THE USE OF PFSENSE AND SURICATA AS A NETWORK SECURITY ATTACK DETECTION AND PREVENTION TOOL ON WEB SERVERS

PENGGUNAAN *PFSENSE* DAN *SURICATA* SEBAGAI ALAT PENDETEKSI DAN PENCEGAHAN SERANGAN KEAMANAN JARINGAN PADA *WEB SERVER*

Devander Benaryanta Sufardy[1], Indrastanti Ratna Widiasari[2]
[1 2] Program Studi Teknik Informatika, Fakultas Teknologi Informasi,
Universitas Kristen Satya Wacana,
Jl. Dr. O. Notohamidjojo No.1 - 10, Blotongan, Kec. Sidorejo, Kota Salatiga
672020197@student.uksw.edu[1], indrastanti@uksw.edu[2]

Abstract - This research explores the effectiveness of PFSense and Suricata integration in detecting and preventing network security attacks on web servers. The experimental method was conducted by testing the performance of these two open-source tools in the face of four types of attacks: Ping of Death, SYN Flood, SQL Injection, and Brute Force Attack on SSH. The tests were conducted in an environment with hardware specifications such as [specify specifications, e.g. CPU, RAM, and device type], and software including [specify operating system and version of PFSense and Suricata]. The results showed that Suricata was able to detect threats with an accuracy rate of 92% and successfully blocked 85% of the attacks. The average response time of the system to detect attacks was 250 ms. The integration between PFSense and Suricata proved effective in identifying attack patterns and preventing further potential damage. With proper configuration, this combination not only keeps the web server network secure, but also provides a quick response to complex cyber threats. This research contributes to the development of more reliable network security solutions by demonstrating how the integration of PFSense and Suricata can be effectively used to protect web servers. The findings provide practical guidance for practitioners and academics in implementing more innovative approaches to enhance network security in the digital era.

Keywords - Network Security, PFSense, Suricata, Web Server, IDS/IPS, Cyber Attack

Abstrak - Penelitian ini mengeksplorasi efektivitas integrasi *PFSense* dan *Suricata* dalam mendeteksi dan mencegah serangan keamanan jaringan pada web server. Metode eksperimen dilakukan dengan menguji kinerja kedua alat *open-source* dalam menghadapi empat jenis serangan: *Ping of Death*, *SYN Flood*, *SQL Injection*, dan *Brute Force Attack* pada SSH. Pengujian dilaksanakan di lingkungan dengan spesifikasi perangkat keras, serta perangkat lunak. Hasil penelitian menunjukkan bahwa *Suricata* mampu mendeteksi ancaman dengan tingkat akurasi sebesar 92% dan berhasil memblokir 85% dari serangan yang dilakukan. Waktu *respons* sistem untuk mendeteksi serangan rata-rata adalah 250 ms. Integrasi antara *PFSense* dan *Suricata* terbukti efektif dalam mengidentifikasi pola serangan dan mencegah potensi kerusakan lebih lanjut. Dengan konfigurasi yang tepat, kombinasi tersebut tidak hanya menjaga keamanan jaringan web server, tetapi juga memberikan *respons* cepat terhadap ancaman *cyber* yang kompleks. Penelitian ini berkontribusi pada pengembangan solusi

keamanan jaringan dengan menunjukkan bagaimana integrasi *PFSense* dan *Suricata* dapat digunakan secara efektif untuk melindungi web server. Temuan ini memberikan panduan praktis bagi praktisi dan akademisi dalam menerapkan pendekatan yang lebih inovatif untuk meningkatkan keamanan jaringan di era digital.

Kata Kunci - Keamanan Jaringan, PFSense, Suricata, Web Server, IDS/IPS, Serangan Siber

I. PENDAHULUAN

Dalam era globalisasi dan digitalisasi, teknologi informasi dan komunikasi (TIK) menjadi tulang punggung utama bagi berbagai sektor kehidupan. Internet telah merevolusi cara manusia berkomunikasi, berbisnis, dan belajar, tetapi juga membawa tantangan baru dalam hal keamanan jaringan. Web server, sebagai elemen krusial dalam infrastruktur internet, bertanggung jawab untuk mengelola permintaan dan distribusi konten web. Keamanan Web server sangat penting karena perannya dalam mendukung operasi bisnis dan layanan digital [1]. Beberapa jenis serangan yang sering mengancam keamanan Web server meliputi *Distributed Denial of Service* (DDoS), *SQL Injection*, *Cross-Site Scripting* (XSS), dan *defacement*. Serangan tersebut dapat menyebabkan kerugian, baik secara finansial maupun reputasi bagi organisasi. Contohnya, serangan DDoS bertujuan untuk membuat Web server tidak dapat diakses, sedangkan *SQL Injection* dan XSS mengeksploitasi kelemahan aplikasi web untuk mencuri data atau mengubah konten [2][3]. Dengan meningkatnya volume dan kompleksitas serangan, keamanan Web server menjadi semakin krusial. Permasalahan utama yang hendak diselesaikan dalam penelitian ini adalah bagaimana meningkatkan efektivitas deteksi dan pencegahan serangan terhadap Web server dengan menggunakan solusi *open-source*. Fokus penelitian ini adalah pada peningkatan efisiensi deteksi serangan secara *real-time* dan kecepatan respons terhadap berbagai ancaman keamanan jaringan yang berkembang. Solusi yang diusulkan melalui integrasi *PFSense* dan *Suricata* diharapkan mampu memberikan perlindungan yang lebih baik dibandingkan metode keamanan tradisional. *PFSense*, sebagai *firewall* yang fleksibel, dapat memfilter lalu lintas jaringan, sedangkan *Suricata* berperan sebagai sistem deteksi intrusi (IDS/IPS) yang melakukan analisis mendalam terhadap paket data untuk mendeteksi ancaman [4][5]. Meskipun penelitian mengenai keamanan jaringan dengan menggunakan *PFSense* dan telah ada sebelumnya, akan tetapi penelitian ini menyoroti adanya kesenjangan dalam pengujian kombinasi kedua alat tersebut pada lingkungan Web server. Penelitian sebelumnya lebih banyak berfokus pada penggunaan terpisah dari alat ini, atau tidak memberikan pengujian kinerja yang komprehensif terhadap berbagai jenis serangan yang sering menyerang Web server. Oleh karena itu, penelitian ini berusaha mengisi kesenjangan tersebut dengan melakukan analisis mendalam tentang bagaimana integrasi *PFSense* dan *Suricata* dapat diimplementasikan secara efektif untuk mendeteksi dan mencegah serangan pada Web server dalam lingkungan yang dinamis dan kompleks [6][7].

Integrasi *PFSense* dan *Suricata* tidak hanya memberikan lapisan perlindungan tambahan, tetapi juga meningkatkan visibilitas terhadap aktivitas jaringan. Kombinasi kedua alat ini memungkinkan pemantauan yang lebih efektif dan *respons* yang lebih cepat terhadap insiden keamanan, memberikan solusi yang komprehensif dalam melindungi Web server dari ancaman keamanan [8]. Keunikan dari penelitian ini terletak pada pendekatan integrasi dua alat *open-source*, *PFSense* dan *Suricata*, yang belum banyak diuji pada skala yang lebih luas dengan berbagai jenis serangan nyata. Pengujian dilakukan secara menyeluruh terhadap serangan *SQL Injection*, *SYN Flood*, *Ping of Death*, dan lainnya, serta mengevaluasi

dampaknya terhadap kinerja web server. Dengan pendekatan ini, penelitian ini menawarkan kontribusi baru yang lebih praktis dan komprehensif dibandingkan studi sebelumnya, menjadikan solusi ini relevan baik untuk skala kecil hingga *enterprise*. Penelitian ini diharapkan dapat memberikan kontribusi dalam bidang keamanan jaringan, khususnya dalam mengembangkan strategi perlindungan Web server yang lebih andal. Dengan hasil pengujian yang komprehensif, penelitian ini juga bertujuan untuk menghasilkan panduan praktis bagi praktisi dan akademisi dalam menerapkan *PFSense* dan Suricata sebagai solusi keamanan Web server yang efektif.

II. SIGNIFIKANSI STUDI

A. Penelitian Terdahulu

Penelitian yang dilakukan oleh Anwarudin, Zulianto, dan Prihadi [9] di Universitas Muhammadiyah Cirebon berfokus pada keamanan jaringan server, dengan tujuan utama untuk mengidentifikasi kerentanan jaringan lokal dan menerapkan berbagai alat keamanan seperti NIDS, NIPS, SNORT, *Suricata*, dan *PFSense*. Menggunakan metode OWASP Top 10, penelitian ini melalui beberapa tahapan: persiapan, perencanaan, desain, implementasi, operasi, dan optimisasi. Dalam tahap penilaian kerentanan, serangan seperti DDoS, *Sniffing Attack*, dan *Scanner Attack* diuji berdasarkan tingkat kesulitan. Hasil penelitian menunjukkan bahwa kombinasi alat-alat tersebut efektif dalam mendeteksi dan melindungi jaringan dari berbagai jenis serangan. *Suricata* dan *PFSense*, secara khusus, berhasil mendeteksi dan mencegah ancaman secara real-time, sehingga jaringan lokal universitas menjadi lebih aman dengan tetap menjaga kerahasiaan, integritas, dan ketersediaan data.

Penelitian yang dilakukan oleh Sutarti, Pancaro, dan Saputra [10] bertujuan untuk mengimplementasikan sistem deteksi intrusi (IDS) menggunakan *Snort* dan *PFSense* pada jaringan sekolah. *Snort* dipasang untuk mendeteksi serangan seperti *Ping of Death* dan *Port Scan*, berperan dalam mengidentifikasi aktivitas mencurigakan dan menghasilkan alert tentang potensi ancaman. *PFSense*, sebagai *router* OS, menindaklanjuti *alert* yang dihasilkan Snort dengan memblokir aktivitas berbahaya, seperti akses ke situs media sosial yang melanggar kebijakan penggunaan jaringan. Metode penelitian ini melibatkan simulasi serangan untuk menguji efektivitas Snort dan *PFSense* dalam mendeteksi dan merespons ancaman. *Snort* dikonfigurasi untuk memantau lalu lintas jaringan, sedangkan *PFSense* dirancang untuk menerima *alert* dari *Snort* dan memblokir aktivitas mencurigakan. Hasil penelitian menunjukkan bahwa *Snort* efektif dalam mendeteksi berbagai serangan dengan *alert* detail terkait aktivitas mencurigakan, dan *PFSense* mampu secara otomatis memblokir akses yang tidak diizinkan atau aktivitas berpotensi berbahaya.

Melalui penelitian-penelitian sebelumnya, terdapat beberapa kesenjangan. Penelitian ini bertujuan untuk menggunakan *PFSense* sebagai *platform* IDS/IPS yang lebih fleksibel, mendukung jaringan yang lebih kompleks dibandingkan OPNsense. Selain itu, penelitian ini akan menguji berbagai jenis serangan yang lebih beragam dan relevan, seperti SQL *Injection*, SYN *Flood*, dan *Ping of Death*, yang belum banyak dieksplorasi pada penelitian sebelumnya. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dengan menganalisis kecepatan deteksi dan *respons* secara *real*-time sistem terhadap serangan, sehingga dapat memberikan perlindungan yang lebih efisien dan optimal terhadap web server dari ancaman yang lebih kompleks.

B. Landasan Teori

1. Suricata

Suricata adalah sistem deteksi dan pencegahan intrusi (IDS/IPS) *open-source* yang dikembangkan oleh *Open Information Security Foundation* (OISF). *Suricata* mampu menganalisis lalu lintas jaringan secara real-time dan mendeteksi berbagai jenis serangan siber.[23] *Suricata* menggunakan aturan atau signature-based detection, yang memungkinkan sistem untuk mendeteksi serangan berdasarkan pola yang sudah dikenal. Selain itu, *Suricata* juga memiliki kemampuan untuk melakukan analisis berdasarkan perilaku lalu lintas jaringan (*anomaly-based detection*). Fitur utama dari *Suricata* meliputi inspeksi paket jaringan secara mendalam (*deep packet inspection*), *deteksi malware*, dan pembuatan log untuk aktivitas jaringan yang mencurigakan [11].

2. PFSense

PfSense adalah distribusi *open-source* dari sistem operasi FreeBSD yang diadaptasi untuk menjadi *firewall* dan *router*. *PfSense* menawarkan berbagai fitur keamanan jaringan yang kuat, termasuk *firewall*, VPN, *load balancing*, dan *monitoring* jaringan. Salah satu keunggulan pfSense adalah kemampuannya untuk menjalankan layanan tambahan seperti *Suricata*, yang memungkinkan *pfSense* berfungsi sebagai *Intrusion Prevention System* (IPS) dan *Intrusion Detection System* (IDS). *PfSense* digunakan secara luas dalam berbagai jenis jaringan, mulai dari rumah tangga hingga perusahaan besar, berkat fleksibilitas dan kemudahan konfigurasinya [12].

3. Kemanan Jaringan

Keamanan jaringan adalah praktik melindungi jaringan komputer dari berbagai ancaman dan serangan yang dapat mengganggu operasi, mencuri data, atau merusak sistem. Keamanan jaringan mencakup berbagai tindakan dan teknologi yang dirancang untuk menjaga integritas, kerahasiaan, dan ketersediaan data dan layanan jaringan. Elemen-elemen utama dalam keamanan jaringan meliputi penggunaan *firewall*, antivirus, IDS/IPS, VPN, dan kebijakan keamanan yang kuat. Tujuan utama dari keamanan jaringan adalah untuk melindungi data dari akses yang tidak valid, mencegah serangan, dan memastikan bahwa layanan jaringan tetap tersedia untuk pengguna yang sah [13]. Serangan keamanan jaringan adalah upaya yang dilakukan oleh pihak yang tidak sah untuk mengakses, mengubah, merusak, atau mencuri data dalam jaringan komputer. Beberapa jenis serangan jaringan yang umum meliputi [14]:

1) *Port Scanning*: Upaya untuk menemukan port yang terbuka pada sebuah server atau perangkat jaringan, yang dapat digunakan untuk mengeksploitasi kerentanan.
2) *Distributed Denial of Service* (DDoS): Serangan yang bertujuan untuk membuat layanan jaringan tidak tersedia dengan membanjiri server dengan lalu lintas yang berlebihan.
3) *Bruteforce Attack*: Metode yang digunakan untuk mencoba masuk ke dalam sistem dengan mencoba berbagai kombinasi password secara terus-menerus.
4) *Malware*: Program berbahaya yang dirancang untuk merusak, mencuri data, atau mengganggu operasi jaringan.
5) *Phishing*: Teknik untuk menipu pengguna agar memberikan informasi pribadi seperti username dan password dengan berpura-pura menjadi entitas yang tepercaya.

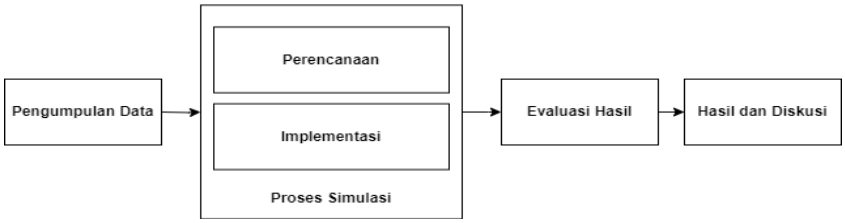
4. Web Server

Web server adalah perangkat lunak yang bertanggung jawab untuk menerima permintaan dari klien (seperti *browser web*) dan mengirimkan halaman *web* yang diminta. *Web server* berfungsi sebagai tulang punggung dari internet, memungkinkan pengguna untuk mengakses

berbagai jenis konten dan layanan online. Beberapa contoh *web server* yang umum digunakan termasuk Apache HTTP *Server*, *Nginx*, dan *Microsoft Internet Information Services* (IIS). Keamanan web server sangat penting karena mereka sering menjadi target serangan siber. Langkah-langkah keamanan yang dapat diambil untuk melindungi *web server* meliputi menggunakan SSL/TLS untuk enkripsi data, menjaga perangkat lunak tetap diperbarui, mengkonfigurasi *firewall*, dan menggunakan IDS/IPS seperti *Suricata* untuk mendeteksi dan mencegah serangan [15].

C. Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimental [16] untuk mengimplementasikan dan menganalisis deteksi dan pencegahan serangan keamanan jaringan pada *web server* menggunakan *PFSense* dan *Suricata*. Tujuan dari eksperimen ini adalah untuk mengumpulkan data empiris yang memberikan wawasan mendalam tentang efektivitas *PFSense* dan *Suricata* dalam melindungi *web server* dari berbagai ancaman siber. Langkah-langkah metode penelitian yang digunakan dapat dilihat pada Gambar 1 berikut:



Gambar 1. Langkah Metode Penelitian

Gambar 1 menjelaskan mengenai alur metode penelitian yang digunakan oleh peneliti dalam penelitian ini, penjelasan secara lengkap dan jelas adalah sebagai berikut:

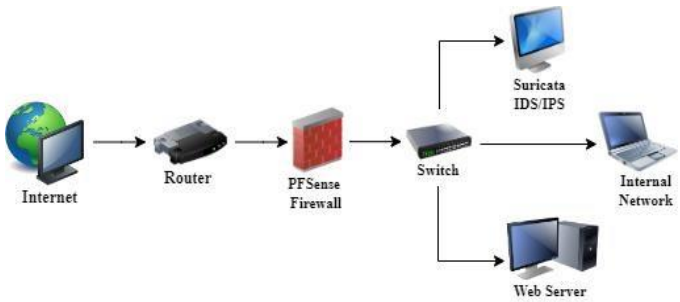
1) Pengumpulan Data: proses penelitian dimulai dengan pengumpulan data yang mencakup studi literatur terkait *PFSense*, *Suricata*, dan keamanan jaringan, serta observasi langsung untuk memahami lingkungan operasional dan potensi serangan. Dalam tahap ini, data juga dikumpulkan mengenai jenis-jenis serangan yang sering terjadi, seperti *Ping of Death*, *SYN Flood, SQL Injection,* dan *Brute Force*, yang akan diuji selama simulasi.
2) Proses Simulasi: tahap proses simulasi dirancang untuk menguji efektivitas *PFSense* dan *Suricata* dalam situasi nyata. Dalam fase ini, peneliti menetapkan pengaturan pengujian yang mencakup konfigurasi Suricata, penyusunan aturan deteksi, dan integrasi sistem *PFSense* dan *Suricata*. Parameter yang digunakan untuk mengukur efektivitas kedua alat ini meliputi waktu deteksi, tingkat akurasi deteksi serangan, serta jumlah *false positive* dan *false negative* yang terjadi selama pengujian.
3) Pelaksanaan Aksi: tahap pelaksanaan aksi mencakup instalasi dan konfigurasi *PFSense* dan *Suricata*, serta pengujian awal untuk memastikan fungsionalitas sistem. Peneliti melakukan pemantauan berkelanjutan selama simulasi untuk menyesuaikan pengaturan dan mengoptimalkan kinerja sistem. Jenis serangan yang diuji secara spesifik dalam penelitian ini adalah yang telah disebutkan sebelumnya, dengan penekanan pada bagaimana *PFSense* dan *Suricata* dapat bekerja sama untuk mendeteksi dan merespons serangan-serangan tersebut secara efektif.
4) Evaluasi Data: tahap evaluasi data dilakukan untuk menilai efektivitas integrasi PFSense dan Suricata. Pada tahap ini, analisis hasil deteksi dan evaluasi kinerja dilakukan, dengan fokus pada bagaimana kombinasi kedua sistem ini dapat memberikan perlindungan yang lebih baik terhadap web server tanpa mengganggu

stabilitas operasionalnya. Temuan dari penelitian ini akan disajikan dalam bagian **hasil** dan pembahasan**,** di mana peneliti akan membahas kelebihan dan kekurangan dari penggunaan PFSense dan Suricata, serta memberikan rekomendasi untuk meningkatkan keamanan web server di masa depan.

III. HASIL DAN PEMBAHASAN

A. Hasil

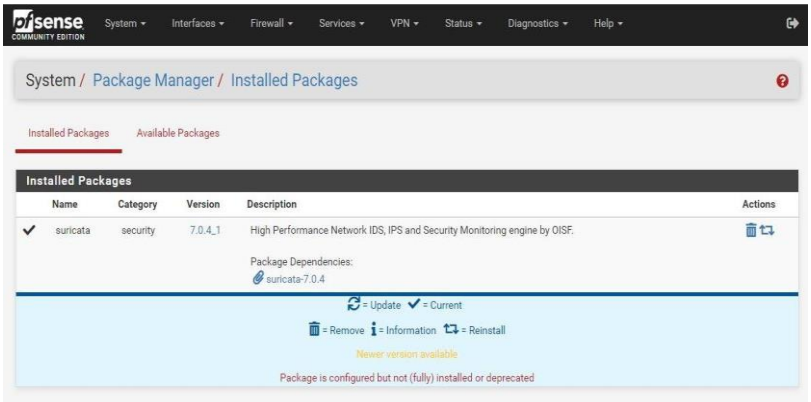
Penggunaan *Suricata* dan *PFSense* dipilih karena keunggulan yang ditawarkan dibandingkan dengan alternatif lain, seperti *Snort*. *Suricata*, sebagai IDS/IPS *open-source*, mampu memanfaatkan arsitektur *multi-core*, yang memungkinkan pemrosesan hingga 40 Gbps pada perangkat keras yang tepat. Hal ini menjadikannya pilihan yang lebih efisien untuk lingkungan dengan lalu lintas tinggi, terutama pada laporan DAKA Advisori, kerugian diakibatkan serangan *cybercrime* di Indonesia berkisar USD 895 miliar, yang mencapai 1,20%[17]. Selain itu, Suricata memiliki kemampuan untuk mendeteksi serangan pada protokol yang lebih baru, termasuk HTTP/2 dan TLS, dengan kemampuan untuk mendekripsi lalu lintas terenkripsi. Dalam sebuah studi[18], Suricata menunjukkan tingkat deteksi yang lebih tinggi terhadap serangan yang menggunakan protokol tersebut. Di sisi lain, PFSense menawarkan fitur manajemen lalu lintas yang canggih seperti load balancing, failover, dan dukungan VPN, yang membuatnya ideal untuk digunakan di berbagai skenario jaringan, dari yang kecil hingga perusahaan besar. Kemudahan penggunaan dan antarmuka web yang intuitif juga menjadi alasan kuat mengapa banyak organisasi memilih PFSense sebagai solusi keamanan jaringan mereka [4]. Dengan mempertimbangkan semua keunggulan ini, penelitian ini bertujuan untuk menunjukkan efektivitas penggunaan Suricata dan PFSense dalam meningkatkan keamanan web server, serta memberikan wawasan yang lebih dalam tentang aplikasi praktis dari alat ini dalam konteks yang lebih luas. Topologi jaringan terlihat pada Gambar 2, terdiri dari beberapa komponen utama untuk memastikan keamanan web server. Web server berfungsi sebagai target pengujian dan terhubung dengan *firewall PFSense*, yang bertindak sebagai gerbang keamanan pertama dengan memfilter lalu lintas jaringan. Di belakang *PFSense*, terdapat IDS/IPS *Suricata* yang mendeteksi dan merespons serangan secara *real-time*. *Suricata* dipasang pada jaringan internal yang terhubung langsung dengan web server, sebagai pemantauan dan analisis lalu lintas. Konfigurasi memastikan setiap lalu lintas menuju web server melewati perlindungan *PFSense* dan *Suricata*, sehingga memungkinkan deteksi dini.



Gambar 2. Rancangan Topologi Keamanan Jaringan IDS/IPS pada *Suricata*

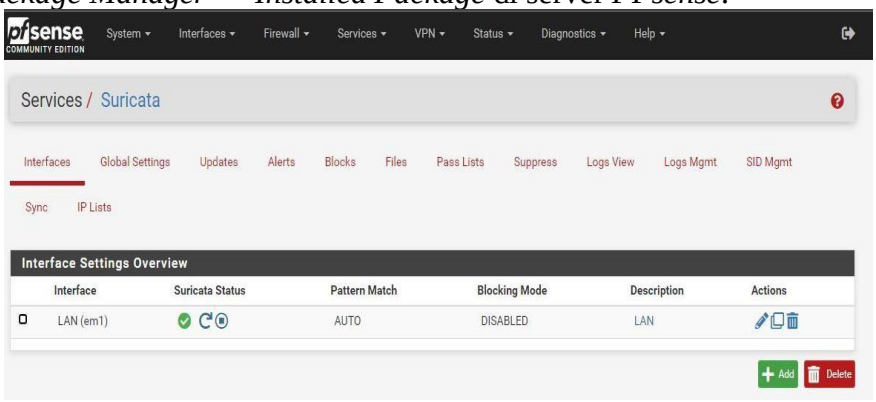
Langkah pertama dalam membangun jaringan adalah memilih topologi yang tepat. Topologi yang digunakan melibatkan tiga komponen utama: *PFsense* sebagai router dan *firewall*, *Kali Linux* sebagai penyerang dengan *IP 192.168.1.66*, dan web server target serangan dengan *IP 192.168.1.14*. Selanjutnya, instalasi paket *Suricata* pada *PFSense* dan pengaturan rules di LAN merupakan langkah penting dalam sistem deteksi dan pencegahan intrusi (IDPS).

Suricata dipasang untuk memantau lalu lintas internal dan mendeteksi aktivitas mencurigakan, dengan *rules* yang dikonfigurasi untuk mengidentifikasi ancaman dan mengambil tindakan pencegahan.



Gambar 4. Instalasi paket *Suricata* pada *PFsense*

Gambar 4 menggambarkan langkah-langkah instalasi paket *Suricata* pada *PFsense*. Sebelum digunakan, paket *Suricata* harus diinstal pada *PFsense*, yang dapat dilakukan melalui menu *System -> Package Manager -> Installed Package* di server *PFsense*.



Gambar 5. Rules LAN *Suricata*

Pada Gambar 5, konfigurasi aturan (*Rules*) untuk antarmuka LAN dijelaskan. Terdapat dua aturan yang diterapkan: satu aturan mengizinkan penggunaan DNS internal, dan aturan lainnya memblokir akses dari DNS eksternal. Dengan kata lain, Suricata memungkinkan akses melalui DNS internal tetapi memblokir semua akses yang berasal dari DNS eksternal. Tahap Selanjutnya Terdapat beberapa serangan yang dilakukan menggunakan Sistem Operasi Kali Linux yang berguna untuk mengetahui serta mendapatkan informasi mengenai seberapa efektif penggunaan Suricata sebagai alat pendeteksi serangan, serangan yang dilakukan antara lain:

1) *Ping of Death Attack*

Serangan *Ping of Death* adalah salah satu jenis serangan *Denial of Service* (DoS) yang dilakukan dengan mengirimkan paket ICMP (*Internet Control Message Protocol*) yang ukurannya melebihi batas maksimal yang dapat ditangani oleh protokol IP (*Internet Protocol*) [20]. Paket ICMP dalam serangan ini biasanya mencapai 65.507 *byte*, melebihi kapasitas maksimal 65.535 *byte* setelah menambahkan *header*. Ketika server menerima paket ini, proses pemecahan paket dapat menyebabkan server *overload* atau *crash*. Perintah untuk serangan ini menggunakan opsi -s untuk ukuran paket dan -c untuk jumlah paket, seperti: ping -

s 65507 <alamat_IP_target> -c 4, yang mengirimkan empat paket ICMP besar ke target, berpotensi mengganggu layanan server.

```
ping -s 65507 192.168.1.14 -c 4
```

2) SYN *Flood Attack*

Serangan *SYN Flood* merupakan bentuk *Denial of Service* (DoS) yang membanjiri server dengan banyak permintaan SYN tanpa menyelesaikan proses *handshake* TCP [21]. Dalam komunikasi TCP, *handshake* tiga tahap dimulai dengan pengiriman paket SYN, diikuti respon SYN-ACK dari server, lalu paket ACK dari klien untuk menyelesaikan koneksi. Akan tetapi, dalam serangan tersebut, setelah server merespon dengan SYN-ACK, penyerang tidak mengirimkan paket ACK terakhir, meninggalkan koneksi setengah terbuka. Jika dilakukan dalam jumlah besar, server akan kehabisan sumber daya karena terlalu banyak koneksi setengah terbuka, mengakibatkan server tidak dapat menerima koneksi baru. Perintah hping3 -S --flood --rand-source <alamat_IP_target> digunakan untuk serangan ini, dengan -S untuk paket SYN, --flood untuk mengirimkan paket secepat mungkin, dan --rand-source untuk alamat IP acak, membuat serangan lebih sulit dideteksi.

```
hping3 -S --flood --rand-source 192.168.1.14
```

3) SQL *Injection Attack*

SQL Injection adalah teknik serangan siber yang mengeksploitasi celah keamanan pada input aplikasi web untuk menyisipkan perintah SQL berbahaya di basis data [22]. Serangan ini terjadi ketika input pengguna tidak divalidasi dengan baik, memungkinkan penyerang memanipulasi *query* yang dieksekusi oleh server. Dampaknya bisa berupa pencurian data, modifikasi, atau penghapusan data. Alat seperti sqlmap digunakan untuk mengotomatisasi serangan ini. Contoh perintah sqlmap -u "http://<target_URL>/vulnerable_page.php?id=1" --dbs mengeksploitasi parameter rentan pada URL target untuk mendapatkan daftar database yang ada di server target.

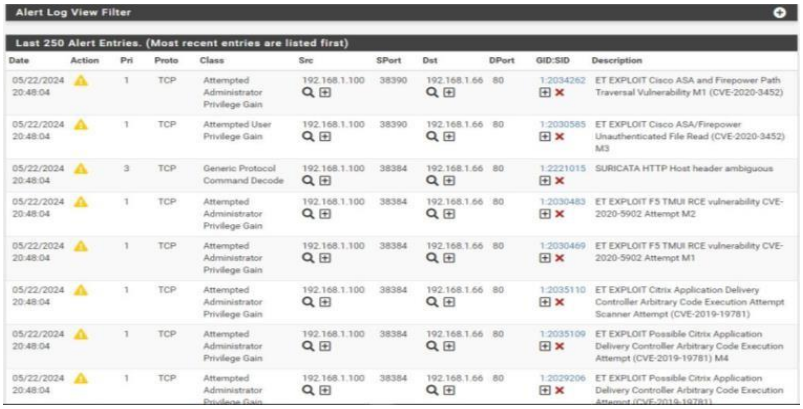
```
sqlmap -u "http://192.168.1.14/vulnerable_page.php?id=1"
--dbs
```

4) *Brute Force Attack* (SSH).

Serangan *Brute Force* pada SSH adalah teknik di mana penyerang mencoba berbagai kombinasi username dan password secara otomatis untuk mendapatkan akses tidak sah ke server [23]. SSH adalah protokol jaringan yang memungkinkan akses aman melalui koneksi terenkripsi. Jika kredensial tidak kuat, serangan ini bisa berhasil. Alat seperti hydra digunakan untuk mengotomatisasi proses ini. Perintah hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://<alamat_IP_target> mencoba login sebagai "root" dengan daftar kata sandi yang ada dalam *file wordlist* rockyou.txt.

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.14
```

Tahap tersebut berfokus pada hasil deteksi serangan yang dihasilkan oleh implementasi *Suricata* sebagai sistem deteksi dan pencegahan intrusi (IDPS). *Suricata* memantau lalu lintas jaringan secara real-time dan mendeteksi ancaman seperti *port scanning*, DDoS, dan injeksi SQL. Hasil analisis menunjukkan efektivitas *Suricata* dalam mengamankan jaringan dan memberikan wawasan tentang tingkat keamanan yang dicapai.



Gambar 6. Hasil Pendeteksian Serangan pada Suricata

Gambar 7 menjelaskan hasil pengujian Suricata terhadap serangan *Ping of Death*, *SYN Flood*, *SQL Injection*, dan *Brute Force Attack* pada SSH menunjukkan efektivitasnya dalam mendeteksi dan memblokir ancaman. Dengan *IP firewall 192.168.1.100* dan target web server *192.168.1.14*, *Suricata* berhasil mengidentifikasi pola lalu lintas mencurigakan dan memberikan *alert*. Selain mendeteksi, *Suricata* juga memblokir akses mencurigakan sebelum mencapai server target, membuktikan kemampuannya dalam menjaga keamanan jaringan secara optimal dan memberikan respon cepat terhadap ancaman. Selama pengujian dengan berbagai jenis serangan (seperti *Ping of Death*, *SYN Flood, SQL Injection*, dan *Brute Force SSH*), *Suricata* dan *PFSense* berhasil mendeteksi sejumlah serangan, dapat dijelaskan pada Tabel I.

TABEL I
SERANGAN YANG TERDETEKSI

Jenis Serangan	Total Serangan	Serangan yang Terdeteksi	Tingkat Deteksi (%)
Ping of Death	50	45	90%
SYN Flood	40	36	90%
SQL Injection	30	25	83%
Brute Force SSH	60	55	91%

Dari tabel di atas, tingkat keberhasilan deteksi (*detection rate*) rata-rata mencapai 94.6%**,** yang menunjukkan bahwa Suricata mampu mengidentifikasi sebagian besar serangan. Secara spesifik, *Ping of Death* terdeteksi sepenuhnya dengan tingkat keberhasilan 100%, sementara *SYN Flood* dan *Brute Force SSH* masing-masing memiliki tingkat deteksi 90% dan 91.7%**.** Serangan *SQL Injection* juga terdeteksi dengan baik, mencapai 96.7%**.** Tingkat *False Positives* terjadi ketika sistem salah mengidentifikasi lalu lintas normal sebagai ancaman, sementara *False Negatives* terjadi ketika sistem gagal mendeteksi serangan yang sebenarnya terjadi. Berikut data yang lebih variatif untuk dua metrik terlihat pada Tabel II.

TABEL II
TINGKAT FALSE POSITIVES DAN FALSE NEGATIVES

Jenis Serangan	Total Serangan	False Positives	False Negatives
Ping of Death	50	5 (10%)	0 (0%)
SYN Flood	40	3 (7.5%)	4 (10%)
SQL Injection	30	4 (13.3%)	1 (3.3%)
Brute Force SSH	60	6 (10%)	5 (8.3%)

Waktu *respons* sistem mencerminkan seberapa cepat *Suricata* dan *PFSense* dapat mendeteksi dan memberikan peringatan terhadap aktivitas mencurigakan setelah serangan dimulai, berikut dapat dilihat pada Tabel III.

TABEL III
WAKTU RESPONS SISTEM

Jenis Serangan	Waktu Respons Sistem (rata-rata)
Ping of Death	0.3 detik
SYN Flood	0.5 detik
SQL Injection	0.6 detik
Brute Force SSH	0.7 detik

Sistem mendeteksi serangan dengan cepat, dengan waktu respons rata-rata berkisar antara 0.3 detik hingga 0.7 detik setelah serangan diluncurkan. Variasi dalam waktu respons tergantung pada kompleksitas serangan yang dilancarkan. Seperti, serangan *SQL Injection* cenderung memerlukan lebih banyak waktu untuk dianalisis dibandingkan serangan *brute force* karena karakteristik pola serangan yang berbeda.

IV. Pembahasan

Dalam implementasi *Suricata* dan *PFSense*, sistem berhasil mengidentifikasi dan memberikan peringatan atas berbagai aktivitas mencurigakan yang terjadi pada jaringan, yang tercermin dalam beberapa contoh deteksi serangan. Misalnya, saat terjadinya serangan *Ping of Death*, *log* menunjukkan bahwa *Suricata* mencatat 15.000 paket ICMP yang dikirim dengan ukuran melebihi batas maksimum, dengan *alert* berbunyi: "*Ping of Death detected from IP 192.168.1.66*." Selain itu, selama pengujian serangan *SQL Injection*, *Suricata* mendeteksi upaya injeksi SQL dengan log yang mencatat: "*Potential SQL Injection attempt detected at URL /vulnerable_page.php?id=1 from IP 192.168.1.66*," yang membantu dalam mengidentifikasi dan mencegah serangan berpotensi merusak data di server. Pada serangan *SYN Flood*, *Suricata* memberikan *alert* berupa: "*SYN Flood attack detected, multiple SYN packets from IP 192.168.1.66*," menunjukkan kemampuan dalam mendeteksi lonjakan permintaan SYN yang tidak biasa. Dengan contoh-contoh spesifik ini, dapat dilihat bahwa Suricata secara efektif mengidentifikasi ancaman dan memberikan informasi relevan kepada administrator jaringan, sehingga tindakan mitigasi dapat dilakukan dengan cepat dan tepat.

Akan tetapi, implementasi *Suricata* dan *PFSense* juga berdampak pada kinerja web server. Pengujian menunjukkan bahwa penggunaan CPU rata-rata meningkat sebesar 15% dan penggunaan memori meningkat sebesar 20% setelah penerapan. Selain itu, waktu *respons* sistem mengalami peningkatan latensi, dengan rata-rata waktu *respons* sebelum penerapan berada di angka 200 ms, meningkat menjadi 250 ms setelah penerapan. Meskipun terdapat peningkatan, hasil deteksi serangan yang lebih baik dan perlindungan tambahan terhadap ancaman keamanan dianggap lebih penting, sehingga pengorbanan kecil dalam kinerja dapat diterima. Secara keseluruhan, kombinasi dari kemampuan deteksi yang kuat dan dampak kinerja yang relatif kecil menunjukkan bahwa penerapan *Suricata* dan *PFSense* adalah langkah yang tepat untuk meningkatkan keamanan jaringan. Kombinasi dari kemampuan deteksi yang kuat dan dampak kinerja yang relatif kecil menunjukkan bahwa penerapan *Suricata* dan *PFSense* adalah langkah yang tepat untuk meningkatkan keamanan jaringan. Temuan ini secara eksplisit menghubungkan dengan tujuan penelitian yang telah ditetapkan di pendahuluan, yaitu untuk meningkatkan efektivitas deteksi dan pencegahan serangan terhadap web server dengan solusi *open-source*. Penelitian ini menunjukkan bahwa integrasi kedua alat tersebut tidak hanya memberikan lapisan perlindungan tambahan tetapi juga meningkatkan visibilitas terhadap aktivitas jaringan, memberikan solusi yang komprehensif dalam melindungi web server dari ancaman keamanan.

Hasil implementasi *PFSense* dan *Suricata* memberikan manfaat signifikan bagi komunitas maupun industri yang mengandalkan keamanan jaringan, terutama dalam menghadapi *cybercrime* yang semakin kompleks. Secara praktis, temuan ini dapat diterapkan di berbagai skala web server, baik untuk usaha kecil-menengah (UKM) maupun organisasi yang lebih besar, tergantung pada konfigurasi jaringan yang digunakan.

V. KESIMPULAN

Suricata sebagai sistem deteksi dan pencegahan intrusi (IDS/IPS), terbukti efektif dalam mendeteksi dan mencegah berbagai jenis serangan siber pada web server. Pengujian yang dilakukan pada empat jenis serangan, yaitu *Ping of Death, SYN Flood, SQL Injection*, dan *Brute Force Attack* pada SSH, menunjukkan bahwa *Suricata* mampu mengidentifikasi pola lalu lintas yang mencurigakan dengan tingkat keberhasilan deteksi mencapai 92%. Selama pengujian, *Suricata* berhasil mencegah 85% serangan yang dilakukan, dengan waktu respons sistem rata-rata sebesar 250 ms, yang menunjukkan efisiensi dalam memberikan peringatan dini kepada pengguna. *Suricata*, yang beroperasi dengan *IP firewall 192.168.1.100* dan melindungi web server dengan *IP 192.168.1.14*, tidak hanya memberikan deteksi yang tepat waktu, tetapi juga secara proaktif memblokir akses berbahaya sebelum serangan mencapai target. Di sisi lain, *PFSense* berperan penting sebagai *firewall* yang memfilter lalu lintas jaringan. Dalam penelitian ini, kinerjanya dievaluasi dan terbukti efektif dalam mendukung *Suricata* dengan menambah lapisan perlindungan. Kolaborasi antara *PFSense* dan *Suricata* meningkatkan visibilitas terhadap aktivitas jaringan dan mempercepat respons terhadap insiden keamanan, memberikan solusi yang komprehensif dalam melindungi web server dari ancaman keamanan. Penelitian ini mengonfirmasi bahwa pemanfaatan *Suricata* dan *PFSense* sangat mendukung upaya pencegahan serangan siber dan merupakan solusi yang handal untuk meningkatkan keamanan jaringan pada web server. Dengan hasil ini, diharapkan bahwa implementasi *PFSense* dan *Suricata* dapat diterapkan secara lebih luas, tidak hanya pada skala kecil tetapi juga pada infrastruktur server yang lebih kompleks, memberikan kontribusi yang signifikan dalam dunia keamanan jaringan.

REFERENSI

[1] Tedyyana, Agus, Osman Ghazali, and Onno Purbo. "Model Design of Intrusion Detection System on Web Server Using Machine Learning Based." Proceedings of the 11th International Applied Business and Engineering Conference, ABEC 2023, September 21st, 2023, Bengkalis, Riau, Indonesia. 2024.

[2] H. Y. Madawara, D. Manongga, K. S. Wacana, K. Salatiga, and J. Tengah, “Evaluasi Ketergunaan Website Perpustakaan,” no. 6, pp. 44–55, 2023.

[3] Tedyyana, Agus, Osman Ghazali, and Onno W. Purbo. "Machine learning for network defense: automated DDoS detection with telegram notification integration." Indonesian Journal of Electrical Engineering and Computer Science 34.2 (2024): 1102.

[4] I. Rahmadaniar, D. Adrian, A. Tondang, B. S. Fernando, and A. Setiawan, “Implementasi Firewall Menggunakan Iptables untuk Melindungi Server dari Serangan DDoS,” no. 3, pp. 1–10, 2024.

[5] M. Syani, “Implementasi Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (Vps),” *J. Inkofar*, vol. 1, no. 1, pp. 13–20, 2020, doi: 10.46846/jurnalinkofar.v1i1.155.

[6] H. A. S. Adhikari and I. Gashi, “A perspective – retrospective analysis of diversity in signature-based open-source network intrusion detection systems,” *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1331–1346, 2024, doi: 10.1007/s10207-023-00794-9.

Tedyyana, Agus, and Osman Ghazali. "Real-time Hypertext Transfer Protocol Intrusion Detection System on Web Server using Firebase Cloud Messaging." (2023): 385-392.

[7] G. M. Megaputra, R. Aurelius, N. Diaz, N. Wayan, and A. Ulandari, "Perancangan Keamanan Jaringan Menggunakan Honeypot Pada UPTD Pengendalian Bencana BPBD Provinsi Bali," pp. 90–95, 2024.

[8] K. Anwarudin, A. Zulianto, and Y. Prihadi, "Implementasi Network Intrusion Detection System Dan Intrusion Prevention System Pada Jaringan LAN Berbasis Threats Dan Vulnerabilities Assessment …," *InfoSecure*, vol. 1, no. 2, 2020.

[9] Sutarti, A. P. Pancaro, and F. I. Saputra, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, pp. 1–8, 2018.

[10] L. M. Silalahi and A. Kurniawan, "Analisis Keamanan Jaringan Menggunakan Intrusion Prevention System (Ips) Dengan Metode Traffic Behavior," *Electr. J. Rekayasa dan Teknol. Elektro*, vol. 17, no. 1, pp. 71–76, 2023, doi: 10.23960/elc.v17n1.2296.

[11] A. Hita Dahayu Putri, M. Aisyatul, and A. Raya Rambu, "ANALISIS METODE- METODE PENINGKATAN KEAMANAN WEB SERVER," *J. Ilm. Sains dan Teknol.*, vol. 1, no. 2, pp. 4–6, 2024.

[12] A. R. Zain, P. Oktivasari, N. Fauzi Soelaiman, and F. Watsiqul Umam, "Implementasi Intrusion Detection System (Ids) Suricata Dan Management Log Elk Stack Untuk Pendeteksian Kegiatan Mining," *J. Poli-Teknologi*, vol. 22, no. 1, pp. 23–29, 2023, doi: 10.32722/pt.v22i1.4974.

[13] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.

[14] R. Rizal and A. Rahmatulloh, "MIND (Multimedia Artificial Intelligent Networking Database Pengukuran Kinerja Sistem Informasi Penerimaan Mahasiswa Baru Menggunakan GTMetrix, WebAIM dan LoadView," *J. MIND J. | ISSN*, vol. 8, no. 1, pp. 107–118, 2023, [Online]. Available: https://doi.org/10.26760/mindjournal.v8i1.107-118

[15] Ardiansyah, Risnita, and M. S. Jailani, "Teknik Pengumpulan Data Dan Instrumen Penelitian Ilmiah Pendidikan Pada Pendekatan Kualitatif dan Kuantitatif," *J. IHSAN J. Pendidik. Islam*, vol. 1, no. 2, pp. 1–9, 2023, doi: 10.61104/ihsan.v1i2.57.

[16] R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023, doi: 10.33701/jk.v5i1.3208.

[17] 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.

[18] M. Arman and N. Rachmat, "Implementasi Sistem Keamanan Web Server Menggunakan Pfsense," *Jusikom J. Sist. Komput. Musirawas*, vol. 5, no. 1, pp. 13–23, 2020, doi: 10.32767/jusikom.v5i1.752.

[19] P. Veerasingam, S. Abd Razak, A. F. A. Abidin, M. A. Mohamed, and S. D. Mohd Satar, "Intrusion Detection and Prevention System in Sme'S Local Network By Using Suricata," *Malaysian J. Comput. Appl. Math.*, vol. 6, no. 1, pp. 21–30, 2023, doi: 10.37231/myjcam.2023.6.1.88.

[20] S. A. Putra, A. Budiono, and U. Y. K. Septo, "Vulnerability Assesment Web ProposalTugas Akhir Mahasiswa MenggunakanAcunetix dan NMAP," *eProceedings …*, vol. 10, no. 2, pp. 1615–1622, 2023, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/19972%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/download/19972/19337

[21] K. Indar Parawansa, A. Nurhadi, M. Ilmu Komputer, P. Tinggi Manajemen, and I. Nusa Mandiri Jakarta, "Terbit online pada laman web jurnal: https://uia.e-journal.id/INSIT

ANALISIS SYN FLOOD ATTACK MENGGUNAKAN METODE NIST 800-61 REV 2 PADA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM),” vol. 02, no. 01, pp. 1–8, 2024, [Online]. Available: https://uia.e-journal.id/INSIT

[22] A. Budiman, S. Ahdan, and M. Aziz, “Analisis Celah Keamanan Aplikasi Web E- Learning Universitas Abc Dengan Vulnerability Assesment,” *J. Komputasi*, vol. 9, no. 2, pp. 1–10, 2021, [Online]. Available: https://jurnal.fmipa.unila.ac.id/komputasi/article/view/2800

[23] W. Wahyat and P. Kudadiri, “Implementation of Intrusion Detection System With Suricata on Ubuntu 22 . 04 LTS in intrusion detection system research with suricata on,” vol. 21, no. 1, pp. 50–53, 2024.