ANALISIS KINERJA *ANOMALY-BASED INTRUSION DETECTION SYSTEM* (IDS) DALAM MENDETEKSI SERANGAN DOS (*DENIAL OF SERVICES*) PADA JARINGAN KOMPUTER

I Gusti Ngurah Arya Sucipta[1], I Made Widhi Wirawan [2], Agus Muliantara [3]
Program Studi Teknik Informatika, Jurusan Ilmu Komputer,
Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana

ABSTRAK

Sistem Deteksi Intrusi berdasarkan anomali adalah sistem keamanan jaringan yang berfungsi untuk mendeteksi adanya gangguan-gangguan pada jaringan komputer dengan cara mendeteksi gangguan-gangguan tersebut berdasarkan pola-pola anomali yang ditimbulkan. Serangan *Denial of Services* (DoS) adalah salah satu contoh jenis serangan yang dapat mengganggu infrastruktur dari jaringan komputer, serangan jenis ini memiliki suatu pola khas, dimana dalam setiap serangannya akan mengirimkan sejumlah paket data secara terus-menerus kepada target serangannya. Dengan menggunakan metode deteksi anomali, serangan DoS dapat dideteksi dengan mengidentifikasi pola-pola anomali yang ditimbulkan. Metode deteksi berdasarkan anomali memiliki tingkat kesalahan deteksi yang cukup besar, namun memiliki keunggulan untuk mendeteksi jenis-jenis pola serangan baru.

Sistem Deteksi Intrusi mempunyai kemampuan untuk menganalisa trafik jaringan dan mengenali adanya intrusi yang datang atau yang sedang terjadi dengan membangun *baseline* sebagai dasar untuk membedakan trafik normal dan abnormal. *Baseline* yang tepat sangat menentukan terhadap terdeteksinya suatu serangan, maka dari itu dalam penelitian ini fokus untuk meneliti Sistem Deteksi Intrusi berdasarkan anomali dinama informasi dari *baseline* dibangun berdasarkan karakteristik jaringan yang sebenarnya untuk dapat menentukan nilai *baseline* yang terbaik. Kinerja dari sistem telah diuji melalui simulasi serangan, dimana Sistem Deteksi Intrusi berdasarkan anomali memiliki tingkat akurasi sebesar 87,5 % untuk serangan DoS UDP Flood.

Kata Kunci : Anomali, *Threshold, Denial of Services*, Sistem Deteksi Intrusi

ABSTRACT

Anomaly-based Intrusion Detection System is a system of network security which functions to detect attacks on the computer networks based on the resultannt patterns of anomaly. Denial of Services (DoS) is one example of the kind of attacks that can disrupt the infrastructure of computer networks, this type of attack has a specific pattern, in which every attack it will send a number of packets continuously to the target. By using of anomaly detection method, DoS attacks can be detected by identifying the resultant anomaly patterns. The anomaly detection method may make big false alarm, but it has excellence to detect new types of attack patterns.

Intrusion Detection System have the capabilities to analyze network traffic and recognize incoming and on-going intrusion with build a baseline as a basis to determining normal and abnormal traffic. Determine the appropriate baseline is important to detect a attack activity, therefore on this paper focus to study anomaly-based Intrusion Detection System where the information of baseline is built from the actual characteristics of the network in order to determine the best baseline value. The performance of the system was tested through attacks simulation, it was shown that the anomaly-based Intrusion Detection System has a degree of accuracy, it was 87,5 % for UDP Flood DoS attacks.

***Keyword**: Anomaly, Threshold, Denial of Services, Intrusion Detection System*

1. Pendahuluan

Intrusion Detection System (IDS) adalah salah satu sistem yang dirancang sebagai bagian dari sistem keamanan jaringan komputer yang penting perananya dalam menjaga intergritas dan validitas serta memastikan ketersediaan layanan bagi seluruh pengguna. Serangan (Denial of Services) DoS merupakan suatu bentuk ancaman pada jaringan komputer yang dapat memanipulasi sumber daya (*resource*) yang dimiliki oleh komputer target sehingga tidak dapat menjalankan fungsinya dengan benar, serta secara tidak langsung akan mencegah pengguna legal lain untuk mendapatkan layanan dari komputer tersebut [3].

Anomaly-based IDS teknik yang digunakan untuk mendeteksi serangan adalah dengan memonitoring aktivitas jaringan dalam kurun waktu tertentu kemudian menetapkan suatu nilai batas (*threshold*) berdasarkan parameter tertentu yang selanjutnya akan menjadi dasar acuan (*baseline*) untuk mendeteksi serangan [1]. Adanya penyimpangan terhadap nilai *threshold baseline* dapat mengindikasikan terdapatnya aktivitas serangan yang dapat diklasifikasikan sebagai suatu anomali jaringan. *Anomaly-based* IDS efektif dalam mendeteksi pola serangan baru tetapi pada umumnya memiliki tingkat akurasi yang rendah serta tingginya tingkat *false positive* [5].

Dalam penelitian ini, peneliti fokus terhadap pendeteksian serangan DoS dengan menggunakan *Anomaly-based* IDS, dimana serangan sendiri akan disimulasikan pada kondisi trafik yang berbeda-beda. Pada penelitian ini trafik jaringan normal dan abnormal akan dilihat perbedaannya dari nilai *threshold* yang diperoleh, dimana nilai *threshold* ini diperoleh melalui proses pengukuran dan pengamatan serta diverifikasi sehingga nilai *threshold* yang diperoleh dapat secara tepat untuk dijadikan sebagai nilai *threshold* untuk dapat mendeteksi serangan DoS pada jaringan komputer.

2.Tinjauan Pustaka

2.1 *Anomaly-based* IDS

IDS atau sistem deteksi gangguan adalah proses pemantauan peristiwa yang terjadi dalam suatu sistem komputer atau jaringan dan menganalisis adanya kemungkinan tanda-tanda insiden, pelanggaran atau ancaman terhadap kebijakan keamanan komputer, kebijakan penggunaan legal, atau praktek-praktek standar keamanan. *Anomaly-based detection* adalah proses membandingkan suatu kondisi aktivitas yang dianggap normal terhadap kejadian yang diamati untuk mengidentifikasi adanya penyimpangan yang signifikan [4].

Mengenali sebuah anomali bisa dilakukan dengan cara analisis secara visual dengan melihat adanya anomali pada aliran trafik pada jaringan, tentunya dengan bantuan *software flow analysis* seperti Wireshark [1].

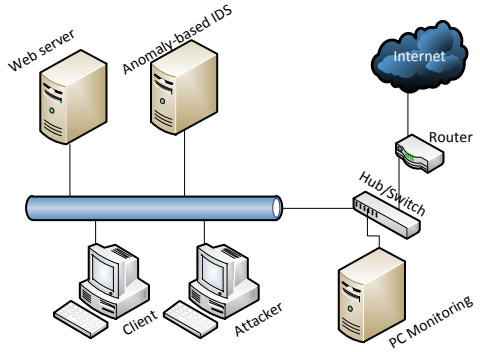
2.2 Membangun *Baseline*

Baseline adalah tindakan pengukuran dan penilaian kinerja dari jaringan berdasarkan kondisi *real-time*. Untuk membangun suatu *baseline* dibutuhkan adanya uji coba dan pelaporan dari konektifitas secara fisik, penggunaan jaringan yang normal, penggunaan protokol, puncak pengunaan jaringan dan rata-rata penggunaan *throughput* jaringan [8]. *Baseline* berisikan informasi mengenai *threshold*, dimana menentukan nilai *threshold* merupakan suatu keharusan untuk membantu sistem deteksi intrusi (IDS) dalam membuat suatu keputusan yang baik dalam mengidentifikasi atau mendeteksi adanya suatu serangan [10].

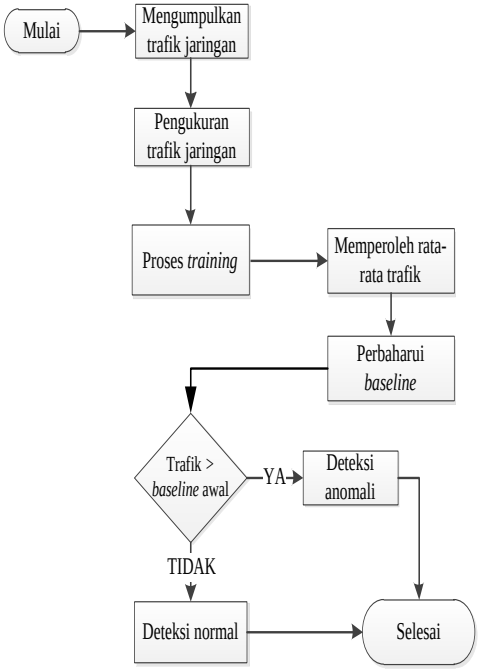
Nilai *threshold* bisa ditentukan dengan menggunakan statis atau dinamik *threshold*. Dinamik *threshold* membutuhkan suatu proses *training* atau catatan sejarah penggunaan trafik jaringan sebelum nilai dari *threshold* dapat ditentukan.

3. Desain Sistem *Anomaly-Based IDS*

Secara fisik desain [6] topologi jaringan penelitian ini menggunakan beberapa perangkat. *Router* berperanan sebagai *netflow generator*, yakni memonitor aktivitas lalu lintas trafik jaringan dan mengirimkannya kepada *netflow collector* melalui protokol Netflow [2]. Terdapat perangkat PC sebagai *server* dan sebagai PC monitoring, dimana aktivitas jaringan akan dipantau dengan *software* Cacti dan *web server* sebagai target serangan.



Gambar 1. Desain Topologi Jaringan



Gambar 2. Flowchart *anomaly detection*

Alur proses pendeteksian serangan DoS berdasarkan deteksi anomali pada aliran trafik jaringan ditunjukkan pada gambar 2. Adapun penjelasan dari tahapan proses deteksi anomali adalah sebagai berikut:

1. Proses awal adalah sistem akan menangkap dan mencatat setiap komunikasi data yang keluar ataupun masuk dari setiap *host* yang ada dalam jaringan.
2. Setiap informasi yang diperoleh akan akan dilakukan perhitungan untuk mendapatkan informasi pemakaian rata-rata seperti informasi trafik, aliran data, serta *bandwidth* yang terjadi selama rentang waktu periode *training*.
3. Jika dalam pengukuran trafik dilakukan dalam periode *traning* maka informasi rata-rata trafik yang diperoleh akan memperbaharui informasi trafik yang sudah ada untuk selanjutnya digunakan sebagai informasi dari *baseline*. *Baseline* sendiri berisikan informasi seperti rata-rata data bytes tiap detik, paket tiap detik, total aliran data dan total bytes yang diambil dalam interval jam, hari maupun minggu. Namun jika pengukuran trafik dilakukan bukan pada saat periode training, maka informasi yang diperoleh pada pengukuran ini akan dibandingkan dengan informasi *baseline* yang telah ada sebagai acuan dalam mendeteksi terdapatnya anomali pada jaringan.
4. Jika pada saat pengukuran trafik jaringan terjadi bukan pada periode *training*, maka apabila terdapat informasi trafik yang melebihi dari informasi yang telah ditetapkan sebagai *baseline* maka sistem akan melaporkan terdapatnya anomali pada jaringan, jika informasi yang diukur tidak melanggar dari *baseline* yang telah ditetapkan sebelumnya maka sistem akan melaporkan sebagai keadaan normal.
5. Dalam setiap tahapan *training periode* informasi *baseline* yang sudah ada akan terus diperbaharui dengan informasi baru. Proses mendapatkan nilai *baseline* adalah proses yang berkelanjutan dimana jika suatu nilai *baseline* belum mampu untuk mendeteksi adanya anomali, maka akan dilakukan proses *training*

Baseline	***Parameter***		
	Avg packets (/s)	Avg traffic (kb/s)	Avg flows (/s)
Baseline 1	86,2	398	10,2
Baseline 2	4,7	14,4	2,4
Baseline 3	148,2	546	30,2

kembali berdasarkan dari karakteristik trafik yang dimiliki jaringan untuk mendapatkan nilai *baseline* yang tepat.

3.1. Desain Pengujian Sistem

Dalam pengujian ini akan dievaluasi berdasarkan pada tingkat akurasi deteksi terhadap serangan dan tingkat kesalahan deteksi [9]. Akurasi didefinisikan sebagai persentase dari aliran trafik serangan yang secara benar diklasifikasikan sebagai serangan DoS [3] dibandingkan dengan jumlah total serangan, sedangkan kesalahan deteksi dapat diartikan sebagai kesalahan sistem dalam memberikan tanda peringatan atau tidak terhadap suatu kondisi yang sedang diamati. Nilai akurasi akan diperoleh dengan melakukan pengujian serangan DoS pada sistem, kemudian membandingkan total serangan yang terdeksi dengan total jumlah serangan yang uji cobakan. Sedangkan untuk nilai kesalahan deteksi diperoleh dengan menganalisis data *log* dari sistem dan membandingkan data antara total kejadian yang salah terdeteksi dengan total serangan [7].

$$\textbf{Rerata Akurasi} = \frac{\text{Total serangan terdeteksi}}{\text{Total serangan}} \times 100\%$$

$$\textbf{Kesalahan deteksi} = \frac{\text{Total kejadian salah terdeteksi}}{\text{Total serangan}} \times 100\%$$

4. Pengujian

Dari proses *training* yang dilakukan diperolehlah informasi yang akan dijadikan sebagai *baseline*

Tabel 1. Informasi *baseline*

4.1 Pengujian Pertama

Tes	Aktivitas	Durasi (menit)	Attack packet (KB)	Avg Background Packets (p/s)	Avg Attack Packets (p/s)	Anomaly IDS	Status
1	Serangan	10	4	69,7	129.7	Terdeteksi	Benar
2	Serangan	15	8	109	562,1	Terdeteksi	Benar
3	Serangan	15	3	42	122,3	Terdeteksi	Benar
4	Serangan	10	2	58	80,2	Tidak Terdeteksi	Salah
5	Bukan Serangan	10	0	40.9	0	Tidak Terdeteksi	Benar
6	Bukan Serangan	15	0	121	0	Terdeteksi	Salah
7	Bukan Serangan	10	0	89	0	Terdeteksi	Salah
8	Bukan Serangan	15	0	32	0	Tidak Terdeteksi	Benar

Tabel 2. Pengujian pertama

Pada pengujian kesalahan deteksi, pada *Anomaly* IDS dengan *baseline* yang ditetapkan, untuk aktivitas bukan serangan dalam hal ini disimulasikan dengan sharing file, sistem mendeteksi aktivitas tersebut sebagai serangan, dimana secara keseluruhan dari pengujian pertama terdapat 2 aktivitas bukan serangan namun terdeteksi sebagai serangan.

4.2 Pengujian Kedua

Tes	Aktivitas	Durasi (menit)	Attack packet (KB)	Avg Background Packets (p/s)	Avg Attack Packets (p/s)	Anomaly IDS	Status
1	Serangan	10	4	5	70	Terdeteksi	Benar
2	Serangan	15	8	10,2	135	Terdeteksi	Benar
3	Serangan	10	3	2	94,6	Terdeteksi	Benar
4	Serangan	10	2	67	189,8	Terdeteksi	Benar
5	Bukan Serangan	10	0	11,8	0	Terdeteksi	Salah
6	Bukan Serangan	10	0	15	0	Terdeteksi	Salah
7	Bukan Serangan	15	0	102	0	Terdeteksi	Salah
8	Bukan Serangan	15	0	89	0	Terdeteksi	Salah

Tabel 3. Pengujian kedua

Pada pengujian yang kedua, dengan informasi dari *baseline* yang di perbaharui melalui proses *training* kedua untuk karakteristik dari serangan yang diberikan tidak jauh berbeda dengan pada saat pengujian pertama. Pada pengujian dengan aktivitas serangan, *Anomaly* IDS berhasil mendeteksi setiap serangan yang diberikan.

4.1 Pengujian ketiga

Tes	Aktivitas	Durasi (menit)	Attack packet (KB)	Avg Background Packets (p/s)	Avg Attack Packets (p/s)	Anomaly IDS	Status
1	Serangan	10	4	79,7	329.7	Terdeteksi	Benar
2	Serangan	10	8	323	262,1	Terdeteksi	Benar
3	Serangan	15	3	98,4	162,3	Terdeteksi	Benar
4	Serangan	15	6	102,2	479	Terdeteksi	Benar
5	Bukan Serangan	10	0	107	0	Tidak Terdeteksi	Benar
6	Bukan Serangan	10	0	90	0	Tidak Terdeteksi	Benar
7	Bukan Serangan	10	0	115	0	Tidak Terdeteksi	Benar
8	Bukan Serangan	15	0	168,3	0	Terdeteksi	Salah

Tabel 4. Pengujian ketiga

Pada pengujian ketiga, pada pengujian deteksi serangan, untuk *anomaly* IDS mampu mendeteksi total 4 dari 4 jumlah upaya serangan yang diberikan dalam jaringan. Karakteristik serangan sendiri tidak berbeda dengan karakteristik serangan pada pengujian sebelumnya, namun pada saat pengujian ketiga ini dilakukan *background traffic* yang terdapat pada jaringan lebih ramai jika dibandingkan pada pengujian sebelumnya, adanya *background traffic* yang cukup besar ini mempengaruhi tingkat kesalahan deteksi dari *Anomaly* IDS, hal ini terlihat dari adanya aktivitas bukan serangan terdeteksi serangan, dikarenakan trafik yang ditimbulkan relatif besar.

Berdasarkan pengukuran tingkat akurasi *Anomaly-based* dalam mendeteksi serangan DoS UDP Flood, memperoleh persentase akurasi 87,5 %.

5. Kesimpulan

Dari penelitian yang telah dilakukan, maka beberapa kesimpulan yang dapat ditarik adalah:

1. Berdasarkan pada pengujian dengan simulasi serangan, *Anomaly-based* IDS dengan informasi *baseline* yang dinamis dari 3 kali proses pembentukan *baseline* yang dilakukan, informasi pada *baseline* ketiga yang paling memiliki tingkat akurasi paling tinggi untuk serangan DoS UDP Flood yakni sebesar 87,5 %.
2. Masih terdapatnya tingkat kesalahan deteksi yang cukup tinggi pada *Anomaly-based* IDS, disebabkan oleh informasi suatu *baseline* yang dibangun tidak selalu memberikan hasil yang terbaik pada saat digunakan dalam kondisi jaringan yang berbeda-beda, hal ini dapat dilihat dari tingkat kesalahan deteksi dari *baseline* 1 dan *baseline* 2 yakni 25% dan 50%.

Daftar Pustaka

[1] Barford, P., & Plonka, D. (2006). Characteristics of Network Traffic Flow Anomalies. *ACM SIGCOMM Internet Measurement Workshop*.

[2] Ding, J. (2009). *Advances in Network Management.* USA: Taylor & Francis Group.

[3] Douligeris, C., & Serpanos, D. N. (2007). *Network security: current status and future directions.* Canada: John Wiley & Son Sons inc.

[4] Flickenger, R., & Team. (2007). *Wireless Networking in the Developing World Second Edition.* England: wsfii organization.

[5] Jain, P., & Shrivastava, S. K. (2011). Effective Anomaly based Intrusion Detection using Rough Set Theory and Support Vector Machine. *International Journal of Computer Applications Volume 18*.

[6] Jogiyanto, H. (2008). *Metodologi Penelitian Sistem Informasi.* Yogyakarta: ANDI.

[7] Pukkawanna, S., & dkk. (2007). Lightweight Detection of DoS Attack. *In Proc. of IEEE ICON2007*.

[8] Scarfone, K., & Mell, P. (2010). Guide to Intrusion Detection and Prevention Systems (IDPS). *Computer Security Resource Center (National Institute of Standards and Technology)*.

[9] Siris, V. A., & Papaglou, F. (2006). Application of anomaly detection algorithms for detecting SYN Flooding Attacks. *Journal Computer Communications Volume 29 Issue 9*.

[10] Stamford, S. P. (2002). How to Own the Internet in Your Spare Time. *In*

Proceeding of USENIX Security Symposium.