INTRUSION PREVENTION SYSTEM PADA SERVER FAKULTAS TEKNIK UNIVERSITAS MATARAM

Intrusion Prevention System On Mataram University Server

Arief Taufikurrahman1[1], L.A. Syamsul Irfan Akbar2[1], IBK Widiartha3[2]

ABSTRAK

Pada era internet dan sistem informasi saat ini, isu keamanan menjadi hal sangat penting. Keamanan pada sisi server harus terjamin untuk menjaga aspek availability dari sebuah sistem informasi. Denial of Services (DOS) adalah salah satu jenis serangan yang sangat disukai untuk menghabiskan sumber daya pada jaringan ataupun server, sehingga pengguna yang sah tidak akan bisa mengakses server. Paper ini membahas rancang bangun Intrusion Prevention System (IPS) untuk mendeteksi dan mencegah serangan DDoS pada server. Sistem IPS yang dirancang terdiri dari Snort yang berfungsi untuk mengaudit lalu lintas data menuju server dan IPTable sebagai firewall.

Kata kunci *: Denial of Service, Snort, IPS.*

ABSTRACT

In the era of the Internet and information systems at this time, the issue of computer network security becomes very important. Security on the server side should be secured to keep the aspect of availability of an information system. Denial of Service (DOS) is one of the types of attacks that are favored to spend resources on the network or server, so that legitimate users can not access the server. This paper discusses the design of Intrusion Prevention System (IPS) to detect and prevent DDoS attacks on the server. IPS system designed consists of Snort that serves to audit the data traffic to the server and a firewall iptables.

Keywords : Denial of Service, Snort, IPS.

PENDAHULUAN

Dalam perkembangan teknologi informasi dan telekomunikasi, sistem jaringan komputer menjadi salah satu sistem yang memiliki peranan utama dalam mendistribusi-kan informasi dengan cepat dan efisien. Setiap sistem jaringan komputer harus memiliki kemampuan untuk menjaga ketersediaan layanannya serta menjaga keamanan dari informasi yang ada di dalamnya. Keamanan jaringan komputer merupakan bagian dari sistem jaringan komputer yang memiliki kemampuan untuk melindungi dan mencegah segala macam usaha penyerangan dan penyusupan oleh pihak yang tidak berhak terhadap sistem jaringan tersebut.

Sistem yang baik adalah sistem yang dapat mendeteksi serangan maupun penyusup di dalam sistem jaringan komputer. Tetapi tidak semua sistem dapat mengambil tindakan lanjut atau pencegahan terhadap aksi tersebut, dikarenakan sistem masih bergantung pada *administrator* jaringan dalam menanggulangi masalah. Sehingga hal tersebut sangat tidak efektif terutama saat *administrator* tidak melakukan monitoring lalu lintas data dalam jaringan. Oleh karena itu dibutuhkan suatu sistem yang dapat mendeteksi dan mencegah segala macam aktivitas yang mengancam keamanan jaringan komputer. Sistem ini diharapkan dapat bekerja secara otomatis sehingga memudahkan administrator dalam melakukan pemulihan layanan dengan cepat

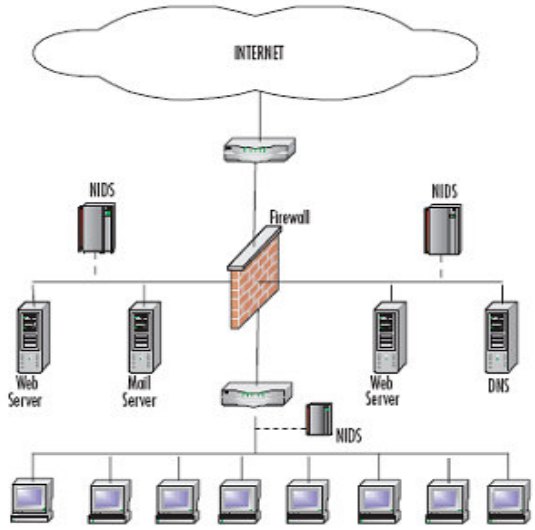
LANDASAN TEORI

IDS (*Intrusion Detection System*) (Arief MR) adalah sebuah sistem yang melakukan pengawasan terhadap lalu lintas jaringan dan pengawasan terhadap kegiatan – kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan yang mencurigakan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus, IDS juga merespon terhadap lalu lintas data yang tidak normal melalui aksi pemblokiran *user* ataupun alamat IP. Pada umumnya, terdapat dua jenis

[1]Jurusan Teknik Elektro, Fakultas Teknik Universitas Mataram, Nusa Tenggara Barat, Indonesia
[2]Jurusan Teknik Informatika, Fakultas Teknik Universitas Mataram, Nusa Tenggara Barat, Indonesia
arief@elektro08.com, [2]irfan@te.ftunram.ac.id, [3]widi@ti.ftunram.ac.id

IDS, yaitu *Network* IDS (NIDS) dan *Host* IDS (HIDS).

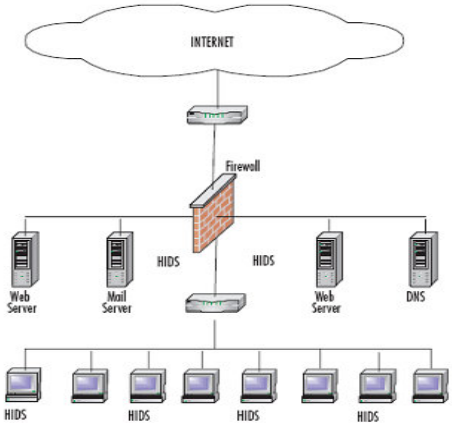
NIDS. NIDS (*Network Intrusion Detection System*) merupakan IDS mengawasi seluruh segmen jaringan dimana NIDS ditempatkan. NIDS menyadap seluruh komunikasi yang ada dijaringan tersebut, tanpa memilah-milah paket data yang lewat. Sebagai tambahan NIDS harus terhubung dengan *span port* di *switch* atau *network tap*. *Span port* dan *network tap* berfungsi untuk menduplikasi seluruh paket data yang lewat. NIDS harus ditempatkan pada posisi yang memungkinkan untuk bisa memonitor seluruh jaringan.



Gambar 1 Skema NIDS

HIDS. HIDS (*Host Intrusion Detection System*) merupakan IDS yang berjalan pada *host* yang berdiri sendiri dalam jaringan dan hanya melindungi sistem dimana HIDS tersebut berada, dan beroperasi tanpa memilih data yang lewat. Namun kelemahannya adalah kinerja CPU menjadi lebih tinggi dan membebani *host* karena HIDS tidak memilah data yang lewat. HIDS membuka semua tambahan informasi lokal dan mengaitkannya dengan keamanan, termasuk *system calls*, modifikasi *file system*, dan *system log*. Keuntungan lain dari HIDS adalah kemampuan untuk mengatur *rule* sangat baik bagi kebutuhan host.

IPS. IPS (*Intrusion Prevention System*) (Stiawan D) adalah pendekatan yang sering digunakan untuk membangun system keamanan komputer, IPS mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat serangan telah teridentifikasi, IPS akan menolak akses (*block*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak sepeti layaknya *Firewall* yang akan melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail.



Gambar 2 Skema HIDS

IPS menggunakan *signatures* untuk mendeteksi aktivitas dalam jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat di cegah sedini mung kin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal. Jadi *early detection* dan *prevention* menjadi penekanan pada IPS ini.

Snort. Snort IDS Verdian KH., (2010), merupakan IDS *open source* yang secara *defacto* menjadi standar IDS di industri. Snort dapat diimplementasikan dalam jaringan yang *multiplatform*, salah satu kelebihannya adalah mampu mengirimkan *alert* dari mesin Unix atupun Linux ke *platform* Microsoft Windows dengan melalui *Server Message Block* (SMB). Snort dapat bekerja dalam 3 modus : *sniffer mode* (penyadap), *packet logger* dan *network intrusion detection mode*. Modus kerja yang akan digunakan dalam membangun sistem pencegahan penyusupan adalah modus kerja *network intrusion detection*. Snort memiliki kemampuan untuk mengumpulkan *data log* seperti *alert* dan yg lainnya ke dalam *database*.

Snort diciptakan untuk menjadi IDS berbasiskan *open source* yang berkualitas tinggi. Snort di desain untuk dapat digabung

dengan *tools* yang sudah ada dan kemampuan ekspansi yang tinggi.

Serangan *Denial of Service* (*DoS Attack).* Serangan *Denial of Service* (DoS) (Dharma MAA), adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

Serangan – serangan lainnya akhirnya dikembangkan untuk mengeksploitasi kelemahan yang terdapat didalam sistem operasi layanan jaringan atau aplikasi untuk menjadikan sistem, layanan jaringan, atau aplikasi tersebut tidak dapat melayani pengguna, atau bahkan mengalami crash.

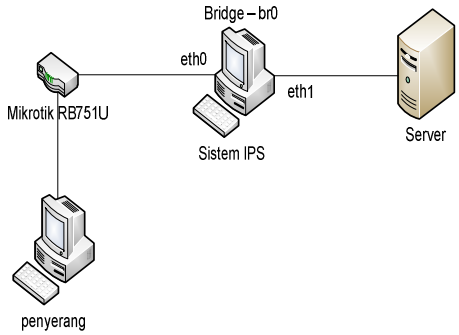
Low Orbit Ion Cannon. *Low Orbit Ion Cannon* (LOIC) merupakan *software* berbasis Windows yang digunakan untuk melakukan *Network Stressing* dan serangan DoS yang ditulis dalam bahasa C#. LOIC melakukan serangan DoS dengan membanjiri server target menggunakan paket TCP dan UDP dengan tujuan untuk mengganggu pelayanan dari server tersebut.

LOIC telah digunakan oleh aktifis dunia maya Anonymous untuk melancarkan serangan, berikut beberapa kasus dari serangan Anonymous yang terkenal dengan menggunakan LOIC :

- *Project Chanology* yang menyerang *website* dari The Church of Scientology pada tahun 2008.
- *Operation Payback* yang menyerang *website* dari Recording Industry Association of America pada tahun 2010.
- *Operation Deepthroat* yang menyerang *website* dari 9gag pada tahun 2011.
- *Operation Megaupload* yang menyerang *website* dari UMG yang merupakan perusahaan yang menggiring Megaupload ke pengadilan pada tahun 2012.

METODE PENELITIAN

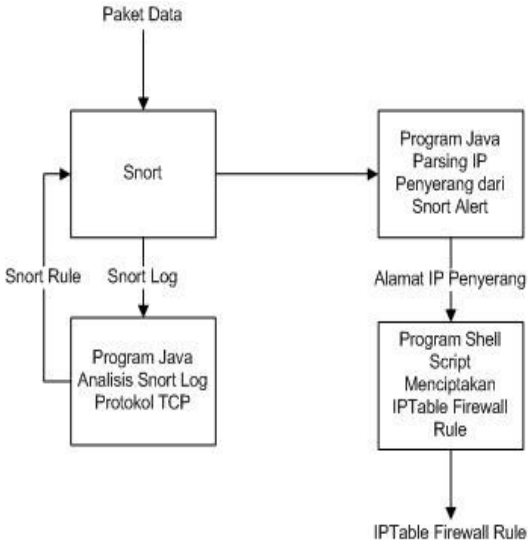
Rancangan Sistem. Pada penelitian ini, IPS dibangun pada jaringan lokal dengan menggunakan model *Network* IPS (NIPS). Berikut rancangan sistem yang akan digunakan :



Gambar 3 Rancangan IPS Pada Jaringan Lokal

IPS akan berada di depan server dan menghubungkan antara server dan *router* dengan menggunakan sistem *bridge*. IPS akan melakukan pemantuan terhadap lalu lintas paket data dengan melakukan *packet sniffing* pada sistem *bridge* sehingga dapat dianalisis oleh IPS. Apabila terdapat potensi serangan, IPS akan melakukan blok terhadap paket data tertentu sehingga paket data tersebut tidak menuju server.

Perangkat Lunak IPS. Perangkat lunak IPS akan disusun sebagai berikut :



Gambar 4 Blok Diagram Perangkat Lunak IPS

Berdasarkan blok diagram pada gambar 4, perangkat Lunak IPS terdiri dari empat program yaitu :

a. Snort

Snort bertidak sebagai *Intrusion Detection System* yang dimana akan melakukan *packet sniffing*, *packet printing*, menghasilkan *Snort alert* apabila terdapat potensi serangan berdasarkan *Snort rule*.

b. Program Java Analisis *Snort Log* Protokol TCP

Program ini dibuat dengan menggunakan bahasa pemrograman java dan berfungsi untuk menganalisis *Snort log* dan menciptakan *Snort rule* untuk protokol TCP.

c. Program Java Parsing Alamat IP Penyerang dari *Snort Alert*

Program ini dibuat dengan menggunakan bahasa pemrograman java dan berfungsi untuk melakukan parsing terhadap *Snort alert* untuk mendapatkan alamat IP dari penyerang yang kemudian akan disimpan ke dalam *file*.

d. Program *Shell Script* Untuk Menciptakan *IPTable Firewall Rule*

Program ini dibuat dengan menggunakan bahasa Shell Script dan berfungsi untuk membaca file yang berisi alamat IP penyerang dan menjadikan alamat IP tersebut sebagai acuan untuk menciptakan *IPTable Firewall rule*.

HASIL DAN PEMBAHASAN

Pengujian Program dan Snort Rule. Berikut hasil pengujian dari program dan Snort Rule pada ketiga protokol.

Protokol UDP. Berdasarkan hasil pengujian, simulasi serangan pada protokol UDP dapat dideteksi sebesar 100 persen dan hasilnya dapat dilihat pada tabel 1.

Tabel 1 Simulasi Serangan UDP Dengan Variasi Parameter Dari LOIC

No.	IP	Payload	Thread	Kecepatan Serangan (millisecond/ms)	Snort Alert
1.	192.168.1.20	serangan LOIC kedua	10	0.020 ms	YA
2.	192.168.1.20	serangan LOIC kedua	5	0.510 ms	YA
3.	192.168.1.20	serangan LOIC kedua	1	31.20 ms	YA
4.	192.168.1.40	menyerang UDP LOIC	1	0.020 ms	YA
5.	192.168.1.40	menyerang UDP LOIC	5	0.510 ms	YA
6.	192.168.1.40	menyerang UDP LOIC	10	31.20 ms	YA

Protokol TCP. Berdasarkan hasil pengujian, simulasi serangan pada protokol TCP dapat dideteksi sebesar 72.72 persen dan hasilnya dapat dilihat pada tabel 2.

Tabel 2 Simulasi Serangan UDP Dengan Variasi Parameter Dari LOIC

No.	IP	Payload	Thread	Kecepatan Serangan (millisecond/ms)	Snort Alert
1.	192.168.1.211	simulasi serangan Snort pada server	10	0.12 ms	YA
2.	192.168.1.212	simulasi serangan untuk server	5	10 ms	YA
3.	192.168.1.213	mencoba serangan diperuntukkan server	10	20 ms	YA
4.	192.168.1.214	mencoba seranganSnort pada server	5	10 ms	YA
5.	192.168.1.218	Mencoba serangan SNORT	1	0.12 ms	YA
6.	192.168.1.219	Mencoba serangan UNTUK server	5	20 ms	YA
7.	192.168.1.220	Mencoba serangan snort	10	0.12 ms	YA
8.	192.168.1.221	Mencoba serangan Untuk server	1	20 ms	YA
9.	192.168.1.215	simulasi serangan pada server	10	0.12 ms	TIDAK
10.	192.168.1.216	simulasi serangan pada server	5	10 ms	TIDAK
11.	192.168.1.217	simulasi serangan pada server	1	20 ms	TIDAK

Protokol HTTP. Berdasarkan hasil pengujian, simulasi serangan pada protokol UDP dapat dideteksi sebesar 100 persen dan hasilnya dapat dilihat pada tabel 3.

Tabel 3 Simulasi Serangan HTTP Dengan Variasi Parameter Dari LOIC

No.	IP	Thread	Kecepatan Serangan (millisecond/ms)	Snort Alert
1.	192.168.1.100	10	0.12 ms	YA
2.	192.168.1.110	5	10 ms	YA
3.	192.168.1.120	1	20 ms	YA
4.	192.168.1.130	1	0.12 ms	YA
5.	192.168.1.140	5	10 ms	YA
6.	192.168.1.150	10	20 ms	YA

Serangan yang dapat dideteksi akan menghasilkan Snort Alert yang kemudian akan dijadikan referensi untuk menciptakan IPTable Firewall Rule yang berfungsi untuk memberikan perintah terhadap *firewall* sehingga serangan dapat dicegah.

KESIMPULAN

Dari penelitian yang telah dilakukan, dapat ditarik kesimpulan sebagai berikut:

1. Topologi *Network Intrusion Prevetion System* (NIPS) dapat digunakan untuk melindungi server tanpa harus melakukan perubahan langsung terhadap server.
2. Serangan pada protokol UDP, TCP dan HTTP dapat dicegah oleh IPS dengan mengubah IPTable Firewall.
3. Paket data serangan pada protokol TCP dengan payload yang terstruktur dan tidak memiliki kata yang berulang – ulang tidak dapat dianalisis oleh program java sehingga tidak dianggap sebagai paket data serangan.
4. Paket data serangan pada protokol HTTP dengan payload yang memiliki struktur normal dan dikirim berulang – ulang tidak dapat dideteksi oleh IPS.

DAFTAR PUSTAKA

Arief MR., "*Penggunaan IDS (Intrusion Detection System) Untuk Pengamanan Jaringan Komputer"*, STMIK Amikom Yogyakarta, pp : 1-2.

Dharma MAA., "*Mekanisme Serangan DOS, DDOS & Cara Penanggulangannya"*, Universitas Siwijaya, pp : 7-10.

Dwiyanto P., Rahmana SR., Rahman A., 2009, "*Studi Kasus Perancangan Intrusion Prevention System Terhadap Serangan Man-In-The-Middle Pada Jaringan Lokal"*, Universitas Bina Nusantara, pp : 8-10, 48-56.

Susanto B., "*Protokol Transport (TCP/UDP)"*, Universitas Gunadharma, pp: 1, 3.

Stiawan D.," *Intrusion Prevention System (IPS) dan Tantangan Dalam Pengem-bangannya"*, Universitas Sriwijaya, pp : 1.

Verdian KH., 2010, *Perancangan Sistem Keamanan Jaringan Komputer Berbasis Snort Intrusion Detection System dan IPTables Firewall*, Universitas Sumatera Utara, pp : 10-14.