IMPLEMENTASI SNORT INLINE MODE DAN ELK STACK UNTUK DETEKSI DAN MITIGASI SERANGAN PADA INFRASTRUKTUR LAYANAN DIGITAL PENDIDIKAN BERBASIS DOCKER

Vian Maulana Fatah[1], Achmad Noercholis[2], Fransiska Sisilia Mukti[3]
[1,2,3]Fakultas Teknologi dan Desain, Institut Teknologi dan Bisnis Asia Malang,
[1]viannmf24@gmail.com, [2]anoercholis@asia.ac.id, [3]ms.frans@asia.ac.id

ABSTRACT

The rapid development of digital education services has increased educational institutions' dependence on information technology infrastructure. Various cyber threats such as brute force attacks, port scanning, ping sweep, and denial-of-service attacks can disrupt service availability and interfere with academic and administrative activities. Therefore, an effective security mechanism is required to detect and mitigate cyberattacks in real time. This study aims to implement a Snort Inline Mode-based Intrusion Prevention System integrated with the ELK Stack (Elasticsearch, Logstash, Kibana) within a Docker-based digital education services infrastructure environment. The research employed an experimental method by developing a containerized architecture consisting of attacker, digital education service server, Snort IPS, Filebeat, Logstash, Elasticsearch, and Kibana containers. Active mitigation was implemented using Netfilter Queue (NFQUEUE), enabling Snort to inspect and block malicious traffic before reaching the target server. Four attack scenarios were tested, including SSH Brute Force, ICMP Ping Sweep, TCP Port Scan, and TCP SYN Flood. The results indicate that the system successfully detected and mitigated all attack scenarios with a mitigation success rate of 100% and response times below one second. Furthermore, ELK Stack integration provided centralized and real-time security monitoring through Kibana dashboards, facilitating threat analysis and security management. The findings demonstrate that the combination of Snort Inline Mode and ELK Stack in a Docker environment can serve as an effective security solution to support the reliability, security, and availability of digital education services infrastructure.

Keywords: Snort Inline Mode, ELK Stack, Docker, Digital Education Services Infrastructure, Intrusion Prevention System

ABSTRAK

Perkembangan layanan digital di lingkungan pendidikan telah meningkatkan ketergantungan institusi pendidikan terhadap infrastruktur teknologi informasi. Berbagai ancaman siber seperti brute force attack, port scanning, ping sweep, dan denial of service berpotensi mengganggu ketersediaan layanan serta memengaruhi aktivitas akademik dan administrasi yang bergantung pada sistem digital. Oleh karena itu, diperlukan mekanisme keamanan yang mampu mendeteksi dan memitigasi serangan secara real-time. Penelitian ini bertujuan mengimplementasikan sistem Intrusion Prevention System (IPS) berbasis Snort Inline Mode yang diintegrasikan dengan ELK Stack (Elasticsearch, Logstash, Kibana) pada lingkungan infrastruktur layanan digital pendidikan berbasis Docker. Metode penelitian yang digunakan adalah eksperimen dengan membangun arsitektur container yang terdiri atas kontainer attacker, server layanan digital pendidikan, Snort IPS, Filebeat, Logstash, Elasticsearch, dan Kibana. Mekanisme mitigasi aktif memanfaatkan Netfilter Queue (NFQUEUE) sehingga Snort mampu melakukan inspeksi dan pemblokiran paket berbahaya sebelum mencapai server tujuan. Pengujian dilakukan menggunakan empat skenario serangan yaitu SSH Brute Force, ICMP Ping Sweep, TCP Port Scan, dan TCP SYN Flood. Hasil penelitian menunjukkan bahwa sistem berhasil mendeteksi dan memitigasi seluruh serangan dengan tingkat keberhasilan mitigasi sebesar 100% dan waktu respons kurang dari satu detik. Integrasi ELK Stack juga berhasil menyediakan monitoring keamanan terpusat dan real-time melalui dashboard Kibana yang interaktif. Penelitian ini menyimpulkan bahwa kombinasi Snort Inline Mode dan ELK Stack pada lingkungan Docker dapat menjadi solusi keamanan yang efektif untuk mendukung keandalan, keamanan, dan ketersediaan infrastruktur layanan digital pendidikan.

Kata Kunci: Snort Inline Mode, ELK Stack, Docker, Infrastruktur Layanan Digital Pendidikan, Intrusion Prevention System

A. Pendahuluan

Transformasi digital telah mendorong institusi pendidikan untuk memanfaatkan berbagai layanan berbasis teknologi informasi dalam mendukung aktivitas akademik dan administrasi. Penggunaan komunikasi nirkabel untuk tujuan pribadi dan komersial telah berkembang dengan begitu cepat, dan teknologi Wi-Fi kini telah tersebar di semua tempat termasuk kantor pemerintahan, perusahaan swasta, dan institusi Pendidikan (Sisilia Mukti et al., 2019). Ancaman terhadap infrastruktur digital tersebut terus berkembang seiring dengan pesatnya digitalisasi di berbagai sektor kehidupan (Denanta Alviani et al., 2024).

Berkembangnya jaringan internet bukan lagi sebagai suatu hal yang mewah, melainkan menjadi sebuah kebutuhan di setiap bidang (Susdyastama Putra et al., 2020).
Gangguan terhadap sistem layanan digital Pendidikan dapat berdampak langsung pada proses belajar mengajar, menghambat akses informasi akademik, serta menurunkan kualitas layanan pendidikan. Oleh karena itu, institusi pendidikan perlu memastikan bahwa infrastruktur digital yang digunakan memiliki mekanisme perlindungan yang memadai terhadap berbagai ancaman keamanan siber.

Ancaman siber yang umum terjadi pada layanan berbasis jaringan antara lain brute force attack, ping sweep, port scanning, dan denial of service attack. Berbagai ancaman tersebut berpotensi mengganggu operasional layanan digital apabila tidak ditangani secara efektif (Pratikno R et al., 2025). Keamanan jaringan komputer bertujuan untuk menjaga agar data di dalamnya tetap aman, utuh, dan valid, serta membantu mencegah risiko seperti penyusupan atau ancaman yang dapat merusak fungsi jaringan (Suci Sekar Sari & Agus Tedyyana, 2024). Brute force attack dilakukan dengan mencoba berbagai kombinasi username dan password secara berulang untuk memperoleh akses tidak sah ke dalam sistem. Ping sweep digunakan untuk mengidentifikasi host aktif dalam suatu jaringan, sedangkan port scanning dimanfaatkan untuk menemukan layanan yang terbuka pada server target. Selain itu, denial of service attack dapat menyebabkan layanan menjadi tidak tersedia akibat tingginya lalu lintas jaringan yang diterima oleh server.

Salah satu solusi yang dapat diterapkan untuk meningkatkan keamanan jaringan adalah Intrusion Prevention System (IPS). IPS merupakan kombinasi antara fasilitas *blocking capabilities* dari *firewall* dan kedalaman inspeksi paket data dari Intrusion Detection System (IDS) (Pradipta & Asmunin, 2017). Berbeda dengan Intrusion Detection System (IDS) yang hanya memberikan notifikasi atau peringatan, IPS dapat melakukan pemblokiran lalu lintas berbahaya secara otomatis sebelum mencapai target. Salah satu perangkat lunak open source yang banyak digunakan dalam implementasi IPS adalah Snort. Snort mampu beroperasi sebagai IPS dalam mode inline melalui integrasi dengan Netfilter Queue (NFQUEUE) yang secara aktif memblokir paket berbahaya sebelum mencapai server, dan telah terbukti menunjukkan response time lebih cepat serta penggunaan sumber daya CPU yang lebih efisien dibandingkan pendekatan keamanan berbasis honeypot (Ernawati & Rachmat, 2021).

Selain kemampuan deteksi dan mitigasi, monitoring keamanan secara real-time juga menjadi kebutuhan penting dalam pengelolaan infrastruktur digital pendidikan. ELK Stack yang terdiri atas Elasticsearch, Logstash, dan Kibana merupakan platform yang banyak digunakan untuk pengelolaan log dan visualisasi data keamanan. Integrasi Snort dengan ELK Stack telah dibuktikan mampu memproses dan memvisualisasikan data alert secara efektif untuk mendukung deteksi ancaman jaringan secara real-time (Robbani et al., 2025).

Penelitian sebelumnya telah banyak membahas implementasi Snort sebagai Intrusion Detection System maupun pemanfaatan ELK Stack sebagai sistem monitoring keamanan. Selain itu, pendekatan berbasis Network Access Control (NAC) juga telah digunakan sebagai solusi keamanan jaringan terpusat pada infrastruktur TI modern (Ramadhan et al., 2026). Namun sebagian besar penelitian masih berfokus pada fungsi deteksi pasif dan belum mengintegrasikan kemampuan mitigasi aktif menggunakan Snort Inline Mode dengan visualisasi keamanan secara real-time dalam lingkungan Docker. Berdasarkan permasalahan tersebut, penelitian ini bertujuan mengimplementasikan Snort Inline Mode yang diintegrasikan

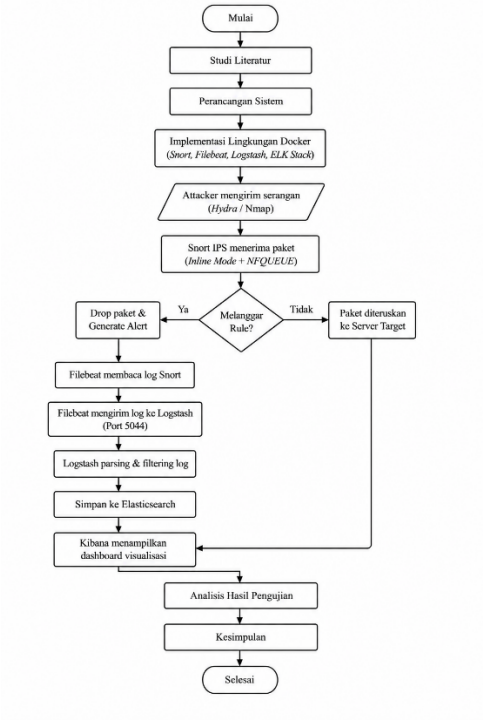
dengan ELK Stack pada lingkungan Docker untuk mendeteksi dan memitigasi berbagai jenis serangan jaringan secara real-time.

B. Metode Penelitian

Penelitian ini menggunakan metode eksperimen (experimental research) dengan pendekatan kuantitatif untuk mengimplementasikan dan mengevaluasi sistem keamanan jaringan berbasis Intrusion Prevention System (IPS) menggunakan Snort Inline Mode yang diintegrasikan dengan ELK Stack pada lingkungan Docker. Metode eksperimen dipilih karena penelitian berfokus pada pengujian langsung terhadap kemampuan sistem dalam mendeteksi dan memitigasi berbagai jenis serangan jaringan.

1. Desain Penelitian

Tahapan penelitian dilakukan secara sistematis mulai dari studi literatur, perancangan sistem, implementasi lingkungan Docker, konfigurasi Snort Inline Mode dan ELK Stack, simulasi serangan, pengumpulan data, analisis hasil pengujian, hingga penarikan kesimpulan. Metode eksperimen telah banyak digunakan dalam penelitian keamanan jaringan, di antaranya melalui perancangan topologi, instalasi sistem, konfigurasi kebijakan keamanan, serta pengujian fitur-fitur keamanan yang diterapkan (Hamzah & Prihanto, 2025).



Gambar 1 Alur Penelitian Implementasi Snort Inline Mode dan ELK Stack

2. Arsitektur Sistem

Lingkungan pengujian dibangun menggunakan Docker Container untuk memastikan konsistensi konfigurasi dan kemudahan replikasi sistem. Seluruh layanan dihubungkan melalui jaringan virtual Docker Bridge Network.

Komponen sistem terdiri atas:

a. Attacker Container: Container Ubuntu yang digunakan untuk

mensimulasikan aktivitas serangan menggunakan tools keamanan seperti Hydra, Nmap, dan Hping3.

b. Server Infrastruktur Layanan Digital Pendidikan: Server yang berperan sebagai representasi layanan digital pada lingkungan pendidikan dan digunakan sebagai target pengujian keamanan.
c. Snort IPS Container: Container yang menjalankan Snort Inline Mode sebagai Intrusion Prevention System. Snort dikonfigurasi menggunakan DAQ NFQUEUE sehingga mampu melakukan inspeksi dan pemblokiran paket secara langsung.
d. Filebeat Container: Berfungsi untuk membaca log keamanan yang dihasilkan Snort dan mengirimkannya ke Logstash secara real-time.
e. Logstash Container: Digunakan untuk memproses, memfilter, dan mengkategorikan log keamanan sebelum diteruskan ke Elasticsearch.
f. Elasticsearch Container: Berfungsi sebagai media penyimpanan dan pengindeksan data log keamanan.
g. Kibana Container: Digunakan untuk menampilkan visualisasi log keamanan dalam bentuk dashboard monitoring secara real-time.

3. Konfigurasi Snort Inline Mode

Snort dikonfigurasi dalam mode Inline dengan memanfaatkan mekanisme Netfilter Queue (NFQUEUE). Snort dapat bekerja dalam tiga mode, yaitu sebagai penyadap (sniffer), penyimpan data (packet logger), dan sebagai pendeteksi serangan (network intrusion detection) (Mahendra & Mukti, 2022). Seluruh paket jaringan yang masuk akan diarahkan ke antrean NFQUEUE menggunakan aturan iptables sebelum diperiksa oleh Snort. Pada konfigurasi ini, Snort dapat melakukan dua tindakan utama yaitu ACCEPT (mengizinkan paket diteruskan) apabila tidak terdeteksi sebagai ancaman, dan DROP (memblokir paket) apabila memenuhi aturan deteksi yang telah ditentukan. SNORT merupakan gabungan dari protokol analisis dan pendeteksi penyusupan yang berguna untuk merespon kejadian-kejadian yang sedang terjadi pada jaringan komputer secara *real-time* (Purba & Efendi, 2020).

4. Skenario Pengujian

Serangan DoS dan port scan merupakan serangan yang umum

terjadi pada komputer yang terhubung ke jaringan, di mana DoS berasal dari satu perangkat sedangkan DDoS melibatkan lebih dari satu perangkat dengan menggunakan paket data besar yang dapat membebani dan memblokir akses ke server (Awal & Gusman, 2023). Snort merupakan sistem yang dapat mendeteksi berbagai jenis ancaman pada jaringan komputer, mulai dari ancaman ICMP, TCP, maupun UDP (Santi & Mulyanto, 2024). Berdasarkan kemampuan tersebut, pengujian dalam penelitian ini dirancang menggunakan empat jenis serangan yang mencakup protokol-protokol tersebut:

a. SSH Brute Force Attack: Serangan dilakukan menggunakan Hydra untuk mencoba berbagai kombinasi kredensial secara berulang pada layanan SSH.
b. ICMP Ping Sweep: Serangan dilakukan untuk mengidentifikasi host aktif dalam jaringan menggunakan paket ICMP Echo Request.
c. TCP Port Scan: Pengujian dilakukan menggunakan Nmap untuk mendeteksi port yang terbuka pada server target.
d. TCP SYN Flood: Serangan dilakukan menggunakan Hping3 untuk mengirimkan paket SYN dalam jumlah besar guna mengganggu ketersediaan layanan.

Dampak serangan siber sangat luas, mencakup kerugian finansial, penurunan kepercayaan terhadap institusi, kebocoran data penting, serta risiko terhadap keamanan operasional suatu organisasi (Wulandari et al., 2025).

5. Teknik Pengumpulan dan Analisis Data

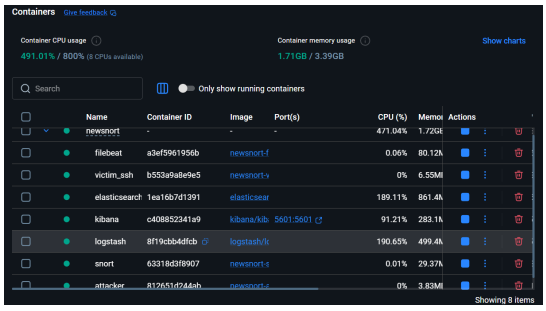
Data penelitian diperoleh melalui observasi langsung terhadap hasil pengujian sistem, meliputi log deteksi serangan yang dihasilkan oleh Snort, jumlah serangan yang berhasil dideteksi, jumlah paket yang berhasil dimitigasi, waktu respons sistem dalam melakukan mitigasi, dan visualisasi log keamanan melalui dashboard Kibana. Analisis data dilakukan dengan membandingkan hasil deteksi dan mitigasi terhadap setiap skenario serangan yang diuji.

C. Hasil Penelitian dan Pembahasan

1. Implementasi Infrastruktur Berbasis Docker

Implementasi sistem menggunakan Docker Compose dengan seluruh container berjalan pada jaringan

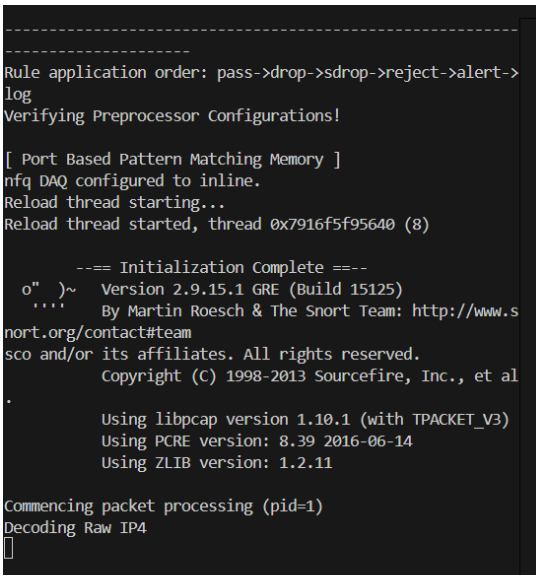
Docker Bridge, memungkinkan komunikasi antar layanan berlangsung dengan baik. Docker dipilih karena memberikan keuntungan berupa kemudahan *deployment*, isolasi layanan, dan konsistensi lingkungan pengujian.



Gambar 2 Implementasi Container Docker

2. Implementasi Snort Inline Mode

Snort dikonfigurasi menggunakan Inline Mode dengan memanfaatkan mekanisme Netfilter Queue (NFQUEUE). Pendekatan ini memungkinkan seluruh paket yang melintas diperiksa terlebih dahulu oleh Snort sebelum diteruskan ke server tujuan. Snort dapat dioperasikan dalam tiga mode yaitu: *sniffer mode* untuk menampilkan paket secara *real-time*, *packet logger mode* untuk mencatat paket ke dalam file, dan *network intrusion detection mode* yang menjalankan Snort beserta file konfigurasi yang telah ditentukan (Purba & Efendi, 2020). Mode Inline memungkinkan Snort tidak hanya mendeteksi aktivitas serangan, tetapi juga melakukan tindakan mitigasi secara langsung melalui aksi DROP terhadap paket yang melanggar aturan keamanan. Pada penelitian ini Snort dikonfigurasi untuk melakukan inspeksi dan pemblokiran paket secara aktif, sejalan dengan penerapan Snort sebagai IDPS yang telah terbukti mampu mendeteksi serangan *Port Scanning*, *Brute Force*, dan *DDoS* pada lingkungan jaringan nyata (Pradita & Pramono, 2024).



Gambar 3 Implementasi Snort Inline Mode Menggunakan NFQUEUE

3. Implementasi ELK Stack

ELK Stack merupakan kombinasi komponen Elasticsearch, Logstash, dan Kibana yang berguna untuk mengumpulkan log yang kemudian

divisualisasikan dalam bentuk grafis (F. S. Mukti & Sukmawan, 2021). Integrasi ELK Stack dilakukan untuk mendukung proses monitoring keamanan secara real-time. Filebeat digunakan untuk membaca log yang dihasilkan oleh Snort. Elasticsearch merupakan mesin pencari open source yang memungkinkan pencarian, penyimpanan, dan analisis data dalam skala besar secara cepat dan real-time menggunakan penyimpanan berorientasi dokumen berbasis JSON (Yudhistira & Fitrisia, 2023). Logstash menangani data yang diterima menggunakan pipeline pemrosesan yang terdiri dari tiga tahap yaitu input, filter, dan output (Setiyawan et al., 2023). Adapun Kibana merupakan platform yang didedikasikan untuk visualisasi, pencarian, kueri, dan analisis data yang berfokus pada data yang disimpan dalam indeks Elasticsearch (Yudhistira & Fitrisia, 2023).


{"log.level":"info","@timestamp":"2026-05-29T01:45:16.701Z","log.logger":"monitoring","log.origin":{"file.name":"log/log.go","file.line":187},"message":"Non-zero metrics in the last 30s","service.name":"filebeat","monitoring":{"metrics":{"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":115208192}}}},"cpu":{"system":{"ticks":42760,"time":{"ms":550}},"total":{"ticks":232260,"time":{"ms":4470},"value":232260},"user":{"ticks":189500,"time":{"ms":3920}}},"handles":{"limit":{"hard":1048576,"soft":1048576},"open":76},"info":{"ephemeral_id":"3d5fdf73-2d5c-4708-a962-f5b50029fb11","uptime":{"ms":1740339},"version":"8.11.0"},"memstats":{"gc_next":77244776,"memory_alloc":55131888,"memory_total":15316661032,"rss":86994944},"runtime":{"goroutines":358}},"filebeat":{"events":{"active":6210,"added":88064,"done":90112},"harvester":{"open_files":66,"running":66}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":88064,"active":4096,"batches":43,"total":88064},"read":{"bytes":258},"write":{"bytes":3065834}},"pipeline":{"clients":1,"events":{"active":4097,"published":88064,"total":88064},"queue":{"acked":88064}}},"registrar":{"states":{"current":66,"update":88064},"writes":{"success":22,"total":22}},"system":{"load":{"1":4.94,"15":4.59,"5":5.08,"norm":{"1":0.6175,"15":0.5738,"5":0.635}}}},"ecs.version":"1.6.0"}}

Gambar 4 Proses Pengiriman dan Pemrosesan Log Menggunakan Filebeat dan Logstash

4. Hasil Deteksi dan Mitigasi Serangan

Pengujian dilakukan terhadap empat jenis serangan yang umum ditemukan pada lingkungan jaringan. Setiap serangan dijalankan dari container attacker menuju server infrastruktur layanan digital pendidikan yang berada di belakang Snort Inline Mode.

Tabel 1 Hasil Pengujian Deteksi dan Mitigasi Serangan

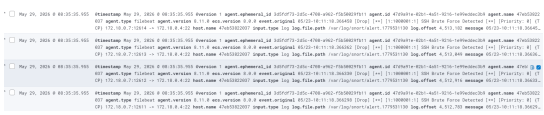
No	Jenis Serangan	Tools	Parameter Trigger	Status Mitigasi	Waktu Respons
1	SSH Brute Force	Hydra	5 koneksi / 60 detik	DROP (100 %)	< 1 Detik

2	ICMP Ping Sweep	Ping/Nmap	Setiap ICMP Echo	DROP (100 %)	< 1 Detik
3	TCP Port Scan	Nmap	20 SYN / 10 detik	DROP (100 %)	< 1 Detik
4	TCP SYN Flood	Hping3	100 SYN / 10 detik	DROP (100 %)	< 1 Detik

Berdasarkan hasil pengujian pada Tabel 1, sistem berhasil mendeteksi dan memitigasi seluruh serangan yang dilakukan. Tingkat keberhasilan mitigasi mencapai 100% pada seluruh skenario pengujian. Hasil tersebut menunjukkan bahwa Snort Inline Mode yang dikombinasikan dengan NFQUEUE mampu berfungsi sebagai Intrusion Prevention System (IPS) aktif yang efektif dalam mencegah ancaman jaringan secara real-time.

4.1 Hasil Deteksi SSH Brute Force

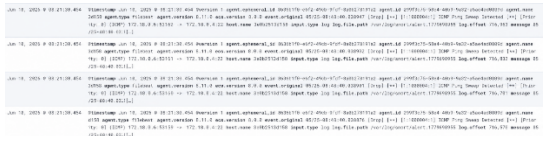
Pengujian SSH Brute Force dilakukan menggunakan Hydra dengan mencoba berbagai kombinasi username dan password terhadap layanan SSH yang berjalan pada server target. Ketika jumlah koneksi melebihi batas yang ditentukan pada rules Snort, sistem secara otomatis menghasilkan alert dan melakukan pemblokiran paket. Seluruh aktivitas brute force berhasil dideteksi dan dihentikan sebelum memperoleh akses ke sistem.



Gambar 5 Deteksi Serangan SSH Brute Force

4.2 Hasil Deteksi ICMP Ping Sweep

Pengujian ICMP Ping Sweep dilakukan menggunakan paket ICMP Echo Request untuk mengidentifikasi host aktif dalam jaringan. Snort berhasil mendeteksi aktivitas pemindaian jaringan dan melakukan pemblokiran terhadap paket yang dikirimkan oleh penyerang. Keberhasilan mitigasi ini menunjukkan bahwa sistem mampu mengurangi kemungkinan penyerang memperoleh informasi awal mengenai topologi jaringan.



Gambar 6 Deteksi Aktivitas ICMP Ping Sweep

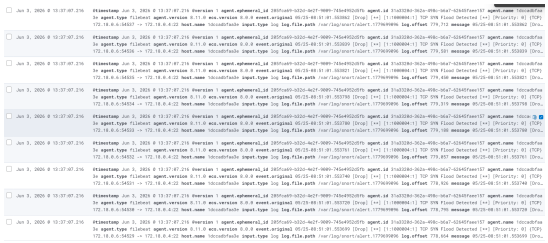
4.3 Hasil Deteksi TCP Port Scan

Port scanning merupakan langkah awal yang sering digunakan penyerang untuk memetakan layanan dan kerentanan pada sistem target (Intan Sabila et al., 2025). Pada pengujian ini, aktivitas TCP Port Scan dilakukan menggunakan Nmap dengan metode TCP SYN Scan. Aktivitas scanning berhasil dideteksi oleh Snort berdasarkan jumlah paket SYN yang dikirimkan dalam interval waktu tertentu. Sistem berhasil melakukan pemblokiran sehingga informasi mengenai port terbuka pada server tidak dapat diperoleh oleh penyerang.

Gambar 7 Deteksi Aktivitas TCP Port Scan

4.4 Hasil Deteksi TCP SYN Flood

Pengujian TCP SYN Flood dilakukan menggunakan Hping3 dengan mengirimkan sejumlah besar paket SYN secara terus menerus ke server target. Snort berhasil mengidentifikasi pola lalu lintas yang tidak normal dan melakukan tindakan pemblokiran secara otomatis. Layanan pada server tetap dapat berjalan dengan baik setelah mitigasi dilakukan.



Gambar 8 Deteksi Serangan TCP SYN Flood

5. Monitoring Keamanan Menggunakan ELK Stack

Selain melakukan deteksi dan mitigasi, penelitian ini juga mengintegrasikan ELK Stack sebagai platform monitoring keamanan. Filebeat mengirimkan log dari Snort menuju Logstash yang melakukan pemrosesan dan kategorisasi log sebelum disimpan ke Elasticsearch. Log yang telah diindeks kemudian divisualisasikan melalui dashboard Kibana secara real-time. Dashboard menampilkan informasi mengenai jumlah serangan, jenis serangan, waktu kejadian, serta alamat IP yang terlibat dalam aktivitas jaringan.

Gambar 9 Dashboard Monitoring Keamanan Menggunakan Kibana

C. Pembahasan

Hasil penelitian menunjukkan bahwa implementasi Snort Inline Mode yang terintegrasi dengan ELK

Stack mampu memberikan perlindungan aktif terhadap berbagai jenis ancaman jaringan. Tingkat keberhasilan mitigasi sebesar 100% menunjukkan bahwa pendekatan IPS lebih efektif dibandingkan sistem deteksi pasif yang hanya menghasilkan notifikasi tanpa melakukan tindakan pencegahan. Efektivitas sistem keamanan semacam ini akan semakin optimal apabila diterapkan pada infrastruktur jaringan yang dirancang dengan baik, mengingat kualitas sinyal dan penempatan Access Point yang tepat turut memengaruhi stabilitas koneksi yang menjadi landasan operasional sistem IPS (Sisilia Mukti et al., 2021). Hal ini sejalan dengan temuan (Pratikno R et al., 2025) yang menyatakan bahwa sebagian besar metode yang digunakan dalam analisis keamanan jaringan seperti Penetration Testing masih bersifat pasif dan terbatas pada identifikasi kerentanan, tanpa disertai mekanisme pencegahan otomatis.

Penggunaan NFQUEUE memungkinkan Snort melakukan inspeksi terhadap seluruh paket sebelum diteruskan ke server tujuan. Mekanisme ini memberikan kemampuan pemblokiran secara langsung sehingga ancaman dapat dihentikan sebelum berdampak pada layanan yang dilindungi. Integrasi ELK Stack memberikan nilai tambah berupa kemampuan monitoring keamanan secara terpusat dan real-time melalui dashboard Kibana.

Dalam konteks infrastruktur layanan digital pendidikan, implementasi sistem ini berpotensi meningkatkan ketersediaan layanan dan menjaga keberlangsungan aktivitas pembelajaran. Meskipun menunjukkan hasil yang sangat baik, penelitian ini masih memiliki keterbatasan karena pengujian hanya dilakukan terhadap empat jenis serangan dan belum mencakup serangan terdistribusi yang melibatkan banyak sumber secara bersamaan.

D. Kesimpulan

Penelitian ini berhasil mengimplementasikan Snort Inline Mode yang diintegrasikan dengan ELK Stack pada lingkungan Docker untuk mendeteksi dan memitigasi serangan jaringan secara *real-time* pada infrastruktur layanan digital pendidikan.

Pengujian terhadap empat skenario serangan yaitu SSH Brute Force,

ICMP Ping Sweep, TCP Port Scan, dan TCP SYN Flood menunjukkan tingkat keberhasilan mitigasi sebesar 100% dengan waktu respons di bawah satu detik. Dashboard Kibana berhasil menampilkan informasi serangan secara visual dan *real-time* sehingga memudahkan administrator dalam analisis dan pengambilan keputusan.

Kombinasi Snort Inline Mode dan ELK Stack pada lingkungan Docker terbukti efektif sebagai solusi keamanan infrastruktur layanan digital pendidikan. Penelitian selanjutnya dapat dikembangkan dengan skenario serangan yang lebih kompleks, pengujian skala besar, integrasi notifikasi otomatis, serta penerapan *machine learning* untuk deteksi ancaman yang lebih adaptif.

DAFTAR PUSTAKA

Awal, H., & Gusman, A. P. (2023). IMPLEMENTASI INTRUSION DETECTION PREVENTION SYSTEM SEBAGAI SISTEM KEAMANAN JARINGAN KOMPUTER KEJAKSAAN NEGERI PARIAMAN MENGGUNKAN SNORT DAN IPTABLES BERBASIS LINUX. In *Jurnal Sains Informatika Terapan (JSIT) E-ISSN* (Vol. 2, Number 2). Bulan Juni.

Denanta Alviani, C., Setiawan Padi, A., & Puspitasari, N. (2024). *SEMINAR NASIONAL AMIKOM SURAKARTA (SEMNASA) 2024 KEAMANAN SIBER DI MASA DEPAN : TANTANGAN DAN TEKNOLOGI YANG DIBUTUHKAN*.

Mahendra, D., & Mukti, F. (2022). Sistem Deteksi dan Pengendalian Serangan Denial of Service pada Server Berbasis Snort dan Telegram-API Detection and Control System of Denial of Service Attack on Server Based on Snort and Telegram-API. In *Agustus* (Vol. 21, Number 3).

Ernawati, T., & Rachmat, F. F. F. (2021). Network Security with Cowrie Honeypot and Snort Inline-Mode as Intrusion Prevention System. *Jurnal RESTI*, *5*(1), 180–186. https://doi.org/10.29207/resti.v5i1.2825

Hamzah, R. A., & Prihanto, A. (2025). Implementasi Cowrie Honeypot Dan Snort Inline-Mode Untuk Mendeteksi Serangan Brute-Force Dan Simulasi Deteksi Serangan Dos. *Journal of Informatics and Computer Science*, *07*(2).

Intan Sabila, M., Tahir, M., Dwi Mardania, S., & Ilham Arifin, R. (2025). IMPLEMENTASI SNORT SEBAGAI IDS DALAM MENDETEKSI SERANGAN PORT SCANNING NMAP PADA SIMULASI JARINGAN VIRTUAL.

In *Jurnal Mahasiswa Teknik Informatika)* (Vol. 9, Number 4).

Mukti, F. S., & Sukmawan, R. M. (2021). INTEGRATION OF LOW INTERACTION HONEYPOT AND ELK STACK AS ATTACK DETECTION SYSTEMS ON SERVERS. In *Jurnal Penelitian Pos dan Informatika* (Vol. 11, Number 1).

Pradipta, Y. W., & Asmunin. (2017). *Implementasi Intrusion Prevention System (IPS) Mengggunakan IPTABLES Linux IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT DAN IP TABLES BERBASIS LINUX*. www.snort.org.

Pradita, G., & Pramono, A. (2024). IMPLEMENTASI MONITORING KEAMANAN JARINGAN PADA SERVER UBUNTU MENGGUNAKAN SNORT INTRUSION DETECTION PREVENTION SYSTEM (IDPS) DAN TELEGRAM BOT SEBAGAI MEDIA NOTIFIKASI DI PT SS UTAMA. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 8, Number 4).

Pratikno R, Trinata C, & Hertantyo G. (2025). KAJIAN+LITERATUR+ANALISIS +KEAMANAN+JARINGAN. *Pendas : Jurnal Ilmiah Pendidikan Dasar*, *20*(2), 2477–2143.

Purba, W. W., & Efendi, R. (2020). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI: Jurnal Teknologi Informasi*, *17*(2), 143–158.

Ramadhan, A., Kom, S., Kom, M., & Rafif Hadi Kusmawan, M. (2026). *Implementasi Cisco ISE (Identity Service Engine) sebagai Network Access Control (NAC) untuk Meningkatkan Keamanan Akses Jaringan pada Simulasi Infrastruktur TI Modern*.

Robbani, F. D., Haryatmi, E., Riyadi, T. A., Supono, R. A., Kurniawan, A. B., & Rosdiana. (2025). Implementation of an Intrusion Detection System Using Snort and Log Visualization Using ELK Stack. *International Journal of Engineering, Science and Information Technology*, *5*(3), 220–228. https://doi.org/10.52088/ijesty.v5i3.901

Santi, N., & Mulyanto, Y. (2024). ANALISIS KELAYAKAN JARINGAN KOMPUTER MENGGUNAKAN ALAT SNIFFING DAN INTRUSION DETECTION SYSTEM (IDS) (STUDI KASUS : FITRIA_HOTSPOT). In *Jurnal Mahasiswa Teknik Informatika* (Vol. 8, Number 4).

Setiyawan, A., Pinandito, A., & Purnomo, W. (2023). *Pengembangan Sistem Informasi Log Management Server Monitoring Menggunakan ELK (Elastic Search, Logstash dan*

Kibana) Stack pada Aplikasi Padichain di PT. Bank Rakyat Indonesia (Vol. 7, Number 5). http://j-ptiik.ub.ac.id

Sisilia Mukti, F., Arbiyanto Sulistyo, D., & ASIA Malang, S. (2019). ANALISIS PENEMPATAN ACCESS POINT PADA JARINGAN WIRELESS LAN STMIK ASIA MALANG MENGGUNAKAN ONE SLOPE MODEL. *Jurnal Ilmiah Teknologi Informasi Asia*, *13*(1).

Sisilia Mukti, F., Dani Prasetyo Adi, P., Arman Prasetya, D., Sihombing, V., Rahanra, N., Yuliawan, K., & Simatupang, J. (2021). Integrating Cost-231 Multiwall Propagation and Adaptive Data Rate Method for Access Point Placement Recommendation. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 12, Number 4). https://doi.org/10.14569/IJACSA.2021.0120494

Suci Sekar Sari, & Agus Tedyyana. (2024). Analisis Efektivitas Rule Snort dalam Mendeteksi Serangan Jaringan. *Repeater : Publikasi Teknik Informatika Dan Jaringan*, *2*(4), 01–15. https://doi.org/10.62951/repeater.v2i4.194

Susdyastama Putra, Y., Indriastuti, M. T., & Mukti, S. (2020). OPTIMALISASI NILAI THROUGHPUT JARINGAN LABORATORIUM MENGGUNAKAN METODE HIERARCHICAL TOKEN BUCKET (STUDI KASUS: STMIK ASIA MALANG). In *Jurnal Ilmiah NERO* (Vol. 5, Number 2).

Wulandari, T., Yudisthira, Y. F., P.H, K. C., Wibowo, M. A., & Andrew, C. (2025). Algoritma LightGBM untuk Deteksi Aktivitas Cyber Espionage Melalui Dataset Serangan Siber. *JUSIFOR : Jurnal Sistem Informasi Dan Informatika*, *4*(2), 213–219. https://doi.org/10.70609/jusifor.v4i2.8489

Yudhistira, A., & Fitrisia, Y. (2023). MONITORING LOG SERVER DENGAN ELASTICSEARCH, LOGSTASH DAN KIBANA (ELK). *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *8*(1), 124–134. https://doi.org/10.36341/rabit.v8i1.2975