Analisis Komparatif Snort dan Suricata Sebagai *Signature-Based Intrusion Detection System*

Muhammad Hafizh Kamil
Departement of Information System
Telkom University
Bandung, Indonesia
hahzkamil@student.telkomuniversity.com

Rd. Rohmat Saedudin
Departement of Information System
Telkom University
Bandung, Indonesia
rdrohmad@telkomuniversity.ac.id

Mochamad Teguh Kurniawan
Departement of Information System
nama organisasi
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

Seiring meningkatnya ancaman siber seperti serangan Denial of Service (DoS), penerapan Intrusion Detection System (IDS) menjadi langkah strategis untuk menjaga stabilitas dan keamanan jaringan. Penelitian ini membahas perbandingan kinerja dua sistem deteksi intrusi berbasis signature, yaitu Snort dan Suricata, dalam mendeteksi serangan SYN Flood pada lingkungan jaringan simulasi. Metode yang digunakan dalam penelitian ini adalah PPDIOO, yang mencakup tahapan dari perencanaan hingga pengoperasian sistem. Lingkungan pengujian dibangun menggunakan GNS3 dan Virtual Machine dengan sistem operasi Ubuntu dan Kali Linux. IDS dikonfigurasi dengan aturan khusus untuk mendeteksi paket SYN dari protokol TCP, dan pengujian dilakukan sebanyak lima kali dengan durasi 30 detik tiap pengujiannya. Hasil evaluasi menunjukkan bahwa Snort memiliki tingkat akurasi rata-rata 72%, sementara Suricata berada pada 65%. Snort unggul dalam empat dari lima pengujian dan menunjukkan akurasi tertinggi sebesar 83%. Perbedaan performa ini menunjukkan bahwa Snort lebih unggul dalam hal konsistensi dan akurasi deteksi serangan dibandingkan Suricata. Penelitian ini diharapkan dapat menjadi referensi dalam memilih IDS yang tepat untuk kebutuhan jaringan organisasi.

***Kata kunci*— Keamanan Jaringan, IDS, LAN, Suricata, Snort, GNS3**

I. PENDAHULUAN

Di era digital yang semakin maju, ancaman siber juga terus meningkat. Keamanan jaringan menjadi aspek kritis sebuah organisasi. Serangan *Denial of Service* (DoS) menjadi salah satu ancaman siber tersebut. Berdasarkan laporan Cloudfare, ada 20,5 juta serangan DoS yang diblokir oleh Cloudfare pada kuartal pertama 2025 [1]. *Denial of Service* atau DoS ini dirancang untuk mengganggu atau bahkan menghentikan layanan jaringan dengan membanjiri sistem target menggunakan lalu lintas data dalam jumlah besar secara terus-menerus, sehingga menyebabkan server menjadi tidak responsif dan tidak dapat diakses oleh pengguna yang sah. [2].

Serangan DoS bukan hanya mengganggu kelangsungan operasional, tetapi juga dapat menimbulkan kerugian finansial dan reputasi yang signifikan. Maka dari itu, penting untuk mengambil langkah-langkah proaktif dalam melindungi jaringan mereka dari serangan siber yang berpotensi merugikan [3].

.

Salah satu solusi yang dapat diterapkan adalah penggunaan *Intrusion Detection System (IDS)*[4]. IDS adalah sistem yang dirancang untuk memonitor lalu lintas jaringan secara real-time dan mendeteksi aktivitas mencurigakan atau pelanggaran kebijakan keamanan [5]. Namun ada berbagai macam pilihan IDS yang sering digunakan seperti Snort dan Suricata, yang memiliki kelebihan dan kekurangan. Evaluasi semacam ini dapat membantu para pengelola jaringan dalam memilih solusi IDS yang paling sesuai dengan kebutuhan infrastruktur yang dimiliki.

Permasalahan yang mendasari penelitian ini berfokus pada bagaimana tingkat akurasi antara dua sistem *Intrusion Detection System* (IDS) berbasis signature, yaitu Snort dan Suricata, dalam mendeteksi serangan pada jaringan. Tujuan utama dari penelitian ini adalah untuk menganalisis akurasi pendeteksian antara Snort dan Suricata sebagai IDS. Dengan melakukan perbandingan performa kedua sistem, penelitian ini diharapkan dapat memberikan gambaran yang lebih jelas mengenai kemampuan masing-masing dalam mengidentifikasi serangan, khususnya serangan Denial of Service (DoS), pada lingkungan jaringan simulasi.

Penelitian ini memiliki beberapa batasan untuk menjaga fokus dan ruang lingkupnya tetap terkendali. Pertama, pengujian dilakukan dalam lingkungan jaringan simulasi, bukan pada jaringan nyata. Kedua, penelitian ini hanya membandingkan kemampuan deteksi dari Snort dan Suricata tanpa membahas fitur-fitur lain seperti logging atau integrasi sistem. Ketiga, pendekatan metodologi yang digunakan adalah siklus PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize), namun dalam penelitian ini hanya dilakukan hingga tahap Operate.

Penelitian ini diharapkan dapat memberikan beberapa manfaat. Bagi peneliti, hasil studi ini dapat menambah pemahaman mendalam mengenai performa Snort dan Suricata sebagai solusi IDS dalam konteks pengamanan jaringan. Bagi organisasi, penelitian ini dapat dijadikan sebagai referensi dalam menentukan pilihan perangkat IDS yang sesuai untuk kebutuhan pengamanan sistem jaringan dan sistem informasi. Selain itu, penelitian ini juga diharapkan dapat memberikan kontribusi pada literatur ilmiah yang membahas analisis kinerja perangkat lunak IDS dalam lingkungan jaringan

II. KAJIAN TEORI

A. *Intrusion Detection System* (IDS)

Intrusion detection system merupakan proses untuk memeriksa kejadian yang terjadi pada sebuah sistem komputer atau jaringan dan menganalisanya untuk mencari kemungkinan adanya insiden, yang di mana merupakan penyerangan atau ancaman terhadap keamanan komputer yang akan terjadi [6]. Proses ini diautomasikan yang nantinya akan dilaporkan kepada administrator keamanan [7].

B. Metode Pendeteksian IDS

Metode pendeteksian IDS yang sering digunakan yaitu *Signature Based* dan *Anomaly Based*. *Signature* merupakan sebuah pola yang dimiliki dari ancaman yang sudah diketahui. *Signature-based detection* merupakan sebuah sistem pendeteksian yang membandingkan pola ancaman yang dimiliki dengan kejadian yang diamati untuk mengidentifikasi kemungkinan insiden. Teknologi signature-based secara luas digunakan karena banyak serangan yang memiliki *signature* yang jelas dan berbeda-beda. Namun, metode ini memiliki kelemahan terhadap jenis serangan baru yang belum terdaftar dalam database dari signature yang digunakan. Maka dari itu pada metode ini diharuskan untuk terus dilakukan pembaruan secara berkala [7].

Anomaly-based detection merupakan metode pendeteksian yang bekerja dengan membandingkan aktivitas yang dianggap normal dengan kejadian yang diamati untuk mencari penyimpangan yang signifikan. IDS dibuatkan profil untuk memantau karakteristik dari aktivitas dalam sebuah periode waktu. Metode ini memiliki kelemahan di mana sistem dapat memberikan peringatan *false positive* (FP)

C. Serangan Siber

serangan siber merupakan tiap tindakan siber yang tidak sah yang bertujuan untuk melanggar kebijakan keamanan suatu aset siber dan menyebabkan kerusakan, gangguan, atau gangguan pada layanan atau akses terhadap informasi dari aset siber nasional tersebut [NO_PRINTED_FORM] [8].

III. METODE

Dalam penelitian ini, proses perancangan dan analisis menggunakan metode PPDIOO dengan lingkup penelitian yang dibatasi hingga tahap *Operate* saja. Untuk melakukan evaluasi terhadap implementasi sistem tersebut, dilakukan pengujian serangan pada sistem untuk memastikan apakah penelitian ini berhasil untuk menjawab permasalahan yang telah ditetapkan sebelumnya. Untuk dapat melakukan pengujian tersebut, peneliti akan melakukan serangan SYN Flood terhadap sistem. Parameter yang digunakan untuk melakukan evaluasi adalah membandingkan jumlah peringatan yang dikeluarkan oleh Snort dan Suricata dengan ekspektasi peringatan dari total paket yang terkirim

A. Spesifikasi Perangkat

Perangkat keras yang akan digunakan pada penelitian ini memiliki spesifikasi sebagai berikut:

TABEL 1
Spesifikasi Perangkat Keras

Komponen	Informasi	Spesifikasi
Perangkat Utama	*Processor*	AMD Ryzen 7 5800H with Radeon Graphics @3.20Ghz
	Memory	16384MB RAM
	SSD	954 GB
	System Type	64-bit operating system, x64-based processor
	Operating System	Windows 11 Home Single Language
Virtual Machine (Attacker)	*Processor*	4 Core
	Memory	2048MB RAM
	Disk	80GB
	System Type	64-bit operating system
	Operating System	Kali Linux
Virtual Machine (IDS)	*Processor*	2 core
	Memory	4096
	Disk	20GB
	System Type	64-bit
	Operating System	Ubuntu Linux

Perangkat lunak yang akan digunakan pada penelitian ini memiliki spesifikasi sebagai berikut:

TABEL 2
Spesifikasi Perangkat Lunak

Software	Versi
VMWare WorkStation	16.1.2
GNS3	2.2.54
Snort	2.9.20
Suricata	8.0.0

B. Serangan

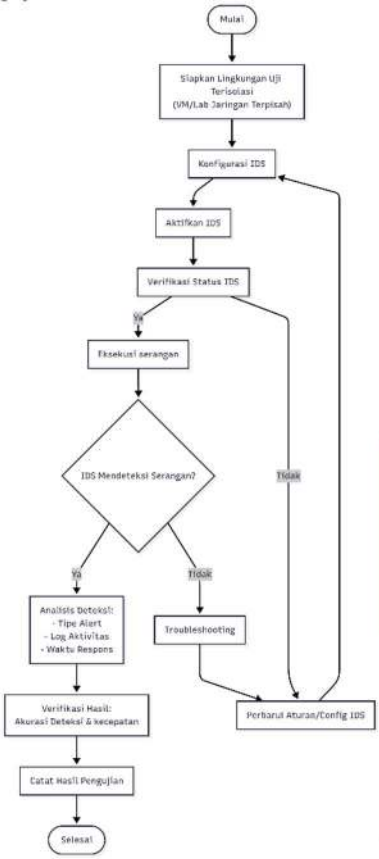
Serangan yang akan digunakan untuk menunjang penelitian ini adalah SYN Flooding attack. SYN Flood dipilih sebagai salah satu serangan Denial-of-Service (DoS) yang memanfaatkan kelemahan fundamental dalam protokol TCP three-way handshake. Penyerang membanjiri server dengan mengirimkan paket SYN yang harus dijawab server, hal ini dapat mempengaruhi sumber daya. Hping3 digunakan untuk melakukan SYN Flood attack. Untuk menjalankan SYN Flood dapat menggunakan perintah:

SYN flood attack

```
hping3 -S --flood -p 80 -V [ip tujuan]
```

Perintah “timeout” dengan parameter “30s” digunakan untuk membatasi waktu serangan dijalankan dalam 30 detik. Parameter “-S” yaitu *SYN Flag* yang digunakan sebagai pemilihan bahwa jenis koneksi yang digunakan adalah TCP. Parameter “-p 80” digunakan untuk menetapkan port yang akan diserang. Port 80 digunakan karena port 80 biasanya terbuka sebagai koneksi HTTP. Parameter “—flood” digunakan sebagai perintah untuk membanjiri ip tujuan dengan paket dan mengabaikan balasan ACK. Parameter “--rand-source” digunakan untuk menyamarkan sumber ip penyerang dengan mengacak ip sumber. Untuk melakukan analisis dilakukan uji serangan sebanyak 5 kali dengan waktu 30 detik di tiap pengujiannya

C. Alur pengujian

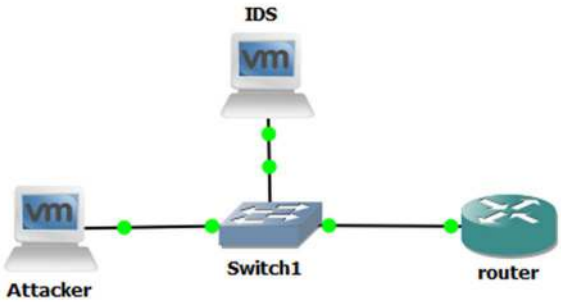


GAMBAR 1
Alur Pengujian

Alur pengujian ini merupakan rangkaian langkah implementasi IDS pada jaringan dan pengujian sistem dengan melakukan serangan.

D. Topologi

Di pengujian pada penelitian ini, digunakan sebuah topologi sederhana untuk mempermudah penelitian. Topologi dibuat pada perangkat lunak GNS3.



GAMBAR 2
Topologi pada GNS3

Pada topologi ini, digunakan satu router tersambung melalui 1 Switch ke IDS dan host penyerang. Penyerang menggunakan *Virtual Machine* Kali Linux dan IDS menggunakan *Virtual Machine* Ubuntu Linux.

E. Konfigurasi

Kedua IDS tersebut menggunakan aturan yang sama pada custom *local rule* yaitu:

```
alert tcp any any -> $HOME_NET any (msg:"SYN Flood
Attack"; flags: S; flow:stateless; detection_filter: track by_dst,
count 5, seconds 1; sid:1000025;)
```

"alert tcp any any" digunakan untuk peringatan serangan dengan protokol tcp dengan sumber dan port asal dari manapun. "-> $HOME_NET any" merupakan tujuan paket yang datang, yaitu variabel $HOME_NET yang berisikan IP yang dijaga oleh Suricata dan untuk port manapun. Kunci deteksi terletak pada dua bagian utama. Pertama, aturan mencari paket dengan *flag* SYN aktif (flags: S;), yang merupakan paket permintaan awal untuk membuka koneksi TCP (*Three-way Handshake*). Kedua, aturan menggunakan detection_filter (detection_filter: track by_dst, count 5, seconds 1;) untuk menentukan ambang batas serangan. Filter ini menghitung jumlah paket SYN yang menuju ke alamat IP tujuan yang sama (track by_dst). Jika dalam 1 detik terdapat 5 paket SYN atau lebih menuju satu alamat IP tujuan, maka kondisi ini dianggap sebagai indikasi serangan SYN Flood dan peringatan akan diaktifkan.

Penggunaan "flow:stateless;" menunjukkan bahwa aturan ini bekerja secara stateless, artinya Snort tidak perlu melacak status koneksi TCP yang lengkap. Ia cukup memeriksa karakteristik paket individual SYN dan menghitung frekuensinya ke satu tujuan. "Sid 1000025" adalah *identifier* unik untuk aturan ini dalam kumpulan aturan Snort agar dapat dengan mudah dibedakan. Tujuan utama aturan ini adalah memberikan deteksi dini terhadap upaya membanjiri server dalam jaringan lokal dengan permintaan koneksi palsu (SYN), yang dapat menghabiskan sumber daya server dan menyebabkan layanan menjadi tidak responsif

IV. HASIL DAN PEMBAHASAN

Dalam pengujian 5 kali serangan dengan masing-masing 30 detik, Suricata dan Snort memberikan hasil sebagai berikut:

TABEL 3
Hasil Uji Suricata

Pengujian	Total Paket Terkirim	Jumlah Alert	Ekspektasi Alert	Akurasi
uji 1	1696042	200408	339208.4	59%
uji 2	1796910	187135	359382	56%
uji 3	1573298	185902	314659.6	64%
uji 4	1370447	218943	274089.4	73%
uji 5	1397508	231282	279501.6	72%
Total	**7834205**	**1023670**	**1566841**	**65%**

TABEL 4
Hasil Uji Snort

Pengujian	Total Paket Terkirim	Jumlah *Alert*	Ekspektasi *Alert*	Akurasi
uji 1	1356584	224356	271316.8	83%
uji 2	1510638	188856	302127.6	74%
uji 3	1369639	203209	273927.8	82%
uji 4	1553297	187258	310659.4	72%
uji 5	1443157	235567	288631.4	78%
Total	**7233315**	**1039246**	**1446663**	**72%**

Berdasarkan data hasil pengujian, Snort secara keseluruhan menunjukkan kinerja akurasi yang lebih dengan total akurasi 72% dibandingkan Suricata dengan 65%. Snort mencapai akurasi tertinggi 83% pada uji 1 dengan jumlah peringatan 224.356, sementara itu Suricata memuncak pada uji 4 di 73%.

V. KESIMPULAN

Berdasarkan hasil pengujian deteksi serangan SYN Flood yang dilakukan sebanyak lima iterasi dengan durasi masing-masing 30 detik, diperoleh bahwa Snort memiliki tingkat akurasi yang lebih tinggi dibandingkan Suricata. Rata-rata akurasi Snort mencapai 72%, sedangkan Suricata hanya sebesar 65%. Snort secara konsisten unggul dalam empat dari lima kali pengujian, dengan akurasi tertinggi sebesar 83% pada pengujian pertama. Sementara itu, Suricata mencatatkan akurasi tertingginya sebesar 73% pada pengujian keempat, namun menunjukkan performa yang cukup rendah pada pengujian kedua dengan akurasi hanya 56%. Secara keseluruhan, Snort menunjukkan performa pendeteksian yang lebih stabil dan konsisten dibandingkan Suricata dalam mengidentifikasi serangan SYN Flood.

Saran untuk penelitian selanjutnya adalah agar dilakukan analisis lebih mendalam terhadap faktor-faktor yang memengaruhi performa deteksi, seperti kemungkinan adanya *bottleneck* pada sistem atau konfigurasi yang kurang optimal. Selain itu, disarankan untuk memperluas jenis serangan yang digunakan dalam pengujian, agar hasil analisis mencerminkan kemampuan IDS dalam menghadapi berbagai skenario serangan yang lebih kompleks dan beragam. Peninjauan ulang terhadap parameter deteksi yang digunakan juga perlu dilakukan, guna memastikan bahwa sistem IDS telah dikonfigurasi secara optimal untuk mendeteksi ancaman dengan tingkat akurasi yang tinggi.

REFERENSI

[1] O. Yoachimik and J. Pacheco, “Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare’s 2025 Q1 DDoS Threat Report.” [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/

[2] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” Apr. 2004. doi: 10.1145/997150.997156.

[3] A. Aarthy Devi, A. K. Mohan, and M. Sethumadhavan, “Wireless Security Auditing: Attack Vectors and Mitigation Strategies,” in *Procedia Computer Science*, Elsevier B.V., 2017, pp. 674–682. doi: 10.1016/j.procs.2017.09.153.

[4] I. Makris *et al.*, “A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions,” Dec. 20, 2024, *Elsevier Ireland Ltd*. doi: 10.1016/j.cosrev.2024.100717.

[5] R. Bace and P. Mell, “NIST Special Publication on Intrusion Detection Systems Intrusion Detection Systems,” Nov. 2001.

[6] A. A. Mohammed, “Design and Implementation of Network Intrusion Detection System Based on Embedded System,” Dec. 2015, doi: 10.13140/RG.2.2.20356.17282.

[7] K. A. Scarfone and P. M. Mell, “SP 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS),” National Institute of Standards & Technology, Gaithersburg, MD, USA, 2007.

[8] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: https://doi.org/10.1016/j.egyr.2021.08.126.