IMPLEMENTASI DAN ANALISIS DETEKSI SERANGAN JARINGAN PADA WEB SERVER NFT MENGGUNAKAN SURICATA

Phillnov Yohanes Pinontoan[1], Irwan Sembiring[2]
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi,
Universitas Kristen Satya Wacana
Email: [1]philpinontoan@gmail.com, [2]irwan@uksw.edu

ABSTRAK

Penelitian ini berfokus pada masalah keamanan jaringan yang menjadi krusial bagi perusahaan teknologi blockchain dan Non-Fungible Token (NFT) yang rentan terhadap serangan siber seperti DDoS, injeksi SQL, dan malware. Serangan ini tidak hanya menyebabkan kerugian finansial tetapi juga merusak reputasi dan kepercayaan pengguna. Suricata, sebagai sistem deteksi dan pencegahan intrusi open-source, menawarkan berbagai fitur untuk memonitor dan menganalisis lalu lintas jaringan secara real-time. Penelitian ini mengevaluasi efektivitas Suricata dalam mendeteksi ancaman pada web server NFT melalui pendekatan eksperimental. Pengujian dilakukan dengan metode scanning port, web penetration testing, DDoS, dan identifikasi kerentanan sistem web server menggunakan alat seperti NMap, Hping3, Nikto, dan Metasploit. Hasil menunjukkan bahwa Suricata mampu mencatat aktivitas mencurigakan dan mencegah anomali dengan integrasi firewall PFsense. Implementasi Suricata memberikan informasi deteksi serangan web scanning, meskipun tidak memiliki aturan shared object seperti perangkat lunak intrusi lainnya. Penelitian ini memberikan rekomendasi bagi pengembang dan operator platform NFT untuk melindungi aset digital mereka dari serangan siber, serta berkontribusi pada peningkatan keamanan jaringan di sektor NFT.

Kata Kunci: *Blockhain, Non-Fungible Token,* Keamanan Jaringan*, Suricata, PFSense, Web Server.*

ABSTRACT

This research focuses on the critical issue of network security for blockchain technology and Non-Fungible Token (NFT) companies, which are vulnerable to cyberattacks such as DDoS, SQL injection, and malware. These attacks not only cause financial losses but also damage reputation and user trust. Suricata, an open-source intrusion detection and prevention system, offers various features to monitor and analyze network traffic in real-time. This study evaluates the effectiveness of Suricata in detecting threats on NFT web servers through an experimental approach. Testing methods include port scanning, web penetration testing, DDoS, and identifying web server vulnerabilities using tools such as NMap, Hping3, Nikto, and Metasploit. The results show that Suricata can log suspicious activities and prevent anomalies when integrated with the PFsense firewall. While Suricata provides information on web scanning attacks, it lacks shared object rules found in other intrusion software. This research offers recommendations for

ISSN 2798-141X

NFT platform developers and operators to protect their digital assets from cyberattacks and contributes to improving network security in the NFT sector. Thus, this study is highly relevant in the digital era, where information and data security are top priorities for business continuity and user privacy protection.

Keywords: *Blockchain, Non-Fungible Token, Network Security, Suricata, PFSense, Web Server.*

PENDAHULUAN

Dengan pesatnya perkembangan teknologi informasi dan digital, keamanan jaringan menjadi aspek krusial yang harus diperhatikan oleh berbagai institusi dan perusahaan, termasuk yang bergerak dalam bidang teknologi *blockchain* dan *Non-Fungible Token* (NFT) (Fachmi & Mayesti, 2022). NFT telah menjadi fenomena global dalam beberapa tahun terakhir, menawarkan cara baru untuk memiliki, memperdagangkan, dan mengautentikasi aset digital unik. Namun, peningkatan minat dan nilai ekonomi dalam NFT juga menarik perhatian para pelaku kejahatan siber yang mencari celah untuk mengeksploitasi sistem ini (Sulistianingsih & Kinanti, 2022).

Web server yang digunakan untuk mendukung platform NFT seringkali menjadi target serangan siber (Fandy dkk, 2022). Serangan ini dapat berupa *Distributed Denial of Service* (DDoS), injeksi SQL, *malware*, hingga exploitasi kelemahan zero-day. Serangan-serangan ini tidak hanya dapat menyebabkan kerugian finansial yang signifikan, tetapi juga merusak reputasi dan kepercayaan pengguna terhadap platform tersebut (Kusuma, 2021). Oleh karena itu, diperlukan solusi keamanan yang efektif untuk mendeteksi dan mencegah ancaman ini.

Suricata, sebagai sebuah sistem deteksi intrusi (*Intrusion Detection System/IDS*) dan pencegahan intrusi (*Intrusion Prevention System/IPS*) *open-source*, menawarkan berbagai fitur yang kuat untuk memonitor dan menganalisis lalu lintas jaringan secara real-time (Arrasy & Noertjahyana, 2022). *Suricata* mampu mendeteksi berbagai macam ancaman siber dengan menggunakan aturan yang dapat dikustomisasi serta dukungan terhadap berbagai format data dan protokol jaringan (Syani, 2020). Implementasi *Suricata* pada *web server* NFT bertujuan untuk meningkatkan keamanan dengan cara mendeteksi aktivitas mencurigakan atau berbahaya sebelum mereka dapat merusak sistem.

Berdasarkan latar belakang permasalahan yang dikemukakan, penelitian ini akan membahas implementasi dan analisis efektivitas *Suricata* dalam mendeteksi ancaman keamanan pada *web server* NFT. Melalui penelitian ini, diharapkan dapat ditemukan strategi dan metode yang optimal dalam meningkatkan keamanan jaringan, serta memberikan rekomendasi bagi pengembang dan operator *platform* NFT untuk melindungi aset digital mereka dari serangan siber. Dengan demikian, penelitian ini tidak hanya berkontribusi pada peningkatan keamanan jaringan di sektor NFT, tetapi juga memberikan wawasan dan solusi praktis bagi implementasi keamanan pada *web server* secara umum. Hal ini sangat relevan di era digital saat ini, di mana keamanan informasi dan data menjadi prioritas utama bagi keberlangsungan bisnis dan perlindungan privasi pengguna.

ISSN 2798-141X

KAJIAN TEORI

Penelitian Terdahulu

Berikut adalah beberapa penelitian yang telah dilakukan oleh peneliti terdahulu, Penelitian dari Stephani dkk (2020), penelitian ini bertujuan mengimplementasikan *Intrusion Detection System* (IDS) menggunakan Suricata pada *web server* di Jurusan Teknologi Informasi Politeknik Negeri Padang. IDS ini diharapkan dapat *memonitor traffic web server*, mendeteksi dan mencegah penyusup, serta mengidentifikasi aktivitas mencurigakan dalam *log Suricata*. Sistem ini juga akan mendeteksi serangan *web scanning* dengan *tools* seperti *Dirbuster* dan *Skipfish*, serta serangan DDoS menggunakan *slowloris*. Tujuan akhirnya adalah menggantikan sistem pertahanan manual yang dilakukan oleh administrator dengan sistem yang lebih cepat dan optimal. Penelitian ini menggunakan metode *Action Research* dengan tahapan diagnosis untuk mengidentifikasi masalah serangan pada *web server*, perencanaan tindakan yang melibatkan persiapan alat seperti *OPNsense* dengan *Suricata, file rules,* dan laptop penyerang, intervensi berupa pelaksanaan serangan dan konfigurasi Suricata untuk mendeteksinya, evaluasi dengan mengumpulkan dan mengevaluasi *log Suricata* untuk memastikan deteksi serangan, dan refleksi untuk menyimpulkan hasil pengujian serta menambah rule guna meningkatkan keamanan. Hasil penelitian menunjukkan bahwa implementasi IDS menggunakan *Suricata* pada *OPNsense* berhasil mendeteksi dan mencegah serangan terhadap *web server*. Pengujian dengan *Dirbuster, Skipfish, dan slowloris* membuktikan efektivitas *Suricata* dalam mengidentifikasi aktivitas mencurigakan dan serangan, sehingga sistem ini mampu meningkatkan keamanan *web server* secara signifikan.

Penelitian selanjutnya dari Anugrah dkk (2022) menemukan bahwa Penelitian ini bertujuan menguji efektivitas *Suricata* sebagai *Intrusion Prevention System* (IPS) dalam melindungi *web server* dari serangan SQL *Injection* menggunakan SQLMap. Fokusnya adalah mengevaluasi efektivitas rules yang diterapkan dan parameter response time selama serangan. Penelitian dilakukan di Laboratorium PSD menggunakan jaringan LAN statis. *Suricata* diinstal pada PC yang berfungsi sebagai *router* dan *server* IPS, dengan *normal user* dan *attacker* menggunakan Windows 10, serta *web server* dan *server* IPS menggunakan Ubuntu 20.04. Masalah yang dihadapi adalah meningkatkan keamanan jaringan untuk mencegah penyalahgunaan sumber daya melalui serangan SQL *Injection*. Metode penelitian melibatkan pengujian response time sebanyak 30 kali selama serangan berlangsung, dengan *Suricata* mendeteksi serangan melalui signature rules. Hasilnya menunjukkan rata-rata waktu respons *Suricata* adalah 4,260633 milidetik, menunjukkan bahwa *Suricata* mampu mendeteksi dan merespons serangan SQL *Injection* dengan cepat. *Rules* yang efektif adalah yang menggunakan beberapa kode ASCII sebagai kata kunci. Dengan demikian, *Suricata* terbukti efektif sebagai IPS dalam melindungi *web server* dari serangan SQL *Injection* dengan waktu respons yang cepat dan rules yang andal.

Penelitian lainnya dari Zain dkk (2023), Penelitian ini bertujuan mengimplementasikan *Intrusion Detection System* (IDS) menggunakan *Suricata* dan manajemen *log* ELK *Stack* untuk meningkatkan keamanan jaringan komputer. Suricata dipilih karena kemudahannya dalam konfigurasi *rules*, sementara ELK *Stack* mempermudah monitoring keamanan jaringan melalui manajemen log yang efisien.

ISSN 2798-141X

Penelitian ini menguji kinerja sistem IDS *Suricata* dan manajemen log ELK *Stack* melalui parameter *Functional Test*, *Response Time, Detection Rate,* dan *memory usage* akibat kegiatan *web mining*. Tantangan utamanya adalah melindungi komputer dalam jaringan dari ancaman dan serangan, serta mempermudah monitoring dan analisis keamanan. Pengujian komprehensif dilakukan untuk mengevaluasi efektivitas deteksi serangan, kecepatan respons sistem, dan penggunaan memori. Hasil penelitian menunjukkan bahwa *Suricata* berhasil mendeteksi serangan dan kegiatan *web mining* secara efektif, dengan hasil deteksi ditampilkan melalui antarmuka web ELK *Stack*. *Functional Test* memastikan sistem berfungsi dengan baik, *Response Time* menunjukkan respons cepat terhadap serangan, *Detection Rate* tinggi mengindikasikan kemampuan deteksi ancaman yang baik, dan *memory usage* analisis menunjukkan efisiensi penggunaan memori selama kegiatan *web mining*. Implementasi IDS menggunakan *Suricata* dan ELK *Stack* terbukti efektif dalam meningkatkan keamanan jaringan dan mempermudah proses monitoring.

Penelitian lainnya dari Wijaya dkk (2023), penelitian ini bertujuan mendeteksi dan mencegah gangguan atau intrusi pada *web server*, mengurangi ketergantungan pada administrator dalam merespons gangguan secara manual. Metode eksperimen digunakan dengan menerapkan *OPNsense* sebagai *Host Intrusion Prevention System* (HIPS) untuk keamanan *web server*. Dokumentasi hasil eksperimen dilakukan untuk analisis dan menghasilkan rekomendasi perancangan sistem keamanan *web server*. Masalah utama adalah ketergantungan pada administrator yang dapat menyebabkan keterlambatan dalam deteksi dan pencegahan intrusi. Hasil penelitian menunjukkan bahwa *OPNsense* efektif sebagai HIPS untuk mengamankan *web server* di jaringan LAN, mampu mencegah *Port Scanning* dan SQL *injection*. Selain itu, *OPNsense* melindungi *web server* dengan *Web Application Firewall* (WAF) / *Intrusion Prevention System* (IPS). Aplikasi *Metasploit* yang mencoba melakukan DOS *Attack* terhadap web server tidak diizinkan melalui eth0. Dengan demikian, implementasi *OPNsense* sebagai HIPS terbukti efektif dalam melindungi *web server* dari berbagai serangan.

Penelitian terakhir dari Alamsyah dkk (2020), tujuan dari penelitian ini adalah untuk mengimplementasikan *Intrusion Detection and Prevention System* (IDPS) yang mampu mendeteksi dan memblokir serangan dari penyusup dalam jaringan komputer. Permasalahan utama yang ingin diatasi adalah serangan yang dilakukan oleh penyusup, seperti *port scanning* dan penetrasi menggunakan *port-port* terbuka seperti *telnet* dan ftp, yang dapat membahayakan keamanan jaringan komputer. Metode penelitian yang digunakan adalah *Intrusion Detection and Prevention System* (NIDPS) yang dikolaborasikan dengan IP *Tables*. NIDPS berfungsi untuk mendeteksi dan melakukan blokir terhadap serangan yang terjadi, sedangkan IP Tables bertugas untuk memfilter paket data yang masuk dan menjatuhkan paket data yang terindikasi serangan. Hasil penelitian menunjukkan bahwa dengan adanya sistem IDPS ini, serangan dapat dideteksi secara efektif dan pencegahan dilakukan dengan memblokir paket data yang dikirim oleh penyusup melalui *port scanning*, serangan ftp, dan *telnet*. Dengan demikian, keamanan jaringan komputer dapat ditingkatkan secara signifikan melalui implementasi sistem IDPS yang efektif.

ISSN 2798-141X

Landasan Teori

Keamanan jaringan adalah praktik melindungi integritas, kerahasiaan, dan ketersediaan data serta sumber daya di dalam jaringan komputer. Hal ini mencakup berbagai teknologi, perangkat, dan proses untuk mencegah akses yang tidak sah, penyalahgunaan, dan penolakan layanan (Jaelani dkk, 2023). Tujuan utama keamanan jaringan adalah melindungi data dari ancaman internal dan eksternal, mengamankan transmisi data, dan memastikan bahwa sistem tetap berfungsi sebagaimana mestinya (Mulyanto & Fari, 2022).

Web server adalah target umum bagi serangan siber karena mereka mengelola dan menyimpan data yang sensitif serta menjalankan aplikasi yang penting bagi pengguna. Beberapa jenis serangan yang sering menargetkan *web server* meliputi (Hijriyannto, 2023): *Distributed Denial of Service* (DDoS): Serangan yang bertujuan untuk membuat layanan tidak dapat diakses oleh pengguna dengan membanjiri server dengan lalu lintas berlebih.Injeksi SQL: Serangan di mana penyerang menyisipkan kode SQL berbahaya ke dalam permintaan yang dikirimkan ke basis data, memungkinkan mereka untuk mengakses atau memodifikasi data. *Malware*: Perangkat lunak berbahaya yang dirancang untuk merusak, mencuri data, atau mengganggu operasi sistem. Exploitasi *Zero-Day*: Serangan yang memanfaatkan kerentanan perangkat lunak yang belum diketahui oleh pembuatnya.

Teknologi *Non-Fungible* (NFT) adalah jenis aset digital yang mewakili kepemilikan unik atas suatu item atau konten digital yang tersimpan di *blockchain*. NFT berbeda dengan mata uang kripto seperti *Bitcoin* atau *Ethereum* karena setiap NFT memiliki atribut yang berbeda dan tidak dapat dipertukarkan secara langsung dengan NFT lain. Teknologi ini memungkinkan autentikasi dan perdagangan aset digital seperti seni, musik, video, dan item dalam game (Hapsari dkk, 2023).

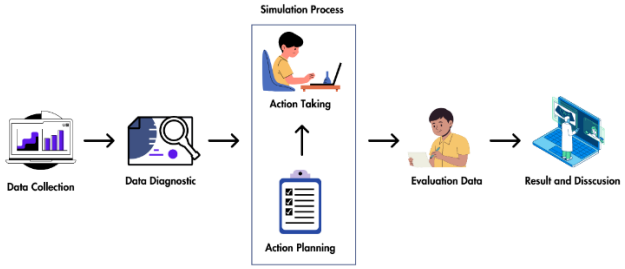
Suricata adalah sistem deteksi dan pencegahan intrusi (IDS/IPS) *open-source* yang dikembangkan oleh *Open Information Security Foundation* (OISF). *Suricata* mampu menganalisis lalu lintas jaringan secara real-time untuk mendeteksi aktivitas mencurigakan atau berbahaya. Beberapa fitur utama *Suricata* meliputi (Yesha dkk, 2024): *Signature-Based Detection*: *Suricata* menggunakan basis data tanda tangan untuk mendeteksi serangan yang dikenal berdasarkan pola yang telah ditentukan. *Protocol Analysis*: *Suricata* dapat memeriksa dan menganalisis berbagai protokol jaringan untuk mengidentifikasi anomali dan serangan. *File Extraction*: *Suricata* dapat mengekstrak file yang ditransmisikan melalui jaringan dan memeriksanya terhadap tanda tangan malware. *High Performance*: *Suricata* dirancang untuk menangani lalu lintas jaringan dengan throughput tinggi, menjadikannya cocok untuk lingkungan dengan kebutuhan kinerja tinggi.

METODOLOGI PENELITIAN

Penelitian ini akan menggunakan pendekatan eksperimental (Ali dkk, 2023) untuk mengimplementasi dan menganalisis Deteksi Serangan Jaringan pada *Web Server* NFT Menggunakan *Suricata*. Eksperimen ini bertujuan untuk mengumpulkan data empiris yang dapat memberikan wawasan mendalam tentang efektivitas *Suricata* dalam

ISSN 2798-141X

keamanan jaringan dalam ekosistem *blockchain*. Langkah-langkah metode penelitian dapat dilihat pada Gambar 1.



Gambar 1. Langkah Penelitian

Adapun Langkah-langkah pada Gambar 1 dapat dijelaskan sebagai berikut:

Data Collection (Pengumpulan Data): Tahap pengumpulan data bertujuan untuk mengumpulkan informasi dan data yang relevan dengan penelitian ini. Proses pengumpulan data mencakup: Studi Literatur: Mengumpulkan informasi dari berbagai sumber seperti buku, jurnal ilmiah, artikel, dan dokumen terkait tentang *Suricata*, keamanan jaringan, serangan pada *web server*, dan teknologi NFT. Observasi: Melakukan observasi langsung pada web server NFT untuk memahami lingkungan operasional dan jenis serangan yang mungkin terjadi.

Data Diagnostic (Diagnosis Data): Tahap diagnosis data bertujuan untuk menganalisis data yang telah dikumpulkan dan mengidentifikasi potensi ancaman serta pola serangan. Proses diagnosis data meliputi: Analisis Lalu Lintas Jaringan: Memeriksa data lalu lintas jaringan untuk mengidentifikasi anomali dan aktivitas mencurigakan. Evaluasi *Log Server*: Menganalisis *log server* untuk mendeteksi tanda-tanda serangan seperti percobaan akses yang tidak sah, kesalahan autentikasi, dan aktivitas mencurigakan lainnya. Identifikasi Kerentanan: Mengidentifikasi kerentanan dalam sistem yang dapat dieksploitasi oleh penyerang.

Simulation Process (Proses Simulasi): Proses simulasi bertujuan untuk menguji efektivitas *Suricata* dalam mendeteksi dan merespons serangan pada *web server* NFT. Tahap ini terdiri dari dua sub-tahapan utama, yaitu perencanaan aksi dan pelaksanaan aksi.

*Action Planning (*Perencanaan Aksi): Perencanaan aksi melibatkan penyusunan strategi dan rencana untuk mengimplementasikan *Suricata* pada *web server* NFT. Proses ini mencakup: Konfigurasi *Suricata*: Menentukan parameter konfigurasi *Suricata* yang sesuai untuk lingkungan *web server* NFT, Penyusunan Aturan Deteksi: Menyesuaikan aturan deteksi *Suricata* untuk mengidentifikasi ancaman yang spesifik terhadap *web server* NFT. Rencana Implementasi: Menyusun rencana implementasi yang mencakup langkah-langkah detail untuk mengintegrasikan *Suricata* ke dalam sistem yang ada.

Action Taking (Pelaksanaan Aksi): Pelaksanaan aksi melibatkan implementasi Suricata sesuai dengan rencana yang telah disusun. Proses ini mencakup: Instalasi dan Konfigurasi: Melakukan instalasi dan konfigurasi *Suricata* pada *web server* NFT sesuai dengan parameter yang telah ditentukan, Pengujian Sistem: Melakukan pengujian awal

ISSN 2798-141X

untuk memastikan bahwa *Suricata* berfungsi dengan baik dan dapat mendeteksi serangan dan Pemantauan dan Penyesuaian: Memantau kinerja *Suricata* dan melakukan penyesuaian konfigurasi jika diperlukan untuk mengoptimalkan deteksi ancaman.

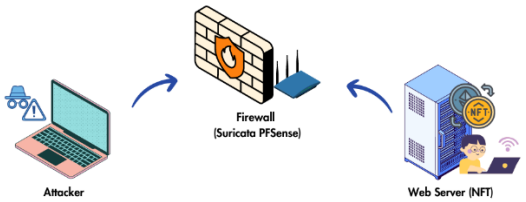
Evaluation Data (Evaluasi Data): Tahap evaluasi data bertujuan untuk menilai efektivitas dan kinerja Suricata dalam mendeteksi dan merespons serangan pada *web server* NFT. Proses evaluasi meliputi: Analisis Hasil Deteksi: Menganalisis hasil deteksi *Suricata* untuk menilai akurasi dan efisiensi dalam mengenali serangan. Evaluasi Kinerja: Mengukur dampak penggunaan *Suricata* terhadap kinerja dan stabilitas *web server* NFT.

Result and Discussion (Hasil dan Pembahasan): Tahap hasil dan pembahasan bertujuan untuk menyajikan temuan penelitian dan mendiskusikan implikasinya. Proses ini mencakup: Presentasi Hasil: Menyajikan hasil analisis dan evaluasi kinerja *Suricata* dalam bentuk yang terstruktur dan mudah dipahami, Pembahasan Temuan: Membahas temuan utama, termasuk kekuatan dan kelemahan *Suricata* dalam mendeteksi serangan pada *web server* NFT dan Rekomendasi: Memberikan rekomendasi untuk meningkatkan keamanan *web server* NFT berdasarkan hasil penelitian dan temuan yang diperoleh.

HASIL DAN PEMBAHASAN

Hasil Pengujian

Pada tahap hasil dan pembahasan, penjelasan metode penelitian difokuskan pada analisis dan pengujian perangkat lunak. Proses analisis menunjukkan adanya kelemahan dalam sistem untuk mendeteksi serangan jaringan. *Web server* memerlukan sistem keamanan yang mampu melindungi dari berbagai jenis serangan dan upaya penyusupan atau pemindaian oleh pihak ketiga atau *attacker*. Tahap perancangan kemudian mengimplementasikan konfigurasi yang diperlukan berdasarkan hasil analisis sebelumnya. Gambar 2 menunjukkan skema perancangan IDS, di mana penyerang berada di luar *web server*. Serangan dapat masuk melalui *internet*, melewati *router,* dan kemudian diperiksa oleh sistem IDS *Suricata*. Pemeriksaan serangan oleh *Suricata* dilakukan dengan dua metode: pertama, metode *signature-based* yang mencocokkan lalu lintas jaringan dengan basis data yang berisi pola serangan yang umum terjadi; kedua, metode *anomaly-based* yang membandingkan pola serangan yang sedang dipantau dengan pola serangan yang dikenal.



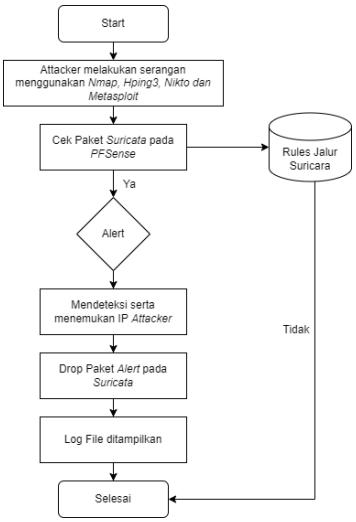
Gambar 2. Topologi Keamanan Jaringan IDS menggunakan *Suricata*

IDS yang digunakan adalah *Suricata* pada sistem operasi *Ubuntu Linux*, yang bertujuan melindungi *real server*, *client server*, dan jaringan di bawahnya. *Suricata* memerlukan paket dan *library* untuk pembangunannya, serta paket untuk aturan (*rules*)

ISSN 2798-141X

yang sangat penting karena IDS bekerja berdasarkan aturan tersebut. Aturan ini berupa skrip yang dapat mengenali tindakan penyusupan yang sedang terjadi pada jaringan yang dilindungi oleh sistem IPS. IPS menggunakan *firewall* untuk memblokir paket yang sesuai dengan aturan yang dibuat.

Dalam membangun jaringan atau *server*, langkah pertama adalah menentukan bentuk topologi (Rezki dkk, 2021) yang akan digunakan yang telah dijelaskan pada Gambar 2. Topologi yang dirancang memerlukan tiga komponen penting: *PFsense* sebagai *router* sekaligus *firewall* yang akan mendeteksi serangan dari *Kali Linux*, yang berfungsi sebagai penyerang. IP *Address* dari *Kali Linux* adalah 192.168.1.100 dan dari *PFsense* adalah 192.168.1.66. Objek yang akan diserang adalah *web server* dengan IP Address 192.168.1.9 yang merupakan *web server* dari NFT. Metode pengujian yang digunakan ada dua, dengan empat alat: metode *scanning port* menggunakan alat *NMap*, metode *Web Penetration Testing* dan Ddos menggunakan alat *Hping3*, metode identifikasi *web server* untuk mengevaluasi kerentanan sistem *web server* menggunakan alat *Nikto* dan metode *Web Penetration testing* menggunakan *metasploit*.



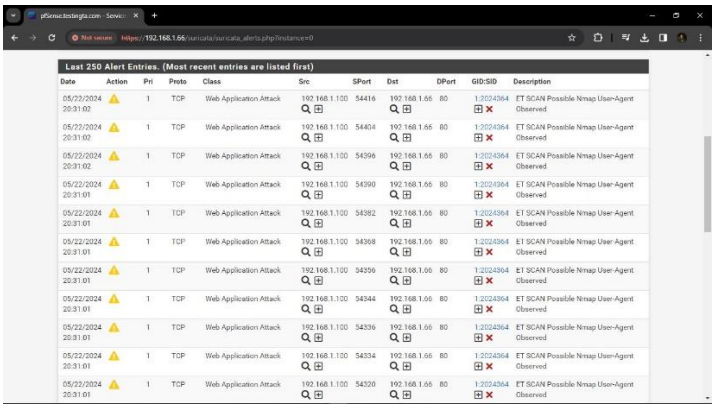
Gambar 3. *Flowchart* sistem *Suricata* dalam mendeteksi serangan

Flowchart pada Gambar 3 menjelaskan secara menyeluruh cara kerja sistem *Suricata*. Paket data yang mengarah ke *server* pertama kali diperiksa oleh *Suricata*. Kemudian, paket data tersebut dicocokkan dengan *Rules Suricata*. Jika paket data tersebut terdeteksi sebagai serangan, *Suricata* akan menghasilkan peringatan dan membuat *Log File* (Veerasingam dkk, 2023). Pada *Pfsense*, terdapat aturan-aturan yang memungkinkan pengguna untuk mengatur bagaimana *Suricata* beroperasi. Pengguna dapat menyesuaikan aturan *Suricata* untuk memblokir atau mengizinkan serangan yang ditujukan ke *Web Server*.

Untuk mengetahui apakah *suricata* atau metode deteksi penyerangan telah berjalan dengan baik dan benar, peneliti melakukan beberapa pengujian antara lain sebagai berikut: Pengujian *Scanning Port* menggunakan *Nmap*, Menggunakan sistem operasi *Kali Linux* sebagai *attacker*, dengan alat *Nmap*, Buka *terminal* pada *Kali Linux*

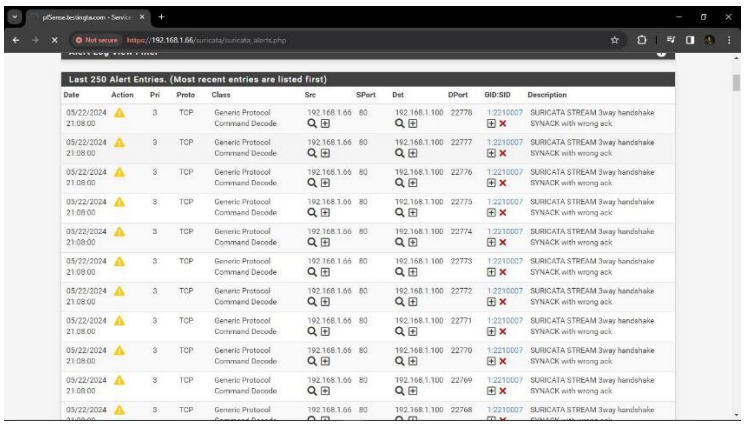
ISSN 2798-141X

dan ketikan perintah "*nmap -a (ip target)"*, tunggu hingga proses *scanning* selesai, *Suricata* melalui *PFsense*, mendapatkan *alert* serangan yang menyerang *web server* yang sedang digunakan dan Hasil *alert* yang ditampilkan pada *suricata* melalui *PFsense* dapat dilihat pada menu *services -> suricata -> alert,* tampilannya dapat dilihat pada Gambar 4.



Gambar 4. Hasil *Alert Nmap* yang ditemukan *Suricata* pada *PFsense*

Pengujian berikutnya yaitu *Web Penetration Testing* dan *Ddos* menggunakan alat *Hping3* Menggunakan sistem operasi *Kali Linux* sebagai *attacker*, dengan alat *Hping3*, Buka *terminal* pada *Kali Linux* dan ketikan perintah "*hping3 -I u1 -S –p 80 (ip target)"*, tunggu hingga proses *scanning* selesai, *Suricata* melalui *PFsense*, mendapatkan *alert* serangan yang menyerang *web server* yang sedang digunakan dan Hasil *alert* yang ditampilkan pada *suricata* melalui *PFsense* dapat dilihat pada menu *services -> suricata -> alert*.



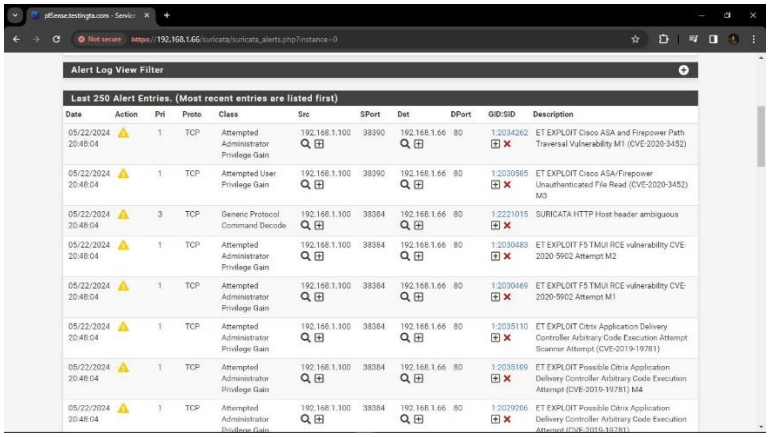
Gambar 5. Hasil *Alert Web Penetration* dan *Ddos* yang ditemukan *Suricata*

Pada Gambar 5, *Suricata* mendeteksi kemungkinan serangan TCP SYN *Flood* pada *server web*. Serangan SYN *Flood* adalah jenis serangan DoS (*Denial-of-Service*) yang bertujuan untuk membanjiri *server* dengan paket TCP SYN (Parawansa dkk, 2024). Paket SYN adalah paket TCP yang dikirim oleh klien ke server untuk memulai

ISSN 2798-141X

koneksi TCP. Dalam serangan SYN Flood, penyerang mengirimkan sejumlah besar paket SYN ke *server* tanpa menyelesaikan koneksi. Hal ini menyebabkan *server* kehabisan sumber daya, seperti memori dan CPU, sehingga tidak dapat melayani permintaan yang sah dari klien lain.

Pengujian Berikutnya yaitu *Webserver Vulnerability Scanning* menggunakan alat *Nikto* dengan cara Menggunakan sistem operasi *Kali Linux* sebagai *attacker*, dengan alat *Nikto*, Buka *terminal* pada *Kali Linux* dan ketikan perintah "*nikto -h (ip target)"*, tunggu hingga proses *scanning* selesai, *Suricata* melalui *PFsense*, mendapatkan *alert* serangan yang menyerang *web server* yang sedang digunakan dan Hasil *alert* yang ditampilkan pada *suricata* melalui *PFsense* dapat dilihat pada menu *services -> suricata -> alert*.



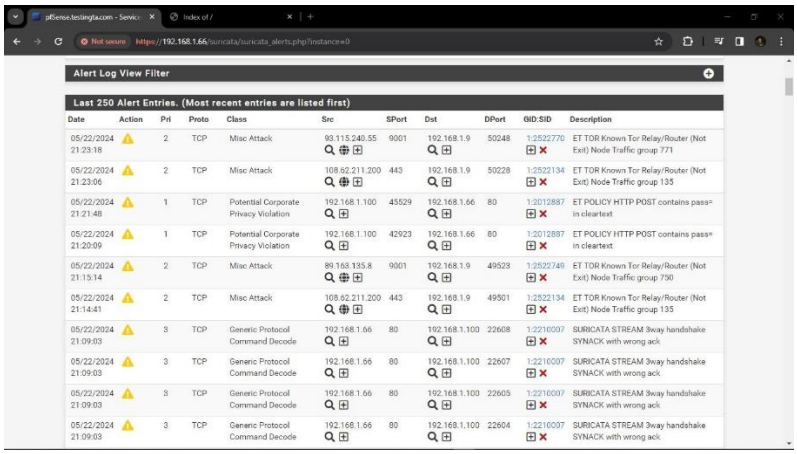
Gambar 6. Hasil *Webserver Vulnerability Scanning* yang ditemukan *Suricata*

Pada Gambar 6 *Alert Suricata* ini menunjukkan kemungkinan upaya eksploitasi kerentanan CVE-2020-3452 pada *Cisco ASA* dan *Firepower*. Kerentanan ini dapat memungkinkan penyerang untuk mendapatkan akses *privileged* pada perangkat dan melakukan tindakan berbahaya (Budiman dkk, 2021).

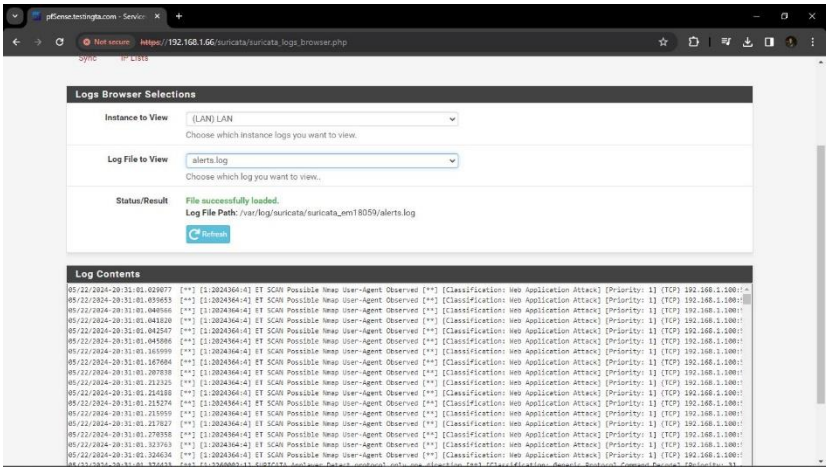
Pengujian selanjutnya yaitu *Metasploit* menggunakan alat *msfconsole* dengan cara Menggunakan sistem operasi *Kali Linux* sebagai *attacker*, dengan alat *msfconsole*, Buka *terminal* pada *Kali Linux* dan ketikan perintah "*msfconsole",* Ketika fitur *msfconsole* terbuka ketikan perintah *"use exploit/multi/http/php_cgi_arg_injection"*, Setelah terbuka ketikan perintah *"RHOST (IP Target)"* lalu ketikan perintah *"run"* tunggu hingga proses selesai, *Suricata* melalui *PFsense*, mendapatkan *alert* serangan yang menyerang *web server* yang sedang digunakan dan Hasil *alert* yang ditampilkan pada *suricata* melalui *PFsense* dapat dilihat pada menu *services -> suricata -> alert*.

Pada Gambar 7 *suricata* mendeteksi kemungkinan aktivitas TOR (*The Onion Router*) pada *server web*. TOR adalah jaringan anonim yang memungkinkan pengguna untuk menyembunyikan identitas dan lokasi mereka saat menjelajah internet (Putra dkk, 2022). Suricata mendeteksi pola trafik yang menunjukkan kemungkinan penggunaan node TOR yang bukan merupakan *node exit*. *Node exit* adalah node TOR yang memungkinkan pengguna keluar dari jaringan TOR dan mengakses internet publik.

ISSN 2798-141X



Gambar 7. Hasil *Metasploit* yang ditemukan *Suricata* pada *PFsense*



Gambar 8. Hasil *Metasploit* yang ditemukan *Suricata* pada *PFsense*

Gambar 8 merupakan daftar alert *Suricata* yang terdeteksi. *Alert* tersebut menunjukkan adanya berbagai aktivitas mencurigakan pada *server web* yang dihosting pada alamat IP 192.168.1.9 yang merupakan *web server* dari NFT.

Dengan pengujian yang telah dilakukan dapat ditemukan bahwa *suricata* atau metode deteksi penyerangan telah berjalan dengan baik dan benar dengan *alert* yang telah ditemukan serta peringatan yang diberikan oleh suricata menggunakan *PFsense* untuk mengamankan *webserver* dari NFT.

KESIMPULAN

Implementasi dan Analisis Deteksi Serangan Jaringan pada *Web Server* NFT Menggunakan Suricata menggunakan Sistem Deteksi Intrusi (IDS) *Suricata* yang dibangun dapat memantau lalu lintas di *web server* untuk NFT dan menyimpan hasil deteksi serta memberikan masuknya penyusup ke dalam *web server*. Menggunakan metode *Experimental* pengujian telah dilakukan dengan menggunakan beberapa

ISSN 2798-141X

pengujian antara lain metode *scanning port* menggunakan alat *NMap*, metode *Web Penetration Testing* dan Ddos menggunakan alat *Hping3*, metode identifikasi *web server* untuk mengevaluasi kerentanan sistem *web server* menggunakan alat *Nikto* dan metode *Web Penetration testing* menggunakan *Metasploit* telah berjalan dengan baik dan sesuai dengan *rules* yang diterapkan. Hasil yang didapatkan, *Suricata* juga dapat mencatat aktivitas mencurigakan yang terdeteksi dalam lognya. Implementasi Suricata dengan firewall *PFsense* memungkinkan deteksi dan pencegahan anomali pada *web server* dari serangan penyusup terhadap *web server* NFT yang dimiliki. Penerapan Sistem Deteksi Intrusi (IDS) menggunakan *Suricata* pada *web server* memberikan informasi tentang deteksi serangan *web scanning*. Selain itu, *Suricata* tidak memiliki aturan *shared object* seperti perangkat lunak intrusi lainnya.

DAFTAR PUSTAKA

Alamsyah, H., Riska, A. A. A., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. *JOINTECS (Journal of Information Technology and Computer Science)*, *5*(1), 17. https://doi.org/10.31328/jointecs.v5i1.1240

Ali, A. M., Satriawati, S., & Nur, R. (2023). Meningkatkan Hasil Belajar IPA Menggunakan Metode Eksperimen Kelas VI Sekolah Dasar. *PTK: Jurnal Tindakan Kelas*, *3*(2), 114-121. https://doi.org/10.53624/ptk.v3i2.150

Anugrah, F. T, Ikhwan, S., & Gusti A.G, J. (2022). Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection. *Techné : Jurnal Ilmiah Elektroteknika*, *21*(2), 199–210. https://doi.org/10.31358/techne.v21i2.320

Arrasy, D. R., & Noertjahyana, A. (2022). Analisis perbandingan keakuratan deteksi serangan dan efisiensi pemakaian CPU resources dari tools pendeteksi serangan SNORT dan SURICATA yang di pasang di web server. *Jurnal Infra*, *10*(1), 22-30. http://publication.petra.ac.id/index.php/teknik-informatika/article/view/11894

Budiman, A., Ahdan, S., & Aziz, M. (2021). Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment. *Jurnal Komputasi*, *9*(2), 1–10. https://jurnal.fmipa.unila.ac.id/komputasi/article/view/2800

Fachmi, A., & Mayesti, N. (2022). Tinjauan literatur argumentatif tentang kepemilikan data arsip digital non-fungible token (NFT) pada teknologi blockchain. *Berkala Ilmu Perpustakaan Dan Informasi*, *18*(1), 144–158. https://doi.org/10.22146/bip.v18i1.3989

Fandy, Rosmasari, & Putra, G. M. (2022). Pengujian Kinerja Web Server Atas Penyedia Layanan Elastic Cloud Compute (EC2) Pada Amazon Web Services (AWS). *Adopsi Teknologi Dan Sistem Informasi (ATASI)*, *1*(1), 21–35. https://doi.org/10.30872/atasi.v1i1.45

Hapsari, R. A., Aprinisa, A., & Putri, R. A. (2023). Perlindungan Hukum terhadap Teknologi Non-Fungible Token (NFT) sebagai Identitas Karya Intelektual. *Amsir Law Journal*, *4*(2), 236–245. https://doi.org/10.36746/alj.v4i2.189

Hijriyannto, B. H. (2023). Perbandingan Penerapan Metode Pengamanan Web Server

Menggunakan Mod Evasive Dan Ddos Deflate Terhadap Serangan Slow Post. *Journal of Engineering, Computer Science and Information Technology (JECSIT)*, *1*(2), 88–92. https://doi.org/10.33365/jecsit.v1i1.11

Jaelani, W. L., Yanto, Y., & Khoirunnisa, F. (2023). PENETRATION TESTING WEBSITE DENGAN METODE BLACK BOX TESTING UNTUK MENINGKATKAN KEAMANAN WEBSITE PADA INSTANSI (REDACTED). *Naratif: Jurnal Nasional Riset, Aplikasi dan Teknik Informatika*, *5*(1), 1-8. https://doi.org/10.53580/naratif.v5i1.180

Kusuma, G. H. A. (2021). Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing (JIAC)*, *2*(2), 1-4. http://journal.univpancasila.ac.id/index.php/jiac/article/view/3259

Mulyanto, Y., & Fari, A. A. (2022). Analisis Keamanan Login Router Mikrotik Dari Serangan Bruteforce Menggunakan Metode Penetration Testing (Studi Kasus: Smk Negeri 2 Sumbawa). *Jurnal Informatika Teknologi dan Sains (Jinteks)*, *4*(3), 145-155. https://doi.org/10.51401/jinteks.v4i3.1897

Parawansa, K. I., & Nurhadi, A. (2024). ANALISIS SYN FLOOD ATTACK MENGGUNAKAN METODE NIST 800-61 REV 2 PADA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM). *INFORMATIKA SAINS TEKNOLOGI*, *2*(1), 1-8. https://uia.e-journal.id/INSIT

Putra, A. D., Santoso, J. D., & Ardiansyah, I. (2022). Analisis Malicious Software Trojan Downloader Pada Android Menggunakan Teknik Reverse Engineering (Studi Kasus: Kamus Kesehatan v2.apk). *Building of Informatics, Technology and Science (BITS)*, *4*(1), 69–79. https://doi.org/10.47065/bits.v4i1.1515

Rezki, M., Ihsan, M. I. R., & Ambarsari, D. A. (2021). Animasi Interaktif Klasifikasi Jangkauan Dan Topologi Jaringan Komputer Berbasis Android Sebagai Media Belajar. *Computer Science (CO-SCIENCE)*, *1*(2), 113–122. https://doi.org/10.31294/coscience.v1i2.466

Stephani, E., Fitri Nova, & Ervan Asri. (2020). Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *1*(2), 67–74. https://doi.org/10.30630/jitsi.1.2.10

Sulistianingsih, D., & Kinanti, A. K. (2022). Hak Karya Cipta Non-Fungible Token (NFT) Dalam Sudut Pandang Hukum Hak Kekayaan Intelektual. *Krtha Bhayangkara*, *16*(1), 197-206. https://doi.org/10.31599/krtha.v16i1.1077

Syani, M. (2020). Implementasi Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (Vps). *Jurnal Inkofar*, *1*(1), 13–20. https://doi.org/10.46846/jurnalinkofar.v1i1.155

Veerasingam, P., Abd Razak, S., Abidin, A. F. A., Mohamed, M. A., & Mohd Satar, S. D. (2023). Intrusion Detection and Prevention System in Sme'S Local Network By Using Suricata. *Malaysian Journal of Computing and Applied Mathematics*, *6*(1), 21–30. https://doi.org/10.37231/myjcam.2023.6.1.88

Wijaya, A. W. A., Kalsum, T. U & Riska. (2023). Penerapan OPNsense Sebagai Sistem

Keamanan Web Server Menggunakan Metode Host Instrusion Prevention System. *JURNAL AMPLIFIER: JURNAL ILMIAH BIDANG TEKNIK ELEKTRO DAN KOMPUTER*, *13*(2), 91-100. https://doi.org/10.33369/jamplifier.v13i2.31514

Yesha, I. P., Ariwanta, A., Yota, K., Aryanto, E., & Gunadi, I. G. A. (2024). *SURICATA ACCURACY OPTIMIZATION BASED ON LIVE ANALYSIS USING ONE- CLASS SUPPORT VECTOR MACHINE METHOD AND STREAMLIT FRAMEWORK OPTIMASI AKURASI SURICATA BERBASIS LIVE ANALYSIS MENGGUNAKAN METODE ONE-CLASS SUPPORT VECTOR MACHINE DAN FRAMEWORK*. *5*(2), 415–427.

Zain, A. R., Oktivasari, P., Fauzi Soelaiman, N., & Watsiqul Umam, F. (2023). Implementasi Intrusion Detection System (Ids) Suricata Dan Management Log Elk Stack Untuk Pendeteksian Kegiatan Mining. *Jurnal Poli-Teknologi*, *22*(1), 23–29. https://doi.org/10.32722/pt.v22i1.4974

ISSN 2798-141X