Jurnal FUSE – Teknik Elektro
|Vol. 3 | No. 1 | Halaman 37 – 44 | [Juni][2023]

Implementasi *Intrusion Detection System* (IDS) Menggunakan *Snort* Berbasis SMS *Gateway* Untuk Keamanan Jaringan

Diki Rustandi[1], Iik Muhamad Malik Matin[2], Tri Arif Wiharso[3]

[1,3]Fakultas Teknik Universitas Garut, Garut, Jawa Barat, 44151, Indonesia
[2]Teknik Multimedia dan Jaringan, Politeknik Negeri Jakarta, Kota Depok, Jawa Barat, 16425, Indonesia

Korespondensi: dikirustandi0211@gmail.com

ARTICLE HISTORY

Received:06-06-2023	***Revised:23-06-2023***	***Accepointed:26-06-2023***

Abstrak

Penggunaan jaringan berkembang pesat bahkan sampai di dunia pendidikan. Banyak sekolah yang memanfaatkan jaringan komputer untuk menunjang pembelajaran. Salah satunya SMK Tarbiyatul Aulad Cikajang. Jaringan yang terkoneksi ke internet akan mudah terkena serangan dari pihak yang tidak bertanggungjawab. Keamanan jaringan harus diutamakan untuk melindungi jaringan. Salah satu sistem keamanan yang dapat digunakan untuk melindungi jaringan adalah menerapkan *Intrusion Detection System* (IDS). *Snort* merupakan salah satu IDS terbaik yang dapat digunakan secara gratis. Metode yang digunakan untuk mendapatkan data yang akurat yaitu dengan melakukan studi literatur, observasi lapangan dan pengujian sistem. Pengujian dilakukan sebelum dan setelah sistem dibuat. Pengujian dilakukan menggunakan serangan jaringan berupa *port scanning* dan DDOS *attacks*. Hasil pengujian sebelum sistem dibuat serangan jaringan tidak terdeteksi oleh server. Sedangkan hasil pengujian setelah sistem dibuat, server mampu mendeteksi dan memblok serangan tersebut dan memberikan notifikasi berupa SMS kepada administrator. Hasil notifikasi SMS terdapat *delay* selama 2 detik dibandingkan dengan waktu apabila dilihat dari tampilan *console*.

Kata kunci: IDS, Keamanan Jaringan, *Snort*, SMS *Gateway*.

Implementation of Intrusion Detection System (IDS) Using SMS Gateway-Based Snort for Network Security

Abstract

The use of the network is growing rapidly even in the world of education. Many schools use computer networks to support learning. One of them is SMK Tarbiyatul Aulad Cikajang. Network connected to the internet will be easily attacked by irresponsible parties. Network security must come first to protect the network. One of the security systems that can be used to protect the network is implementing an Intrusion Detection System (IDS). Snort is one of the best IDS that can be used for free. The method used to obtain accurate data is by conducting literature studies, field observations and system testing. Testing is done before and after the system is built. Testing is carried out using network attacks in the form of port scanning and DDOS attacks. The test results before

the system is made network attacks are not detected by the server. While the test results after the system is created, the server is able to detect and block the attack and give the notifications via SMS to administrator. The results of SMS notifications have a delay of 2 seconds compared to the time when viewed from the console display.

Keywords: IDS, Network Security, Snort, SMS Gateway

1. Pendahuluan

Perkembangan teknologi khususnya dalam bidang jaringan membuat berbagai fungsi teknologi dan alat tumbuh dengan cepat dan baik. Penggunaan jaringan berkembang sangat pesat bahkan di dunia pendidikan. Banyak sekolah yang memanfaatkan jaringan untuk menunjang proses pembelajaran untuk siswa-siswinya. Dengan adanya jaringan lokal yang terintegrasi dengan internet di sekolah, siswa ataupun guru dapat memanfaatkan jaringan lokal tersebut untuk menyimpan data dan berbagi data. Dibalik kemudahan penggunaan teknologi tersebut, ada baiknya menyimpan data dengan sangat baik agar terbebas dari serangan yang tidak diinginkan. Keamanan data adalah masalah penting bagi setiap organisasi. Setiap institusi atau lembaga harus memiliki pencegah akses terbuka dari pihak yang tidak aman [1].

Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), telah mendeteksi indikasi peningkatan serangan siber yang menargetkan sistem elektronik di beberapa sektor, termasuk sektor akademik. Untuk mengantisipasi dampak dari serangan siber tersebut, BSSN menghimbau agar setiap organisasi/institusi meningkatkan kewaspadaan dan menerapkan langkah antisipasi terhadap serangan siber tersebut. Salah satu antisipasi yang dihimbau oleh BSSN adalah mengimplementasikan parameter keamanan salah satunya *Intrusion Detection System* [2].

SMK Tarbiyatul Aulad Cikajang merupakan salah satu sekolah di Kabupaten Garut yang mempunyai jaringan lokal yang terintegrasi dengan internet dan biasa digunakan oleh siswa maupun guru dalam menunjang pembelajaran, seperti untuk menyimpan data dan berbagi data. Selain itu jaringan lokal di SMK Tarbiyatul Aulad Cikajang juga sering digunakan untuk kegiatan Ujian Sekolah Berstandar Komputer (USBK) dan Asesmen Nasional Berbasis Komputer (ANBK). Apabila terjadi serangan terhadap server dalam jaringan tersebut, maka akan membuat server sulit untuk diakses oleh siswa maupun oleh guru. Peran administrator jaringan sangat penting untuk keamanan data karena mempunyai akses penuh dalam jaringan. Seorang administrator harus mampu memberikan keamanan terhadap data yang masuk di dalam jaringan tersebut. Selain itu, administrator jaringan harus mengetahui serangan apa yang terjadi pada jaringan tersebut agar administrator jaringan dapat memantau jaringan secara *real time*. Sehingga dibutuhkan *tools* untuk mencatat serangan-serangan apa saja yang terjadi pada jaringan tersebut.

Berdasarkan permasalahan tersebut, maka dapat mengimplementasikan parameter keamanan jaringan yaitu *Intrusion Detection System* (IDS). *Intrusion Detection System* (IDS) adalah perangkat yang secara otomatis dapat memantau lalu lintas jaringan yang mencurigakan. IDS memberi tahu administrator sistem dan jaringan jika terjadi anomali

ISSN **2797-815X**
P-ISSN **2797-8745**

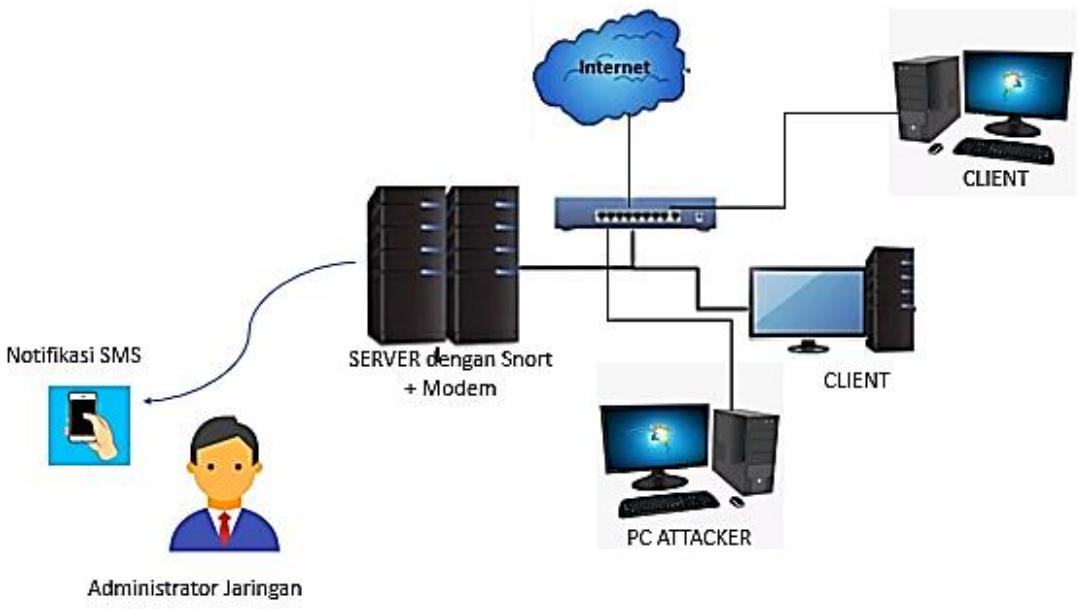
atau kecurigaan terhadap paket yang masuk. Salah satu IDS terbaik adalah *Snort*. *Snort* merupakan sebuah perangkat lunak yang sumbernya bersifat bebas *(open source)* dan konfigurasi mudah serta penggunaan *rules* yang fleksibel. Ketika serangan baru terjadi dapat dengan mudah menambahkannya ke *rules database*. *Snort* juga memiliki kemampuan untuk menganalisis paket data mentah[3]. Untuk memonitoring jaringan tersebut dapat menggunakan SMS *Gateway*, dimana dengan adanya SMS *Gateway* ini akan memudahkan administrator jaringan sehingga dapat memantau jaringan tidak hanya di depan komputer karena SMS *Gateway* akan memberikan notifikasi berupa SMS ketika ada serangan yang mencurigakan masuk secara *real time*. Selain itu, SMS *Gateway* dapat diterima oleh semua jenis *handphone*.

2. Metode

Metode yang digunakan untuk mendapatkan data yang akurat yaitu dengan melakukan studi literatur, observasi lapangan, penyiapan kebutuhan sistem, dan pengujian sistem. Studi literature dan observasi lapangan dilakukan untuk mencari data sebelum sistem diterapkan. Penyiapan kebutuhan dilakukan untuk mempersiapkan *hardware* dan *software* yang digunakan dalam penelitian termasuk merancang skema jaringan untuk sistem yang akan diterapkan. Pengujian dilakukan dengan mengunakan serangan jaringan berupa *port scanning* menggunakan Zenmap dan DDOS *attacks* menggunakan LOIC. Pengujian dilakukan pada saat sistem sebelum dan setelah diterapkan. Hal ini dilakukan agar dapat terlihat perbedaan sebelum dan setelah sistem diterapkan.

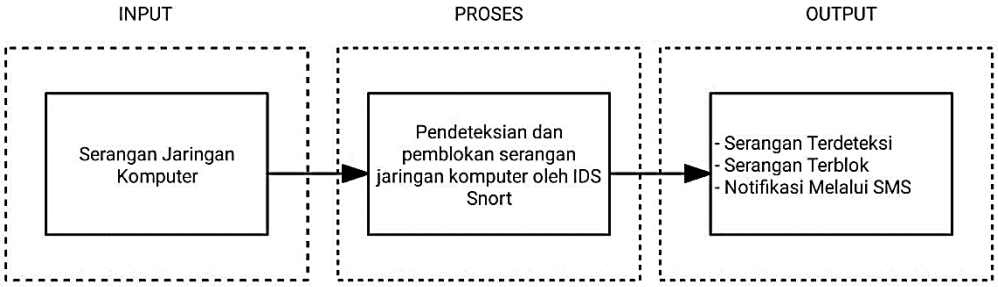
2.1 Skema Jaringan

Pada Gambar 1, terdapat server yang telah diterapkan sistem kemudian terdapat PC Attacker yang digunakan untuk menguji sistem. Setelah sistem diterapkan, *administrator* jaringan akan mendapatkan notifikasi SMS apabila terjadi serangan jaringan.



Gambar 1. Skema Jaringan

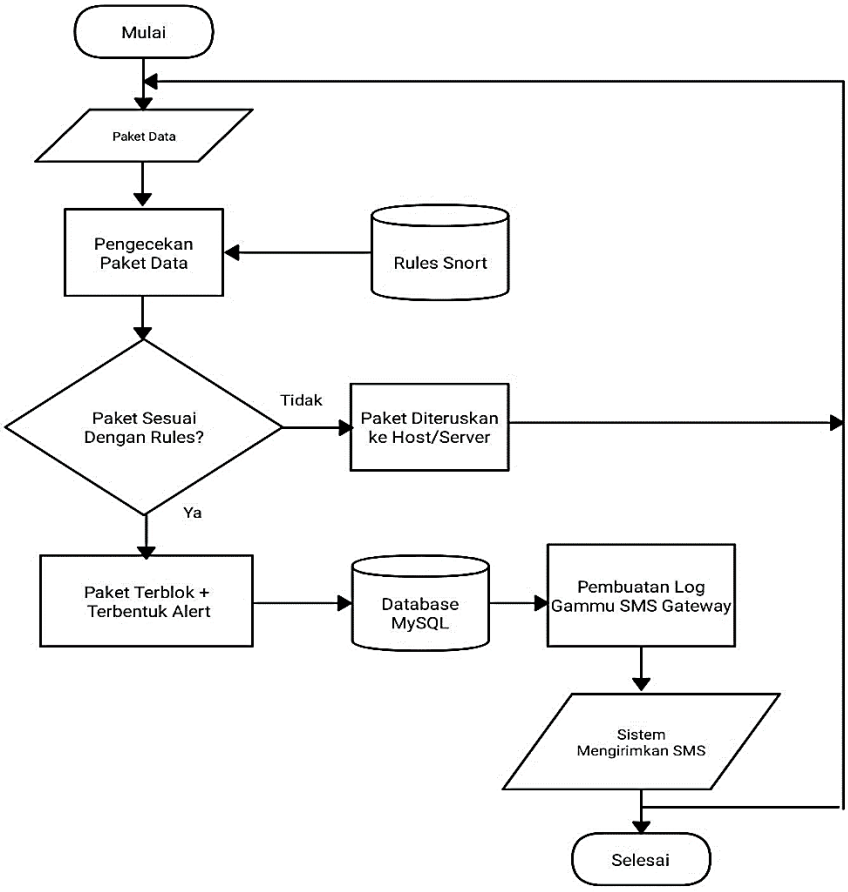
2.2 Diagram Blok



Gambar 2. Diagram Blok.

Pada gambar 2, terlihat bahwa terdapat beberapa bagian pada blok diagram, yaitu ada *input*, proses dan *output*. Pada bagian input terdapat serangan jaringan komputer menggunakan jenis serangan *port scanning* dan DDOS *attacks* yang dilakukan dengan menggunakan aplikasi serangan. Pada bagian proses terdapat sistem *Intrusion Detection System* (IDS) *Snort*, pada proses ini dapat mendeteksi serangan jaringan komputer yang terjadi dan juga dapat memblok serangan yang terjadi dengan mengkonfigurasi *snort*nya. Pada bagian *output* serangan akan terdeteksi dan terblok oleh sistem dan akan ada notifikasi berupa SMS kepada administrator jaringan pada saat terjadi serangan secara *real time*.

2.3 *Flowchart*



Gambar 3. *Flowchart.*

ISSN **2797-815X**
P-ISSN **2797-8745**

Gambar 3, menjelaskan tentang tahapan-tahapan dari sistem yang dirancang, tahapan tersebut adalah sebagai berikut.

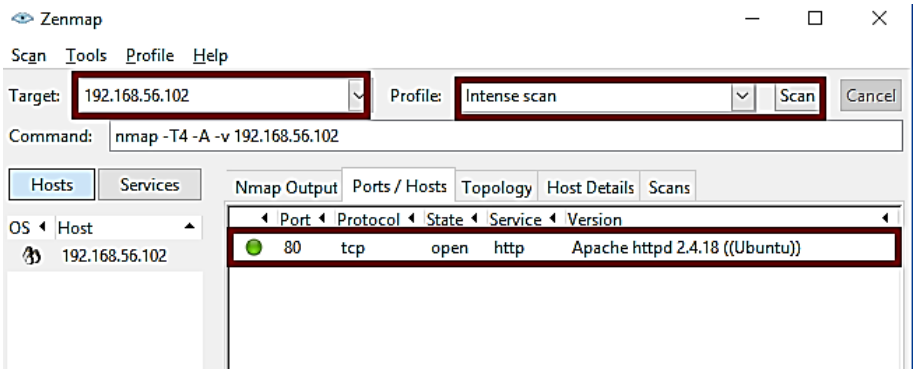
1. PC *Attackers* akan memberikan paket data berupa serangan jaringan terhadap sistem IDS yang telah dirancang, kemudian IDS dengan *Snort* akan mendeteksi paket data yang masuk dan mencocokkannya dengan *rules* yang telah dibuat dan dikonfigurasi dalam sistem.
2. Apabila paket yang masuk ke dalam jaringan sesuai dengan *rules* yang ada di sistem, maka sistem akan mendeteksi paket yang masuk sebagai serangan yang membahayakan dan *Snort* akan memblok paket yang masuk dan menyimpannya sebagai *log* di dalam *My*SQL kemudian sistem akan mengirimkan notifikasi melalui SMS menggunakan *gammu* SMS *Gateway*. Setelah itu sistem akan mengecek kembali paket data yang masuk selanjutnya.
3. Apabila paket yang terdeteksi tidak sesuai dengan *rules* yang ada di sistem, paket akan langsung diteruskan ke *host/ server***.** Setelah itu sistem akan mengecek kembali paket data yang masuk selanjutnya.

3. Hasil dan Pembahasan

Hasil yang didapatkan berupa data hasil dari pengujian sebelum dan sesudah sistem diterapkan. Berikut adalah hasil pengujiannya:

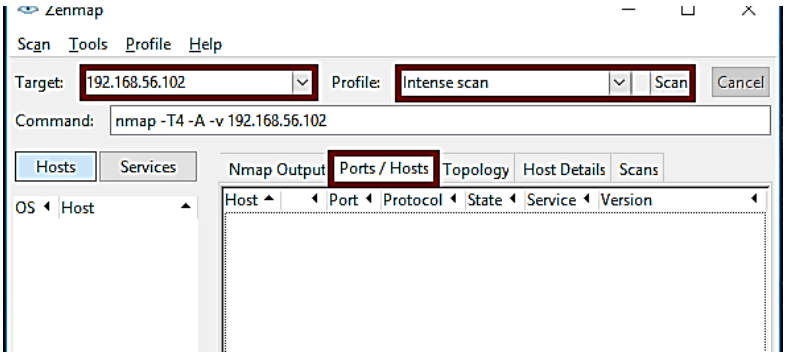
3.1 Hasil Pengujian *Port Scanning* Sebelum dan Setelah Sistem Diterapkan

Port Scanning adalah serangan yang bekerja dengan mencari *port* yang terbuka pada suatu jaringan komputer. Hasil dari *port scanning* akan didapatkan letak kelemahan sistem jaringan komputer tersebut[4]. Pengujian dilakukan dengan menggunakan Zenmap. Hasil dari pengujian *port scanning* sebelum sistem diterapkan dapat dilihat pada Gambar 4.



Gambar 4. Pengujian *Port Scanning* Sebelum Sistem Diterapkan

Berdasarkan hasil pengujian *port scanning* sebelum diterapkan sistem dapat terlihat bahwa ada 1 *port* dari server dengan *IP Address* 192.168.56.102 yang terbuka yaitu *port* 80 dengan protokol HTTP. Setelah sistem diterapkan, tidak ada *port* yang terdeteksi karena diblok oleh sistem, seperti terlihat pada Gambar 5.



Gambar 5. Pengujian *Port Scanning* Setelah Sistem Diterapkan

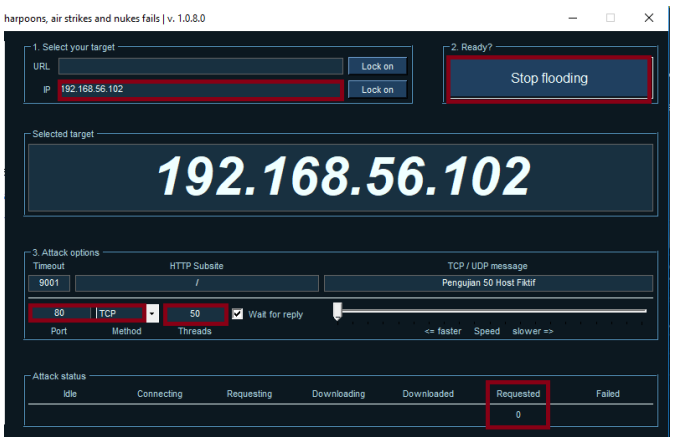
3.2 Hasil Pengujian DDOS *attacks* Sebelum dan Setelah Sistem Diterapkan

Distributed Denial of Service (DDOS) merupakan salah satu serangan yang bekerja dengan cara mengirimkan *request* ke server berulang kali dengan bertujuan membuat server menjadi sibuk menanggapi *request* dan server akan mengalami kerusakan atau *hang* [5]. *Connectivity attack* membanjiri komputer dengan volume *request* koneksi yang tinggi, sehingga semua *resources* (sumber daya) sistem operasi komputer yang ada tidak dapat memproses lebih lama permintaan dari pengguna yang sah[6].
Pengujian DDOS *attack* menggunakan *Low Orbit Ion Cannon* (LOIC). Hasil pengujian sebelum sistem diterapkan dapat menyebabkan kinerja sistem meningkat, seperti terlihat pada tabel 1.

Tabel 1. Data Hasil Serangan DDOS *Attack* Sebelum Sistem Dibuat

No	Jumlah *Host*	Waktu	CPU	Memori	Riwayat Jaringan	
					Kecepatan	Total
1	50	10 menit	26,6 %	908.4 MB (60.8%)	3 - 6 M/s	1018 MB
2	500	10 menit	31,1 %	916.9 MB (60.9%)	2.5 – 5 M/s	1.1 GB
3	1000	10 menit	37,2%	919 MB (61.5%)	2.5 – 5 M/s	1.2 GB

Hasil pengujian setelah sistem diterapkan, *attacker* tidak dapat memberikan *host fiktif* kepada server sehingga kinerja server normal seperti biasa. PC *Attacker* di blok dan tidak dapat melakukan DDOS *attacks* terhadap server, seperti terlihat pada Gambar 6.



Gambar 6. Hasil Pengujian DDOS *Attack* Setelah Sistem Diterapkan

ISSN **2797-815X**
P-ISSN **2797-8745**

3.3 Notifikasi Ketika Terjadi Serangan Setelah Sistem Diterapkan

Ketika sistem diterapkan ketika ada serangan terjadi maka akan ada notifikasi melalui *console* / terminal dan juga notifikasi melalui SMS [7]. Dari hasil pendeteksian serangan tersebut, terdapat waktu yang dapat dilihat ketika serangan itu terdeteksi. Hasil pendeteksian serangan tersebut dapat dilihat pada tabel 2.

Tabel 2. Data Waktu Pendeteksian Serangan

NO	JENIS SERANGAN	WAKTU SERANGAN TERJADI		*DELAY*
		CONSOLE	NOTIFIKASI SMS	
1.	*Port scanning*	09:18:22	09:18:24	2 detik
2.	DDOS *attacks*	09:33:17	09:33:19	2 detik

Berdasarkan tabel 2, ketika serangan terdeteksi, perbandingan waktu yang terdeteksi di *console* dan pada saat notifikasi SMS terdapat *delay* yaitu selama 2 detik.

4. Kesimpulan

Sistem yang telah dibuat berhasil diterapkan dimana pada saat sebelum pengujian sistem dapat diserang oleh *Attacker.* Sedangkan setelah sistem diterapkan, *Attacker* tidak dapat melakukan serangan dan langsung diblok. Ketika ada serangan terdapat notifikasi melalui SMS dan terdapat *delay* 2 detik apabila dibandingkan dengan pendeteksian di *console*.

Ucapan Terima Kasih

Puji dan syukur penulis panjatkan kepada Allah SWT atas berkat dan rahmat-Nya, penulis dapat menyelesaikan penelitian ini. Penulis menyadari penelitian ini tidak akan selesai tanpa bantuan dari berbagai pihak. Untuk itu, penulis mengucapkan terima kasih kepada Program Studi Teknik Elektro di Fakultas Teknik, Universitas Garut dan semua pihak yang telah terlibat dalam penelitian ini.

Daftar Pustaka

[1] T. Aprilianto, S. Jatmika, and I. Wicaksono, "Perancangan Sistem Pendeteksi Serangan Pada Server Jaringan Komputer Menggunakan *Snort* Berbasis SMS *Geteway*," *J. Tek.*, vol. 11, no. 1, p. 1055, 2019.

[2] Anonim, "Peringatan Indikasi Peningkatan Aksi Peretasan Sistem Elektronik di Indonesia," 2021. [Online]. Available: https://bssn.go.id/peringatan-indikasi-peningkatan-aksi-peretasan-sistem-elektronik-di-indonesia/. [Accessed: 05-Mar-2022].

[3] Anonim, "*Snort - Network Intrusion Detection & Prevention System*" 2021. [Online]. Available: https: /www.*snort*.org/. [Accessed: 06-Mar-2022].

[4] A. Syaimi, P. Utami, L. Lidyawati, and Z. Ramadhan, "Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan *SNORT* IDS dan

Honeyd," *J. Reka Elkomika ©TeknikElektro | Itenas J. Online Inst. Teknol. Nas. J. Reka Elkomika*, vol. 1, no. 4, pp. 2337–439, 2013.

[5] R. Hermawan, "Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)," *Anal. Konsep Dan Cara Kerja Serangan Komput. Distrib. Denial Serv.*, vol. 5, no. 1, pp. 1–14, 2013.

[6] D. T. Yuwono, "*Analysis Performance Intrusion Detection System in Detecting Cyber-Attack on Apache Web Serve*r," *IT J. Res. Dev.*, vol. 6, no. 2, pp. 169–178, 2022.

[7] 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.

ISSN **2797-815X**
P-ISSN **2797-8745**