Jurnal Ilmu Komputer & Agri-Informatika

Tersedia secara *online* di:
http://journal.ipb.ac.id/index.

Volume 8 Nomor 2 halaman 90 – 94
e ISSN: 2654-9735, p ISSN: 2089-6026

Analisis Kinerja *Intrusion Detection System* pada Deteksi Anomali dengan Metode *Decision Tree* Terhadap Serangan Siber

Analysis of Intrusion Detection System Performance on Anomaly Detection with Decision Tree Method Against Cyber Attacks

MUAMMAR FADHLURROHMAN[1]*, ANITA MULIAWATI[1], BAYU HANANTO[1]

Abstrak

Intrusion Detection System (IDS) merupakan sebuah sistem yang melakukan pengawasan terhadap *lalu lintas* jaringan dan terhadap kegiatan-kegiatan yang mencurigakan atau yang membahayakan di dalam sistem jaringan. Salah satu teknik pendeteksian IDS adalah deteksi anomali. Teknik ini melibatkan pola lalu lintas sebuah serangan yang sedang dilakukan oleh penyerang dengan membandingkan kegiatan yang sedang dipantau dengan kegiatan normal untuk mendeteksi adanya sebuah kejanggalan. Berdasarkan hasil penelitian, *IDS yang dikembangkan* dapat mendeteksi 72 dari 175 serangan. Hal itu dikarenakan pendeteksian anomali memerlukan perubahan *lalu lintas* yang sangat signifikan pada saat aktivitas normal dengan aktivitas saat terjadinya serangan, sehingga *IDS* menganggap adanya sebuah anomali pada jaringan tersebut dan dapat mendeteksi adanya sebuah percobaan serangan.

Kata Kunci**:** *Intrusion Detection System, Anomali, Keamanan Siber.*

Abstract

Intrusion detection system is a system that controls network traffic and suspicious or harmful activities in the network system. One of the IDS detection techniques is anomaly detection. This technique involves the traffic pattern of an attack being carried out by the attacker by comparing the activity being monitored with normal activities to detect any irregularities. Proposed IDS can detect 72 out of 175 attacks. That is because anomaly detection requires a very significant change in traffic during normal activity with activity during an attack, so IDS considers an anomaly on the network and can detect an attempted attack.

*Keywords**:** Intrusion Detection System, Anomaly, Cyber Security*.

PENDAHULUAN

Pada dunia digital saat ini, hampir semua orang menggunakan teknologi komputer yang terhubung dengan dunia internet. Dengan kemajuan teknologi internet saat ini kebutuhan serta pekerjaan dapat dengan mudah dikerjakan, semua informasi yang kita butuhkan dapat kita temui dengan internet menggunakan fitur "Google Search". Dengan kemajuan internet pula kita dapat berkomunikasi dengan siapapun dari jarak yang jauh sekalipun, atau kita bisa juga membagikan yang diinginkan.

Dengan perkembangan teknologi internet yang sangat pesat, ada pula orang yang tidak bertanggung jawab memanfaatkan hal tersebut untuk melakukan sebuah penyerangan untuk bisa masuk dalam sistem komputer sehingga mendapatkan data-data penting dan menjadi sebuah keuntungan bagi orang yang tidak bertanggung jawab. Contoh kejadian tersebut terjadi pada bulan Oktober tahun 2016. Videotron yang terpasang pada Kawasan Jakarta Selatan menayangkan sebuah video porno pada saat lalu lintas sedang ramai, sehingga pengendara yang melewati kawasan tersebut banyak yang berhenti dan mengakibatkan kehebohan pada kawasan tersebut (Pratomo 2016).

[1]Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta, Jakarta Selatan, 12450
*Penulis Korespondensi: Tel/Faks: 085718034265; Surel: Muammar@upnvj.ac.id

Intrusion detection system (IDS) dapat menjadi tambahan keamanan tanpa adanya manusia yang selalu berada di depan layer komputer. IDS dapat memberikan laporan mengenai tipe-tipe serangan yang sedang terjadi yang disimpan dalam sebuah log sehingga celah pada sistem yang harus diperbaiki atau diperkuat sistem keamanannya dapat diketahui. Berdasarkan penjelasan tersebut, penelitian ini dilakukan untuk mengetahui kinerja *IDS* yang menggunakan *decision tree* untuk mengidentifikasi pola apa yang menyebabkan *intrusion detection* tersebut dalam mendeteksi adanya serangan anomali.

METODE

Studi Literatur

Pada tahapan ini dipelajari hal-hal yang terkait dengan penelitian ini dari beberapa buku-buku, jurnal ataupun sumber resmi lainnya. Rujukan yang digunakan adalah beberapa penelitian yang sudah pernah dilakukan sebelumnya. Terdapat dua acuan utama dalam melakukan penelitian ini, yaitu perbandingan penggunaan sumber daya komputer pada Intrusion detection system dengan menggunakan metode *anomaly-based* dan *signature-based*. (Alviana dan Sumitra 2018) dan mengenai analisis keamanan jaringan IDS dengan cara memonitori *lalu lintas* pada server web sehingga dapat mengetahui jika ada penyusup yang memasuki server web (Stephani *et al.* 2020).

Perancangan Perangkat Lunak

Pada tahapan ini penulis merancang perangkat-perangkat yang akan digunakan pada penelitian ini. Perangkat keras yang digunakan berupa laptop Asus A442U dengan spesifikasi prosesor Intel(R) Core(TM) i5-8250U CPU @1.60 GHz – 1.80 GHz, RAM 12 GB, *harddisk* 1 TB, dan VGA NVIDIA. Sementara perangkat lunak yang digunakan dalam penelitian ini adalah Sistem Operasi Windows 10 Enterprise 64-Bit, Virtual Box versi 6.1.4 r 136177, Virtual Machine Ubuntu versi 20.10, Virtual Machine Kali linux versi 2020.3, Metasploit v5.0.100-dev, Suricata versi 6.0.2, dan Wireshark 3.0.7.

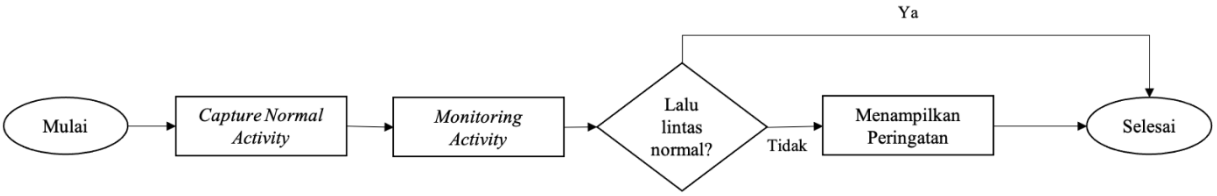
Melakukan Pengujian

Pada tahapan ini pengujian dilakukan pada sistem yang sudah dirancang (Gambar 1). Penelitian ini menguji deteksi anomali pada *IDS* dengan sebuah simulasi serangan dengan total 175 di 5 kategori serangan terhadap server. Pertama-tama *IDS* mencatat aktivitas normal pada server berupa *lalu lintas jaringan* serta jumlah paket yang terhubung pada jaringan. Aktivitas normal ini digunakan sebagai pembanding aktivitas normal dan aktivitas tidak normal. Setelah mencatat aktivitas normal, IDS memantau, memeriksa, dan membandingkan lalu lintas dengan lalu lintas normal yang sudah dicatat. Jika terdapat aktivitas yang berubah secara signifikan, IDS akan mendeteksi aktivitas tersebut sebagai serangan dan mengeluarkan peringatan pada log. Jika aktivitas yang dipantau normal, IDS anomali melewatkan aktivitas tersebut dan dianggap sebagai aktivitas normal (Alviana dan Sumitra 2018). Aktivitas yang dipantau dapat dilihat dengan menggunakan Wireshark. Setelah itu, data aktivitas tersebut dianalisis menggunakan *decision tree* untuk mengetahui kinerja deteksi anomali pada IDS.

HASIL DAN PEMBAHASAN

Hasil Pengujian Sistem

Berdasarkan dari Tabel 1, didapatkan bahwa dari 175 total pengujian hanya 72 dari semua serangan yang dapat dideteksi, oleh karena itu bahwa rata-rata akurasi yang didapat dari pengujian tersebut sebesar 41.14286% dari total pengujian.



Gambar 1 Pengujian Serangan *Intrusion Detection System* (Stephani *et al.*, 2020)

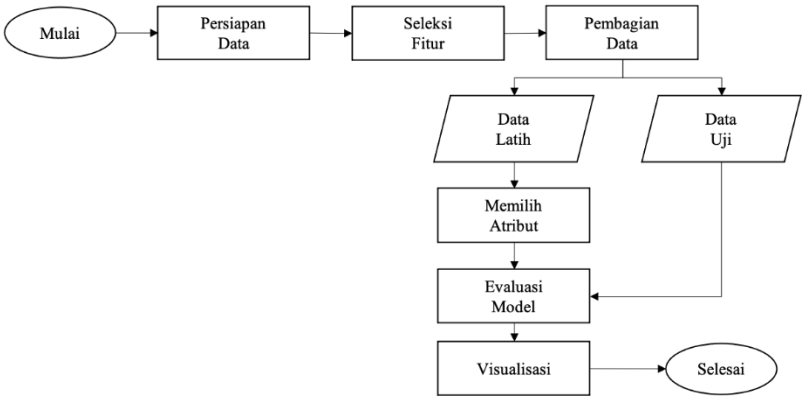
Tabel 1 Hasil Pengujian Serangan terhadap IDS

No	Jenis Serangan	Total Serangan	Total terdeteksi	Waktu terdeteksi (s)
1	Ping Flood	35	1	0,196799
2	SYN Flood	35	35	64,210000
3	FTP Brute Force	35	0	-
4	Malware	35	1	1,120000
5	HeavyTraffic	35	35	13,980152
	TOTAL	175	72	79,50695

Analisis Anomali *Intrusion Detection System* dengan Menggunakan *Decision Tree*

Pada tahap ini (Gambar 2) dilakukan analisis dengan membandingkan *lalu lintas* sebelum *dan* sesudah terjadinya serangan dengan menggunakan Wireshark dengan memerhatikan *lalu lintas jaringan*, paket yang diterima per detik, dan jumlah total paket sebelum dan sesudah terjadinya serangan. Dalam tahapan ini digunakan sebuah program dengan algoritma *Decision Tree* untuk memprediksi kinerja *intrusion detection system* dalam mendeteksi sebuah anomali.

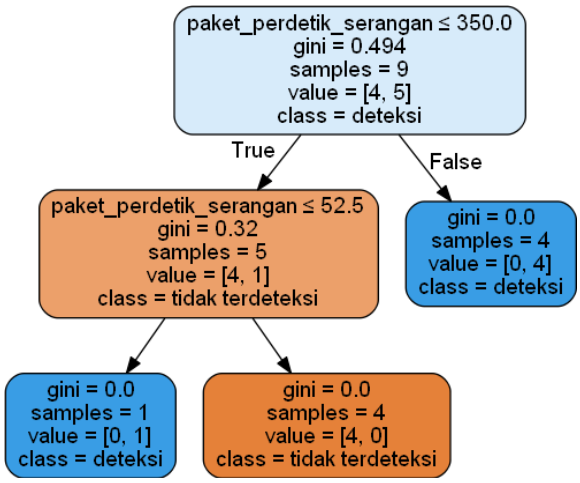
- **Persiapan Data***:* Pada penelitian ini, diambil 9 sampel (Tabel 2) dari serangan yang sudah dilakukan dari 5 kategori serangan, 9 data sampel ini diambil sebagai perwakilan lalu lintas dari kelima kategori serangan pada saat serangan yang dilakukan itu terdeteksi dan tidak terdeteksi oleh sistem IDS.
- **Seleksi Fitur***:* Setelah mengumpulkan data, data tersebut dibedakan menjadi 2 tipe, tipe pertama sebagai fitur yaitu: *jaringan* normal, *jaringan* serangan, jumlah paket normal, jumlah paket serangan, paket per detik normal, dan paket per detik serangan. Data tipe kedua yang digunakan sebagai sebagai kelas atau label yaitu: label.
- **Pembagian Data***:* Setelah menyeleksi fitur data, data kemudian dibagi menjadi data latih dan data uji dengan rasio 75% data latih dan 25% sebagai data uji untuk mengetahui performa algoritma yang sudah dilatih. Hasil dari pembagian data yaitu 6 sampel sebagai data latih dan 3 sampel sebagai data uji.
- **Memilih Atribut***:* Pada tahap ini, digunakan atribut *gini index* sebagai penentu node-node pohon keputusan dengan mencari nilai minimum pada nilai *gini index.*
- **Evaluasi Model***:* Evaluasi model pada penelitian ini yaitu dengan mencari akurasi prediksi decision tree pada data tersebut. Hasil akurasi model d*ecision tree* adalah 100%, dimana akurasi tersebut sudah bagus dalam melakukan pengujian.
- **Visualisasi***:* Visualisasi model yang sudah diuji dalam bentuk *decision tree* (Gambar 3).



Gambar 2 *Proses analisis anomali pada IDS.*

Tabel 2 Data Trafik yang didapat pada Wireshark

Network normal (kb/s)	Network serangan (kb/s)	Jumlah paket normal	Jumlah paket serangan	Paket perdetik normal	Paket perdetik serangan	Label
6	35	282	70500	50	600	Terdeteksi
7	10	175	691	50	100	Tidak terdeteksi
7	22	175	33054	50	1500	Terdeteksi
6	90	177	453	50	100	Tidak terdeteksi
7	60	164	367	40	100	Tidak terdeteksi
7	4500	164	3967	40	3000	Terdeteksi
8	1000	188	6733	19	6000	Terdeteksi
7	50	174	288	20	80	Tidak terdeteksi
8	7	156	330	20	25	Terdeteksi



Gambar 3 Visualisasi *decision tree*.

Berdasarkan *decision tree* pada Gambar 3, kita dapat simpulkan bahwa *IDS* akan menganggap adanya anomali jika paket_perdetik_serangan yang didapat melebihi 350 paket dari keadaan normal, jika kita analisa, pada paket_perdetik_serangan < 52.5 memiliki 5 sampel yang seharusnya dikategorikan sebagai kelas tidak terdeteksi, tetapi berdasarkan dari visualisasi tersebut, 1 dari 5 sampel tersebut dikategorikan sebagai kelas terdeteksi. Sampel inilah yang dapat dikategorikan sebagai *false positive*, yang seharusnya tidak terdeteksi berdasarkan pohon keputusan di atas, akan dideteksi oleh IDS sebagai suatu serangan.

SIMPULAN

Dalam mendeteksi sebuah anomali, *IDS* membandingkan sebuah traffic pada sebuah server dalam kondisi normal dengan kondisi saat terjadinya serangan. Jika perubahaan *lalu lintas* pada paket perdetiknya mencapai 350 paket, IDS akan menganggap itu sebagai anomali dan mendeteksi sebagai suatu serangan. *IDS* dapat meyebabkan *false alarm* sehingga IDS mendeteksi suatu lalu lintas yang bukan sekarang sebagai sebuah serangan.

DAFTAR PUSTAKA

Alviana S, Sumitra ID. 2018. Analisis pengukuran penggunaan sumber daya. *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*. 7(1):27-34.

Hartawan IB, Satwika IS. 2016. *Rancang Bangun Laboratorium Virtual Berbasis Cloud Computing di STMIK SITKOM Indonesia*. S@cies.

Lukman L, Suci M. 2020. Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache. *Respati*. Jul 10;15(2):6-15.

Nazwita N, Ramadhani S. 2017. Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata. Di dalam: Seminar Nasional Teknologi Informasi Komunikasi dan Industri, 19 Mei 2017. hlm 308-317.

Stephani E, Nova F, Asri E. 2020. Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server. *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*.1(2):67-74.