Research Article
Forbis: Journal Forensic Business Information Systems
Published online on: https://journal.universitasmulia.ac.id/index.php/forbis **1 (1) Januari 2024**

ANALISIS KOMPARASI INTRUTION DETECTION SYSTEM BERBASIS SNORT DENGAN SURICATA UNTUK KEAMANAN JARINGAN
(Studi Kasus: Astara Hotel Balikpapan)

Irvan Kurniawan[1], Djumhadi[2], Wahyu Nur Alimyaningtias[3], Darmawan Setiya Budi[4]*

[1,2,3,4] Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia

email: [1] irvankurniawan@students.universitasmulia.ac.id, [2] djumhadi@universitasmulia.ac.id, [3] wahyu.nur@universitasmulia.ac.id, [4] darmawan.setiyabudi@gmail.com
[*]Correspondence

ARTICLE INFO

Article History
Received : 12 Desember 2023
Revised : 21 Januari 2024
Accepted : 22 Januari 2024
Available online : 22 Januari 2024

Keywords:
Suricata, Snort, intrusion detection

Please cite this article in IEEE style as:

ABSTRACK

Intrusion Detection System (IDS) is a vital element in network security which functions to identify suspicious activity and attacks on the system. Suricata and Snort are the two leading platforms which are widely used in IDS. Although the main goal of both is the same, which is to protect the network from threats, there are differences in the method of detection and response to attacks. This study aims to compare Suricata and Snort in various key aspects, including detection performance, scalability, features, architecture, and ability to deal with new and complex attacks. The research methodology involves testing performance with various attack datasets, feature analysis, and evaluating performance with variations in network load

ABSTRAK

Deteksi Intrusi (IDS) merupakan elemen vital dalam keamanan jaringan yang berfungsi untuk mengidentifikasi aktivitas mencurigakan dan serangan di dalam sistem. Suricata dan Snort adalah dua platform terkemuka yang banyak digunakan dalam IDS. Meskipun tujuan utama keduanya sama, yaitu melindungi jaringan dari ancaman, namun terdapat perbedaan dalam metode deteksi dan respon terhadap serangan. Penelitian ini bertujuan untuk membandingkan Suricata dan Snort dalam berbagai aspek kunci, termasuk kinerja deteksi, skalabilitas, fitur, arsitektur, dan kemampuan menghadapi serangan baru dan kompleks. Metodologi penelitian melibatkan pengujian kinerja dengan berbagai dataset serangan, analisis fitur, dan evaluasi performa dengan variasi beban jaringan.

1. Pendahuluan

Keamanan server merupakan salah satu isu yang penting dalam dunia teknologi informasi, terutama dalam pengelolaan dan pemeliharaan data dan informasi yang sensitife dan penting.

Seiring dengan meningkatnya jumlah pengguna internet dan pengguna aplikasi dan layanan online, ancaman keamanan terhadap server semakin meningkat [1]–[3].

Hotel merupakan salah satu industri yang sangat bergantung pada teknologi informasi dan jaringan komputer. Jaringan komputer yang terdapat pada hotel biasanya digunakan untuk mengelola sistem reservasi, manajement kamar, dan pemerosesan pembayaran. Namun, keamanan jaringan hotel menjadi isu yang sangat penting, mengingat bahwa hotel sering kali menyimpan data sensitive tentang tamu, seperti nomor kartu kredit, paspor dan data pribadi lainnya. Selain itu, serangan siber pada jaringan hotel dapat berdampak buruk pada reputasi hotel dan mengganggu pengalaman tamu.

Salah satu cara untuk meningkatkan keamanan jaringan hotel adalah dengan menggunakan IDS (Intrusion Detection System). IDS adalah sebuah sistem keamanan yang dapat mendeteksi serangan siber dan aktivitas mencurigakan pada jaringan computer [4]–[6]Dengan menggunakan IDS, hotel dapat mengidentifikasi serangan siber dan memperoleh informasi penting tentang serangan tersebut. IDS bekerja dengan memantau lalu lintas jaringan dan mencari pola yang mencurigakan atau perilaku abnormal pada jaringan. Setelah menemukan pola atau perilaku tersebut, IDS akan mengirimkan notifikasi kepada administrator jaringan hotel agar dapat segera menangani masalah tersebut.

Dengan menggunakan IDS/IPS, hotel dapat meningkatkan keamanan jaringan mereka dan melindungi data sensitif tamu mereka. Selain itu, IDS/IPS juga membantu hotel dalam mematuhi peraturan keamanan data yang ada dan meningkatkan kepercayaan tamu terhadap hotel tersebut[7]–[10].

Berdasarkan latar belakang yang tujuan penelitian ini yakni Bagaimana cara meningkatkan keamanan server pada jaringan lokal hotel dengan menggunakan IDS/IPS berbasis Snort dan Suricata dan apa manfaat yang dapat diperoleh dari penggunaan IDS/IPS dalam menjaga keamanan data dan sistem pada hotel.

2. Metode Penelitian

2.1. Alur Penelitian

Penelitian ini menggunakan metode analisis-kualitatif fokus pada tingkat keberhasilan deteksi lalu lintas yang tepat dengan aturan sistem deteksi intrusi "IDS". Data tersebut digunakan untuk mengamati log sebagai data serangan yang berhasil atau tidak berhasil terdeteksi oleh (IDS) dan memeriksa lalu lintas jaringan.

Adapun alur penelitian untuk menjamin integritas pengujian ditunjukkan pada gambar 1.

Gambar 1. Alur Penelitian

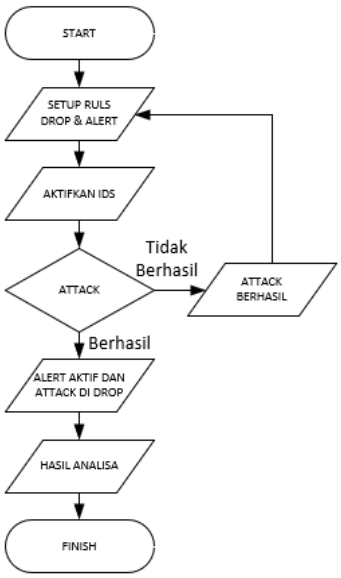
Merujuk pada gambar 3.1 merupakan flowchart metode penelitian yang akan dilakukan untuk meneilit perbedaan penggunaan IDS Suricata dengan IDS Snort.

2.2. Studi Literatur

Studi literatur adalah serangkaian kegiatan yang berkenaan dengan metode pengumpulan data pustaka,membaca dan mencatat, serta mengelolah bahan penelitian. Studi Litelatur digunakan sebagai panduan pengetahuan dasar untuk melakukan analisis, desain,digunakan dan diuji secara luas langkah-langkah penelitian. Teori dasar diperlukan sebagai dukungan pencarian ini adalah serangan DDOS, Nmap, Legion, IDS suricata dan IDS snort[11].

2.3. Pengujian Aplikasi

Pengujian aplikasi digunakan untuk memahami aplikasi yang akan di gunakan sebelum melakukan pengujian di lapangan atau di tempat yang akan dipasang IDS tersebut.



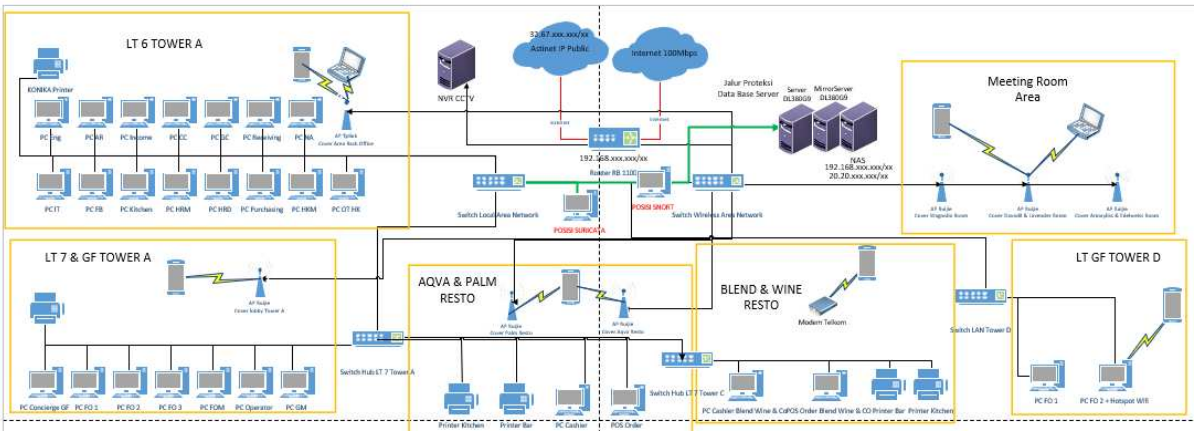
Gambar 2. Alur Pengujian Aplikasi

Merujuk pada gambar 3.2 merupakan alur flowchart pengujian dengan penjelasan sebagai berikut:

- *Setup rules* dan *alert*, melakukan *config rules alert* dan *drop* pada IP dan Port yang akan diproteksi sehingga proteksi bisa sesuai denga yang kita inginkan.
- Aktifkan IDS, memastikan IDS dalam kondisi *Active* agar *rules* dapat berjalan.
- Attack, melakukan attack dengan menggunakan tools attack seperti serangan DDOS, Scaning port dengan Nmap, Wireshark Attack dan Legion. Jika serangan tidak berhasil maka tidak ada alert dan harus membenarkan Rules agak keamanan berjalan dengan semestinya.
- Hasil dan Analisa, jika Alert aktif maka ip attack akan di Drop sesuai dengan perintah Rules yang kita buat jika ada serangan makan ada Alert dan IP penyerang akan di Drop.

2.4. Pengujian Lapangan

Pengujian lapangan adalah melakukan secara langsung dengan perangkat yang ada di server hotel dan menguji efektifitas antara Snort dan Suricata dengan aplikasi Attack yang sudah dipersiapkan. Adapun topologi jaringan ditampilkan pada gambar 3.



Gambar 3. Topologi jaringan yang ada di Astara Hotel Balikpapan

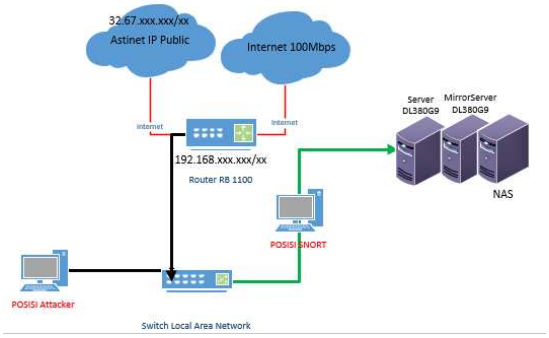
3. Hasil dan Pembahasan

Hasil dan analisa membahas hasil performa dari ke dua IDS dengan serangan yang telah di siapkan dengan pengujian langsung kepada perangkat server dan jaringan. Menganalisa apakah saat aplikasi sudah di jalankan dan dilakukan penyerangan apakah aplikasi berjalan dengan semestinya atau ada kendala tertentu dari dua IDS yang akan di uji. Jika aplikasi berjalan maka IDS akan mengeluarkan

peringatan dan melakukan Drop pada IP yang melakukan penyerangan sehingga tidak ada Virus yang akan mencuri dan menginfeksi data. Berdasarkan penelitian di atas maka disimpulkan untuk penambahan keamanan jaringan di Astara Hotel Balikpapan menggunakan Suricata sebagai Intrution Detection System (IDS) dengan mengandalkan multi-threaded yang memungkinkan untuk memproses banyak tugas sehingga dapat mengamankan 3 server sekaligus daripada snort yang tidak dapat memproses banyak tugas sekaligus dikarenakan snort menggunakan Single-threaded. Suricata memiliki aturan yang dapat di update setiap harinya dengan perintah Suricata-Update, sedangkan snort lebih banyak membaca forum/komunitas agar user dapat melakukan pembaruan pada aturan yang di ada di local.rules.

3.1. Snort

Dalam proses pengimplementasian snort dibutuhkan sebuah konfigurasi rule untuk menjalankan memberikan instruksi, serta gambar topologi untuk memberikan gambaran sebuah serangan untuk ditangkap oleh snort. Topologi snor terlihat pada gambar 4.



Gambar 4. Topologi Snort

Merujuk pada gambar 4 menjelaskan topologi yang digunkan pada IPS Snort menggunakan konfigurasi jaringan bridged. peneliti melakukan konfigurasi pada perangkat langsung tanpa melalui virtual machine sehingga dapat memberikan hasil yang real sesuai dengan apa yang terjadi di lapangan.

```
ids@ids-server:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort
.conf -i enp2s0
07/30-14:26:33.758047  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attem
pted Information Leak] [Priority: 2] {ICMP} 192.168.0.8 -> 192.168.0.2
```

Gambar 5. Hasil Defanse dari Attack NMAP

Gambar 5 merupakan proses di mana sebuah serangan diujikan dan kemudian didapatkan hasil defense dari scanning nmap yakni sebuah Alert ICMP PING NMAP.

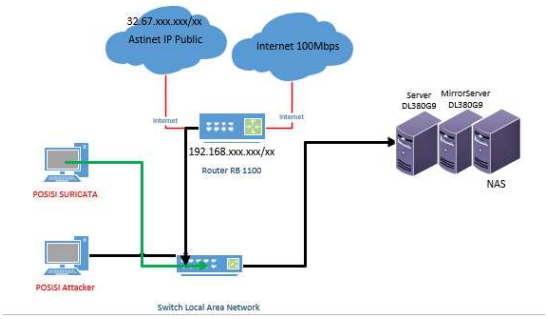
```
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.156.138.206:3022 -> 19
2.168.0.2:80
07/30-14:31:42.870311  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.218.229.164:3032 -> 19
```

Gambar 6. Hasil Defance dari Attack Hping3

Merujuk pada gambar 4.6 merupakan hasil defence dari serangan DDOS dengan aplikasi hping3 dengan hasil Aler BAD-TRAFFIC loopback traffic.

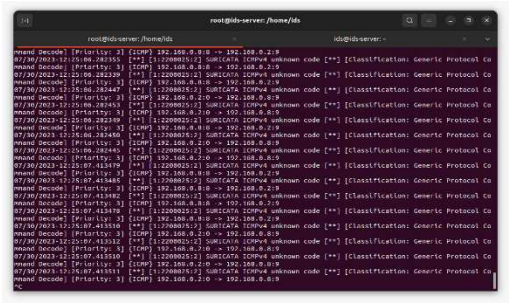
3.2. Suricata

Suricata adalah sebuah sistem deteksi intrusi (IDS) dan pencegahan intrusi (IPS) yang memiliki arsitektur multi-threaded. Suricata menggunakan aturan dan analisis protokol untuk mengidentifikasi aktivitas mencurigakan dalam lalu lintas jaringan. Suricata digunakan dalam pengujian kedua dengan topologi yang di tampilkan pada gambar 7.



Gambar 7. Topologi Suricata

Merujuk pada gambar 7 menjelaskan posisi IDS Suricata tanpa menggunakan konfigurasi bridge. peneliti melakukan konfigurasi pada perangkat langsung tanpa melalui virtual machine sehingga dapat memberikan hasil yang real sesuai dengan apa yang terjadi di lapangan.



Gambar 8. Hasil defence dari NMAP attack.

Merujuk pada gambar 4.8 merupakan hasil defence dari scanning nmap dengan hasil Alert SURICATA ICMPV4 uknown code.

Gambar 9. Hasil defence dari Hping 3 Attack

3.3. Hasil Komparasi

Berdasarkan perbandingan antara Suricata dan Snort, dapat disimpulkan bahwa Suricata menonjol dengan arsitektur multi-threaded yang mendukung pemrosesan tugas secara bersamaan, performa yang lebih baik di lingkungan dengan lalu lintas tinggi, serta kemampuan deteksi intrusi tingkat lanjut. Suricata juga memudahkan penyiapan dan manajemen aturan melalui antarmuka web dan konfigurasi YAML. Di sisi lain, Snort menawarkan kompatibilitas yang lebih luas dengan perangkat dan sistem operasi karena keberadaannya yang lebih lama, cocok untuk lingkungan dengan sumber daya terbatas, namun cenderung memiliki keterbatasan kinerja di lingkungan dengan lalu lintas tinggi. Snort menggunakan arsitektur single-threaded dengan fokus pada deteksi berbasis aturan dan analisis protokol, serta memerlukan konfigurasi tradisional dan manajemen aturan manual. Kesimpulan ini memberikan gambaran tentang kelebihan dan kekurangan masing-masing sistem sesuai dengan kebutuhan pengguna. Berikut hasil perbandingan disajikan dalam bentuk tabel 1.

Tabel 1. Tabel Perbandingan

SURICATA	SNORT
Arsitektur multi-threaded memungkinkan pemrosesan banyak tugas yang efisien secara bersamaan.	Arsitektur single-threaded
Suricata-Update untuk mengelola dan memperbarui kumpulan aturan.	Kompatibilitas yang lebih luas dengan perangkat, sistem operasi, dan alat pihak ketiga karena kehadiran pasarnya yang lebih lama
Kemampuan deteksi dan pencegahan intrusi tingkat lanjut.	Fokus pada deteksi berbasis aturan dan analisis protokol
Performa lebih baik di lingkungan dengan lalu lintas tinggi.	Performa lebih baik di lingkungan dengan sumber daya terbatas
Mendukung mode inline dan pasif.	Mendukung mode inline dan pasif
Penggunaan sumber daya yang efisien memungkinkan penanganan volume lalu lintas yang besar dengan lebih baik	Penggunaan sumber daya yang lebih rendah membuatnya cocok untuk lingkungan dengan sumber daya terbatas
Arsitektur multi-utas memberikan peningkatan kinerja	Arsitektur single-threaded mungkin memiliki batasan kinerja di lingkungan dengan lalu lintas tinggi

Dapat diskalakan karena penggunaan sumber daya dan kemampuan penanganan lalu lintas yang efisien	Mungkin kurang terukur jika dibandingkan, terutama di lingkungan dengan lalu lintas tinggi
Tidak ada antarmuka web bawaan (Tersedia pihak ketiga)	Tidak ada antarmuka web bawaan (Tersedia pihak ketiga)
Konfigurasi berbasis YAML menyederhanakan penyiapan	Metode konfigurasi tradisional
Suricata-Update untuk manajemen aturan yang disederhanakan	Manajemen dan pembaruan aturan manual
Penyiapan lebih mudah berkat antarmuka web dan konfigurasi YAML	Mungkin memerlukan lebih banyak penyesuaian dan upaya konfigurasi

4. Kesimpulan

Berdasarkan penelitian dan pembahasan yang dilakukan pada tugas akhir mengenai komparasi suricata dan snort untuk penerapan di Astara Hotel Balikpapan Menggunakan Metode analisis-kualitatif dapat disimpulkan bahwa: IPS Snort menggunakan mode bridge sebagai jembatan sedangkan IDS Suricata langsung terkoneksi dengan menuju pada ip server. IPS Snort melakukan scanning secara menyeluruh sehingga pada ip yang tidak terkena serangan akan tetap dilakukan scanning berbeda dengan IDS suricata hanya standby dan aktif hanya pada saat ada serangan/peringatan saja. Rules yang di gunakan IPS Snort sudah disediakan sehingga aplikasi hanyak melakukan configurasi jaringan berbeda dengan rules IDS Suricata yang harus melakukan konfigurasi rules manual untuk terhadap serangan tertentu seperti serangan DOS/DDOS dan scanning.

Berdasarkan beberapa kesimpulan di atas peneliti menyimpulkan dengan menggunakan IDS Suricata untuk jaringan yang akan di instalasi pada Astara Hotel Balikpapan sebagai pengamanan jaringan ke dua setelah firewall pada router. Dikarenakan tingkat akurasi dan reflek aplikasi yang sangat andal daripada menggunakan IPS snort yang terlalu lama untuk membaca serangan.

5. Referensi

[1] J. E. W. Prakasa, "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi," *Jurnal Ilmiah Teknologi Informasi Asia*, vol. 14, no. 2, p. 75, May 2020, doi: 10.32815/jitika.v14i2.452.

[2] A. Wijayanto, I. Riadi, and Y. Prayudi, "TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 2, pp. 208–217, Mar. 2023, doi: 10.29207/resti.v7i2.4589.

[3] A. Wijayanto, I. Riadi, Y. Prayudi, and T. Sudinugraha, "Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, no. 2, pp. 156–169, Jul. 2022, doi: 10.26594/register.v8i2.2953.

[4] M. Muqorobin, Z. Hisyam, M. Mashuri, H. Hanafi, and Y. Setiyantara, "Implementasi Network Intrusion Detection System (NIDS) Dalam Sistem Keamanan Open Cloud Computing," *Majalah Ilmiah Bahari Jogja*, vol. 17, no. 2, pp. 1–9, Jul. 2019, doi: 10.33489/mibj.v17i2.205.

[5] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 1, no. 2, pp. 67–74, Dec. 2020, doi: 10.30630/jitsi.1.2.10.

[6] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 4, no. 2, p. 413, Apr. 2020, doi: 10.30865/mib.v4i2.2037.

[7] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, Jan. 2022, doi: 10.14421/jiska.2022.7.1.46-55.

[8] Y. Arta, "Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal," *IT JOURNAL RESEARCH AND DEVELOPMENT*, vol. 2, no. 1, pp. 43–50, Nov. 2017, doi: 10.25299/itjrd.2017.vol2(1).979.

[9] E. Risyad, M. Data, and E. S. Pramukantoro, "Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam

Mendeteksi Serangan TCP SYN Flood," 2018. [Online]. Available: http://j-ptiik.ub.ac.id

[10] L. Lukman and M. Suci, "Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache," *Respati*, vol. 15, no. 2, p. 6, Jul. 2020, doi: 10.35842/jtir.v15i2.343.

[11] Z. A. Tyas, A. Firdonsyah, and W. Ramdhani, "Analisis Keamanan Jaringan dari Serangan DoS pada Sistem Inventaris Sanggar Tari Natya Lakshita menggunakan IDS," *INFORMAL: Informatics Journal*, vol. 7, no. 3, p. 258, Dec. 2022, doi: 10.19184/isj.v7i3.34943.