EFEKTIFITAS PENERAPAN IDS DAN IPS DALAM PENCEGAHAN FLOODING DATA (DDoS) TERHADAP SUMBER DAYA JARINGAN

Hafni[1], Dedy Syamsuar[2], Edi Surya Negara[3]

Program Magister Teknik Informatika
Universitas BinaDarma
[1]hafni19@yahoo.com,
[2,3]dedy_syamsuar@binadarma.ac.id, e.s.negara@binadarma.ac.id
[1]Jl. Perindustrian II KM9 No H-7, Palembang, 30124, Indonesia
[2,3]Jl. A.YaniNo.12,Palembang30624,Indonesia

Abstrak

Flooding (membanjiri) data pada sumber daya jaringan adalah hal mudah di lakukan oleh seorang yang ingin belajar hacker. Distributed Daniel of Service (DDoS) adalah salah satu cara untuk melakukan flooding data. Flooding data pada sumber daya jaringan dengan melakukan permintaan layanan webserver secara terus menerus, dalam jangka waktu tertentu yang akan menyebabkan server tidak bisa melayani permintaan normal. Sehingga akhirnya server yang melayani permintaan akan down. Salah satu tools yang digunakan untuk mencegah terjadinya flooding data adalah Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS). Paper ini akan melakukan penelitian tentang efektifitas IDS dan IPS dalam pencegahan flooding data dalam sebuah jaringan. Sehingga nantinya akan mendapat nilai yang jelas tentang efektifitas IDS dan IPS yang akan memberikan masukan kepada lembaga atau instansi yang akan menggunakan IDS dan IPS. Metode dalam penelitian ini adalah penelitian laboratorium yang dikondisikan mirip dengan jaringan data real yang ada pada instansi atau suatu organisasi. Pengujian dilakukan dengan simulasi serangan terhadap destination webserver yang telah di monitoring oleh IDS dan IPS. Jumlah presentasi pendeteksian seranganakan di hitung berdasarkan True Positive Alarm dan False Positive Alarm. Dalam penelitian ini akan diperoleh kesimpulan penggunakan IDS dan IPS dalam pencegahan flooding data.

Kata kunci: IDS dan IPS, Flooding Data, Network Security

1 PENDAHULUAN

Sistem Keamanan Komputer telah menjadi fokus utama dalam dunia Jaringan Komputer, hal ini disebabkan tingginya ancaman yang mencurigakan (suspicious threat) dan serangan dari Internet. Keamanan Komputer (Security) merupakan salah satu kunci yang dapat mempengaruhi tingkat Reliability (termasuk performance dan availability) suatu internetwork (Deris S., A. Hanan, M. Yazid, 2010, Negara, E.S. 2014, Negara, E.S.2016).

Salah satu ancaman keamanan komputer adalah serangan Distributed Daniel of Service (DDoS) memiliki trend peningkatan setiap tahun, dan ini merupakan ancaman untuk semua website yang ada, tidak tertutup kemungkinan target serangan tidak terfocus pada umumnya yang diketahui. Ini sangat mungkin terjadi karena mudah untuk dilakukan oleh orang awam sekalipun. Teknik yang dilakukan adalah dengan membanjiri jaringan destination dengan paket yang palsu, request layanan yang palsu dan tidak ada nya ontikasi sebelum mendapatkan layanan.

Konsep keamanan jaringan dimulai dengan authentication (otentikasi) yang artinya tindakan mengkonfirmasi kebenaran atribut dari suatu bagian data yang diklaim benar oleh entitas atau user (Negara, E.S 2016).

Pada umumnya menggunakan user ID dan password yang biasa disebut dengan otentikasi satu arah, namun otentikasi satu arah sangat mudah untuk dimanipulasi, untuk meningkatkan keamanan

otentikasi ini, maka diciptakan otentikasi dua arah, dan lebih cendrung aman, misalnya token untuk transaksi internet banking, atau dongle. Setelah dilakukan otentikasi, maka firewall akan meng-izin user tersebut untuk mendapatkan layanan-layanan dari server yang sesuai dengan otentikasi yang dilakukan.

Keamanan jaringan tidak hanya sebatas otentikasi, ini juga mencakup pengawasan terhadap apa saja yang boleh lewat pada jaringan tanpa otentikasi sama sekali, misalnya webserver; apakah semua pengunjung harus di otentikasi untuk bisa mengunjungi web? Tentu tidak. Disini ada celah keamanan jaringan yang harus menjadi perhatian lebih oleh administrator jaringan. Kenapa? Karena sangat mungkin seseorang akan melakukan manipulasi trafik dengan menyamar sebagai pengunjung yang sah dengan membawa flooding data yang banyak, sehingga server akan mengalami kerja extra untuk melakukan layan terhadap permintaan, dan jika permintaan layanan ini dilakukan secara terus menerus dalam jangka waktu yang lama dan dengan jumlah yang banyak, pada akhirnya server tidak akan bisa melayani permintaan dan server down (Negara, E.S., Rachman, B. and Lutfi, A., 2013.)

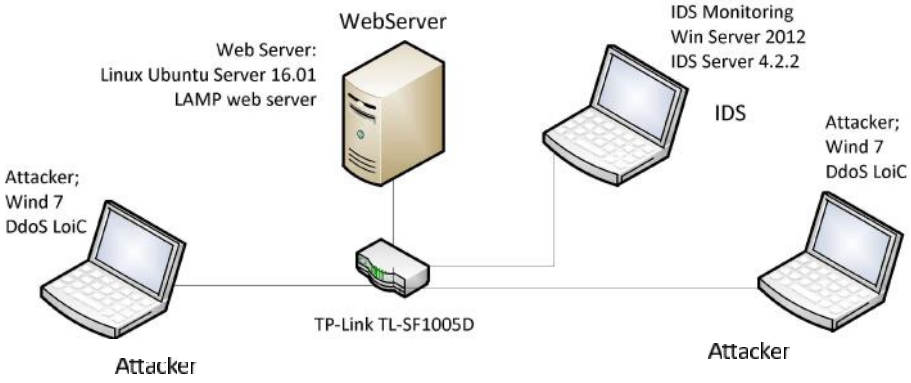
Disini diperlukan suatu alat untuk bisa memonitoring trafik jaringan yang di sebut dengan IDS dan IPS, namun seberapa effektif implementasi alat ini dalam mencegaha serangan DDoS yang akan terjadi diperlukan kajian yang lebih dalam untuk mendapatkan hasil yang akurat (Negara, E.S. 2014). Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) dapat menganalisa trafik data secara real time dan memiliki kemampuan untuk mendeteksi unormaly trafik data berdasarkan pendefenisian oleh administrator jaringan. Antara IDS dan IPS memiliki metode yang berbeda dalam mendeteksi unormaly trafik data pada jaringan. Dengan adanya IDS atau IPS akan bisa dilakukan efektifitas penerapan tool ini untuk menjaga serangan DDoS terhadap sumber daya jaringan, dan administrator jaringan bisa memonitoring secara real time dan mengambil pencegahan lebih lanjut.

2 METODOLOGI PENELITIAN

2.1. Desain dan Metode Penelitian

Pengumpulan data untuk mendapatkan data yang diperlukan sebagai bahan dasar dalam penelitian ini dilakukan dengan simulasi jaringan. Ini akan dilakukan di laboratorium jaringan lokal sehingga dapat melihat hasil yang jelas dalam pengumpulan data.

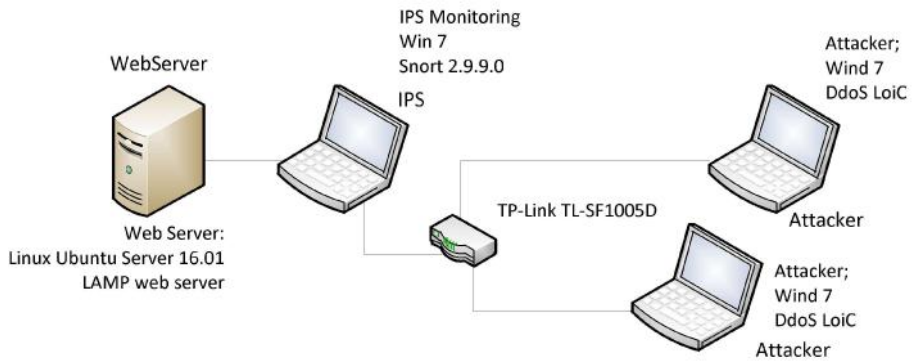
Untuk mendapakan data yang akurat dan jelas maka dibuat desain dari jaringan yang akan di jadikan sebagai simulasi percobaan, adapun topology jaringan yang akan dijadikan sebagai simulasi IDS adalah sebagai berikut:



Gambar1. Topology Jaringan Intrusion Detection System (IDS).

Pengecakan permintaan layanan HTTP yang tidak normal akan membutuhkan waktu, waktu di sini dibatasi berdasarkan besaran paket yang dikirim. Hal pengecekan anomaly paket ini memungkinkan serangan sedang terjadi namun proses pengecekan oleh tools IDS masih berlangsung sebelum memberikan alarm serangan. Implementasi ini dibutuhkan speed jaringan yang mendukung misalnya dengan kecepatan 1Gbps (CAT6e). Dari beberapa simulasi yang dilakukan pengujian ini bisa di install pada server itu sendiri, artinya tidak mengunakan device

tersendiri untuk melakukan monitoring. Untuk topologi pada pengujian IPS ada sedikit perubahan topologi yang tampak seperti gambar dibawah ini;



Gambar2. Topology Jaringan Intrusion Prevention System (IPS).

Pada tolopogi diatas terlihat dengan jelasperbedaan antara IDS dan IPS, Intrusion Detection System hanya mengcopy paket data yang lewat pada switch untuk di bandingkan dengan anomaly signature rule yang telah di buat di system IDS. Jika terjadi pembanjiaran data secara terus menerus dengan ukuran paket data yang tetap maka IPS akan mentriger alarm untuk peringatan bahwa ada penyusup yang masuk. Sedangkan untuk Intrusion Prevension System semua paket dilewatkan ke host dimana IPS terinstal, semua paket akan di anggap tidak normal, atau permintaan layanan yang dianggap tidak normal akan mentriger alarm, sehingga paket yang di tujukan ke target benar-benar tidak sampai atau di blok sebelum mencapai sasaran. Penelitian ini di lakukan dengan pengambilan data simulasi sebanyak serratus kali penyerangan dengan menggunakan sebuah pc sebagai penyerang seperti yang terlihat pada gambar di atas.

2.2. TeknikAnalisa Data

Setelah data dikumpulkan, maka akan dilakukan perhitungan persentasi antara data yang benar-benar terjadi serangan yang di deteksi oleh IDS maupun IPS dengan menggunakan rumus sebagai berikut:

$$TPR = TP/(TP+FN)*100\%$$
$$FPR = TP/(TP+FP)*100\%$$

$$\text{Effectiveness} = \frac{TP+TN}{TP + TN + FP + FN} . 100\%$$

Keterangan :
TPR = True Positive Rate (Alarm berbunyi saat ada serangan)
FPR = False Positive Rate (Alarm tidakber bunyi saat ada serangan)
TP = True Positive (Alarm berbunyi saat ada serangan)
FN = False Negative (Alarm tidak berbunyi saat serangan tidak ada)
FP = False Positive (Alarm tidak berbunyi saat ada serangan)

3. HASIL DAN PEMBAHASAN

3.1. Hasil Pengujian IDSdan IPS

Scenario pengujian di bagi menjadi dua bagian dasar; pertama dengan menggunakan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS), menyediakan layanan pada port 80 dengan layanan webserver seperti table services dibawah ini;

Tabel1. Service yang di ujicoba

Service	Server Characteristics	
	Server Ver	Comm port
HTTP	apache2	80
SMTP	smtpd	25
FTP	proftp	21

IDS server memonitoring trafik yang menuju webserver pada protocol HTTP dan IPS melakukan pengecekan packet data sebelum menuju webserver pada protocol yang sama HTTP.

A. True Positive Rate

Dari pengujian untuk mendapatkan nilai TPR, hampir lebih dari 80% serangan terdeteksi dengan baik oleh IPS Snort 2.9.9.0 dan IDS Server 4,2.

Tabel2. True Positive Rate

IDS/IPS	TPR	
	TP + FN	TP
Snort 2.9.9.0	32	27
IDS Server 4.2.2	32	22

B. False Positive Rate

Serangan sedang terjadi namun IDS dan IPS tidak mebunyikan alarm bernilai 20%, artinya dari 100 serangan yang terjadi hanya 20 serangan yang tidak terdeteksi oleh IDS dan IPS

Tabel3. False Positive Rate

IDS/IPS	FPR	
	TN+FP	TN
Snort 2.9.9.0	182	171
IDS Server 4.2.2	180	153

C. Effektifitas

Setelah melakukan perhitungan TPR dan FPR dalam rumus effectiveness maka di dapat table sebagai berikut;

Tabel 4. IDS dan IPS Effectiveness

IDS/IPS	TPR		FPR		Effectiveness (%)
	TP + FN	TP	TN+FP	TN	
Snort 2.9.9.0	32	27	182	171	97.71
IDS Server 4.2.2	32	22	180	153	82.56

4 KESIMPULAN

Untuk mendapatkan effektifitas IDS dan IPS lebih baik, maka akan dilakukan pengujian lebih dalam dengan jumlah serangan yang tidak hanya focus pada protocol HTTP. Namun untuk pengujian awal telah di dapatkan kesimpulan bahwa IDS dan IPS masih efektif dalam pencegahan flooding data pada sumber daya jaringan..

Daftar Pustaka

GARCIA-TEODORO, P., DIAZ-VERDEJO, J., MACIÁ-FERNÁNDEZ, G. & VÁZQUEZ, E. 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, 28, 18-28.

GONDOHANINDIJO, J. 2012. IPS (Intrusion Prevention System) Untuk Mencegah Tindak Penyusupan/Intrusi. Majalah Ilmiah INFORMATIKA, 3.

GUILLEN, E., PADILLA, D. & COLORADO, Y. Weaknesses and strengths analysis over network-based intrusion detection and prevention systems. 2009 IEEE Latin-American Conference on Communications, 2009. IEEE, 1-5.

LETOU, K., DEVI, D. & SINGH, Y. J. 2013. Host-based Intrusion Detection and Prevention System (HIDPS). International Journal of Computer Applications, 69.

Negara, E.S., 2014. Implementasi Management Network Security Pada Laboratorium CISCO Universitas Bina Darma. *Jurnal Ilmiah Matrik*, *16*(1), pp.11-20.

Edi, S.N., 2014. Optimasi End Users Awareness of Data and System Securities Using IT Audit Methodology and Tools. In *Seminar Nasional Teknologi Informasi dan Komunikasi (SNASTIKOM 2014)* (Vol. 2, pp. 269-274). Sekolah Tinggi Teknik Harapan (STTH) Medan.

Negara, E.S., Rachman, B. and Lutfi, A., 2013. Analysis and Design of Information Security Management System (ISMS) at Computer Network Infrastructure of Bina Darma University.

Negara, E.S., 2016. Network Layer.

Negara, E.S., 2016. Inroduction To Computer Network and Data Communitation.

Negara, E.S., 2016. Network Protocols and Communication.

VISUMATHI, J. & SHUNMUGANATHAN, K. 2010. An Efficient Intrusion Detection System using Computational Intelligence. National Journal of System and Information Technology, 3, 117.

.