IMPLEMENTASI DAN ANALISA *INTRUSION DETECTION SYSTEM* DENGAN TOPOLOGI *DEMILITARIZED ZONE*

Bayu Arofatulloh 1310651001[1], Taufiq Timur Warisaji, S.Kom, M.Kom[2].

Program Sarjana
Bidang keahlian jaringan komputer Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Jember

Bayusaja123@gmail.com[1], Taufiqtimur@unmuhjember.ac.id[2],

ABSTRAK

Intrusion Detection System adalah salah satu cara untuk mengamankan jaringan, banyak *tools* yang bisa digunakan untuk membangun sebuah IDS. Salah satu *tools* IDS yang sering digunakan adalah snort sesuai dengan topologi jaringan yang dibangun. Dan topologi *Demilitarized Zone* (DMZ) bisa digunakan untuk mengamankan jaringan karena posisi DMZ berada diantara *firewall* dan jaringan *privat*. Snort bisa digunakan sebagai *tools* untuk membantu dalam mengenali *Intrusion Detection System* (IDS) dengan tujuan mengamankan jaringan, snort mampu mampu mendeteksi paket yang lewat langsung melalui *network* snort itu sendiri ataupun *network* yang berbeda dengan snort tersebut, contohnya pada topologi *Demilitarized Zone* IDS snort mampu mendeteksi paket yang diarahkan pada *Demilitarized Zone.* Topologi *Demilitarized Zone* dan IDS snort bisa digunakan untuk mengamankan jaringan dari serangan *DoS* ataupun *Port Scanning* karena IDS mampu mendeteksi serangan tersebut persentase tingkat akurasi *Intrusion Detection System* internal terdeteksi 100% untuk serangan *port scanning* dan *flood* port 21. Sedangkan tingkat akurasi *Intrusion Detection System* eksternal *port scanning* tingkat akurasi tertinggi yaitu 99,1 % dan untuk serangan *ping flood* akurasi tertingi hanya serangan *ping flood port 21* yaitu 50%.

Kata Kunci: keamanan jaringan, *Intrusion Detection System*, snort, *Demilitarized Zone.*

I. PENDAHULUAN

Seiring berkembangnya teknologi Informasi dan pemanfaatan komputer untuk kehidupan sehari-hari, hal tersebut dengan sendirinya menimbulkan sebuah permasalahan tersembunyi salah satunya keamanan jaringan. Inti dari keamanan jaringan komputer adalah untuk melindungi sumber daya informasi, perlindungan terhadap media penyimpanan dan aliran sumber informasi agar tidak terjadi kebocoran atau kerusakan informasi.

Masalah pada jaringan ataupun gangguan pada dasarnya dapat dibagi menjadi dua bagian, pertama adalah gangguan internal dan kedua adalah gangguan eksternal. Gangguan internal merupakan gangguan yang berasal dari dalam jaringan itu sendiri, baik dari infrasruktur jaringan internal tersebut, dalam hal ini adalah adanya pihak pihak yang mengetahui kondisi keamanan dan kelemahan dari jaringan tersebut. Gangguan eksternal adalah gangguan yang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin mengganggu keamanan yang ada pada jaringan tersebut. Proses ini bisa terjadi melalui jaringan yang diakses oleh pihak luar yang ingin melakukan gangguan ataupun pengerusakan terhadap jaringan tersebut.

Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, walaupun terkadang ada beberapa organisasi yang menempatkannya pada urutan yang ke sekian setelah hal lain. Namun ketika jaringan mendapat serangan dan terjadi kerusakan sistem, investasi yang dikeluarkan cukup besar untuk melakukan perbaikan sistem. Untuk itu sudah selayaknya investasi di bidang keamanan jaringan lebih diperhatikan, untuk mencegah kerusakan dari ancaman serangan yang saat ini semakin beragam serta semakin canggih. Terlebih lagi ketika jaringan lokal sudah terhubung ke internet maka ancaman serangan terhadap keamanan jaringan seiring semakin meningkat. Oleh karena itu, dibutuhkan suatu sistem untuk menganalisa gangguan atau ancaman yang akan terjadi secara optimal dalam waktu cepat dan otomatis yang hasil keluaran dari serangan tersebut dapat pula menampilkan dalam bentuk informasi. Bahkan keamanan jaringan yang membuat semakin banyaknya *tools* yang akan digunakan untuk mendeteksi bahkan dapat mengambil keputusan apabila terjadi serangan yang masuk ke dalam jaringan. **Snort** bisa digunakan sebagai *tools* untuk membantu dalam mengenali ***Intrusion Detection System* (IDS).** Dan kombinasi *Intrusion Detection System* dengan ***Demilitarized Zone* (DMZ)** bisa mejadi salah satu solusi karena dengan topologi DMZ, posisi DMZ sendiri terletak diantara suatu jaringan *privat* dan jaringan publik (internet).

II. TINJAUAN PUSTAKA

2.1 Jaringan Komputer

Menurut (Sofana, 2008). Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputerautonomous. Dalam bahasa yang dipopulerkan dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer dan perangakat lain (seperti printer, hub, dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel atau media tanpa kabel (nirkabel).

2.2 OSI Layer

OSI Model dibagi menjadi 7 Layer, dengan karakteristik dan fungsiya masing masing, meliputi *application, presentation, session, transport, network, datalink* dan *physical*. Tiap layer harus dapat berkomunikasi dengan layer di atasnya maupun dibawahnya secara langsung melalui sederetan protocol dan standar.

2.3 Pengertian IDS

Menurut (Kusumawati, 2010) *Intrusion Detection System* (IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan, jadi IDS atau Namun IDS ini tidak dapat melakukan tindakan atau pencegahan jika terjadi serangan atau penyusupan di dalam jaringan tersebut dan memang mempunyai kemampuan yang terbatas yang tergantung pada bagaimana melakukan konfigurasi IDS yang baik. IDS yang bermanfaat untuk mengatasi pencegahan terhadap suatu serangan atau penyusupan memang diperlukan suatu pemeliharaan yang mencukupi suatu sistem keamanan secara keseluruhan.

2.3.1 Jenis Sistem Deteksi Intruksi

Sistem deteksi intrusi, jika dari letak sensornya maka terbagi menjadi 3, yaitu Sistem Deteksi Intrusi Host Based, Sistem Deteksi Instrusi Network Based dan Sistem Deteksi Intrusi Application Based.

2.3.2 Jenis *Alert* pada Sistem Deteksi Intrusi

Alert pada sistem deteksi memiliki tingkatan tertentu untuk menunjukkan kevalidan suatu serangan yang ditujukan kepada suatu sistem jaringan komputer. Tingkatan-tingkatan tersebut adalah:

a. True positif
b. True negative

False positif

False negative

2.4 Pengertian Demilitarized Zone (DMZ)

Firewall DMZ atau jaringan *security boundary* yang terletak diantara suatu jaringan *privat* dan jaringan publik (internet). DMZ didefinisikan sebagai sebuah *host* komputer atau jaringan kecil yang dimasukkan kedalam sebuah zona netral diantara sebuah jaringan perusahaan *privat* dan jaringan publik. Konsep DMZ pada dasarnya mengaplikasikan konsep NAT (*Network Address Translation*) dan PAT (*Port Address Translation*). Trafik yang menuju DMZ bisa diizinkan atau ditolak, baik yang berasal dari internet ataupun jaringan *internal.* Lalu lintas data sepenuhnya diatur oleh firewall DMZ.

2.5 Snort

Snort merupakan software paket sniffer dan logger open source yang dibangun berdasarkan library libpcap, juga merupakan Sistem Deteksi Intrusi standar Unix's family baik dalam bentuk Sistem Deteksi Intrusi berbasis Host (HIDS) maupun Sistem Deteksi Intrusi berbasis Jaringan (NIDS), melingkupi *Snort Signatures, Snort Alerts, Snort Logs,* Komponen *Snort* (*Preprocessors, Packet Decoders, Detection Engine, Logging* dan *Alerting System),* dan Struktur *Rule Snort.*

2.6 Jenis Serangan

Menurut Ariyus (2007). Jenis dan serangan yang menggangu jaringan komputer beraneka macam. Serangan-serangan yang terjadi pada sistem komputer di antaranya adalah :

2.6.1. Port Scanning

Port Scanning merupakan suatu proses untuk mencari dan membuka *port* pada suatu jaringan komputer. Dari hasil *scanning* akan didapat letak kelemahan sistem tersebut. Pada dasarnya sistem *port scanning* mudah mendeteksi, tetapi penyerang akan menggunakan berbagai metode untuk menyembunyikan serangan. Penyerang akan mengirimkan paket lain pada *port* yang masih belum ada pada jaringan jaringan tersebut tetapi tidak terjadi respons apapun pada file *log*, kesalahan file atau *device* lainya.

2.6.2. Teknik Scanning

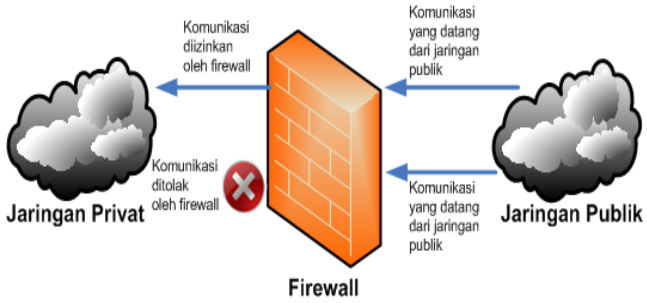
Teknik TCP SYN Scan dikenal sebagai half-opening scanning karena suatu koneksi penuh TCP tidak sampai terbentuk. Sebaliknya, suatu paket SYN dikirimkan ke port sasaran. Bila SYN/ACK diterima dari port sasaran, dapat diambil kesimpulan bahwa port itu berada dalam status listening.

2.6.3. DoS

Pada kondisi normal program utility ping digunakan untuk men-cek beberapa waktu yang dibutuhkan untuk mengirimkan sejumlah data dari suatu komputer ke komputer lain, dimana panjang maksimum paket data yang dapat dikirimkan menurut spesifikasi protokol IP adalah 65.536 byte. menunjukkan program utility ping dan alur serangan Ping of Death. Pada *Ping of Death* data yang dikirim melebihi maksimum paket yang di ijinkan menurut spesifikasi protokol IP. *Ping of Death* mengeksploitasi kelemahan didalam reassembly kembali fragmen paket IP.

2.7 Firewall

Firewall adalah suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman.



III. METODE PENELITIAN

IV. HASIL DAN PEMBAHASAN

4.1 Analisa Serangan IDS

Dalam menganalisa hasil IDS dilakukan 10 ujicoba sesuai dengan yang ada pada skenario uji pada BAB III diatas.

4.1.1 IDS *Port Scanning*

Tabel 4.2 *Daftar IP address dan DNS skenario uji Port Scanning internal*

IP address penyerang	10.101.101.151/24
IP address router yang di DMZ / Dst-NAT	10.20.31.29/29
IP address server uji coba	10.20.30.3/28
IP IDS (Snort)	10.20.30.5/28
Domain server	www.serverujicoba.com

Tabel 4.3 *Daftar IP address skenario uji Port Scanning external*

IP address penyerang	120.188.66.122
IP address router yang di DMZ / Dst-NAT	182.253.188.166/29
IP address server uji coba	10.20.30.3/28
IP IDS (Snort)	10.20.30.5/28

4.1.2 Tingkat Akurasi *Port Scanning* Internal

Hasil ujicoba melalui intenal dari 10 kali ujicoba serangan *port scanning* setiap kali serangan dibaca 100% mulai dari *port* 1 sampai 1023 yang di *scanning* oleh *port scanning* terdeteksi semua sesuai dengan jumlah *port scanning* yang dikirim.

$$\textbf{Akurasi } \textit{port scanning} = \frac{\sum \mathbf{n}}{\sum \mathbf{M}} \mathbf{x\ 100}\%$$

dimana :

$\sum M$ = Jumlah paket/scanning yang dikirim

$\sum n$ = Jumlah paket yang terdeteksi

dengan jumlah ujicoba sebanyak 10 ujicoba,

Jika data hasil ujicoba dimasukan ke dalam rumus tersebut maka akan menghasilkan tabel seperti dibawah ini:

Tabel 4.14 *Akurasi serangan port scanning internal*

Port Scanning Internal			
Ujicoba	**Dikirm**	**Terdeteksi**	**Akurasi**
1	1023	1023	100%
2	1023	1023	100%
3	1023	1023	100%
4	1023	1023	100%
5	1023	1023	100%
6	1023	1023	100%
7	1023	1023	100%
8	1023	1023	100%
9	1023	1023	100%
10	1023	1023	100%
Rata -Rata Akurasi			**100%**

Hitung rata-rata akurasi serangan *port scanning* internal

dengan cara:

$$\textbf{Rata – rata akurasi } \textit{port scanning} = \frac{\sum \textbf{Akurasi}}{\sum \textbf{Ujicoba}}$$

dimana:

$\sum$Akurasi = jumlah keseluruhan akurasi serangan *port scanning* internal

$\sum$Ujicoba = jumlah ujicoba

$$\text{Rata – rata akurasi serangan } \textit{port scanning} \text{ internal} = \frac{\sum \text{Akurasi}}{\sum \text{Ujicoba}}$$

$$\text{Rata – rata akurasi serangan } \textit{port scanning} \text{ internal} = \frac{1000\%}{10} = 100\%$$

Pada ujicoba IDS p*ort scanning* melalui jalur internal dan sesuai dengan cara kerja *port scanning* akan melakukan s*can* ke semua *Port-Port* alamat yang

dituju, dan di ujicoba pada penelitian ini ternyata ketika *port scanning* melakukan *scaning* dari 10 kali ujicoba yang dilakukan menghasilkan akurasi seperti tabel diatas.

4.1.3 Tingkat Akurasi *Port Scanning* Eksternal

Akurasi *port scanning* = $\frac{\sum \mathbf{n}}{\sum \mathbf{M}}$ **x 100%**

dimana :

$\sum M$ = Jumlah paket/scanning yang dikirim

$\sum n$ = Jumlah paket yang terdeteksi

dengan jumlah ujicoba sebanyak 10 ujicoba,

Jika data hasil ujicoba dimasukan ke dalam rumus tersebut maka akan menghasilkan tabel seperti dibawah ini :

Tabel 4.25 *Akurasi serangan port scanning internal*

Port Scanning External			
Ujicoba	**Dikirim**	**Terdeteksi**	**Akurasi**
1	1023	1016	99,3%
2	1023	1016	99,3%
3	1023	1016	99,3%
4	1023	1016	99,3%
5	1023	1016	99,3%
6	1023	1014	99,1%
7	1023	1016	99,3%
8	1023	1016	99,3%
9	1023	1007	98,4%
10	1023	1007	98,4%
Rata – Rata			**99,1%**

Hitung rata-rata akurasi serangan *port scanning* internal

dengan cara:

Rata – rata akurasi *port scanning* = $\frac{\sum \mathbf{Akurasi}}{\sum \mathbf{Ujicoba}}$

dimana:

∑Akurasi = jumlah keseluruhan akurasi serangan *port scanning* internal

∑Ujicoba = jumlah ujicoba

maka :

Rata – rata akurasi serangan *port scanning* internal = $\frac{\sum \text{Akurasi}}{\sum \text{Ujicoba}}$

Rata – rata akurasi serangan *port scanning* internal = $\frac{991\%}{10}$ = 99,1%

Pada ujicoba IDS p*ort scanning* melalui jalur eksternal dan sesuai dengan cara kerja *port scanning* akan melakukan s*can* ke semua *Port-Port* alamat yang dituju, dan di ujicoba pada penelitian ini ternyata ketika *port scanning* melakukan *scaning* dari 10 kali ujicoba yang dilakukan menghasilkan akurasi seperti tabel diatas.

4.2 IDS *Ping Flood*

Tabel 4.26 *Daftar alamat IP address skenario ping flood port 21,22,80 internal*

IP address penyerang	10.10.11.149/24
IP address router yang di DMZ / Dst-NAT	10.20.31.29/29
IP address server uji coba	10.20.30.3/28
IP IDS (Snort)	10.20.30.5/28

Tabel 4.27 *Daftar alamat IP address skenario ping flood port 21,22,80 eksternal*

IP address penyerang	120.188.64.57
IP address router yang di DMZ / Dst-NAT	182.253.188.166/29
IP address server uji coba	10.20.30.3/28
IP IDS (Snort)	10.20.30.5/28

4.2.1 Tingkat Akurasi *Ping Flood*

Untuk menghitung akurasi dari *Ping flood* sesuai dengan hasil ujicoba ke *port* yang dituju dengan melihat hasil dari jumlah nilai relevan (1) pada setiap ujicoba, dan dihitung tingkat akurasi dari serangan *ping flood* sesusi dengan *port* yang dituju dengan rumus sebagai berikut.

Akurasi persentase *ping flood* = $\frac{\sum \textbf{Nilai relevan}}{\sum \textbf{Ujicoba}} \textbf{x } 100\%$

dimana :

∑Nilai relevan = jumlah nilai relevan

∑Ujicoba = jumlah ujicoba

dengan jumlah ujicoba sebanyak 10 ujicoba,

maka :

1. Akurasi *ping flood port* 21 internal
   Akurasi= $\frac{a}{b}$ x 100% = $\frac{10}{10}$ x 100% = 100%
2. Akurasi *ping flood port* 22 internal
   Akurasi = $\frac{a}{b}$ x 100% = $\frac{9}{10}$ x 100% = 90%
3. Akurasi *ping flood port* 80 internal
   Akurasi= $\frac{a}{b}$ x 100% = $\frac{7}{10}$ x 100% = 70%
4. Akurasi *ping flood port* 21 eksternal
   Akurasi = $\frac{a}{b}$ x 100% = $\frac{5}{10}$ x 100% = 50%
5. Akurasi *ping flood port* 22 eksternal
   Akurasi= $\frac{a}{b}$ x 100% = $\frac{4}{10}$ x 100% = 40%
6. Akurasi *ping flood port* 80 eksternal
   Akurasi = $\frac{a}{b}$ x 100% = $\frac{1}{10}$ x 100% = 10%

4.3 Tingkat Akurasi IDS

Tabel 4.34 *Tingkat akurasi IDS internal*

No	Jumlah Ujicoba	Tipe Serangan	Terdeteksi	Akurasi IDS
1	10	Ping Flood port 21	10	100%
2	10	Ping Flood port 22	9	90%
3	10	Ping Flood port 80	7	70%

4	10	Port Scanning	10	100%

Tabel 4.35 *Tingkat akurasi IDS eksternal*

No	Jumlah Ujicoba	Tipe Serangan	Terdeteksi	Akurasi IDS
1	10	Ping Flood port 21	5	50%
2	10	Ping Flood port 22	4	40%
3	10	Ping Flood port 80	1	10%
4	10	Port Scanning	10	99,1%

V. KESIMPULAN

5.1. Kesimpulan

Berdasarkan hasil implementasi dan analisa *Intrusion Detection System* dapat disimpulkan :

1. *Intrusion Detection System* mampu mendeteksi serangan terhadap serangan *port scanning* dan *ping flood* sesuai dengan jumlah ujicoba yang dilakukan baik dari internal maupun eksternal dengan topologi *Demilitarized Zone.*
2. Tingkat akurasi *Intrusion Detection System* internal terdeteksi 100% untuk serangan *port scanning* dan *flood* port 21. Sedangkan tingkat akurasi *Intrusion Detection System* eksternal *port scanning* tingkat akurasi tertinggi yaitu 99,1 % dan untuk serangan *ping flood* akurasi tertingi hanya serangan *ping flood port 21* yaitu 50%.

5.2 Saran

Adapun saran yang diharapkan untuk membantu kesempurnaan *Intrusion Detection System* yang telah dibuat yaitu :

1. Menambah tipe serangan yang lain untuk mengukur akurasi IDS pada topologi DMZ.

2. Diharapkan untuk pengembang menambahkan rule eksekusi terhadap hasil deteksi dalam penelitian selanjutnya.

DAFTAR PUSTAKA

Ariyus, D. (2007). *Intrusion Detection System.* Andi Yogyakarta. Yogyakarta

Babatope, L.O., Babatunde, L., Ayobami, I., (2014). Strategic Sensor Placement for Intrusion Detection in Network-Based IDS. *International Journal of Intelligent Systems and Applications*, pp.61–68. Available at: http://www.mecspress.org/ijisa/ijisa-v6-n2/v6n2-8.html. (Diakses pada tanggal 6 januari 2016)

Harvianto, L.M., (2013), *Analisa dan Implementasi Intrusion Detection System Dengan Metode Misuse Detection-Based*. Program Studi Teknik Informatika Universitas Muhammadiyah Jember, Jember

Hakim, R. S., (2011), Verifikasi *Alert* Berdasarkan Klasifikasi Serangan Pada Deteksi Intrusi Kolaboration. Program D IV Jurusan Teknik Informatika Politeknik Elektronika Negeri Surabaya-Institut Teknologi Sepuluh Nopember, Surabaya

Kusumawati, M., (2010). *Implementasi IDS (Intrusion Detection System) serta Monitoring Jaringan dengan Interface Web Berbasis BASE pada Keamanan Jaringan*. Skripsi, Universitas Indonesia Jakarta, Jakarta

Nugroho. M. A., (2013), Makalah Osi Layer. www.scribd.com/ doc/ 231882916/ MAKALAH-OSI-LAYER-pdf. (Diakses pada tanggal 23 Juli 2016).

O.W. Purbo, (2003), *Ensiklopedia Serangan Denial of Service Attack*, infokomputer.com, hal. 1 – 3 (2003).

Prasadh H. T,. Jennifer, P (2015).” Network Security and Management Using HIDS”. International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 8, 2015.

Prasetya, I.N., Djanali, S., Husni, M., (2014) *Verifikasi Signatur Pada Kalaborasi Sistem Deteksi Intrusi Jaringan Tersebar dengan Honeypot*. Program Studi Teknik Informatika Institut Teknologi Sepuluh Nopember, Surabaya

Rusmanto dan Nuryadi.H., (2003). *Panduan Membangun Networking Berbasis Linux*. Penerbit Dian Rakyat. Jakarta. 2003

Sardana, A, Joshi, RC, (2008)”Autonomous Dynamic Honeypot Routing Mechanism for Mitigating DDoS Attacks in DMZ”,16th IEEE International Conference on ,New Delhi,2008.

Sofana, I., (2008) *Membangun Jaringan Komputer*. Informatika. Bandung.

Wagito. (2007). *Jaringan Komputer-Teori dan Implementasi Berbasis Linux*. Gava Media. Yogyakarta.

Wijaya, B., Rahadi, D.R. & Wijaya, A., (2014). Analisis dan Perancangan Keamanan
Jaringan Menggunakan Teknik Demilitarized Zone (DMZ). *Seminar Nasional*
Teknologi Informasi, Komunikasi dan Managemen, 1, pp.397–403.