PRINSIP : Portal Riset & Inovasi Sistem Perangkat Lunak
Volume 2, Nomor 2, April 2024
http://doi.org/10.59696/prinsip.v2i2.113
e-ISSN : 2985-802X
p-ISSN : 2987-0534

Submit : 04 April 2024

Implementasi Intrusion Prevention System Suricata Sebagai Pengamanan Dari Serangan Dos Dan DDos

[1]Muhammad Rizqy Alim, [2] Riska Nurtantyo Sarbini, [3]Iin Kurniasari
Universitas Islam Kadiri, Kota Kediri, Indonesia
[1]rizqyalim10@gmail.com, [2]riskanurtantyosarbini@gmail.com, [3]iin.kurniasari@uniska-kediri.ac.id

ABSTRAK

SMK PGRI Kras mengalami gangguan jaringan saat pelaksanaan ujian akibat serangan DoS dan DDoS. Penelitian ini bertujuan mengimplementasikan Intrusion Prevention System (IPS) Suricata sebagai solusi perlindungan jaringan. Penelitian menggunakan metode Network Development Life Cycle (NDLC) dengan tahapan analisis, desain, simulasi, implementasi, dan pengujian. Hasil menunjukkan bahwa Suricata efektif dalam meningkatkan performa jaringan, menurunkan packet drop rate, menjaga kestabilan latency, serta efisien dalam penggunaan CPU dan RAM. Implementasi IPS Suricata mampu mendeteksi dan memblokir trafik berbahaya secara real-time tanpa mengganggu trafik sah.

Kata Kunci: Suricata, IPS, DoS, DDoS, Keamanan Jaringan

PENDAHULUAN

Perkembangan teknologi informasi memudahkan akses data namun meningkatkan risiko keamanan jaringan. Internet telah menjadi bagian penting dalam kehidupan sehari-hari, termasuk dalam dunia pendidikan. Sekolah-sekolah mulai menerapkan sistem digital untuk mendukung proses belajar mengajar, manajemen data siswa, serta pelaksanaan ujian berbasis komputer. Namun, ketergantungan terhadap jaringan juga menghadirkan tantangan besar, yaitu ancaman keamanan siber yang semakin kompleks dan canggih.

Keamanan jaringan merupakan salah satu aspek penting dalam menjaga keberlangsungan sistem informasi. Keamanan ini bertujuan untuk melindungi data dan infrastruktur jaringan dari berbagai ancaman, seperti malware, akses ilegal, dan serangan DoS maupun DDoS. Dalam konteks pendidikan, gangguan terhadap jaringan dapat mengakibatkan terhambatnya proses belajar mengajar dan merugikan siswa serta tenaga pendidik.

Salah satu jenis serangan yang umum terjadi adalah Denial of Service (DoS) dan Distributed Denial of Service (DDoS), yaitu upaya untuk membuat layanan jaringan tidak dapat diakses oleh pengguna sah dengan cara membanjiri jaringan dengan lalu lintas data yang tidak sah. Serangan ini berdampak serius terhadap keberlangsungan layanan, terutama pada saat-saat krusial seperti ujian sekolah. SMK PGRI Kras menjadi salah satu sekolah yang mengalami gangguan jaringan saat pelaksanaan ujian akibat serangan semacam ini.

Untuk mengatasi masalah tersebut, diperlukan solusi yang mampu mendeteksi dan menangkal serangan secara real-time. Salah satu sistem yang dapat digunakan adalah Intrusion Prevention System (IPS). IPS berfungsi tidak hanya untuk mendeteksi serangan tetapi juga untuk memblokir lalu lintas mencurigakan secara otomatis. Sistem ini bekerja dengan memantau lalu lintas jaringan dan menerapkan aturan keamanan berdasarkan signature atau pola tertentu dari serangan.

Suricata adalah salah satu tools IPS open-source yang mendukung mode inline, multi-threading, dan kompatibel dengan berbagai sistem operasi. Keunggulan Suricata terletak pada kemampuannya dalam melakukan inspeksi mendalam terhadap paket data, serta mendukung integrasi dengan sistem manajemen log seperti ELK Stack. Suricata juga mendukung penggunaan

rule dari Emerging Threats dan Snort, sehingga memudahkan administrator jaringan dalam mengembangkan sistem deteksi.

Untuk mendukung kinerja Suricata dalam mode inline, digunakan Iptables sebagai tools firewall yang memungkinkan pengalihan lalu lintas jaringan ke NFQUEUE. Dengan konfigurasi tersebut, paket yang masuk ke jaringan akan dianalisis terlebih dahulu oleh Suricata sebelum diteruskan ke tujuan. Kombinasi antara Suricata dan Iptables mampu menciptakan sistem pengamanan jaringan yang proaktif dan efisien.

Suricata memungkinkan administrator jaringan untuk menerapkan aturan (rules) yang spesifik guna memblokir jenis serangan tertentu seperti Ping Flood, SYN Flood, dan HTTP Flood. Dengan implementasi yang tepat, Suricata dapat menjadi solusi efisien dan efektif dalam menjaga stabilitas jaringan dan memastikan kelancaran aktivitas berbasis komputer di sekolah. Penelitian ini berfokus pada implementasi dan evaluasi performa Suricata dalam menghadapi serangan DoS dan DDoS pada jaringan sekolah. Penelitian ini juga diharapkan dapat menjadi rujukan untuk pengembangan sistem keamanan di lingkungan pendidikan lain yang menghadapi masalah serupa.

Berdasarkan latar belakang tersebut, tujuan dari penelitian ini adalah untuk mengimplementasikan Intrusion Prevention System (IPS) Suricata pada jaringan SMK PGRI Kras guna meningkatkan keamanan terhadap serangan DoS dan DDoS, serta menganalisis performa jaringan sebelum dan sesudah penerapan sistem. Penelitian ini diharapkan dapat menjadi solusi efektif dan efisien dalam menjaga kestabilan jaringan, khususnya saat pelaksanaan kegiatan penting seperti ujian berbasis komputer.

Batasan dalam penelitian ini difokuskan pada penerapan sistem IPS Suricata hanya pada jaringan laboratorium komputer di SMK PGRI Kras. Penelitian ini tidak mencakup aspek keamanan fisik jaringan maupun pengujian terhadap jenis serangan siber lainnya di luar DoS dan DDoS.

TINJAUAN PUSTAKA

Keamanan jaringan adalah praktik untuk melindungi jaringan komputer dan data dari akses, modifikasi, dan perusakan yang tidak sah. Dalam era digital, keamanan jaringan sangat penting karena jaringan menjadi tulang punggung komunikasi dan pengelolaan data di berbagai sektor, termasuk pendidikan.

Intrusion Prevention System (IPS) merupakan sistem keamanan yang secara aktif memantau lalu lintas jaringan dan memblokir paket yang dianggap mencurigakan. IPS bekerja secara real-time, berbeda dengan IDS (Intrusion Detection System) yang hanya mendeteksi tanpa memblokir. Sistem ini sangat efektif dalam menangani ancaman siber yang dinamis dan masif seperti serangan DoS dan DDoS.

Suricata adalah salah satu sistem IPS modern yang dikembangkan oleh OISF (Open Information Security Foundation). Suricata memiliki kemampuan multi-threading, packet inspection hingga lapisan aplikasi, dan mendukung perekaman lalu lintas (packet capture). Dibandingkan dengan sistem lain seperti Snort, Suricata memiliki performa lebih tinggi dalam lingkungan trafik yang padat.

Iptables adalah bagian dari netfilter framework pada sistem operasi Linux yang digunakan untuk memfilter dan mengatur lalu lintas jaringan. Dalam implementasi IPS menggunakan Suricata, iptables digunakan untuk mengarahkan paket ke dalam antrian (queue) yang kemudian diproses oleh Suricata.

Penelitian sebelumnya oleh Suhendi dan Cahyo menunjukkan bahwa penggunaan IDS Snort efektif dalam mendeteksi dan mengurangi serangan jaringan. Penelitian Wahyudi dan Utomo menunjukkan efektivitas IPS berbasis Suricata dalam mencegah DDoS dan port scanning. Susanti dkk. mengembangkan sistem kombinasi OSSEC dan Honeypot untuk meningkatkan deteksi. Penelitian Prisscilya dan Santoso menyoroti IDS dalam konteks industri. Nainggolan dkk. menunjukkan penggunaan Snort untuk monitoring DDoS di server Ubuntu. Penelitian-penelitian tersebut memberikan landasan bahwa sistem IPS/IDS dapat digunakan secara efektif dalam lingkungan pendidikan dan industri. Suricata sendiri terus dikembangkan dan digunakan secara luas di berbagai organisasi karena keandalannya dalam mengolah paket secara cepat dan akurat.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan NDLC (Network Development Life Cycle) yang terdiri dari enam tahapan:

1. **Analysis:** Pengumpulan data dari pihak IT SMK PGRI Kras untuk mengidentifikasi celah keamanan jaringan. Observasi juga dilakukan pada infrastruktur jaringan yang digunakan selama pelaksanaan ujian.
2. **Design:** Perancangan topologi dan pemilihan perangkat keras dan lunak. Topologi dirancang menggunakan Suricata secara inline di jaringan laboratorium. Rancangan ini memastikan bahwa semua trafik harus melewati sistem IPS sebelum sampai ke tujuan.
3. **Simulation:** Uji coba dilakukan dengan mensimulasikan serangan DoS dan DDoS menggunakan metode Ping Flood, SYN Flood, dan HTTP Flood. Simulasi ini merepresentasikan ancaman nyata yang sebelumnya terjadi di lingkungan sekolah.
4. **Implementation:** Instalasi Suricata dan konfigurasi NFQUEUE serta iptables untuk mengarahkan trafik ke sistem IPS. Proses ini mencakup pengaturan rules dan penyesuaian buffer agar sistem dapat memproses trafik dalam jumlah besar.
5. **Monitoring:** Pengamatan parameter performa jaringan dan validasi keberhasilan pemblokiran serangan. Data diperoleh menggunakan berbagai tools seperti iperf3, tcpdump, ping, dan htop.
6. **Management:** Dokumentasi dan evaluasi sistem keamanan serta perencanaan untuk pemeliharaan dan pembaruan rules Suricata. Tahap ini juga mencakup saran pengembangan sistem lanjutan yang lebih kompleks.

Alat dan Teknik:

- Tools: Suricata, VirtualBox, IPTables, iperf3, ping, tcpdump, htop
- Pengujian dilakukan dalam tiga kondisi: normal, diserang tanpa IPS, dan diserang dengan IPS aktif
- Parameter pengujian: Throughput, Packet Drop Rate, Latency, CPU & RAM Usage

HASIL DAN PEMBAHASAN

Pengujian dilakukan dalam lima skenario, yaitu kondisi normal tanpa serangan, kondisi saat serangan Ping Flood, HTTP Flood, SYN Flood, dan kondisi setelah IPS Suricata aktif. Setiap skenario dianalisis menggunakan parameter throughput, latency, packet drop, CPU usage, dan RAM usage. Hasil pengukuran disajikan pada Tabel 1 berikut.

Tabel 1 Hasil Pengukuran

Skenario	Throughput	Latency	Packet Drop	CPU Usage	RAM Usage
Normal (Tanpa Serangan)	2.1 Gbps	0.05 ms	0%	0.14%	208 MB
Saat Ping Flood	-	213–593 ms	96.72%	-	-
Saat HTTP Flood	Tinggi tapi fluktuatif	2 ms	66%	-	-
Saat SYN Flood	10.3 Kbps	>500 ms	84.5%	91%	-
Sesudah Suricata Aktif	>1 Gbps	<50 ms	<10%	<55%	<1.2 GB

Dari hasil pengujian tersebut, terlihat bahwa serangan DoS dan DDoS berdampak signifikan terhadap performa jaringan. Saat terjadi serangan Ping Flood dan SYN Flood, latency meningkat drastis dan packet drop sangat tinggi. Throughput bahkan turun hingga 10.3 Kbps pada serangan SYN Flood. Penggunaan CPU juga naik hingga 91%.

Namun, setelah implementasi IPS Suricata, performa jaringan kembali stabil. Throughput meningkat hingga lebih dari 1 Gbps, latency turun menjadi kurang dari 50 ms, dan packet drop berhasil ditekan hingga di bawah 10%. Penggunaan CPU dan RAM pun tetap dalam batas aman, yaitu di bawah 55% dan 1.2 GB.

Pembahasan

Berdasarkan hasil pengujian di atas, dapat disimpulkan bahwa implementasi sistem Intrusion Prevention System (IPS) menggunakan Suricata memiliki dampak signifikan dalam menjaga kestabilan dan keamanan jaringan. Sebelum Suricata diaktifkan, serangan seperti Ping Flood dan SYN Flood menunjukkan degradasi performa jaringan yang sangat parah, ditandai dengan peningkatan latency hingga >500 ms dan packet loss lebih dari 80%.

Suricata, bekerja sama dengan iptables, mampu mengidentifikasi pola trafik berbahaya secara real-time melalui signature-based detection dan melakukan aksi preventif dengan memblokir IP sumber serangan. Selain itu, Suricata juga memanfaatkan deep packet inspection (DPI) untuk memeriksa isi paket secara mendalam, sehingga dapat membedakan trafik sah dan berbahaya.

Efektivitas Suricata dapat dilihat dari kondisi jaringan pasca-implementasi, yang menunjukkan pemulihan throughput dan penurunan latency secara signifikan. Ini membuktikan bahwa Suricata tidak hanya mampu mendeteksi serangan, tetapi juga menjaga kinerja jaringan tetap optimal selama berlangsungnya aktivitas penting seperti ujian berbasis komputer di sekolah.

Dengan kombinasi parameter performa seperti throughput yang kembali >1 Gbps, latency <50 ms, serta efisiensi penggunaan sumber daya, IPS Suricata layak diterapkan di lingkungan jaringan pendidikan sebagai solusi preventif terhadap serangan siber.

Pengujian membuktikan bahwa Suricata mampu mengurangi dampak serangan secara signifikan, bahkan saat serangan diluncurkan secara simultan. Trafik sah tetap berjalan lancar, menunjukkan konfigurasi inline tidak mengganggu koneksi normal. Sistem IPS bekerja real-time dan tidak hanya mendeteksi, tetapi juga mencegah kerusakan lebih lanjut pada sistem jaringan. Dibandingkan dengan kondisi tanpa perlindungan, sistem yang menggunakan Suricata menunjukkan peningkatan drastis dalam kestabilan performa.

KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa implementasi Intrusion Prevention System (IPS) menggunakan Suricata memberikan dampak signifikan terhadap peningkatan keamanan dan kestabilan jaringan di lingkungan sekolah, khususnya di SMK PGRI Kras. Suricata terbukti mampu mendeteksi dan mencegah berbagai jenis serangan DoS dan DDoS seperti Ping Flood, HTTP Flood, dan SYN Flood secara real-time dengan tingkat efektivitas yang tinggi.

Parameter performa jaringan menunjukkan peningkatan setelah Suricata diaktifkan. Throughput meningkat menjadi lebih dari 1 Gbps, latency menurun menjadi di bawah 50 ms, packet drop menurun drastis di bawah 10%, dan penggunaan sumber daya sistem tetap efisien dengan CPU usage di bawah 55% serta RAM usage di bawah 1.2 GB. Hal ini menegaskan bahwa Suricata tidak hanya efektif dalam mendeteksi serangan, tetapi juga tidak membebani sistem secara berlebihan

Secara keseluruhan, implementasi Suricata sebagai IPS layak dijadikan referensi pengembangan sistem keamanan jaringan berbasis *open source* yang handal, ekonomis, dan efisien dalam menghadapi ancaman siber yang semakin kompleks. Penelitian lanjutan disarankan untuk mengembangkan skenario deteksi terhadap jenis serangan lainnya serta mengintegrasikan teknologi pendukung seperti machine learning untuk peningkatan akurasi deteksi.

REFERENSI

Abdillah, Z., & Adytia, P. (n.d.). *Implementasi Intrusion Detection System (IDS) Suricata Untuk Mendeteksi Serangan DDoS Menggunakan Metode TAARA Pada Jaringan Internet di Pixel Esport Arena Samarinda Implementation of Suricata Intrusion Detection System (IDS) for Detecting DDoS Attack*. 1–7.

Apriyanti, W., Erni, Syahlanisyiam, M., Anggraini, Y., Gunawan, S., Tyas Arinanto, R., … Agung, A. L. (2022). Sosialisasi Penggunaan Internet yang Sehat bagi Anak-anak di Yayasan Domyadhu. *Abdi Jurnal Publikasi*, *1*(1), 14. Retrieved from https://jurnal.portalpublikasi.id/index.php/AJP/index

Boukebous, A. A. E., Fettache, M. I., Bendiab, G., & Shiaeles, S. (2023). A Comparative Analysis of Snort 3 and Suricata. *2023 IEEE IAS Global Conference on Emerging Technologies, GlobConET 2023*. https://doi.org/10.1109/GlobConET56651.2023.10150141

Eromosele, C. C. (2025). *Evaluating the Impact of AES-256 Encryption on Network Performance : An Analysis of Transfer Time , Latency and Throughput*. *4*(1), 49–58.

Fahdurohman, R. A., Pradipta, D., & Sarbini, R. N. (2024). *Rancang Bangun Sistem Informasi Arsip Digital Berbasis Web Di Pemerintah Kabupaten Kediri*. (38).

Fidelity, W., & Fidelity, W. (1997). *Otomatisasi karma*. (1), 1–7.

Hendita, G., & Kusuma, A. (1997). Web-Server. *Zeitschrift Für Wirtschaftlichen Fabrikbetrieb*, *92*(1–2), 37–37. https://doi.org/10.1515/zwf-1997-921-220

Kamdan, Somantri, Sundayana, M. G., & Kharisma, I. L. (2023). Rancang Bangun Layanan Private cloud Berbasis Infrastructure as a Service Menggunakan OpenStack dengan Metode Network Development Life Cycle(NDLC). *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *4*(1), 252–262. https://doi.org/10.30865/klik.v4i1.1001

Mahendra, B. A., Kurniadi, H., & Utomo, Y. B. (2024). *MEMONITORING KOMPUTER WINDOWS SERVER*. *3*, 1–8.

Nainggolan, L. F., Saragih, N. F., & Larosa, F. G. N. (2022). Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS. *Jurnal Ilmiah Teknik Informatika*, *2*(2), 1–10. Retrieved from http://ojs.fikom-methodist.net/index.php/METHOTIKA

Nas, M., Ulfiah, F., & Putri, U. (2023). Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan. *Jurnal Teknologi Elekterika*, *20*(2), 92. https://doi.org/10.31963/elekterika.v20i2.4536

Nursabit, A., Apriani, E., & Komaludin, K. (2023). Manajamen Sarana dan Prasarana Pendidikan Jurusan Teknik Komputer Jaringan di Sekolah Menengah Kejuruan Negeri 1 Cijulang. *Jurnal Pelita Nusantara*, *1*(1), 1–5. https://doi.org/10.59996/jurnalpelitanusantara.v1i1.112

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. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 5827–5834. https://doi.org/10.36040/jati.v8i4.10069

Santoso, D., Noertjahyana, A., & Andjarwirawan, J. (2022). Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS. *Jurnal Infra*,

10(1), 1–6.

Santoso, T., & Prisscilya, V. (2021). Implementasi Keamanan Jaringan Menggunakan Intrusion Detection System (IDS) Pada PT. Mega Esa Farma. *INTEGER: Journal of Information Technology*, *6*(1), 1–8. https://doi.org/10.31284/j.integer.2021.v6i1.1205

Suhendi, H., & Cahyo, W. D. (2021). Perancangan Dan Implementasi Keamanan Jaringan Menggunakan Snort Sebagai Intrusion Prevention System (Ips) Pada Jaringan …. *Naratif: Jurnal Nasional Riset …*, *03*(02), 60–68. Retrieved from https://naratif.sttbandung.ac.id/index.php/naratif/article/view/137%0Ahttps://naratif.sttbandung.ac.id/index.php/naratif/article/download/137/71

Susanti, R. E., Muhammad, A. W., & Prabowo, W. A. (2022). Implementasi Intrusion Prevention System (IPS) OSSEC dan Honeypot Cowrie. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *11*(1), 73–78. https://doi.org/10.32736/sisfokom.v11i1.1246

Venu, H., Raju, V. D., Lingesan, S., & Soudagar, M. E. M. (2020). Na Ur. *Energy*, 119091. Retrieved from https://doi.org/10.1016/j.energy.2020.119091

Wahyudi, F., & Utomo, L. T. (2021). Perancangan Security Network Intrusion Prevention System Pada PDTI Universitas Islam Raden Rahmat Malang. *Edumatic: Jurnal Pendidikan Informatika*, *5*(1), 60–69. https://doi.org/10.29408/edumatic.v5i1.3278

Yanuartanti, I., Kurniasari, I., & Alfin, A. A. (2022). Sosialisasi Program Digitalisasi Sekolah Menggunakan Platform Sekolah Pintar Di Mtsn Model Pare, Kabupaten Kediri. *Jurnal Pengabdian Al-Ikhlas*, *8*(2). https://doi.org/10.31602/jpaiuniska.v8i2.8532

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