDOS, Snort and TCP SYN Flood

1. Pendahuluan

Pada zaman modern ini, informasi dan komunikasi tidak hanya melalui koran, pesan singkat dan telepon. Tetapi penyebaran informasi/berita dan komunikasi dengan orang yang berada jauh dari kita, sekarang bisa melalui sebuah Website dan aplikasi yang ada di internet. Sehingga, penyebaran informasi/berita menjadi lebih cepat dan berkomunikasi dengan orang terjauh menjadi lebih ekonomis, bahkan layanan ini sudah menjadi kebutuhan bagi pengguna. Tetapi belakangan ini kerap terjadi penyerangan pada Website yang membuat pengguna tidak dapat mengakses layanan Web Server. Kasus-kasus yang terjadi belakangan ini menimpa salah satu perusahaan IT terbesar yaitu Sony Playstation, yang menyebabkan pengguna tidak dapat mengakses karena terjadi kegagalan layanan [1], insiden juga terjadi pada pertengahan 2009 dimana domain.co.id sempat drop selamat 4 hari [2] .Dikarenakan Server tempat menerima dan melayani permintaan dari pengguna dari Web Browser diserang dengan teknik penyerangan Denial of Service (DOS) yaitu penyerangan dengan satu Attacker dan Distributed Denial of Server (DDOS) yaitu penyerangan dengan lebih dari satu Attacker membanjiri dengan paket-paket kepada Server. Sehingga Server sibuk melayani permintaan paket yang sangat banyak dan membuat kinerja Server menurun. Dan apabila permintaan paket yang lebih banyak lagi akan menyebabkan kerusakan pada perangkat keras atau Server [3].

Kekhawatiran ini tentu bisa dihindari dengan diberikan keamanan pada Server agar terhindar dari serangan yang merugikan. Cara perlindungan yang sering digunakan dengan sebuah metode Intrusion Detection System (IDS) yang dapat mendeteksi dan merekap aktivitas yang mencurigakan masuk ke dalam sebuah sistem atau jaringan. Tetapi IDS ini tidak bisa mencegah atau menghentikan paket serangan, maka dilakukan modifikasi sistem atau metode IDS bernama Intrusion Prevention System(IPS) [4].

Pada tugas akhir ini akan dibuat jaringan virtual dimana akan dilakukan simulasi serangan DOS dan DDOS terhadap sebuah Server melalui protocol TCP yang dilengkapi dengan pertahanan Host Intrusion Prevention System(HIPS) yaitu snort dengan rule IPS yang diusulkan dari penelitian [3][5][6][7][8][9]. Snort IPS ini akan diletakkan di sisi Server dan akan memberikan bukti rekap data saat penyerangan terjadi.

2. Tinjauan Pustaka

2.1 Transmission Control Protocol (TCP)

Suatu protokol yang berada di lapisan transport (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (*connection-oriented*) dan dapat diandalkan (*reliable*).[10]

2.2 *Denial of Service (DOS)* dan *Distributed Denial of Service(DDOS)*

DOS adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan *resource* yang dimiliki oleh *server* tersebut, sampai *server* tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer atau *server* yang diserang tersebut.DDOS adalah salah satu jenis serangan DOS yang menggunakan banyak *host* penyerang untuk menyerang satu target dalam sebuah jaringan atau bisa disebut dengan *botnet*.[11]

Salah satu jenis serangan DOS dan DDOS yaitu : SYN *flood Attack*. Penyerang membuat alamat sumber acak untuk setiap paket. SYN *Flags* yang diatur dalam setiap paket adalah permintaan untuk membuka koneksi baru ke server dari alamat IP palsu. Korban menanggapi alamat IP palsu, kemudian menunggu konfirmasi yang tidak akan pernah sampai (menunggu sekitar 3 menit) dan tabel koneksi korban terisi dengan menunggu balasan, setelah tabel terisi, semua koneksi baru diabaikan pengguna yang sah juga diabaikan, dan tidak dapat mengakses server setelah penyerang berhenti membanjiri server, biasanya kembali ke keadaan normal karena sistem operasi yang lebih baru mengelola sumber daya lebih baik, sehingga lebih sulit untuk meluap tabel, tetapi masih rentan banjir SYN dapat digunakan sebagai bagian dari serangan lain, seperti menonaktifkan satu sisi sambungan dalam pembajakan ICMP, atau dengan mencegah otentikasi atau penebangan di antara server. Serangan "denial-of-service" dicirikan oleh upaya eksplisit oleh penyerang untuk mencegah pengguna layanan yang sah dari menggunakan layanan tersebut. Ada dua bentuk umum serangan DoS: yaitu *crash services* dan *flood services*. [12]

2.3 Host Intrusion Prevention System (HIPS)

Intrusion Prevention system (IPS) merupakan sebuah pengembangan dari sistem *Intrusion Detection System (IDS)* yang hanya berfungsi melakukan pendeteksian terhadap aktifitas yang tidak normal, dalam IPS akan melakukan langkah-langkah pencegahan selanjutnya dengan tujuan menjaga jaringan agar tetap aman.[13]

2.4 Snort

Snort adalah teknologi deteksi intrusi dan pencegahan open source. Snort merupakan Bahasa yang menggabungkan keunggulan signature, protokol dan anomaly berbasis metode inspeksi sebagai IDS dan IPS, Snort dapat melakukan analisis paket *real-time* dan *logging* di jaringan analisis protokol dan pencarian konten / pencocokan adalah fitur yang paling kuat yaitu yang bisa digunakan untuk mendeteksi berbagai serangan seperti *buffer overflow stealth port scan, Probe SMB, footprinting, DOS and DDOS*[14]

2.5 Wireshark

Wireshark adalah penganalisis protokol jaringan terkemuka dan paling banyak digunakan di dunia. Ini memungkinkan Anda melihat apa yang terjadi di jaringan Anda pada tingkat mikroskopis dan merupakan standar de facto (dan sering de jure) di banyak perusahaan komersial dan nirlaba, lembaga pemerintah, dan lembaga pendidikan. Pengembangan Wireshark berkembang berkat kontribusi relawan ahli jaringan di seluruh dunia dan merupakan kelanjutan dari proyek yang dimulai oleh Gerald Combs pada tahun 1998.[18]

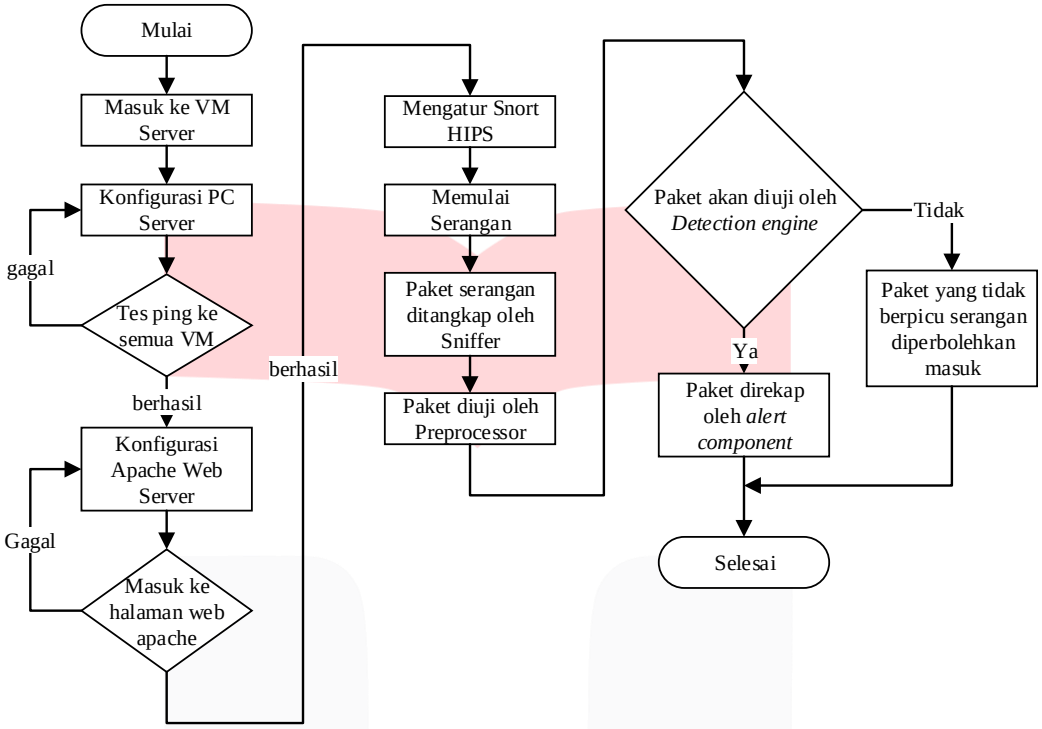
2.6 Zabbix

Lingkup pekerjaan dasar Zabbix LLC adalah pengembangan perangkat lunak open source untuk memantau jaringan dan aplikasi. Selain itu perusahaan menawarkan berbagai layanan profesional yang dirancang untuk memenuhi setiap tuntutan bisnis unik pelanggan termasuk implementasi, integrasi, pengembangan kustom dan layanan konsultasi serta berbagai program pelatihan. Produk andalan perusahaan adalah Zabbix, salah satu perangkat lunak pemantauan sumber terbuka yang paling populer di dunia. Ini sudah digunakan oleh sejumlah besar perusahaan, yang telah memilihnya karena skalabilitas yang nyata, kinerja yang tinggi dan kuat, kemudahan penggunaan dan biaya kepemilikan yang sangat rendah.[19]

3. PERANCANGAN SISTEM

Pada bab ini akan dijelaskan tentang pemodelan sistem dan topologi jaringan virtual menggunakan VMWare dimana di dalamnya akan ada beberapa *Virtual Machine* sebagai penyerang dengan teknik penyerangan DOS dan DDOS terhadap protokol TCP, pertahanan dengan HIPS Snort pada layanan *Web Server*, dan *Client* untuk mengakses *Web Server* disaat sedang terjadi penyerangan.

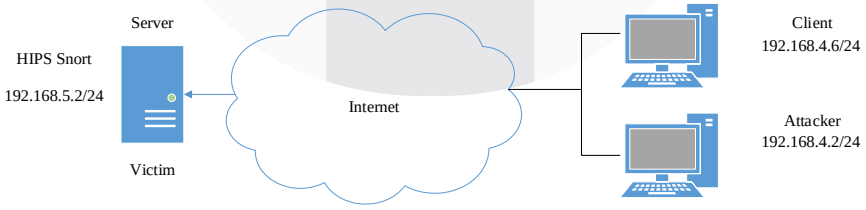
3.1 Diagram Alir Sistem



Gambar 3.1 Proses Kerja HIPS Snort

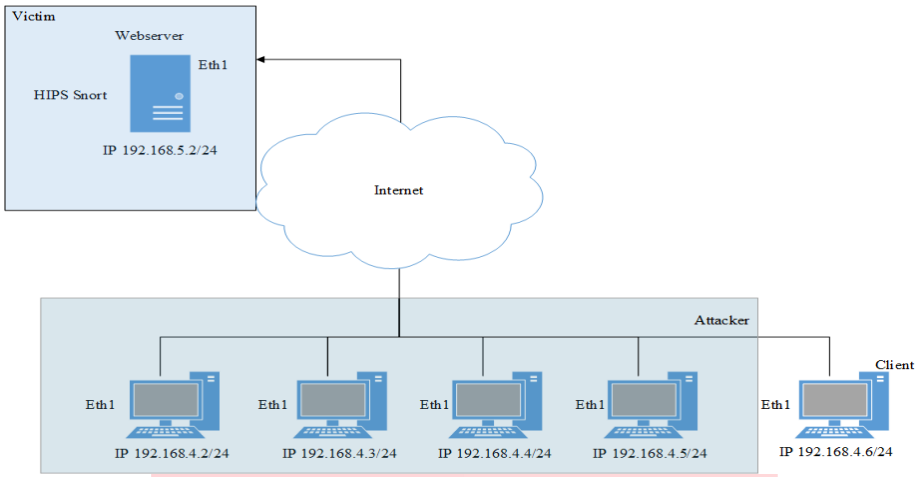
3.2 Skenario Pengujian

Berikut adalah topologi untuk skenario DOS dengan beberapa perangkat, yaitu : dengan sebuah Server, satu Client dan satu Attacker. Untuk menguji ketahanan apakah Snort dapat melakukan block atau drop serangan dari Attacker



Gambar 3.2 Skenario DOS dengan satu *Attacker*

Berikut adalah topologi untuk skenario DDOS dengan beberapa perangkat, yaitu dengan sebuah Server, satu Client dan empat Attacker.



Gambar 3.3 Pengujian DDOS dengan 4 *Attacker*

4. PENGUJIAN DAN ANALISA SISTEM

4.1 Pengujian Snort Tanpa *Rule* dan Dengan *Rule*

Pada pengujian ini, akan memperlihatkan perbedaan antara Snort yang aktif tanpa *rule* dan Snort aktif dengan *rule* saat *Attacker* menyerang.

```
Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=5770)
Decoding Ethernet
```

Gambar 4.1 Pengujian Snort Tanpa *Rule*

Dapat dilihat pada gambar 4.1 tidak terlihat *Alert* atau pendeteksian dan pencegahan pada saat *Attacker* melakukan penyerangan dengan TCP SYN *flood*.

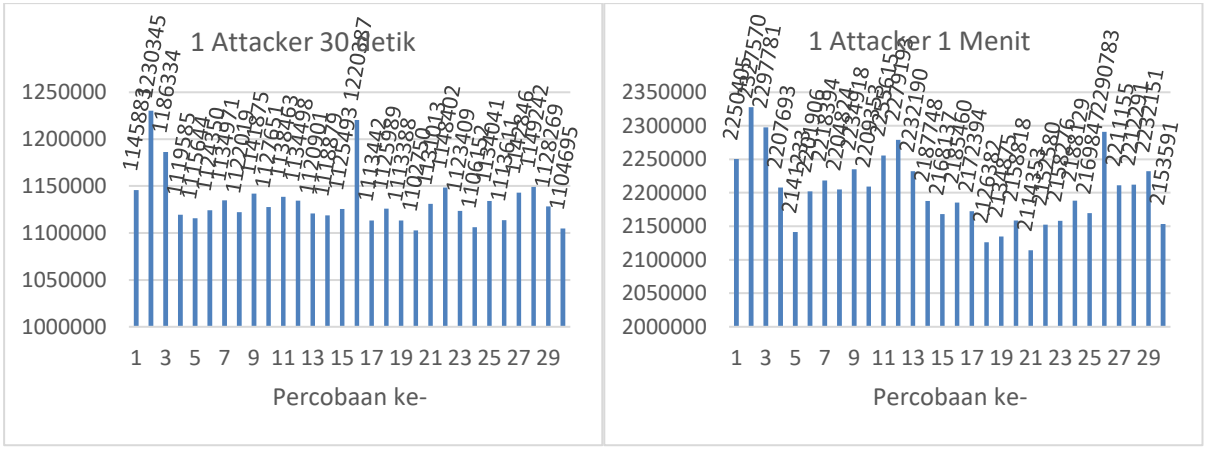
```
07/17-11:13:52.018286  [Drop] [**] [1:1000001:1] TCP SYN flood attack detected a
nd denied [**] [Priority: 0] {TCP} 192.168.5.1:3095 -> 192.168.5.2:0
07/17-11:13:52.020942  [Drop] [**] [1:1000001:1] TCP SYN flood attack detected a
nd denied [**] [Priority: 0] {TCP} 192.168.5.1:3332 -> 192.168.5.2:0
07/17-11:13:52.025306  [Drop] [**] [1:1000001:1] TCP SYN flood attack detected a
nd denied [**] [Priority: 0] {TCP} 192.168.5.1:3638 -> 192.168.5.2:0
```

Gambar 4.2 Pengujian Snort dengan *Rule*

Proses berhasil dilakukan pada gambar 4.2 terlihat *Alert* atau pendeteksian dan pencegahan pada saat *Attacker* melakukan penyerangan dengan TCP SYN *flood*, yang menandakan bahwa *rule* yang diatur pada snort berhasil mendeteksi dan mencegah dengan tanda *Drop* pada *console*.

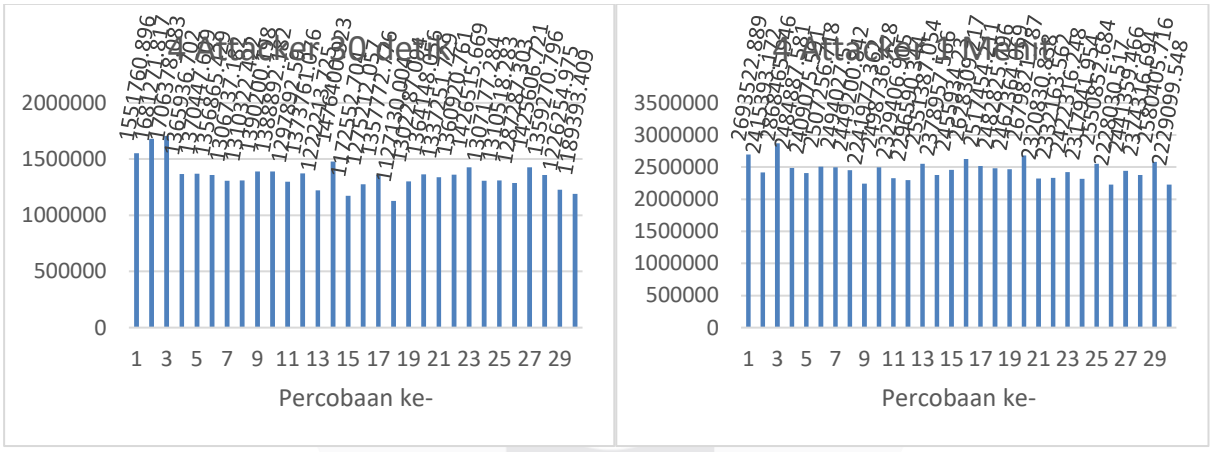
4.2 Pengukuran Total Paket yang Datang

Dilakukan pengukuran sebanyak 30 kali dalam setiap 30 detik dan 1 menit. Agar mendapatkan mengetahui rata-rata jumlah paket yang diterima oleh server. Terdapat skenario pengujian dengan pertambahan jumlah *Attacker*:



Gambar 4.3 Grafik *event* dengan 1 *Attacker* selama 30 detik dan 1 menit

Berdasarkan pada Gambar 4.3, rata-rata paket yang masuk ke server dalam waktu 30 detik sebanyak 1.134.817 dalam waktu 1 menit sebanyak 2.202.602. Terlihat bahwa 1 *Attacker* menyerang server dengan mengirimkan paket yang hampir konsisten pada peningkatan waktu 2 kali lebih lama dan jumlah paket dalam waktu 1 menit hampir 2 kali lipat dari jumlah paket dalam waktu 30 detik.

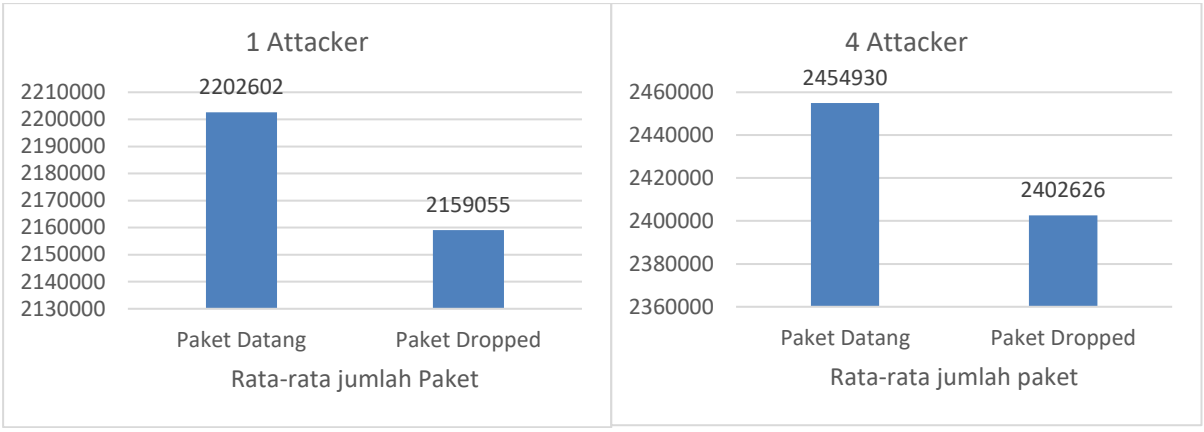


Gambar 4.4 Grafik *event* dengan 4 *Attacker* selama 30 detik dan 1 menit

Berdasarkan Gambar 4.4, rata-rata paket yang masuk ke server dalam waktu 30 detik sebanyak 1.354.279 dan dalam waktu 1 menit sebanyak 2.454.930. Perbandingan rata-rata jumlah paket yang datang pada pengujian 1 dalam waktu 30 detik dengan 1 *Attacker* sebesar 1.134.817 dan pada pengujian 2 dalam waktu 30 detik dengan 4 *Attacker* sebesar 1.345.279, tidak terjadi penambahan jumlah paket yang signifikan.

4.3 Pengukuran dengan Snort

Pengukuran ini membandingkan jumlah paket yang terdeteksi oleh Snort dan Wireshark untuk mendapatkan selisih jumlah paket (yang lewat) dari kedua *monitoring tools.*



Gambar 4.5 Diagram Perbandingan Paket antara 1 *Attacker* dengan 4 *Attacker*

Diagram pada gambar 4.5 merupakan rata-rata perbandingan jumlah paket yang datang ke server dengan jumlah paket yang di*drop* oleh dengan 1 *Attacker*. Rata-rata paket yang datang sebanyak 2.202.602 dan paket yang di*drop* oleh snort sebanyak 2.159.055 atau 97.984%, jadi selisih antara paket yang datang dan paket yang di*drop* oleh snort 43.546 atau sekitar 2.015% paket yang terlewat atau tidak di*drop* oleh snort.

Diagram pada gambar 4.5 merupakan rata-rata perbandingan jumlah paket yang datang ke server dengan jumlah paket yang di*drop* oleh snort pada pengukuran pertama dengan 4 *Attacker*. Rata-rata paket yang datang sebanyak 2.454.930 dan paket yang di*drop* oleh snort sebanyak 2.402.626 atau 97.808%, jadi selisih antara paket yang datang dan paket yang di*drop* oleh snort 52.034 atau sekitar 2.191% paket yang terlewat atau tidak di*drop* oleh snort.

4.4 Pengukuran *Network Traffic*

Karena DOS ini akan menghabiskan *resources* memori maupun *bandwidth*, maka diperlukan analisa pada bagian *Network Traffic* (NT) untuk melihat berapa jumlah *bandwidth* yang dihabiskan oleh DOS dengan melakukan pengujian selama 1 menit, pengujian dengan penambahan jumlah *Attacker* yaitu : 1 *Attacker* dan 4 *Attacker* dengan snort aktif dan snort tidak aktif.

Tabel 4.1 Tabel Nilai *Resources Bandwidth* yang Terpakai

1 Attacker Percobaan ke-	Snort Aktif	Snort Tidak Aktif	4 Attacker Percobaan ke-	Snort Aktif	Snort Tidak Aktif
1	10.38	14.47	1	17.08	19.11
2	17.1	14.61	2	15.49	12.63
3	12.41	19.68	3	17.83	11.66
4	15.97	19.15	4	17.38	16.75
5	14.78	12.39	5	14.56	18.63
6	10.7	15.86	6	16.31	20.14
7	11.82	19.23	7	17.1	13.82
8	10.33	12.9	8	9.39	13.84
9	15.02	15.24	9	10.25	14.38
10	12.24	12.72	10	11.79	14.46
Rata-rata	13.075	15.625	Rata-rata	14.718	15.542

Berdasarkan data pada Tabel 4.2, nilai rata-rata besarnya *bandwidth* yang terpakai pada saat terjadi serangan dengan snort aktif dan snort tidak aktif. Pada skenario penyerangan 1 *Attacker*, saat snort tidak aktif, rata-rata nilai *bandwidth* yang terpakai sebesar 15.62 Mbps dan pada saat snort aktif, rata-rata nilai *bandwidth* yang terpakai sebesar 13,07. Pada skenario skenario penyerangan 4 *Attacker*, saat snort tidak aktif, rata-rata nilai *bandwidth* yang terpakai sebesar 15,54 Mbps dan pada saat snort aktif, rata-rata nilai *bandwidth* yang terpakai sebesar 14,71 Mbps.

Hanya sedikit perbedaan besar *bandwidth*, yang menandakan bahwa maksimum *bandwidth* yang terpakai pada percobaan dengan snort aktif sebesar 17,83 Mbps dan snort tidak aktif sebesar 20,14 Mbps dalam waktu 1 menit pada jaringan VM, maka tidak akan berdampak besar bagi kinerja *web server*.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan perancangan sistem yang telah direalisasikan, análisis untuk tugas akhir tentang sistem pertahanan HIPS Snort dapat ditarik kesimpulan sebagai berikut:

1. *Rule* yang telah dibuat dengan sistem pertahanan HIPS Snort mampu mengenali dan menahan serangan TCP SYN *flood*.
2. Dalam percobaan yang dilakukan sebanyak 30 kali, rata-rata serangan dengan 1 *Attacker* yang datang ke server dalam 30 detik sebanyak 1.134.817 paket dan dalam 1 menit sebanyak 2.202.602 paket. Dan rata-rata serangan dengan 4 *Attacker* yang datang ke server dalam 30 detik sebanyak 1.354.279 paket dan dalam 1 menit sebanyak 2.454.930 paket.
3. Dalam sistem HIPS Snort dengan *rule* yang telah dibuat, dapat menahan serangan dalam waktu 1 menit dengan 1 *Attacker* rata-rata presentase paket serangan yang di*drop* 97.98% dan dengan 4 *Attacker* 97.8 %.
4. Tidak terjadi perbedaan yang signifikan dari besarnya *bandwidth* yang terpakai antara serangan dengan 1 *Attacker* maksimum 19.68 Mbps dengan 4 *Attacker* 20.14 Mbps.
5. Maksimum kecepatan transfer data atau penggunaan internet dalam jaringan VM sekitar 20 Mbps.

5.2 Saran

Untuk pengembangan dari perancangan ini, terdapat beberapa saran agar dapat memperbaiki kekurangan yang ada :

1. Mengganti serangan dengan *Ping of Death* atau ICMP *flood* untuk membandingkan kekuatan serangan.
2. Penempatan sistem pertahanan Snort diletakkan di sisi router, agar terlihat perbandingan kinerja dari Snort.
3. Implementasi Snort IPS tidak dalam jaringan *virtual.*

DAFTAR PUSTAKA

[1] Wang Wei, The Hacker News, Inc August 21, 2017. [online] available : https://thehackernews.com/2017/08/sony-playstation-hacking.html. [Accessed November 20, 2017]

[2] Yuli Setiawan, PSMK KEMDIKBUD, Inc June 9, 2009. [online] available : https://psmk.kemdikbud.go.id/konten/985/ddos-attack-terbukti-masih-efektif-matikan-domain-name-system. [Accessed November 20, 2017]

[3] Samad S. Kolahi, Kiattikul T., Bahman Sarrafpour. " Analysis of UDP DDoS Flood Cyber Attack and Defense Mechanisms on Web Server with Linux Ubuntu 13" Communication, Signal Precessing, and Their Application (ICCSPA), February 2015

[4] Murat Caliskan, Mustafa Ozsiginan, Emin Kugu "Benefits of the Virtualization Technologies with Intrusion Detection and Prevention Systems" 2013 7th International Conference on Application of Information and Communication Technologies, January 2014

[5] J.D.Ndibwile, A. Govardhan, K.Okada, Y.Kadobayashi "Web Server Protection against Application Layer DDoS Attacks using Machine Learning and Traffic Authentication" IEEE Computer Software and Application Conference, September 2015

[6] Awatef Balobaid, Wedad Alawad and Hanan Aljasim. "A Study on the Impacts of Dos and DDoS Attacks on Cloud and Mitigation Techniques" International Conference on Computing, Analytics and Security Trends (CAST), December 2016

[7] Oksana Yevseiseiva, Seyed Milad Helalat. "Analysis of the Impact of the slow HTTP Dos and DDoS Attacks on the Cloud Environment" International Scientific-Practical Conference Problems of Infocommunication. Science and Technology (PIC S&T), October 2017

[8] S.V Athawale, D N Chaudari. "Towards Effective Client-Server Based Advent Intrusion Prevention System for WLAN" International Conference on Computer, Communication and Control (IC4)

[9] Final Task Telkom University "Implementasi dan Analisis Keamanan Jaringan Virtual dengan Layanan Web Server terhadap Serangan Layer 7 DOS dan DDOS". Available : http://openlibrary.telkomuniversity.ac.id/home/catalog/id/138653/slug/implementasi-dan-analisis-keamanan-jaringan-virtual-dengan-layanan-web-server-terhadap-serangan-layer-7-dos-dan-ddos.html [Accessed September, 2017]

[10] Information Sciences Institute, Univer of Southern California "Transmission Control Protocol". September 1981. https://www.ietf.org/rfc/rfc793.txt [Accessed June 26, 2018]

[11] S.T.Zargar, J.Joshi, and D.Tripper, member, IEEE "A Survey of Defense Mechanisms Against Distributed Denial of Service(DDoS) Flooding Attacks" December 28, 2012
[12] Raed M. Bani-Hanim, Zaid Al Ali, Jordan University od Science and Technology Dept. of Network Engineering and Security "SYN Flooding Attacks and Countermeasures: A Survey"
[13] Berbagi Catatan. Available : http://berbagicatatan.web.id/pengertian-ips-intrusion-prevention-system/. [Accessed October 29, 2017] [6] [10]
[14] Snort Manual. Available : https://snort.org/documents/snort-users-manual-html [Accessed June 26, 2018]
[15] http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html [Accessed August 26, 2018]
[16] http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node33.html [Accessed August 26, 2018]
[17] http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node35.html [Accessed August 26, 2018]
[18] Wireshark. Available : https://www.wireshark.org/ [Accessed June 26, 2018]
[19] Zabbix. Available : https://www.zabbix.com/about [Accessed June 26, 2018]