Progresif: Jurnal Ilmiah Komputer
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877
p-ISSN: 0216-3284

Implementasi *Intrusion Prevention System* Menggunakan *Suricata* Sebagai Pengamanan Dari Serangan DDoS

Ismail Heremba[1*], Nourman S. Irjanto[2], Tengadi Boney Bun[3]
Teknik Informatika, Universitas Sepuluh Nopember Papua, Jayapura, Indonesia
*e-mail *Corresponding Author:* ismailheremba013@gmail.com

Abstract

Network security at SMKN 8 ICT Jayapura City is very important to protect data and maintain smooth school operations. Cyber attacks such as Distributed Denial of Service (DDoS) are a serious threat because they can paralyze networks and disrupt the learning process. Suricata, as an Intrusion Prevention System (IPS), plays a role in detecting and preventing attacks by examining data packets in real-time. However, manual security management is a challenge, especially when attacks prevent remote access for remediation. This research aims to implement Suricata as an IPS to proactively prevent attacks, combining IPTables blocking with deep inspection of the IPS. With this solution, SMKN 8 ICT is expected to be able to reduce manual intervention, increase data security, and ensure network stability. Implementing Suricata as an IPS is a strategic step to protect schools from DDoS attacks and support safe administration and learning processes.

Keywords*: Network Security; Cyber Attacks; Distributed Denial of Service*

Abstrak

Keamanan jaringan di SMKN 8 TIK Kota Jayapura sangat penting untuk melindungi data dan menjaga kelancaran operasional sekolah. Serangan siber seperti *Distributed Denial of Service* (DDoS) menjadi ancaman serius karena dapat melumpuhkan jaringan dan mengganggu proses pembelajaran. Suricata, sebagai sistem *Intrusion Prevention System* (IPS), berperan dalam melaksanakan deteksi serta pencegahan serangan dengan memeriksa paket data secara *real-time*. Namun, pengelolaan keamanan yang masih manual menjadi tantangan, terutama saat serangan menghambat akses jarak jauh untuk perbaikan. Penelitian ini bertujuan mengimplementasikan *Suricata* sebagai IPS untuk secara proaktif mencegah serangan, menggabungkan pemblokiran IPTables dengan inspeksi mendalam dari IPS. Dengan solusi ini, SMKN 8 TIK diharapkan dapat mengurangi intervensi manual, meningkatkan keamanan data, dan memastikan stabilitas jaringan. Implementasi *Suricata* sebagai IPS menjadi langkah strategis untuk melindungi sekolah dari serangan DDoS dan mendukung proses administrasi serta pembelajaran yang aman.

Kata kunci: *Keamanan Jaringan; Serangan Siber; Distributed Denial of Service*

1. Pendahuluan

Keamanan jaringan komputer menjadi komponen vital dalam teknologi informasi. Dengan semakin meningkatnya ketergantungan pada jaringan, baik melalui koneksi kabel maupun nirkabel, ancaman terhadap keamanan data menjadi semakin nyata. Kejahatan siber, yang sering kali dilakukan dengan cara memasuki sistem jaringan secara ilegal, dapat berdampak merugikan bagi organisasi. Salah satu ancaman serius yang sering dilalui yakni serangan *Distributed Denial of Service* (DDoS), yang bertujuan untuk membuat server lumpuh dengan membanjirinya dengan lalu lintas yang berlebihan[1].

Keamanan jaringan yang signifikan di SMKN 8 TIK Kota Jayapura. Sekolah ini sangat bergantung pada jaringan komputer untuk kegiatan sehari-hari, namun belum memiliki sistem keamanan jaringan yang memadai. Akibatnya, jaringan komputer sekolah rentan terhadap berbagai serangan siber seperti *Ping Attack, Network Scanning,* dan *DdoS*[2][3]. Kerentanan ini sangat mengkhawatirkan mengingat tingginya tingkat serangan siber di Indonesia[4], termasuk

serangan *DDoS* yang menargetkan institusi pendidikan. Serangan siber tidak hanya mengganggu operasional sekolah, tetapi juga berpotensi membahayakan data sensitif siswa, seperti yang tersimpan dalam aplikasi absensi. Keamanan data siswa menjadi perhatian utama karena data pribadi seperti NISN dan NIK sangat berharga dan rentan disalahgunakan. Kebocoran data dapat merusak reputasi sekolah, menghilangkan kepercayaan dari orang tua dan masyarakat, serta melanggar regulasi perlindungan data. Oleh karena itu, penelitian ini menekankan pentingnya bagi SMKN 8 TIK untuk segera meningkatkan keamanan jaringannya. Mengingat ketergantungan yang semakin besar pada teknologi digital dalam pendidikan, beberapa tahapan keamanan yang kuat sangat penting untuk melindungi data siswa, menjaga kelancaran operasional sekolah, dan memastikan lingkungan belajar yang aman dan terpercaya.

Intrusion Prevention System (IPS) adalah perangkat keamanan jaringan yang memantau dan memblokir aktivitas berbahaya. Dengan menggabungkan kemampuan *firewall* dan inspeksi mendalam, IPS dapat mendeteksi dan mencegah serangan. Sistem memeriksa dan mencatat semua paket data yang masuk, mengenali pola serangan, dan menghentikannya sebelum merusak sistem. IPS memiliki keunggulan yang membedakannya dari alternatif seperti *Content Delivery Network* (CDN), pengaturan tingkat, *blackholing*, dan pusat pembersihan yang biasanya berfokus pada mengurangi dampak setelah serangan[5]. IPS memungkinkan perlindungan menyeluruh terhadap ancaman yang berkembang melalui pencegahan yang proaktif dan terintegrasi. IPS menjadi pilihan yang lebih baik untuk menjamin keamanan jaringan yang berkelanjutan karena dapat merespons ancaman secara cepat dan akurat. Ini terutama berlaku untuk melindungi data absensi dan data siswa dari ancaman siber.

Suricata, selaku sistem deteksi intrusi, menawarkan kemampuan dalam menjalankan deteksi pada aktivitas serangan dengan bantuan aturan yang telah ditetapkan. Namun, banyak sistem pertahanan masih bergantung pada intervensi manual oleh *administrator,* yang sering kali tidak dapat merespons dengan cepat ketika terjadi serangan[4]. Hal ini dapat menyebabkan gangguan signifikan, terutama jika serangan berhasil membuat *server down* dan *administrator* tidak mampu melakukan akses pada sistem dengan cara remote guna melakukan perbaikan.

Berdasarkan permasalahan diatas maka penelitian ini yang "*Implementasi Intrusion Prevention System* (IPS) Menggunakan Suricata Sebagai Pengamanan Dari Serangan DDoS (*Distributed Denial of Service*)" bertujuan untuk mengeksplorasi penerapan solusi keamanan yang lebih efektif[6]. Diharapkan, implementasi ini dapat membuat keamanan jaringan sekolah meningkat serta menjaga data penting dari ancaman serangan DDoS.

2. Tinjauan Pustaka

Pada penilitian yang dilakukan oleh Raihan Fauzi dan ddk pada tahun 2023 yang berjudul "Sistem Keamanan Jaringan Komputer Berbasis Teknik *Intrusion Detection System* (IDS) Untuk Mendeteksi Serangan *Distrubuted Denial Of Service* (DDOS)". Penelitian yang telah dilakukan bertujuan untuk Madrasah Aliyah Negeri Purwakarta merupakan sekolah menengah atas negeri di Kabupaten Purwakarta yang telah menggunakan jaringan komputer untuk mendukung aktivitasnya. Namun, sekolah ini belum menerapkan sistem keamanan jaringan, sehingga rentan terhadap serangan seperti *Ping Attack, Network Scanning*, dan DDoS. Penelitian ini memakai metode *Network Development Life Cycle* (NDLC) yang mencakup lima tahap: analisis, desain, simulasi prototipe, implementasi, serta pemantauan dan manajemen. Hasil penelitian ini adalah rancangan sistem keamanan jaringan dengan basis IDS memakai *Snort dan Portsentry*. Sistem ini mampu mendeteksi serangan seperti Ping ICMP, Nmap (*port scanning*), dan DDoS serta mengirimkan notifikasi saat terjadi serangan. Portsentry juga diterapkan untuk mencegah serangan agar tidak dapat mengakses jaringan sekolah[4].

Pada penelitian Muhammad Khairullah Harto, dan Achmad Basuki pada tahun 2021 dengan judul "Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest". Sejalan akan meningkatnya kompleksitas teknologi jaringan, ancaman serangan DDoS (*Distributed Denial of Service*) semakin menjadi perhatian. Hal ini mendorong kebutuhan akan solusi deteksi yang efektif. Penelitian ini melakukan eksplorasi terhadap penggunaan jaringan SDN (*Software-Defined Networking*) yang dikendalikan oleh Ryu, serta menerapkan algoritma *Random Forest* untuk mengklasifikasikan serangan DDoS. Hasil yang diperoleh menunjukkan angka akurasi yang menjanjikan, yaitu sekitar 90%, dengan waktu deteksi rata-rata mencapai 0,3 detik. Temuan ini membuktikan potensi besar dalam meningkatkan keamanan jaringan terhadap serangan yang terus berkembang. [7].

Pada penelitian yang dilakukan oleh Rayco William pada tahun 2023 Penelitian ini menekankan pentingnya peran *serve*r sebagai komponen utama dalam penyediaan layanan serta penyimpanan data dalam jaringan komputer. Pengelolaan server dilakukan oleh seorang administrator yang bertanggung jawab atas keamanan *server* tersebut. Namun, terdapat beberapa tantangan yang dihadapi, antara lain kesulitan dalam mendeteksi serangan, keterlambatan dalam menerima informasi terkait dengan serangan, serta ketidakefisienan dalam menangani ancaman terhadap *server*. Sebagai solusi atas tantangan tersebut, penelitian ini mengembangkan sistem keamanan *server* yang dilengkapi dengan *Intrusion Prevention System* (IPS) yang terintegrasi dengan aplikasi berbasis web dan *mobile*. Mekanisme deteksi serangan difokuskan pada *Internet Control Message Protocol* (ICMP) dan *Transmission Control Protocol* (TCP), dengan waktu respons sistem sebesar 99,89 milidetik, yang tergolong sangat efisien. Proses mitigasi serangan menggunakan Iptables, di mana sistem *Suricata* mengidentifikasi alamat IP penyerang dan mengklasifikasikan tindakannya ke dalam tiga kategori: *Drop, Reject*, dan *Accept*. Selain itu, administrator dapat mengambil langkah pencegahan segera setelah menerima notifikasi otomatis melalui Telegram, dengan rata-rata waktu pengiriman peringatan sebesar 3,41 detik. Pengujian pada *server* lokal menunjukkan bahwa performa awal CPU berada dalam kisaran 10-19%. Ketika terjadi serangan ping, penggunaan CPU meningkat hingga 21,6%, dengan konsumsi memori mencapai 41,7% dan pemakaian *disk* sebesar 19,6%. Sementara itu, serangan pemindaian *port* menyebabkan lonjakan penggunaan CPU hingga 85,9%, dengan konsumsi memori sebesar 41,9% dan pemakaian disk mencapai 20,3%. Di sisi lain, serangan *ping of death* mengakibatkan pemakaian CPU mencapai puncaknya di angka 90,4%, dengan penggunaan memori sebesar 42,9% dan pemakaian disk sebanyak 20,8%. Berdasarkan simulasi serangan yang dilakukan, peningkatan beban *server* paling signifikan terjadi selama serangan *ping of death*, yang menyebabkan penggunaan CPU mencapai 90,4%. Jikalau serangan ini berlangsung dengan jangka waktu yang panjang, server berisiko untuk tidak responsif atau bahkan mengalami kerusakan sistem. [8].

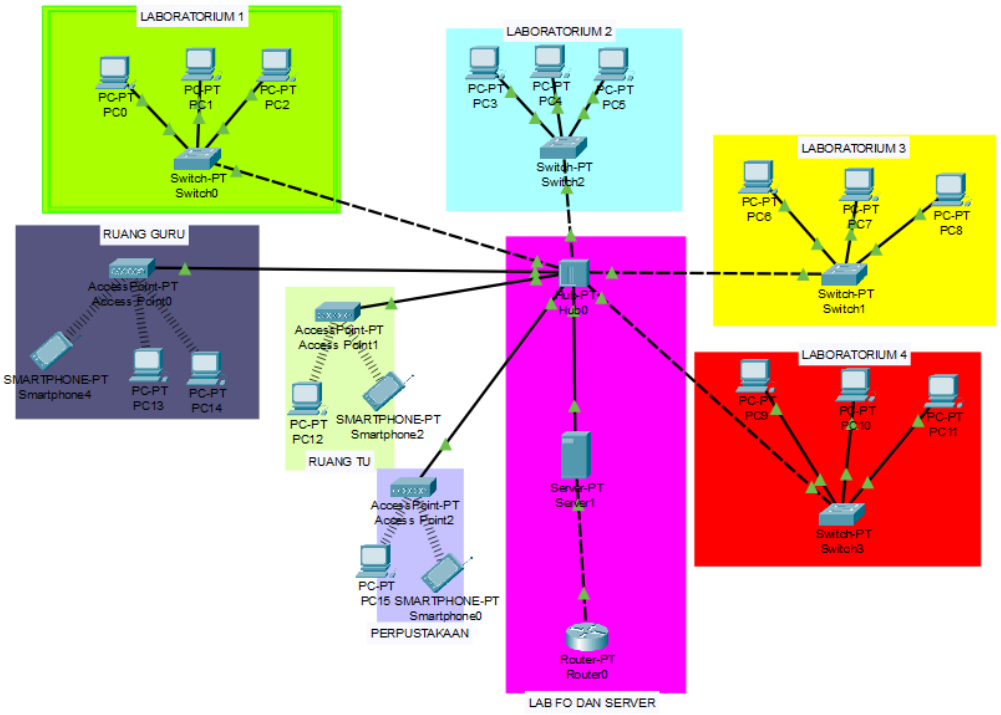
Penelitian ini bertujuan meningkatkan keamanan jaringan di SMKN 8 TIK Kota Jayapura dengan mengimplementasikan *Suricata* sebagai IPS dalam melakukan deteksi serta pencegahan serangan DDoS, seperti hping3 dan Nmap, secara *real-time.* Berbeda dengan pendekatan manual, sistem ini dilengkapi fitur notifikasi otomatis melalui Telegram, memungkinkan respons cepat terhadap ancaman. Di sisi lain, penelitian ini meninjau dampak IPS pada latensi serta *bandwidth* guna memastikan keamanan tidak mengorbankan performa jaringan. Implementasi *Suricata* diharapkan melindungi data penting sekolah dan menjadi model keamanan bagi institusi lain dalam menghadapi serangan siber.

3. Metodologi

3.1 Arsitektur Sistem

Arsitektur sistem yang dipetakan meliputi jaringan lokal SMKN 8 TIK Kota Jayapura yang terhubung ke Internet melalui router utama. Suricata sebagai IPS diinstal pada server khusus dengan *interface* jaringan enp0s3, berfungsi memantau lalu lintas data, mendeteksi ancaman seperti DDoS (hping3, Nmap), dan memblokir serangan secara *real-time.* Sistem ini juga dikonfigurasi untuk mengirim notifikasi otomatis ke Telegram, memberi peringatan kepada admin jaringan.

Topologi jaringan komputer, yang menggambarkan pengaturan fisik atau logis dari koneksi antar perangkat, mengacu pada metode yang dipergunakan dalam menyambungkan sejumlah komputer pada sebuah jaringan. Pola atau struktur koneksi tersebut dapat diwujudkan melalui pemanfaatan kabel fisik maupun teknologi nirkabel [9]. Selama pelaksanaan pengumpulan data, peneliti berhasil memperoleh informasi yang relevan. Data tersebut, yang dikumpulkan melalui metode observasi primer, menghasilkan representasi topologi jaringan di SMK 8. Representasi ini memberikan dasar yang penting bagi peneliti dalam pengembangan sistem yang hendak diimplementasikan bisa disaksikan melalui gambar 2.



Gambar 1 Topologi Jaringan

3.2 Perlatan Penelitian

Penelitian ini dilaksanakan dengan memanfaatkan dua komponen utama, yakni perangkat lunak (*software*) serta perangkat keras (*hardware*).

1) Spesifikasi *Software*

Spesifikasi *software* mengacu pada *software* yang berperan menjadi jembatan pada pelaksanaan penelitian ini. Perangkat lunak yang dipergunakan bisa disaksikan melalui table 1.

Tabel 1 Perangkat Lunak

Nama	Spesifikasi	Kegunaanya
Sistem Operasi	Windows 11	Digunakan untuk pengolahan data hasil uji coba dan pembuatan laporan penelitian.
Sistem Operasi	Ubuntu 24	Menginstal Suricata dan menjalankan IPS untuk mendeteksi serta mencegah serangan DDoS.
Sistem Operasi	kalinux	Melakukan simulasi serangan siber menggunakan tools seperti hping3 dan Nmap.
Mesin Virtual	Virtual box	Membuat lingkungan virtual untuk menguji implementasi Suricata tanpa mengganggu jaringan asli.
Aplikasi Keamanan	suricata	Mengamati lalu lintas jaringan, melaksanakan deteksi, serta pencegahan atas serangan DDoS secara real-time.

2) Spesifikasi Prangkat Keras (*Hardware*)

Spesifikasi perangkat keras adalah perlatan yang digunakan sebagai pendukung dalam melakukan penelitian ini. Table 2 merupakan perangkat keras yang digunakan dalam melakukan penelitian ini.

Tabel 2 Perangkat Keras

Nama	Spesifikasi	Kegunaan	Kegunaan Dalam Uji Coba
Laptop	Lenovo	Mengelola dan memantau Suricata sebagai IPS.	Menjalankan Suricata guna melaksanakan pendeteksian maupun pencegahan mendeteksi dan mencegah serangan DDoS.
Prosessor	Inter core i3 gen 12	Memastikan kinerja optimal dalam menjalankan aplikasi keamanan jaringan	Memproses analisis lalu lintas jaringan secara real-time.
Memori	8GB DDR5 RAM 5600Mhz	Memperlancar multitasking dan analisis paket data	Membantu proses pemantauan serangan dan logging data tanpa lag.
Penyimpanan	512GB PCIe® 4.0 NVMe™ M.2 SSD	Menyimpan log keamanan dan konfigurasi Suricata	Menyimpan data hasil uji coba, seperti log serangan dan analisis performa jaringan.

3) Data Penelitian

Data eksperimen berupa paket data lalu lintas jaringan yang dikumpulkan sebelum dan sesudah implementasi Suricata. Pengujian dilakukan dengan mengirimkan serangan hping3 dan Nmap, serta mengukur parameter seperti jumlah paket yang terdeteksi, tingkat latensi, dan penggunaan bandwidth. Data dikumpulkan dalam 3 skenario: tanpa IPS, IPS aktif tanpa notifikasi, dan IPS aktif dengan notifikasi Telegram.

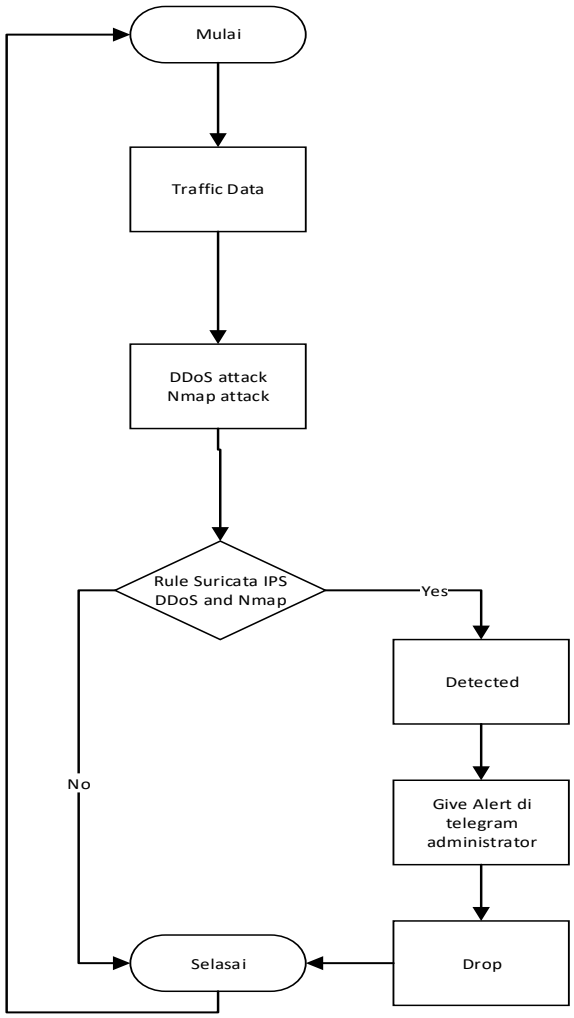
4) Metode Dan Prosedur Eksperimen

Metode : Eksperimen kuantitatif untuk mengukur efektivitas *Suricata* dalam mencegah serangan DDoS.

Prosedur :
1. Instalasi suricata dan konfigurasi IPS serta Telegram Bot
2. Melakukan serangan DDos menggunakan hping3 dan Nmap
3. Mengumpulkan data lalu lintas jaringan menggunakan *Wireshark*
4. Mengukur jumlah serangan terdeteksi, perubahan latensi, dan dampak pada *bandwidth.*
5. Membandingkan hasil pada ketiga scenario untuk menilai efektivitas sistem

Intrusion Prevention System (IPS) ialah perangkat keamanan jaringan yang memantau dan memblokir aktivitas berbahaya secara *real-time*. IPS beroperasi dengan menganalisis lalu lintas jaringan, menlaksanakan pendeteksian pola serangan yang mencurigakan, dan secara otomatis memutuskan tindakan dalam mengupayakan pencegahan serangan sebelum merusak sistem. Dengan memadukan *firewall* dan inspeksi mendalam terhadap paket data, IPS memberikan perlindungan proaktif terhadap berbagai ancaman siber[10][11].

Suricata adalah solusi keamanan jaringan *open sources* yang berfungsi sebagai *Intrusion Detection System* (IDS), IPS, serta *network security monitoring engine*. Dalam konteks IPS, Suricata mampu mendeteksi dan mencegah serangan seperti DDoS dengan menggunakan aturan (*rules*) yang telah dikonfigurasi. Keunggulan utama Suricata terletak pada kemampuannya memproses lalu lintas jaringan secara *multi-threading*, menganalisis paket data di berbagai lapisan jaringan, serta mencatat log serangan untuk analisis lebih lanjut. *Suricata* juga dapat diintegrasikan dengan alat lain untuk meningkatkan efektivitas pemantauan dan respons terhadap serangan[12].



Gambar 2 Skenario Penyerangan DDos Dan *Port Scanning*

Alur kerja IPS menggunakan *Suricata* melibatkan beberapa tahapan penting:

1. **Mulai**: Proses IPS dimulai dengan memantau lalu lintas jaringan (*traffic data*) secara real-time menggunakan Suricata.
2. **Traffic Data**: Semua data yang masuk ke jaringan dikumpulkan dan dianalisis oleh *Suricata*.
3. **Intrusi atau Serangan**: Suricata memeriksa setiap paket data untuk mengidentifikasi potensi ancaman atau serangan.
4. **Pencocokan Aturan** (*Match Rules Database*): Data lalu lintas dibandingkan dengan aturan (rules) yang ada dalam *database Suricata*.
    a. **Jika cocok** (*Yes*): Serangan terdeteksi, kemudian Suricata memberikan peringatan (*Give Alert*) dan mengambil tindakan untuk memblokir atau membuang paket berbahaya (Drop).
    b. **Jika tidak cocok** (*No*): Data dianggap aman dan proses kembali memantau lalu lintas.
5. **Selesai**: Proses ini berjalan secara kontinu, memastikan keamanan jaringan tetap terjaga.

Berdasarkan permasalahan di atas, penelitian ini yang berjudul "Implementasi *Intrusion Prevention System* (IPS) Menggunakan *Suricata* Sebagai Pengamanan Dari Serangan DDoS (*Distributed Denial of Service*)" bertujuan untuk mengeksplorasi penerapan solusi keamanan yang lebih efektif. Diharapkan, implementasi *Suricata* sebagai IPS ini dapat mengupayakan peningkatan keamanan jaringan serta menjaga data fundamental dari ancaman serangan DDoS[13].

4. Hasil dan Pembahasan

Secara umum, pada bagian ini dijabarkan terkait hasil yang didapat melalui tiap tahap penelitian yang dilaksanakan, meliputi

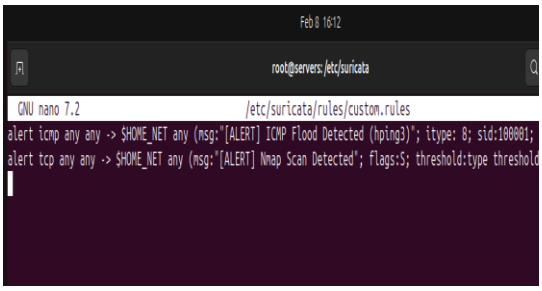
4.1 Implementasi

Implementasi yakni pelaksanaan atau atas suatu rencana yang telah dirancang dengan terperinci sekaligus matang [14]. Biasanya, implementasi dilaksanakan sesudah perencanaan dinilai sempurna. Dalam tahap implementasi, penulis terlebih dahulu melakukan konfigurasi pada sistem *Suricata* yang sebelumnya telah diuji coba. Dalam proses konfigurasi tersebut, peneliti mengatur alamat IP pada server IPS *Suricata* dan Kali Linux untuk penyerang atau pengujian penetrasi, sesuai dengan skema pengujian, berikut adalah data konfigurasi IP *address* bisa disaksikan melalui tabel 1.

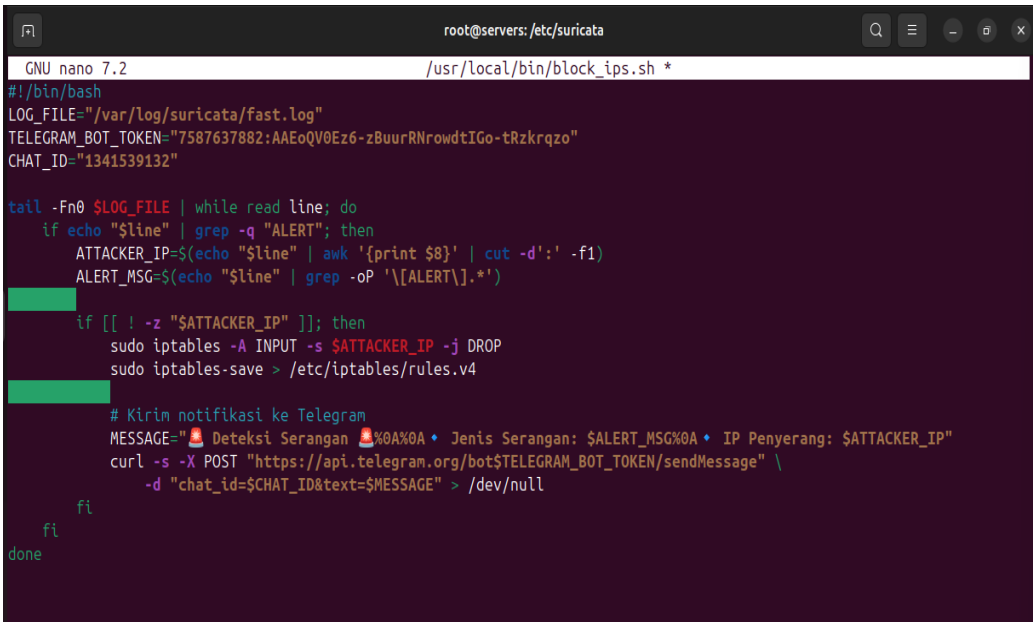
Tabel 1. Konfigurasi IP Address

Ip Address Kali Linux (Penyerang)	Ip Address Ips Suricata
192.168.56.101	192.168.56.108

Suricata dikonfigurasikan untuk mendeteksi serangan tertentu seperti SYN *flood* dan *port scanning*. Ini melibatkan penulisan rules khusus yang mendefinisikan pola lalu lintas jaringan yang mencurigakan. *Rules* ini dimasukkan ke dalam file *custom.rules* di direktori konfigurasi Suricata. *Iptables* digunakan untuk mengarahkan lalu lintas jaringan ke *Suricata*. Ini memungkinkan Suricata untuk berfungsi dalam mode *Intrusion Prevention System* (IPS), di mana dapat memblokir paket yang mencurigakan secara *real-time*. Agar semakin jelas, hal tersebut bisa disaksikan melalui Gambar.



Gambar 3 Konfigurasi *Rule Suricta* & Konfigurasi IP Table



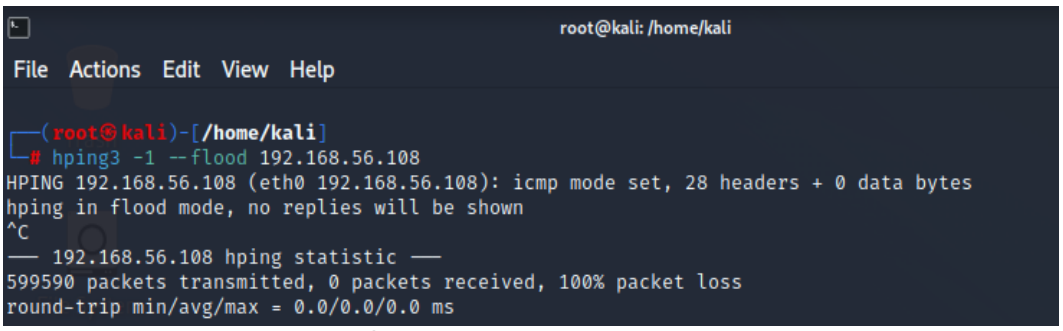
Gambar 4 Konfigurasi Suricata untuk Notifikasi Telegram & Drop IP Penyerangan

Setelah sistem *Suricata* IPS dikonfigurasi untuk mendeteksi dan memblokir serangan, langkah selanjutnya adalah membuat skrip otomatis yang akan Mengambil daftar IP penyerang dari iptables, Memblokir IP tersebut secara permanen menggunakan iptables, Mengirim notifikasi ke Telegram berisi jenis serangan dan alamat IP penyerang. Untuk Agar semakin jelas, hal tersebut bisa disaksikan melalui Gambar 4.

Skrip pada Gambar 4 akan mengambil IP yang telah diblokir oleh Suricata dari iptables, lalu mengirim notifikasi ke Telegram dan menambahkan aturan DROP agar IP penyerang tidak bisa lagi mengakses sistem.

4.2 Serangan DDOs dan *Port Scanning*

Pada pengujian terakhir, dilakukan simulasi serangan DDoS menggunakan metode ICMP *Flood* dengan hping3, serta serangan *port scanning* menggunakan Nmap untuk mengidentifikasi port yang terbuka sebelum serangan DDoS dilakukan. Suricata berhasil mendeteksi aktivitas Nmap *scanning* dan secara otomatis menutup akses ke *port* yang dipindai, sehingga penyerang tidak dapat memperoleh informasi tentang layanan yang berjalan di server.



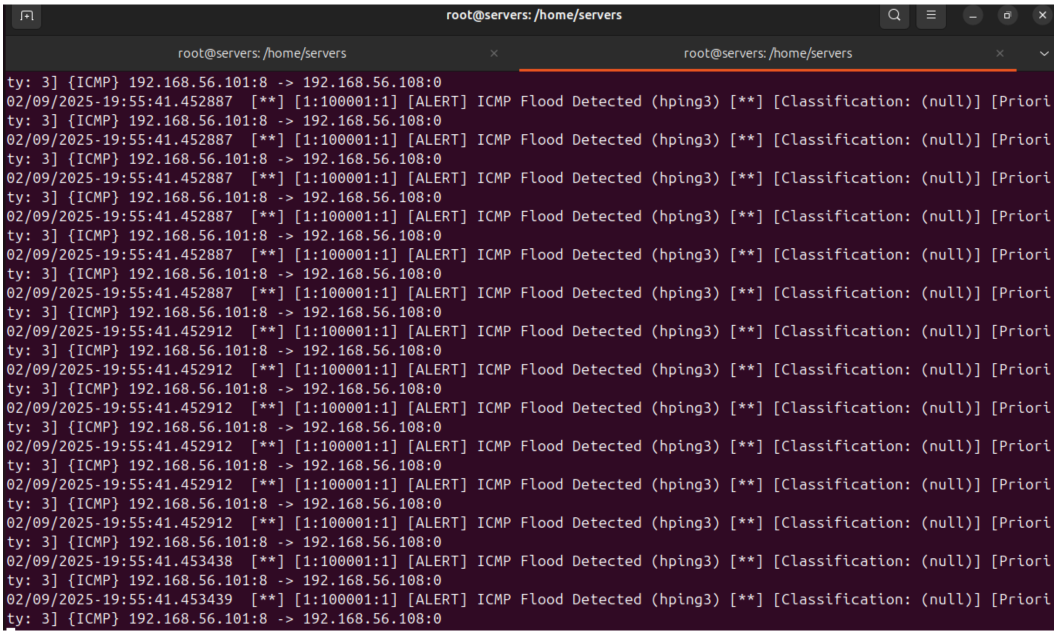
Gambar 5 Serangan DDos

Gambar 6 Serangan *Port Scanning*

Serangan DDoS yang dilakukan menggunakan hping3 mengalami *packet loss* yang signifikan akibat penerapan IPS Suricata, sementara serangan Nmap gagal membaca port pada server karena berhasil difilter oleh sistem pertahanan yang diterapkan.

4.3 Log Serangan Ddos

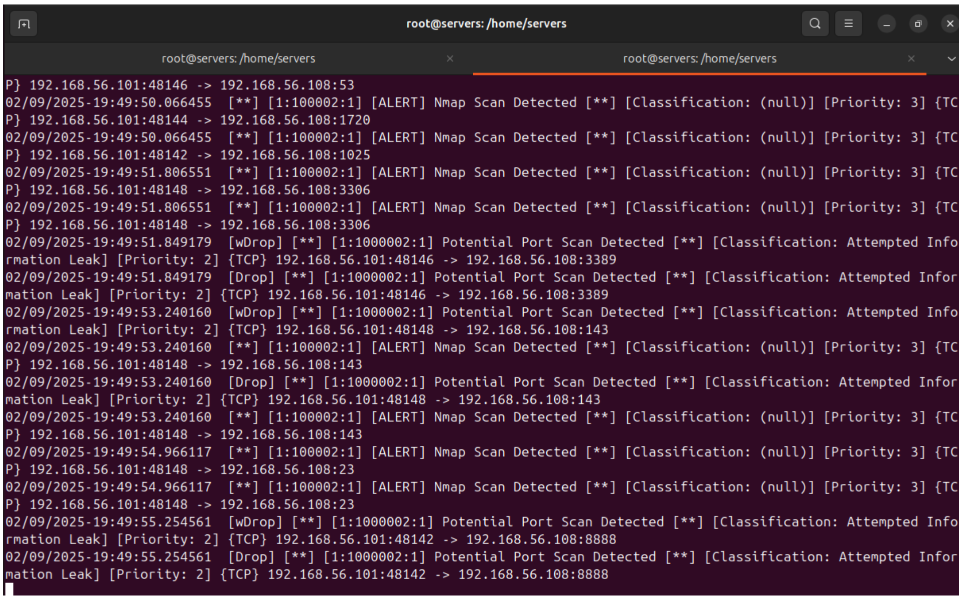
Suricata mencatat log yang berisi waktu kejadian, jenis serangan (Nmap *Scan* dan ICMP *Flood*), tingkat prioritas, protokol yang digunakan, serta alamat IP sumber dan tujuan, memastikan pemantauan keamanan jaringan secara *real-time*.



Gambar 7 Log Serangan DDos

4.4 Log Serangan Port Scanning

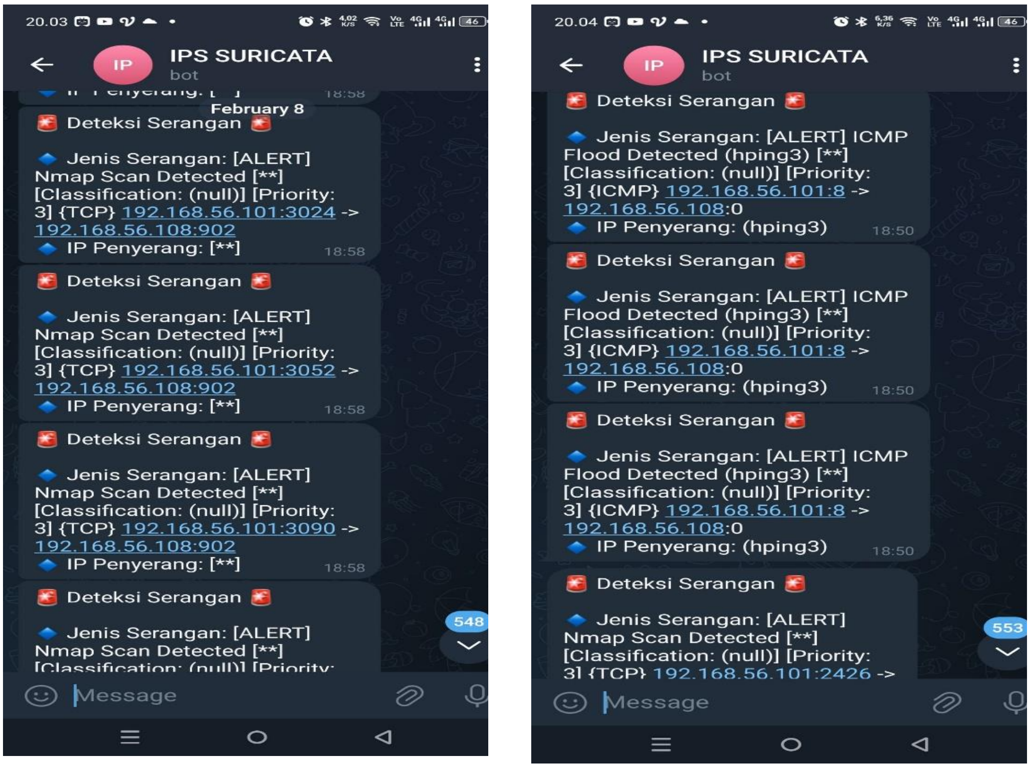
Suricata mencatat log yang berisi waktu kejadian, jenis serangan (Nmap Scan), tingkat prioritas, serta alamat IP sumber dan tujuan, memastikan sistem dapat mendeteksi dan merespons ancaman secara *real-time*.



Gambar 8 Log Serangan *Port Scanning*

4.5 Hasil Notifikasi Serangan DDOs dan Port Scaning

Saat sistem IPS *Suricata* mendeteksi serangan, sistem akan mengirimkan notifikasi ke Telegram yang berisi informasi mengenai jenis serangan dan alamat IP penyerang.



Gambar 9 Notifikasi Serangan DDos & Serangan *Port Scanning*

4.6 Hasil Pengujian dan Pembahasan

Hasil dari metode *penetration test* secara keseluruhan untuk pengujian keamanan jaringan di SMKN 8 TIK Kota Jayapura bisa disaksikan melalui tabel berikut ini. Pengujian ini mencakup berbagai jenis serangan untuk mengukur efektivitas IPS Suricata dalam melaksanakan pendeteksian serta menghalau ancaman yang berpotensi membahayakan keamanan jaringan.

Tabel 3 Waktu Pengujian

Jenis Serangan	Waktu		
	Awal Serangan	Waktu Terdeteksi	Terkirim
hping3 DDoS	19:55:38	19:55:41	19:55:42
Nmap Port Scanning	19:49:48	19:49:51	19:49:52

Pengujian dilakukan dengan dua jenis serangan berbeda, yaitu serangan DDoS menggunakan Hping3 dan pemindaian port dengan Nmap. Waktu mulai serangan dicatat, begitu pula waktu ketika IPS Suricata berhasil mendeteksi dan menghalau serangan tersebut. Selain itu, waktu pengiriman peringatan kepada administrator juga dicatat untuk mengevaluasi kecepatan respons sistem dalam menghadapi ancaman keamanan jaringan.

Tabel 4 Hasil Pengujian

Jenis Serangan	Hasil Pengujian Sistem	Kesimpulan
hping3 DDoS	Terdeteksi	Berhasil
Nmap Port Scanning	Terdeteksi	Berhasil

Dari tabel di atas, bisa disaksikan bahwasanya semua pelaksanaan uji memperoleh hasil yang sejalan dengan yang diinginkan. Sistem *Suricata* sukses mendeteksi dan menghalau setiap jenis serangan yang dilakukan oleh attacker dengan tepat waktu. Pendeteksian serangan meliputi:

1	DDoS Hping3	:	*Suricata* mendeteksi serangan dan memblokir DDoS ini dalam waktu 3 detik setelah serangan dimulai, Ini menunjukkan kemampuan sistem dalam mengidentifikasi dan mencegah lalu lintas jaringan yang mencurigakan dan membatasinya.
2	Nmap *Port Scanning*	:	*Suricata* berhasil mendeteksi aktivitas *port scanning* dalam waktu 3 detik setelah serangan dimulai. Sistem ini mampu mengenali pola scanning yang sering digunakan oleh penyerang untuk mencari celah keamanan. Berkat penerapan IPS dengan fitur *active response, Suricata* tidak hanya mendeteksi serangan tetapi juga secara otomatis menutup akses ke port yang dipindai, sehingga penyerang tidak dapat melihat *port* yang terbuka atau mendapatkan informasi tentang layanan yang berjalan di server. Hal ini secara efektif mencegah eksploitasi lebih lanjut dan meningkatkan keamanan jaringan.

Pendeteksian dan pencegahan serangan dilakukan sesuai dengan skenario yang telah dirancang, mulai dari pemindaian port dengan Nmap hingga serangan DDoS. Semua ancaman berhasil terdeteksi dan diblokir secara *real-time*, membuktikan bahwa IPS *Suricata* mampu mengamankan jaringan secara efektif. Keberhasilan ini menunjukkan bahwa konfigurasi Suricata dan aturan yang diterapkan sudah optimal dalam mendeteksi serta menghalau serangan, sehingga jaringan SMKN 8 TIK Kota Jayapura tetap terlindungi dari potensi ancaman siber.

Penelitian ini berkontribusi signifikan dalam memperkuat temuan-temuan sebelumnya terkait efektivitas *Suricata* sebagai IPS dalam menghadapi serangan DDoS. Berikut adalah analisis perbandingan dengan penelitian terdahulu:

1) Implementasi Suricata sebagai IPS
   a. Penelitian Terdahulu
      menguji efektivitas *Suricata* dalam mempertahankan *web server* dari serangan SQL *Injection* menggunakan SQLMap. Hasilnya memperlihatkan bahwa *Suricata* mampu mendeteksi dan merespons serangan dengan rata-rata waktu respons 4,26 milidetik, membuktikan kemampuannya dalam menghadapi serangan berbasis injeksi[15].
   b. Penelitian Saat Ini
      Fokus pada evaluasi kinerja Suricata guna menjalankan pendeteksian serta pencegahan serangan DDoS. Hasil eksperimen menunjukkan bahwa *Suricata* efektif dalam mengidentifikasi dan memitigasi beragam jenis serangan DDoS, seperti SYN flood dan UDP flood, dengan waktu respons yang kompetitif dan penggunaan sumber daya yang efisien.
2) Perbandingan dengan Sistem IDP/IPS
   a. Penelitian Terdahulu
      membandingkan kinerja Snort dan *Suricata* dalam mendeteksi serangan SYN Flood. Temuan mereka mengindikasikan bahwa Suricata unggul dalam akurasi deteksi dan efisiensi penggunaan sumber daya sistem, sementara *Snort* memiliki kecepatan deteksi yang sedikit lebih tinggi[16].
   b. Penelitian Saat Ini
      Menegaskan keunggulan *Suricata* dalam hal akurasi dan efisiensi sumber daya, khususnya dalam konteks serangan DDoS. Meskipun demikian, penelitian ini juga mencatat bahwa kecepatan deteksi *Suricata* cukup kompetitif, menjadikannya pilihan yang andal untuk mitigasi serangan DDoS.
3) Integrasi dengan Platform Keamanan
   a. Penelitian Terdahulu
      mengimplementasikan IDS menggunakan *Suricata* yang terintegrasi dengan ELK *Stack* untuk manajemen log, meningkatkan kemampuan monitoring dan analisis keamanan jaringan[17].
   b. Penelitian Saat Ini
      Meskipun tidak berfokus pada integrasi dengan *platform* lain, penelitian ini menyoroti fleksibilitas *Suricata* dalam beroperasi sebagai IPS mandiri yang efektif dalam mendeteksi dan mencegah serangan DDoS, serta kemampuannya untuk diintegrasikan dengan alat lain guna memperkuat strategi keamanan jaringan.

Temuan penelitian ini sejalan dan memperkuat hasil-hasil dari penelitian terdahulu, menegaskan bahwa *Suricata* merupakan solusi IPS yang efektif untuk melaksanakan pendeteksian serta mencegah beragam jenis serangan, termasuk DDoS. Kemampuan *Suricata* dalam memberikan waktu respons yang cepat, akurasi deteksi tinggi, dan efisiensi penggunaan sumber daya menjadikannya alat yang andal dalam memperkuat keamanan jaringan.

5. Simpulan

Secara keseluruhan, implementasi Suricata sebagai IPS di SMKN 8 TIK Kota Jayapura memberikan berbagai kelebihan yang signifikan dalam meningkatkan keamanan jaringan sekolah. Kelebihan-kelebihan ini mencakup deteksi dan pencegahan serangan *real-time,* pengurangan ketergantungan pada intervensi manual, peningkatan keamanan data, stabilitas operasional, dan perlindungan efektif terhadap serangan DDoS. Dengan demikian, *Suricata* menjadi solusi yang tepat untuk memperkuat pertahanan jaringan sekolah dan mendukung kegiatan administratif dan pembelajaran yang aman.

Daftar Referensi

[1] A. Muhaimi, I. P. Hariyadi, and A. Juliansyah, “Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram,” *J. Bumigora Inf. Technol.*, vol. 1, no. 2, pp. 167–176, 2019, doi: 10.30812/bite.v1i2.611.

[2] BADAN SIBER DAN SANDI NEGARA RI, “Laporan Keamanan Siber Indonesia (Bssn),” no. 70, 2023.

[3] K. Linux and G. D. Singh, *Napredno penetraciono testiranje alatima Nmap, Metasploit, Aircrack-ng i Empire prevod II izdanja prevod II izdanja*. [Online]. Available: www.kombib.rs

[4] R. Fauzi, Y. Muhyidin, and D. Singasatia, “Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS),” *J. Sains Komput. Inform. (J-SAKTI*, vol. 7, no. 1, pp. 72–86, 2023.

[5] Suwanto Rudy, Ruslianto Ikhwan, and Diponegoro Muhammad, “Implementasi Intrusion Prevention System (Ips),” *Implementasi Intrusion Prev. Syst. Menggunakan Snort Dan Iptable Pada Monit. Jar. Lokal Berbas. Website*, vol. 07, no. 1, pp. 97–107, 2019.

[6] M. F. Asnawi and M. A. Nugroho, “Pengujian Keamanan Jaringan Menggunakan Metode Penetrasi Tes Pada Jaringan Smk Muhammadiyah 1 Wonosobo,” *Device*, vol. 12, no. 2, pp. 110–118, 2022, doi: 10.32699/device.v12i2.3687.

[7] M. K. Harto and A. Basuki, “Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 4, pp. 1329–1333, 2021, [Online]. Available: http://j-ptiik.ub.ac.id

[8] R. William, I. Ruslianto, U. Ristian, J. Prof, H. Hadari, and N. Pontianak, “Implementasi Intrusion Prevention System (IPS) Sebagai Sistem Keamanan Server Berbasis Website dan Aplikasi Mobile Implementation of Intrusion Prevention System (IPS) as a Website-Based Server Security System and Mobile Application,” *J. Comput. Eng. Syst. Sci.*, vol. 8, no. 1, pp. 123–137, 2023, [Online]. Available: www.jurnal.unimed.ac.id

[9] F. Ardiyansyah, K. Setiawan, and N. Sutisna, “Implementation of IDS on Computer Networks Using Snort Based on Telegram Chatbot Implementasi IDS pada Jaringan Komputer Menggunakan Snort Berbasis Chatbot Telegram,” MALCOM: Indonesian Journal of Machine Learning and Computer Science vol. 4, no 4 . October, pp. 1614–1623, 2024.

[10] Safana Hyder Abbas, Wedad Abdul Khuder Naser, and Amal Abbas Kadhim, “Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS),” *Glob. J. Eng. Technol. Adv.*, vol. 14, no. 2, pp. 155–158, 2023, doi: 10.30574/gjeta.2023.14.2.0031.

[11] Prasetyo Taufan, “Pengamanan Jaringan Komputer Dengan Intrusion PreventionSystem (IPS) Berbasis Sms Gateway,” *Teknologipintar.org*, vol. 2, no. 6, pp. 1–13, 2022.

[12] O. Rivaldi and N. L. Marpaung, “Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata,” *INOVTEK Polbeng - Seri Inform.*, vol. 8, no. 1, p. 141, 2023, doi: 10.35314/isi.v8i1.3269.

[13] Yunanri, Riadi, and Yudnana, “Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing,” *Annu. Res. Semin.*, vol. 2, no. 1, pp. 300–304, 2018.

[14] N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, “Implementasi Keamanan Jaringan Menggunakan Port Knocking,” *J. Janitra Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 90–95, 2022, doi: 10.25008/janitra.v2i2.156.

[15] S. M. Syifa Munawarah, Kurniabudi, and Eko Arip Winanto, “Deteksi Serangan DDoS SYN Flood Pada Jaringan Internet of Things (IoT) Menggunakan Metode Deep Neural Network (DNN),” *J. Inform. Dan Rekayasa Komputer(JAKAKOM)*, vol. 4, no. 1, pp. 982–991, 2024, doi: 10.33998/jakakom.2024.4.1.1710.
[16] 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, 2020, doi: 10.35842/jtir.v15i2.343.
[17] T. Rahmawati, N. Karna, S. Y. Shin, M. Adi, and P. Putra, “Enhancing Network Security Through Real-Time Threat Detection with Intrusion Prevention System (Case Study on Web Attack),” vol. 10, no. 4, pp. 1004–1020, 2025, doi: 10.26555/jiteki.v10i4.30380.