JUKANTI
JURNAL PENDIDIKAN TEKNOLOGI INFORMASI

SIMULASI DAN ANALISIS EFEKTIVITAS SISTEM KEAMANAN JARINGAN MENGGUNAKAN *INTRUSION PREVENTION SYSTEM* (IPS) BERBASIS WAZUH

Andika[1], Rissal Efendi[2]

[1,2] *Universitas Kristen Satya Wacana*

E-mail: 672019205@student.uksw.edu, rissal.efendi@uksw.edu

ABSTRAK

Keamanan jaringan komputer menjadi aspek penting di era digital, terutama dengan meningkatnya berbagai ancaman siber yang kompleks dan dinamis. Penelitian ini bertujuan untuk melakukan simulasi sistem keamanan jaringan menggunakan Intrusion Prevention System (IPS) berbasis Wazuh, sebuah platform keamanan open-source yang menawarkan integrasi deteksi, pencegahan, dan pemantauan ancaman. Tingkat akurasi deteksi dari Wazuh sangat tinggi dalam sistem keamanan jaringan. Metodologi penelitian mencakup desain topologi jaringan, konfigurasi sistem Wazuh sebagai IPS, dan pengujian untuk mengukur efektivitasnya dalam mendeteksi serta mencegah ancaman keamanan. Hasil simulasi menunjukkan bahwa Wazuh mampu mengidentifikasi dan mencegah serangan, seperti brute force serta Cross Site Scripting (XSS) attack dengan tingkat akurasi yang memadai. Studi ini memberikan referensi praktis untuk penerapan sistem keamanan jaringan berbasis IPS, khususnya bagi organisasi dengan keterbatasan sumber daya.

Kata Kunci: *Wazuh, Network Security, Intrusion Prevention System, Simulation, Cybersecurity.*

ABSTRACT

Computer network security is a crucial aspect in the digital era, especially with the growing complexity and dynamics of cyber threats. This study aims to simulate a network security system using a Wazuh-based Intrusion Prevention System (IPS), an open-source security platform that integrates threat detection, prevention, and monitoring. Wazuh-based detection accuracy level is very high in network security systems. The research methodology involves designing network topology, configuring Wazuh as an IPS, and conducting tests to evaluate its effectiveness in detecting and mitigating security threats. The simulation results show that Wazuh is capable of identifying and preventing attacks such as brute force and Cross-Site Scripting (XSS) attacks with satisfactory accuracy. This study provides practical insights into implementing an IPS-based network security system, particularly for organizations with limited resources.

Keywords: *Wazuh, Network Security, Intrusion Prevention System, Simulation, Cybersecurity.*

1. PENDAHULUAN

Di era digital yang semakin maju, jaringan komputer telah menjadi menjadi elemen vital di berbagai sektor, baik di sektor bisnis, pendidikan, maupun pemerintahan. Namun, seiring dengan peningkatan penggunaan teknologi, ancaman terhadap keamanan jaringan komputer juga semakin berkembang dalam

Andika, A., & Efendi, M.Kom, R. . SIMULASI DAN ANALISIS EFEKTIVITAS SISTEM KEAMANAN JARINGAN MENGGUNAKAN INTRUSION PREVENTION SYSTEM (IPS) BERBASIS WAZUH. Jurnal Pendidikan Teknologi Informasi (JUKANTI), 8(1), 17–24.
https://doi.org/10.37792/jukanti.v8i1.1454

hal kompleksitas dan frekuensi. Serangan siber seperti brute force attacks, malware injection, hingga Cross-Site Scripting (XSS) semakin sering terjadi, mengakibatkan kerugian besar bagi organisasi yang tidak memiliki sistem keamanan jaringan yang memadai. Sebagai contoh tren serangan siber brute force attacks yang mudah ditemui dikalangan umum seperti penggunaan kata sandi pada aplikasi yang mulai banyak digunakan dan layanan berbasis web (layanan e-commerce, social media). Untuk mengatasi tantangan ini, diperlukan solusi keamanan yang tidak hanya mampu mendeteksi ancaman, tetapi juga dapat mencegah kerusakan yang lebih besar. Salah satu teknologi yang memiliki potensi besar dalam bidang ini adalah Intrusion Prevention System (IPS). IPS berfungsi untuk memonitor lalu lintas jaringan, mengidentifikasi potensi ancaman, dan secara proaktif mencegah serangan sebelum menyebabkan kerusakan.Wazuh, sebagai salah satu platform keamanan open-source, menawarkan kemampuan integrasi untuk deteksi ancaman, pencegahan, dan pemantauan sistem. Keunggulan Wazuh terletak pada fleksibilitasnya yang dapat disesuaikan dengan kebutuhan pengguna serta kompatibilitasnya yang baik dengan berbagai infrastruktur jaringan. Namun, meskipun Wazuh telah banyak digunakan, studi tentang penerapannya sebagai IPS dalam simulasi keamanan jaringan masih terbatas.Penelitian ini bertujuan untuk mensimulasikan sistem keamanan jaringan berbasis Wazuh dengan fokus pada efektivitasnya dalam mendeteksi dan mencegah berbagai jenis serangan siber.

Hasil dari penelitian ini diharapkan dapat menjadi referensi praktis bagi organisasi, khususnya yang memiliki keterbatasan sumber daya, dalam mengimplementasikan sistem keamanan jaringan yang efisien dan efektif, maka penulis tertarik untuk mengambil judul "Simulasi dan Analisis Efektivitas Sistem Keamanan Jaringan menggunakan Intrusion Prevention System (IPS) berbasis Wazuh".

Keamanan jaringan komputer menjadi salah satu fokus utama dalam pengelolaan infrastruktur teknologi informasi. Salah satu cara untuk meningkatkan keamanan jaringan adalah dengan memanfaatkan sistem deteksi dan pencegahan intrusi seperti Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS). Beberapa penelitian terdahulu memberikan gambaran mengenai implementasi teknologi ini dalam menghadapi ancaman siber.

Pada penelitian sebelumnya, simulasi sistem keamanan jaringan berbasis IPS menunjukkan bahwa kombinasi IPS dan Honeypot dapat meningkatkan efektivitas dalam mendeteksi dan mencegah ancaman siber[1]. Selain itu, penggunaan IDS untuk mendeteksi aktivitas port scanning pada jaringan komputer juga memberikan hasil yang signifikan dalam mendeteksi pola aktivitas mencurigakan yang menjadi indikasi awal serangan[2].

Penelitian lainnya membahas penggunaan Snort sebagai sistem pendeteksi serangan. Hasil penelitian menunjukkan bahwa Snort dapat mendeteksi berbagai jenis ancaman dengan aturan yang dapat disesuaikan, memberikan perlindungan yang optimal dalam lingkungan dengan sumber daya terbatas[3]. Simulasi penggunaan IDS juga memberikan pandangan teknis mengenai bagaimana sistem ini mampu mendeteksi serangan serta memberikan peringatan dini terhadap potensi ancaman[4]. Dalam hal itu penelitian ini ingin mengembangkan simulasi sistem keamanan jaringan berbasis IPS yang berfokus pada Wazuh dengan lebih efektif.

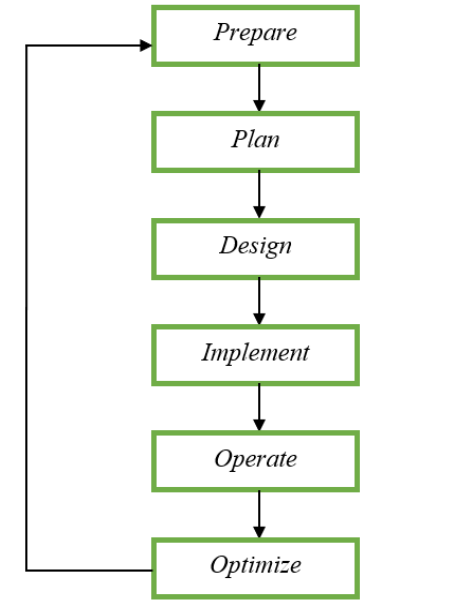
Selain itu, studi tentang perancangan dan analisis sistem keamanan jaringan menekankan pentingnya perencanaan yang matang dalam membangun sistem keamanan yang efektif

untuk mengurangi risiko serangan siber[5]. Implementasi IDS juga dikaji sebagai elemen kunci dalam memberikan notifikasi atas aktivitas mencurigakan, meskipun untuk pencegahan langsung, IDS perlu dikombinasikan dengan IPS[6].

Hasil dari berbagai penelitian ini menunjukkan bahwa pendekatan berbasis IDS dan IPS memberikan solusi yang efektif dalam menghadapi ancaman keamanan jaringan. Penelitian ini melanjutkan studi-studi tersebut dengan fokus pada efektivitas Wazuh sebagai IPS dalam mendeteksi dan mencegah serangan jaringan komputer.

2. METODOLOGI PENELITIAN

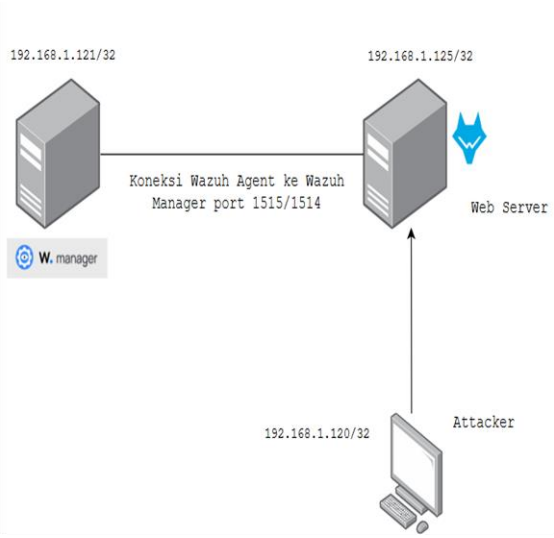
Metode penelitian yang digunakan dalam penelitian ini adalah model PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize)[7]. Dalam hal ini model PPDIOO menawarkan pendekatan yang lebih cocok dalam penelitian untuk implementasi jaringan karena dinilai lebih komprehensif, terstruktur, dan berfokus pada pengoptimalan sistem serta keberlanjutan operasional yang lebih baik dan konteks dalam jangka panjang.



Gambar 1. Tahapan Penelitian

Model penelitian pada Gambar 1, dijelaskan sebagai berikut:

Tahap Prepare dimulai dengan mempersiapkan sumber daya yang diperlukan, termasuk perangkat keras dan perangkat lunak yang dibutuhkan untuk menerapkan Wazuh sebagai sistem keamanan jaringan berbasis IPS. Tahap Plan dilakukan dengan merencanakan strategi implementasi, seperti memilih referensi dari studi sebelumnya mengenai penggunaan Wazuh serta mendalami konsep-konsep terkait keamanan jaringan untuk memahami kebutuhan sistem yang diperlukan dalam penelitian ini. Setelah itu, pada tahap Design, perancangan sistem dilakukan dengan merancang topologi jaringan yang akan diuji serta konfigurasi Wazuh yang akan diterapkan untuk mendeteksi dan mencegah serangan. Pada tahap Implement, Wazuh diterapkan dalam jaringan yang telah dirancang, diikuti dengan pengujian untuk memastikan bahwa sistem berjalan dengan baik dan efektif dalam mendeteksi ancaman keamanan seperti brute force dan Cross-Site Scripting (XSS). Tahap Operate dilakukan dengan mengoperasikan sistem untuk memonitor dan mengelola kinerja Wazuh dalam lingkungan yang sudah diterapkan, guna memastikan bahwa sistem berfungsi sesuai tujuan. Terakhir, pada tahap Optimize, dilakukan evaluasi hasil pengoperasian dan optimasi terhadap sistem yang ada berdasarkan pengujian yang dilakukan, dengan tujuan meningkatkan efektivitas dan akurasi deteksi serta pencegahan ancaman keamanan yang teridentifikasi.



Gambar 2 RancanganTopologi Jaringan

Pada tahap ini penulis menggunakan 1 buah laptop yang terdapat *software Virtual Box* untuk di*install server* dan digunakan sebagai penyerang, untuk penghubung antara *server* dan penyerang menggunakan mode *Bridge*. *Server* dikonfigurasi menggunakan *Wazuh Agent* dan *Active Response* sebagai sistem keamanan. Komputer virtual *client*/Penyerang digunakan untuk melakukan uji coba layanan dan uji coba sistem keamanan yang sudah diimplementasi.

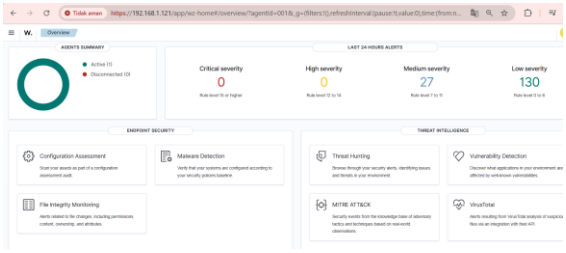
Tabel 1 Pengalamatan Perangkat

3. HASIL DAN PEMBAHASAN

Implementasi " *Simulasi dan Analisis Efektivitas Sistem Keamanan Jaringan menggunakan Intrusion Prevention System (IPS) berbasis Wazuh* " terbagi menjadi 3 bagian, yaitu

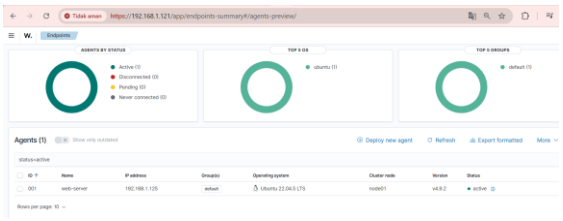
No	Perangkat	Alamat Perangkat
1	*Wazuh Server*	192.168.1.121/32
2	*Web Server*	192.168.1.125/32
3	Penyerang	192.168.1.120/32

implementasi instalasi sistem keamanan *Wazuh Manager, Install Wazuh Agent* dan *Konfigurasi Active Response.*



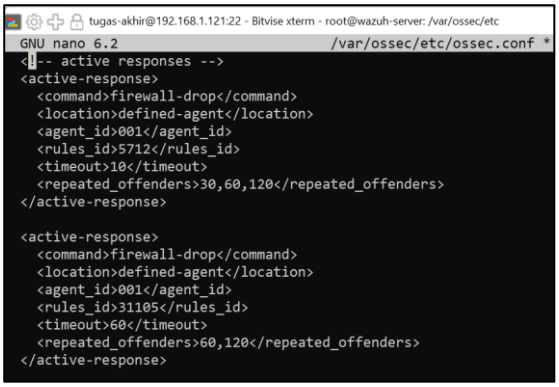
Gambar 3 tampilan *Dashboard Wazuh*

Gambar 3 menunjukan setelah instalasi 3 komponen *wazuh* (*Wazuh Indexer, Manager dan Server*) dashboard wazuh bisa diakses dan siap untuk digunakan.



Gambar 4 tampilan Status Agent Wazuh

Pada **gambar 4** menginformasikan setelah *install agent wazuh* seleasi statusnya dapat dilihat pada *dashboard* untuk mengetahui *agent* aktif atau tidak setelah proses *install*.



Gambar 5 Konfigurasi Active Response

Gambar 5 merupakan konfigurasi *active response* yang nantinya akan

melakukan *block* sesuai pola serangan yang akan dicegah.

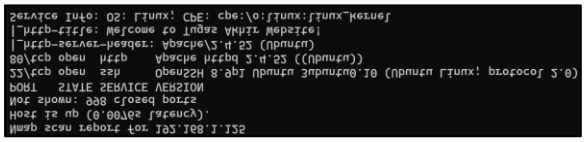
Skenario pengujian untuk Tugas Akhir "Simulasi dan Analisis Efektivitas Sistem Keamanan Jaringan menggunakan *Intrusion Prevention System* (IPS) berbasis Wazuh" adalah sebagai berikut :

1. Penyerang akan melakukan *scanning* untuk mengetahui open port mana saja yang terbuka pada web server.

2. Kemudian akan dilakukan bruteforce attack pada server mengarah ke administrative port 22 (SSH), jika terdapat percobaan gagal login melebihi 3 kali maka IP penyerang akan di block oleh active response.

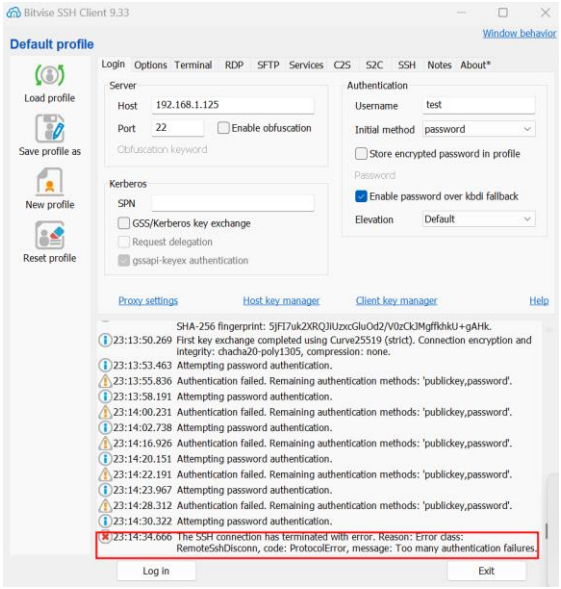
3. Lalu akan dilakukan percobaan serangan Cross Site Scripting (XSS) pada Web page server, jika payload match dengan rule maka request akan di block oleh active response.

4. Setelah itu untuk hasil aktivitas penyerang nantinya bisa dilakukan pengecekan pada dashboard wazuh.



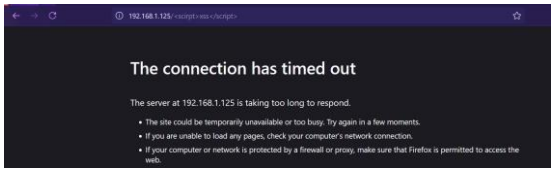
Gambar 6 Scanning port ke *server*.

Gambar 6 Penyerang melakukan *scanning* ke *server* dan hasilnya open port 22 (SSH) dan 80 (HTTP).



Gambar 7 Scanning port ke *server*.

Gambar 7 setelah penyerang melakukan *scanning* ke *server* dan menemukan *open port* 22 (SSH) yang bisa untuk melakukan *remote* ke *server*, kemudian dilakukan percobaan login berulang-ulang dengan menebak *password* server dan saat mencapai percobaan menebak sebanyak 3 kali sesuai rule *active response* yang dibuat aktivitas ter-block.



Gambar 8 Percobaan Serangan Cross Site Scripting (XSS).

Gambar 8 setelah penyerang melakukan *scanning* ke *server* dan menemukan *open port* 80 (HTTP) yang merupakan *web server*, kemudian dilakukan percobaan serangan *Cross Site Scripting (XSS)* dan mendapat respon *time out* atau ter-*block* oleh *active response.*

Gambar 9 Aktivitas Log Menebak Password ter-Block.

Gambar 9 tercatat aktivitas pada *dashboard wazuh* percobaan serangan menebak password server terblock dengan signature Brute Force dengan user yang tidak terdaftar yang log nya tercatat pada *wazuh server*.

Gambar 10 Aktivitas Log Serangan Cross Site Scripting (XSS).

Gambar 10 pada *dashboard wazuh* merekam aktivitas serangan Cross Site Scripting (XSS) terblock dengan signature Cross Site Scripting (XSS) attempt yang log nya tercatat pada *wazuh server*.

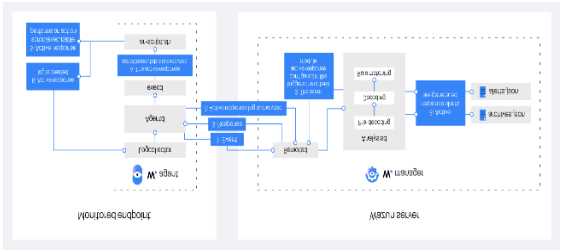
Mengoptimalkan sistem keamanan jaringan yang dibuat dengan memonitoring dan memperbaruhi sistem keamanan jaringan yang telah dibuat dengan cara :

1. Wazuh berbasis open-source sehingga dapat dikembangakan dengan menambahkan fungsi yang dapat disesuaikan dengan kebutuhan dan diintegrasikan dengan tools keamanan jaringan lainya yang kiranya dapat mengamankan sistem pada jaringan.

2. Memperbarui repository ruleset secara berkala untuk menambah signature atau pola serangan.

3. Menambahkan konfigurasi Active Response sesuai kebutuhan agar semua serangan dapat dicegah secara otomatis.

4. Selalu melakukan perbaruan sistem operasi dengan perintah apt-get updated dan upgrade OS Ubuntu agar sistem berjalan dengan baik dan mendapat versi sistem terbaru. Kiranya itulah beberapa cara dalam mengoptimalkan sistem keamanan jaringan yang telah dibuat, ini dimaksudkan agar sistem keamanan jaringan yang dibuat dapat mengikuti perkembangan jaman yang ada.



Gambar 11 Konfigurasi queue Tree

Pada gambar diatas menjelaskan alur sebuah kejadian (event) yang mencurigakan terdeteksi oleh *agent wazuh* (via modul seperti Logcollector atau execd). Kejadian ini bisa berasal dari log sistem, perubahan file, atau aktivitas lainnya. Untuk alurnya kejadian (event) dikirimkan oleh *agent* ke *server wazuh* melalui komponen *Remoted*. Lalu *server wazuh* menganalisis kejadian (event) yang diterima untuk mencocokkannya dengan aturan (rules) yang tersedia. Jika kejadian sesuai dengan aturan *acvite response* maka akan menghasilkan alert "*Active Response*". Kejadian ini akan dicatat dalam file *alerts.json* atau *archives.json*. Kemudian *log* akan dikirim ke *server* untuk dianalisis lebih lanjut atau untuk keperluan pencatatan yang bisa dilihat pada *dashboard*.

Gambar 12 Dashboard Deteksi Wazuh.

Gambar 12 menginformasikan semua deteksi kejadian (event) pada agent wazuh untuk memudahkan analisa jika terdapat anomali pada *server* agar dapat segera ditindaklanjuti.

Tabel 2 Kelebihan dan Kekurangan

Kelebihan	Waktu respon Wazuh yang lebih akurat dan cepat karena setiap kejadian (event) yang masuk langsung secara *real time* di catat dan langsung bisa di lihat statistiknya pada *dashboard*.	Setiap kejadian (event) dapat diidentifikasi apakah *valid* serangan atau tidak dan menyimpannya sebagai pola.
Kekurangan	*Active response* perlu dikonfigurasi apabila ada pola serangan baru, kemampuan untuk pengamanan tergantung pada aturan yang ditentukan.	Membutuhkan banyak *resource* jika terdapat banyak agent yang akan diinstall.

4. KESIMPULAN

Berdasarkan penelitian Simulasi dan Analisis Efektivitas Sistem Keamanan Jaringan menggunakan *Intrusion Prevention System* (IPS) berbasis Wazuh dapat disimpulkan bahwa pengujian yang dilakukan melibatkan pemindaian port, brute-force pada SSH (22), dan serangan XSS pada port HTTP (80), dan dilakukan lebih dari 3 kali percobaan yang dimana serangan ini berhasil diblokir, dan menunjukkan respons yang efektif terhadap potensi pada serangan brute-force. Penelitian ini yang responsif dalam menangkap deteksi kejadian (event) jika terdapat anomali pada sistem dan *Active response* dapat melakukan *Block* bila ada percobaan serangan yang sesuai dengan aturan (rule) yang dapat mencegah penyerang sebelum mereka memiliki kesempatan untuk menyerang keseluruhan sistem, ini dirasa cukup untuk mengamankan dan menganalisis pola serangan penyerang yang ingin mengambil alih ke sistem jaringan komputer dan dengan memperhatikan kekurangan yang ada dapat membuat sistem keamanan ini menjadi lebih baik lagi.

Adapun saran dalam penelitian ini yaitu bila diterapkan pada keamanan jaringan dapat ditingkatkan dengan menambahkan konfigurasi *Active Response* pada *wazuh* sesuai dengan kebutuhan kemudian mengupdate *rule signature* bila ada pola serangan baru dan meningkatkan performa *Server* dengan melakukan *upgrade hardware.*

DAFTAR PUSTAKA

[1] A. Aminanto and W. Sulistyo, "Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery," *Aiti*, vol. 16, no. 2, pp. 135–150, 2020, doi: 10.24246/aiti.v16i2.135-150.

[2] M. Anif, S. Hws, and M. D. Huri, "Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang," *J. TELE, Vol. 13 Nomor 1*, vol. 13, no. 1, pp. 25–30, 2015.

[3] R. N. Dasmen, C. Ariyanto, M. H. Surya, and H. Ramadhan, "Penerapan Snort Sebagai Sistem Pendeteksi Serangan Keamanan Jaringan," *Jurasik (Jurnal Ris. Sist. Inf. dan Tek. Inform.*, vol. 7, no. 1, p. 8, 2022, doi: 10.30645/jurasik.v7i1.409.

[4] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[5] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *Aiti*, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[6] M. Ulfa, "Implementasi Insrusion Detection System (IDS) Di Jaringan Internet Universitas Bina Darma," *J. Imiah MATRIK*, vol. 15, no. 12, pp. 105–118, 2013.

[7] I. Solikin, "Penerapan Metode PPDIOO dalam Pengembangan LAN dan WLAN," *Teknomatika*, vol. 07, no. 01, pp. 65–73, 2017, [Online]. Available: http://ojs.palcomtech.ac.id.