e-ISSN: 2655-867X
p-ISSN: 2655-8611
Volume 7 No. 1 Februari 2025

Intrusion Detection System Menggunakan Snort dan Telegram Sebagai Media Notifikasi

Danu Satin S, Wahyuddin, Ahmad Kautsar, Agus Setyawan
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Serang Raya
Email: danu_s@gmail.com; wahyu.unsera@gmail.com; akautsar@gmail.com; agus.setyawan.unsera@gmail.com.

Diterima:	Diterima Setelah Revisi:	Dipublikasikan:
21 Januari 2025	13 Februari 2025	27 Februari 2025

Abstrak

Intrusion Detection System (IDS) merupakan perangkat atau mekanisme yang dirancang untuk memantau, menganalisis, dan mendeteksi aktivitas mencurigakan dalam jaringan atau sistem komputer, serta melindungi infrastruktur teknologi informasi dari ancaman keamanan seperti serangan siber dan akses tidak sah. Snort, sebagai salah satu solusi IDS, mampu menganalisis lalu lintas jaringan secara real-time dan mendeteksi berbagai ancaman, seperti buffer overflow, port scanning, dan serangan DoS. Penelitian ini menggunakan kombinasi perangkat keras dan perangkat lunak yang diterapkan pada jaringan komputer. Pengujian awal memanfaatkan integrasi Bot Telegram untuk memberikan notifikasi serangan, sedangkan pengujian akhir menilai kemampuan Snort dalam mendeteksi serangan lainnya, seperti DoS, FTP login, dan port scanning. Hasil penelitian menunjukkan bahwa IDS Snort efektif mendeteksi berbagai tipe serangan dengan sistem operasi penyerang yang berbeda, termasuk serangan Port Scan, Ping of Death, FTP, TCP Synflood, dan Denial of Service. Hal ini mengukuhkan Snort sebagai solusi penting dalam meningkatkan keamanan jaringan di era digital.

Kata Kunci: Intrusion Detection System, IDS, Snort, Keamanan Jaringan, Serangan Siber.

Abstract

Intrusion Detection System (IDS) is a device or mechanism designed to monitor, analyze, and detect suspicious activities within a network or computer system, protecting IT infrastructure from security threats such as cyberattacks and unauthorized access. Snort, as one of the IDS solutions, is capable of analyzing network traffic in real-time and detecting various threats, including buffer overflow, port scanning, and DoS attacks. This study employs a combination of hardware and software implemented in a computer network. Initial testing utilized Telegram Bot integration to deliver attack notifications, while the final testing evaluated Snort's capability to detect other types of attacks, such as DoS, FTP login, and port scanning. The results demonstrate that the Snort IDS effectively detects various types of attacks with different attacker operating systems, including Port Scan, Ping of Death, FTP, TCP Synflood, and Denial of Service attacks. These findings establish Snort as an essential solution for enhancing network security in the digital era.

Keywords: *Intrusion Detection System, IDS, Snort, Network Security, Cyberattacks.*

1 PENDAHULUAN

Sistem Deteksi Intrusi (*Intrusion Detection System*, IDS) merupakan salah satu komponen penting dalam keamanan jaringan komputer. IDS berfungsi untuk memantau dan menganalisis aktivitas jaringan guna mendeteksi adanya intrusi atau pelanggaran kebijakan yang dapat membahayakan sistem. Dengan meningkatnya kompleksitas serangan siber, penting bagi organisasi untuk mengimplementasikan IDS yang efektif dan efisien untuk melindungi aset digital mereka (Widodo & Aji, 2022);(Jain & Waoo, 2023).

IDS dapat dibedakan menjadi dua kategori utama: *Network-based Intrusion Detection Systems* (NIDS) dan *Host-based Intrusion Detection Systems* (HIDS). NIDS menganalisis lalu lintas jaringan untuk mendeteksi serangan, sedangkan HIDS memantau aktivitas pada sistem individu. Keduanya memiliki pendekatan yang berbeda dalam mendeteksi intrusi, dan sering kali digunakan secara bersamaan untuk meningkatkan keamanan (Pramila & Gayathri, 2022); (Alviana & Sumitra, 2018). Dalam konteks ini, teknologi pembelajaran mesin dan algoritma canggih, seperti *Neural Networks* dan *Random Forest*, telah diadopsi untuk meningkatkan akurasi deteksi intrusi (Ho et al., 2021); (Putri et al., 2021).

Salah satu tantangan utama dalam implementasi IDS adalah kemampuan untuk memberikan notifikasi secara real-time kepada administrator jaringan. Beberapa penelitian menunjukkan bahwa sistem yang tidak mampu memberikan peringatan tepat waktu dapat menyebabkan serangan tidak terdeteksi, sehingga memberikan celah bagi peretas untuk mengeksploitasi sistem (Purnama, 2023); (Riza, 2022). Oleh karena itu, pengembangan metode notifikasi yang lebih baik, seperti penggunaan aplikasi pesan instan, telah diusulkan untuk meningkatkan respons terhadap ancaman (Purnama, 2023).

Selain itu, IDS juga harus mampu mendeteksi serangan yang belum dikenal atau varian dari serangan yang sudah ada. Pendekatan tradisional sering kali tidak cukup untuk menangani ancaman baru yang muncul, sehingga diperlukan metode yang lebih adaptif dan canggih (Zhu, 2019); (Majidpour & Hasanzadeh, 2020). Penelitian terbaru menunjukkan bahwa penggunaan algoritma pembelajaran mendalam (*deep learning*) dapat meningkatkan kemampuan IDS dalam mendeteksi serangan yang kompleks dan beragam (Majidpour & Hasanzadeh, 2020); (Simanjuntak, 2024). Dalam konteks keamanan siber yang lebih luas, IDS berfungsi sebagai garis pertahanan pertama dalam melindungi sistem dari berbagai ancaman, mulai dari pencurian data hingga serangan yang merusak infrastruktur digital. Dengan meningkatnya ketergantungan pada teknologi informasi, penting bagi organisasi untuk terus memperbarui dan meningkatkan sistem deteksi intrusi mereka agar tetap efektif dalam menghadapi ancaman yang terus berkembang (Maulani, 2023).

Intrusion Detection System (IDS) memiliki peran vital dalam menjaga keamanan jaringan dari berbagai ancaman siber. Snort dapat menganalisis lalu lintas jaringan secara real-time, mendeteksi potensi ancaman seperti serangan *buffer overflow*, *port scanning*, dan akses tidak sah. Dengan kombinasi keandalan, efisiensi, dan kemampuan adaptasi, Snort menjadi salah satu solusi IDS yang sangat penting untuk meningkatkan keamanan jaringan di era digital.

2 KAJIAN PUSTAKA

Sistem Deteksi Intrusi (IDS) memantau lalu lintas data yang melewati jaringan dan bertindak apabila mendeteksi adanya aktivitas yang tergolong sebagai ancaman atau penyusupan. IDS bekerja berdasarkan daftar pola atau tanda tangan serangan yang mencerminkan sistem sedang berada di bawah ancaman atau telah terjadi insiden keamanan. IDS memberikan lapisan pertahanan awal yang esensial dalam menghadapi potensi serangan siber. Ketika upaya akses tidak sah dilakukan terhadap server jaringan, bukti aktivitas tersebut dapat tercatat dalam log sistem, meskipun penyerang berpengalaman sering mencoba menghapus jejak tersebut.

IDS berbasis host memantau aktivitas mencurigakan di setiap sistem, sementara IDS jaringan dapat mendeteksi serangan seperti fragmentasi paket data dengan memeriksa log lalu lintas.

e-ISSN: 2655-867X
p-ISSN: 2655-8611
Volume 7 No. 1 Februari 2025

Walaupun deteksi intrusi secara *real-time* mungkin masih sulit dicapai sepenuhnya, IDS berperan penting sebagai alarm awal terhadap serangan, memungkinkan respons cepat, pencegahan kerusakan, dan pemberitahuan kepada pengguna serta penyimpanan data yang aman.

Snort memiliki arsitektur modular yang memungkinkan integrasi berbagai teknik deteksi, termasuk analisis protokol, pencarian konten, dan analisis lalu lintas (Dharma, 2023), (Widiyanto, 2022). Dengan kemampuan ini, Snort dapat beradaptasi dengan berbagai jenis serangan yang terus berkembang, di mana penyerang sering kali memodifikasi taktik mereka untuk menghindari deteksi (Khraisat & al., 2019). Selain itu, Snort juga dapat berfungsi sebagai sistem pencegahan intrusi (*Intrusion Prevention System* - IPS), yang tidak hanya mendeteksi tetapi juga dapat mengambil tindakan untuk menghentikan serangan yang terdeteksi (Widiyanto, 2022);(Tasneem & al., 2018).

Dalam penerapannya, Snort telah digunakan dalam berbagai lingkungan, termasuk sistem kontrol industri (*Industrial Control Systems* - ICS) dan komputasi awan (*cloud computing*). Dalam konteks ICS, Snort dapat disesuaikan untuk mengatasi tantangan yang dihadapi oleh jaringan yang terisolasi, sehingga memberikan keamanan yang lebih baik tanpa mengganggu integritas operasional (Chen, 2024). Di lingkungan cloud, Snort dapat diintegrasikan dengan langkah-langkah keamanan lainnya untuk memberikan perlindungan menyeluruh terhadap ancaman berbasis jaringan (Muhammad, 2023).

Evaluasi kinerja Snort menunjukkan bahwa meskipun efektif dalam mendeteksi berbagai jenis serangan, ia mungkin menghadapi tantangan dalam lingkungan jaringan berkecepatan tinggi dibandingkan dengan IDS lain seperti *Suricata*, yang dapat menangani *throughput* lebih besar dengan konsumsi sumber daya yang lebih rendah (Shah & Issac, 2018); (Hu & al., 2020). Namun, popularitas *Snort* tetap tinggi di kalangan organisasi karena kemampuannya yang kuat dalam deteksi dan dukungan komunitas yang luas yang terus memperbarui aturan dan fitur (Dharma, 2023), (Abdulrezzak & Sabir, 2023).

2.1 Komponen *Snort*

Snort dibagi kedalam beberapa komponen, komponen tersebut bekerjasama untuk mendeteksi serangan yang berbeda dan untuk menghasilkan keluaran pada format yang diinginkan pada sistem deteksi.

1. Dekoder Paket
   Dekoder paket mengambil paket dari beberapa jenis jaringan yang berbeda antarmuka jaringan dan mempersiapkan paket untuk di proses atau di kirim menuju *detection engine*. Antarmukanya dapat berupa *Ethernet*, SLIP, PPP dan yang lain.
2. *Preprocessor*
   Preprocessor merupakan komponen atau *plug-ins* yang dapat digunakan pada snort untuk menyusun atau mengubah paket data sebelum *detection engine* melakukan beberapa operasi untuk mencari informasi jika paket digunakan oleh penyusup. *Preprocessor* pada snort dapat mendekode-kan URL HTTP, men-defragmentasi paket, menggabungkan kembali aliran TCP dan yang lain. Fungsi ini merupakan bagian yang sangat penting pada sistem deteksi intrusi.
3. *Detection Engine*
   Detection engine merupakan bagian dari snort yang sangat bergantung pada waktu tanggap. Waktu tanggap merupakan waktu yang dibutuhkan untuk merespon paket, hal ini bergantung pada seberapa bagus server yang ada dan seberapa banyak *rules* yang telah didefinisikan. Berikut hal-hal yang mempengaruhi waktu tanggap pada *detection engine* : jumlah *rules*, kekuatan mesin pada sistem, kecepatan bus internal server snort, dan beban pada jaringan

2.2 *Raspberry* Pi

Raspberry Pi adalah salah satu jenis komputer *single board* seukuran kartu kredit yang di kembangkan di Inggris. *Raspberry* Pi dikenalkan oleh yayasan yang dikenal sebagai *Raspberry* Pi

e-ISSN: 2655-867X
p-ISSN: 2655-8611
Volume 7 No. 1 Februari 2025

Foundation. Disebut single board karena semua komponen yang di butuhkan komputer seperti prosesor, memory dan lainnya ada dalam satu papan tunggal. *Raspberry* PI dikembangkan dengan teknik SOC (*System on Chip*) sehingga ukurannya menjadi lebih kecil dan ringkas.

Gambar 1. Raspberry Pi
sumber: en.wikipedia.org

2.3 *Telegram Bot*

Telegram bot adalah sebuah bot atau robot virtual chat yang diprogram secara khusus dengan berbagai perintah untuk menjalankan serangkaian instruksi yang diberikan oleh pengguna. Terdapat dua jenis:

1. *Bot API*
   Bot resmi yang disediakan oleh developer telegram yang merupakan entity tersendiri bot dengan api ini mempunyai kelebihan menerima dan menjalankan perintah dengan batasan yang sudah di tentukan oleh telegram.
2. *Bot Prototype*
   Bot yang tidak disupport oleh pihak telegram, bot ini di jalankan menggunakan aplikasi *client telegram*/ apliaksi telegram yang sering kita pakai dan menggunakan user resmi, seperti akun telegram kita yang dimodifikasi sedemikian rupa sehingga seolah-olah bot tersebut adalah sebuah user biasa.

3 METODE PENELITIAN

3.1 Alat yang digunakan

Tabel 1. Alat Penelitian

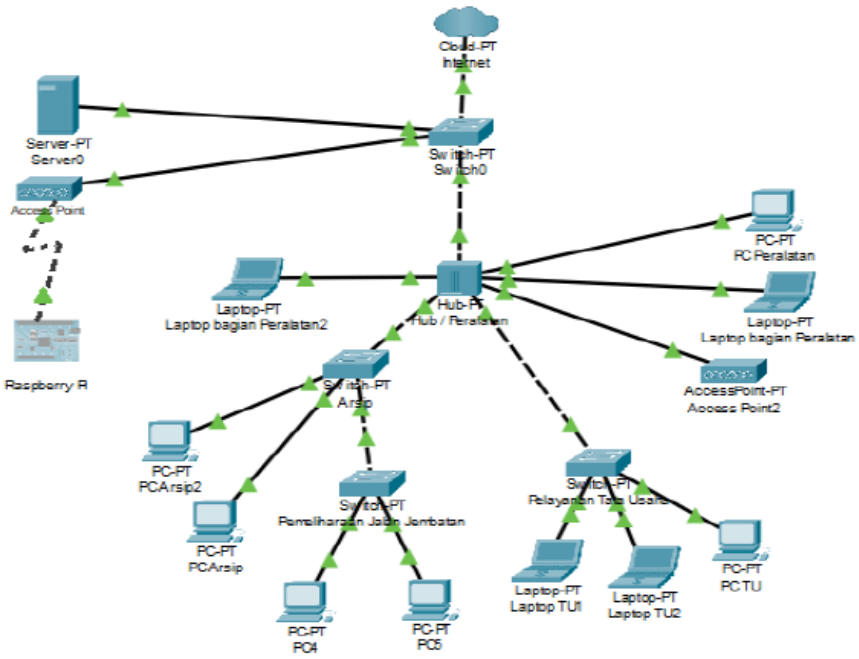
No	Perangkat Keras/Hadware
1	Laptop (untuk test pengujian Traffic data)
2	PC Dekstop (untuk notifikasi via telegram)
3	Kabel jaringan
4	Hp android (untuk notifikasi via Telegram)
5	Raspberry Pi (untuk pemasangan aplikasi)
6	Switch Portable

Tabel 2. Perangkat Lunak

No	Perangkat Lunak/Software
1	Ubuntu
2	Snort
3	Telegram
4	Aplikasi Pen Tester Jaringan

e-ISSN: 2655-867X
p-ISSN: 2655-8611
Volume 7 No. 1 Februari 2025

3.2 Topologi Jaringan



Gambar 2. Topologi Jaringan

3.3 Rancangan Aplikasi

Program Snort IDS dan program Bot Telegram dipasang pada Komputer 1 dan dijadikan system keamanan jaringan IDS Snort, dengan langkah sebagai berikut :

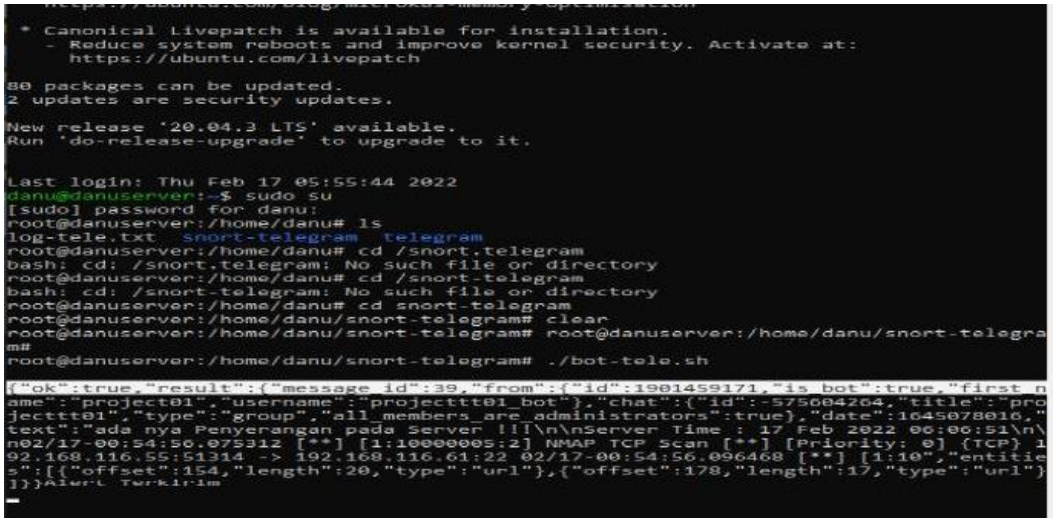
1. Instalasi IDS Snort pada Komputer 1.
2. Lakukan konfigurasi *interface*
3. Buat bot telegram
4. Konfigurasi Snort
5. Konfigurasi *Rule Path*
6. Konfigurasi *Local Rules*
7. Konfigurasi *Nmap Rules*
8. Konfigurasi *Snort Debian*
9. Verifikasi Konfigurasi
10. Konfigurasi Program *bot bash*
11. Membuat hak Akses *Permission*

4 HASIL DAN PEMBAHASAN

4.1 Pengujian Awal

Pengujian awal yang dilakukan adalah dengan melakukan pengecekan fungsi dari Bot Telegram ketika terjadi serangan saat Snort diaktifkan.

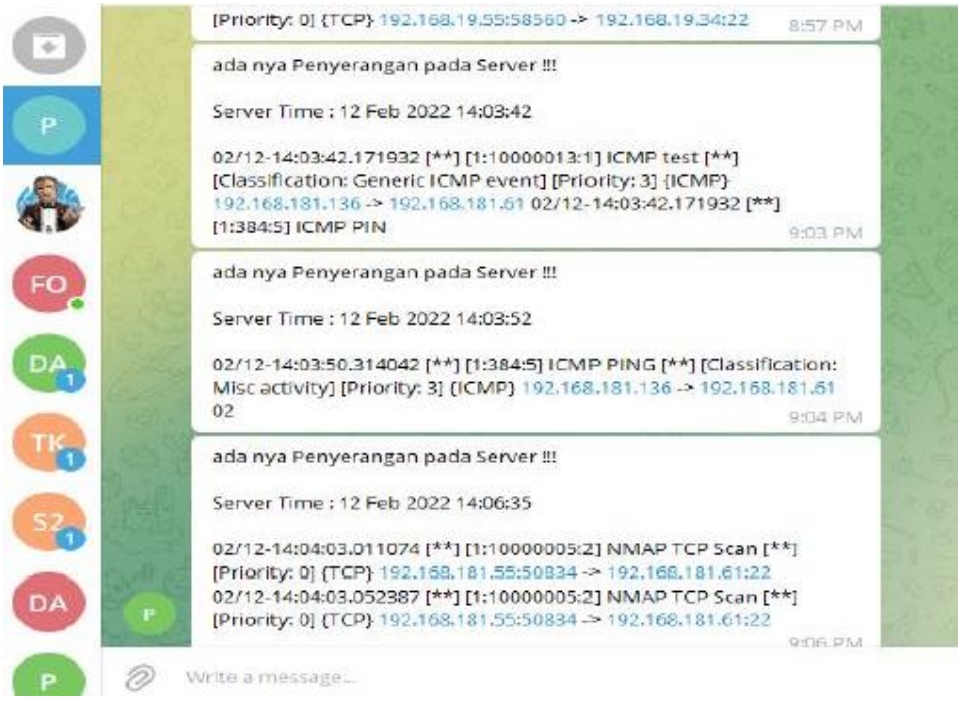
e-ISSN: 2655-867X
p-ISSN: 2655-8611
Volume 7 No. 1 Februari 2025



Gambar 3. *Snort* Status Aktif

Hasil yang diperoleh dalam percobaan fungsi dari bot telegram saat terjadinya penyerangan adalah sebagai berikut:

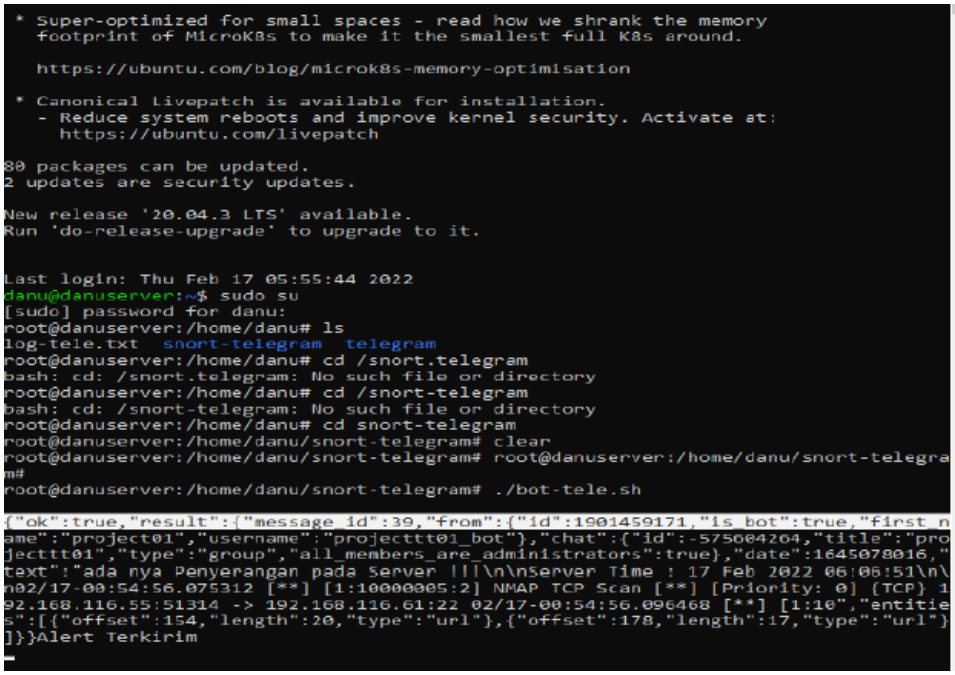
1. Pengujian ping ICMP TEST pada IP Target untuk melihat apakah bot telegram sudah berjalan atau tidak dengan cara melihat hasil Log dan Notifikasi dari Bot Telegram. Saat dilakukan perintah "*ping*", jika konfigurasinya sesuai maka akan terlihat *Log* pada Snort dan Notifikasi di telegram.



Gambar 4. Notofikasi *Alert*.

2. Pegujian serangan ICMP *Ping* dan *Port Scan* pada program *Snort* untuk melihat apakah berhasil atau tidaknya program snort mendeteksi jenis serangan seperti ICMP *Ping* dan *Port Scan*. Saat terdeteksi adanya penyerangan, jika konfigurasi benar maka *snort* akan menampilkan *Log Alert* dan langsung mengirim notifikasi ke telegram.

e-ISSN: 2655-867X
p-ISSN: 2655-8611
Volume 7 No. 1 Februari 2025



Gambar 5. *Log* Penyerangan Snort

4.2 Pengujian Akhir

Pengujian akhir dilakukan melalui pengecekan, apakah snort dapat mendeteksi jenis serangan lain seperti serangan *DoS*, *FTP Login*, *Port Scan* dan lain sebagainya sehingga dapat diketahui sejauh mana fungsionalitas snort dalam mendeteksi serangan.

1. Untuk pengujian pertama dilakukan uji serangan dengan *Port Scan*. Pengujian dilakukan dengan menggunakan program Nmap Scan yang diinstall pada *system* operasi android dan di *custom* dengan Nethunter.

Gambar 6. Hasil Pengujian *Port Scan*

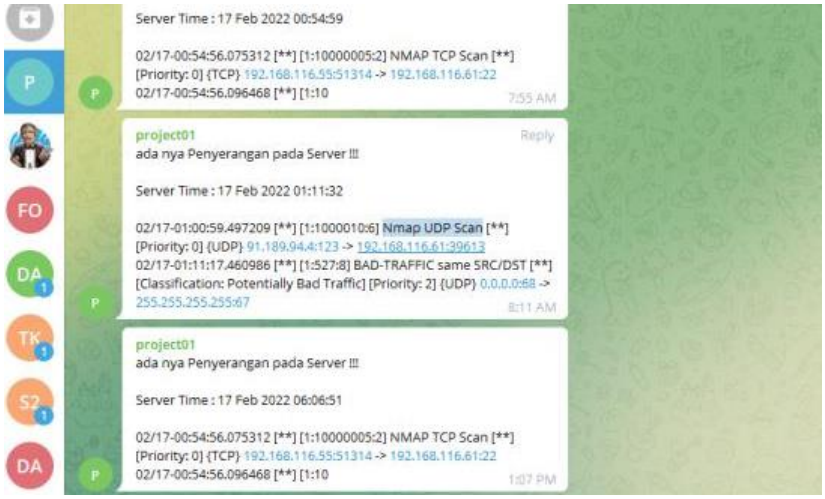
Hasil Pengujian Port Scan pada gambar 6, pada pengujian pertama dapat mendeteksi serangan yang berasal dari *system* operasi android, ditandai oleh adanya permberitahuan *alert* pada *log* snort yang kemudian disusul dengan adanya notifikasi dari telegram bahwa telah terjadi penyerangan dengan tipe penyerangan *NMAP TCP Scan* dengan IP penyerang 192.168.181.136.

e-ISSN: 2655-867X
p-ISSN: 2655-8611
Volume 7 No. 1 Februari 2025

2. Pengujian kedua adalah pengujian serangan *Denial of Service* (DOS) dengan menggunakan program *Low Orbit Ion Cannon* (LOIC). Program Loic ini dipasang pada *system* operasi windows. Berikut adalah hasil dari pengujian serangan dos menggunakan program Loic:

Gambar 7. Hasil Pengujian *Denial of Service*

Hasil pengujian serangan DoS menggunakan program Loic dapat dilihat pada gambar 7. Pada pengujian *Denial of Service*, snort berhasil mendeteksi serangan DoS yang berasal dari *system* operasi windows ditandai oleh adanya permberitahuan *alert* pada *log snort* yang kemudian disusul dengan adanya notifikasi dari telegram bahwa telah terjadi penyerangan. Berikut detail notifikasi yang dihasilkan oleh serangan DoS :



Gambar 8. Detail Notifikasi Pengujian *Denial of Service*

Dalam konteks lalu lintas jaringan yang tinggi, Snort menunjukkan performa yang bervariasi tergantung pada konfigurasi dan lingkungan operasionalnya. Sebuah studi menunjukkan bahwa Snort dapat berfungsi dengan baik dalam mengidentifikasi serangan *Distributed Denial of Service* (DDoS) dalam jaringan yang berbasis Software Defined Networking (Chouikik et al., 2024) , bahwa Snort mampu menangkap data sebelum dan sesudah serangan DDoS, yang menunjukkan kemampuannya dalam mendeteksi dan merespons ancaman secara real-time. Aturan dalam *Snort* dapat mempengaruhi kecepatan deteksi serangan. Semakin banyak aturan yang digunakan, maka semakin lama waktu yang dibutuhkan oleh Snort untuk memproses lalu lintas jaringan dan

mendeteksi serangan. Konsumsi sumber daya *Snort* dapat bervariasi tergantung pada spesifikasi perangkat yang digunakan. Secara umum, Snort memerlukan sumber daya yang cukup untuk menjalankan proses deteksi dan analisis lalu lintas jaringan. Perbandingan efektivitas deteksi *Snort* dengan IDS lain seperti Suricata atau Zeek dapat bervariasi tergantung pada beberapa faktor seperti konfigurasi sistem, jenis serangan yang diuji, dan kompleksitas lalu lintas jaringan yang dianalisis. Pada perangkat dengan spesifikasi rendah, Snort mungkin memerlukan lebih banyak sumber daya CPU dan RAM untuk menjalankan proses deteksi dan analisis. Hal ini dapat menyebabkan kinerja perangkat menjadi lambat dan tidak responsif.

5 SIMPULAN

Hasil dari pengujian awal dan pengujian akhir menunjukkan sistem keamanan jaringan IDS Snort dapat mendeteksi berbagai tipe penyerangan dengan *operating system* penyerang yang berbeda. Jenis serangan yang dapat dideteksi antara lain adalah *Port Scan, Ping of Death, File Transfer Protocol, TCP Synflood, Denial of Service*.

Sistem keamanan jaringan beroperasi non-stop selama 24 jam dan mampu mengirimkan notifikasi alert melalui telegram jika ada serangan terdeteksi. Dengan adanya fitur ini, administrator dapat segera merespons dan mengambil langkah pencegahan yang diperlukan terhadap server yang terancam. Keberadaan sistem ini menjadi krusial dalam menjaga keamanan infrastruktur digital, memastikan bahwa setiap ancaman dapat diidentifikasi secara cepat dan diatasi sebelum dapat menyebabkan dampak serius. Dengan demikian, integritas dan ketersediaan layanan tetap terjaga optimal tanpa mengorbankan keamanan data dan operasional sistem secara keseluruhan.

DAFTAR PUSTAKA

Abdulrezzak, S., & Sabir, F. (2023). An Empirical Investigation on Snort NIDS versus Supervised Machine Learning Classifiers. *Journal of Engineering*. https://doi.org/10.31026/j.eng.2023.02.11

Alviana, S., & Sumitra, I. (2018). Analisis pengukuran penggunaan sumber daya komputer pada intrusion detection system dalam meminimalkan serangan jaringan. *Komputa Jurnal Ilmiah Komputer Dan Informatika*, *7*(1), 27–34. https://doi.org/10.34010/komputa.v7i1.2533

Chen. (2024). A Case Study of Network-Based Intrusion Detection System Deployment in Industrial Control Systems with Network Isolation. *Proceedings of International Conference on Artificial Life and Robotics*. https://doi.org/10.5954/icarob.2024.os1-5

Chouikik, M., Ouaissa, M., Ouaissa, M., Boulouard, Z., & Kissi, M. (2024). Detection and Mitigation of DDoS Attacks in SDN Based Intrusion Detection System. *Bulletin of Electrical Engineering and Informatics*, *13*(4), 2750–2757. https://doi.org/10.11591/eei.v13i4.7570

Dharma. (2023). Network Attack Detection Using Intrusion Detection System Utilizing Snort Based on Telegram. *Bit-Tech*. https://doi.org/10.32877/bt.v6i2.943

Ho, S., Al-Jufout, S., Dajani, K., & Mozumdar, M. (2021). A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network. *IEEE Open Journal of the Computer Society*, *2*, 14–25. https://doi.org/10.1109/ojcs.2021.3050917

Hu, & al., et. (2020). Analysing performance issues of open-source intrusion detection systems in high-speed networks. *Journal of Information Security and Applications*. https://doi.org/10.1016/j.jisa.2019.102426

Jain, J., & Waoo, A. (2023). An artificial neural network technique for prediction of cyber-attack using intrusion detection system. *Journal of Artificial Intelligence Machine Learning and Neural Network*, *32*, 33–42. https://doi.org/10.55529/jaimlnn.32.33.42

Khraisat, & al., et. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*. https://doi.org/10.1186/s42400-019-0038-7

Majidpour, J., & Hasanzadeh, H. (2020). Application of deep learning to enhance the accuracy of

intrusion detection in modern computer networks. *Bulletin of Electrical Engineering and Informatics*, *9*(3), 1137–1148. https://doi.org/10.11591/eei.v9i3.1724

Maulani, I. (2023). Sistem deteksi intrusi cerdas: studi perbandingan algoritma pembelajaran mesin untuk keamanan siber. *Jurnal Sosial Teknologi*, *3*(11), 918–923. https://doi.org/10.59188/jurnalsostech.v3i11.987

Muhammad. (2023). Implementation of IDS Using Snort with Barnyard2 Visualization for Network Monitoring in The Informatics Engineering Computer Lab at Muhammadiyah University Surakarta. *International Journal of Computer and Information System (IJCIS)*. https://doi.org/10.29040/ijcis.v4i4.142

Pramila, P., & Gayathri, M. (2022). Analysis of accuracy in anomaly detection of intrusion detection system using naïve bayes algorithm compared over gaussian model. *ECS Transactions*, *107*(1), 13977–13991. https://doi.org/10.1149/10701.13977ecst

Purnama, T. (2023). Implementasi intrusion detection system (ids) snort sebagai sistem keamanan menggunakan whatsapp dan telegram sebagai media notifikasi. *Jurnal Teknologi Informasi Dan Komunikasi*, *14*(2), 358–369. https://doi.org/10.51903/jtikp.v14i2.726

Putri, N., Zulianto, A., & Suwarningsih, W. (2021). Deteksi intrusi pada basis data menggunakan random forest. *Jurnal ICT Information Communication & Technology*, *20*(2), 387–393. https://doi.org/10.36054/jict-ikmi.v20i2.424

Riza, F. (2022). Sistem deteksi intrusi pada server secara realtime menggunakan seleksi fitur dan firebase cloud messaging. *Jurnal Sistim Informasi Dan Teknologi*. https://doi.org/10.37034/jsisfotek.v5i1.161

Shah, & Issac. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.10.016

Simanjuntak, R. (2024). Meningkatkan keamanan siber dalam lingkungan internet of things (iot) dengan menggunakan sistem deteksi intrusi berbasis pembelajaran mesin. *DIKE*, *2*(2), 62–68. https://doi.org/10.69688/dike.v2i2.106

Tasneem, & al., et. (2018). Intrusion Detection Prevention System using SNORT. *International Journal of Computer Applications*. https://doi.org/10.5120/ijca2018918280

Widiyanto, W. W. (2022). SIMRS Network Security Simulation Using Snort IDS and IPS Methods. *Indonesian of Health Information Management Journal (INOHIM)*, *10*(1), 10–17. https://doi.org/10.47007/inohim.v10i1.396

Widodo, T., & Aji, A. (2022). Pemanfaatan network forensic investigation framework untuk mengidentifikasi serangan jaringan melalui intrusion detection system (ids). *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(1), 46–55. https://doi.org/10.14421/jiska.2022.7.1.46-55

Zhu, L. (2019). A new intrusion detection and alarm correlation technology based on neural network. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1). https://doi.org/10.1186/s13638-019-1419-z