SABER: Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi
Vol.2, No. 1 Januari 2024
e-ISSN: 3025-342X; p-ISSN: 3025-2776, Hal 130-137
DOI: https://doi.org/10.59841/saber.v2i1.666

Implementasi SIEM dan IDS Dalam Monitoring Terhadap Ancaman Serangan Pada WEB Server

Moh Sulthan Arief Rahmatullah [1], Andyana Muhandhatul Nabila [2], Salmaa Satifha Dewi [3], Vira Datry [4], Fathika Afrine Azaruddin [5]
Institut Teknologi Sepuluh Nopember Surabaya

Teknologi Informasi, Fakultas Teknologi Elektro dan Informatika Cerdas,
e-mail: ramasedang@gmail.com [1], aa.andyana823@gmail.com [2], salmaasatifha2020@gmail.com [3], viradatrym@gmail.com [4], afrine5@gmail.com [5]

Abstract: *Information security and data integration are important aspects in managing and maintaining the continuity of web server system operations. The threat of an attack on a web server can have a serious impact on an organization. This is because websites are able to display text, graphic and sound information from anywhere via the internet network. Behind this convenience, there is a risk of cyber security threats in the use of internet-based technology because it can be accessed from anywhere and by anyone who wants to steal sensitive information or take over the system. In this research, the way to overcome this problem is through implementing a SIEM security information system with the wazuh/Teler platform as an IDS which will be installed on the web server to visualize logs and detect threats to network traffic, especially those leading to the web server. The method used in this research is documentation and forensic investigation in researching or analyzing server log data on websites using wazuh and teler.*

Keywords: *IDS, Keamanan Siber, monitoring, SIEM, Wazuh*

Abstrak: Keamanan informasi dan integrasi data menjadi aspek penting dalam mengelola dan menjaga keberlangsungan operasi sistem web server. Ancaman serangan terhadap web server dapat memiliki dampak serius terhadap organisasi. Hal ini karena website mampu menampilkan informasi teks, grafik, serta suara dari manapun melalui jaringan internet. Dibalik kemudahan tersebut, terdapat resiko ancaman keamanan siber dalam penggunaan teknologi berbasis internet karena dapat diakses dari manapun dan oleh siapapun yang ingin mencuri informasi sensitif atau mengambil alih sistem. Dalam penelitian ini, cara mengatasi permasalahan tersebut melalui implementasi sistem informasi keamanan SIEM dengan platform wazuh/Teler sebagai IDS yang akan diinstal pada web server untuk memvisualisasikan log dan mendeteksi adanya ancaman pada lalu lintas jaringan khususnya yang mengarah ke web server. Metode yang digunakan dalam penelitian ini dokumentasi dan investigasi Forensik dalam meneliti atau menganalisis data log server pada website menggunakan wazuh dan teler.

Kata Kunci: IDS, Keamanan Siber, monitoring, SIEM, Wazuh,

Received: November 20, 2023; Accepted: Desember 09, 2023; Published: Januari 31, 2024
** Moh Sulthan Arief Rahmatullah, ramasedang@gmail.com*

PENDAHULUAN

Perkembangan internet pada Teknologi Informasi dan Komunikasi (TIK) terus meningkat seiring berkembangnya zaman. Penggunaan internet seperti pendidikan, sosial budaya, ekonomi, dan kesehatan berkorelasi dengan dampak yang signifikan di mana membawa pengaruh besar dalam proses pertukaran informasi dan komunikasi. Berdasarkan Data Indonesia, tahun 2023, jumlah pengguna internet di Indonesia telah mencapai 212,9 juta yang diperkirakan terus meningkat setiap tahunnya (Rizaty, 2023). Dari sini, dapat disimpulkan bahwa mayoritas penduduk Indonesia sebesar 77% telah memanfaatkan internet sebagai penunjang kemudahan akses informasi dan komunikasi dengan cakupan yang luas.

Salah satu penerapan penggunaan internet yang sering digunakan adalah penerapan aplikasi website yang menggunakan web server dalam memberikan layanan seperti pertukaran informasi dan penyimpanan data. Program yang diakses melalui web browser dengan koneksi jaringan dan protokol HTTP disebut sebagai aplikasi website (Rouse, 2023). Website sendiri mampu menghasilkan beragam informasi data berupa teks, gambar, animasi dan suara yang akan diakses melalui situs internet dan disimpan pada web server. Hal ini mampu mempermudah instansi dalam peningkatan layanan dan berbagi informasi.

Meskipun dengan tersedianya kemudahan akses yang diberikan dari penerapan aplikasi website, perlu adanya kewaspadaan dan pertimbangan matang dalam menjaga keamanan data informasi yang bersifat rahasia. Tanpa adanya pengamanan yang kuat dapat menimbulkan masalah baru berupa resiko ancaman keamanan siber oleh pihak yang tidak bertanggung jawab dalam mengakses data sensitif untuk tujuan yang dapat merugikan berbagai pihak. Semakin banyak pihak yang mengimplementasikan teknologi berbasis internet terutama aplikasi web, maka kemungkinan adanya ancaman serangan siber semakin meningkat.

Mempertimbangkan masalah keamanan siber yang mungkin terjadi akibat kemudahan dan keterbukaan jaringan internet, cara yang dapat diterapkan adalah adanya sistem yang dapat melakukan controlling terhadap arus informasi yang masuk baik mendeteksi maupun menganalisa log segala aktivitas dari sistem guna memastikan data yang sifatnya rahasia tetap terjaga keamanannya dan secara efisien dalam mengambil tindakan selanjutnya terhadap sistem. Salah satu contoh penerapan ini menggunakan *Security Information and Event Management (SIEM)* dan *Intrusion Detection System (IDS)* (Hadi & Putri, 2023).

SIEM merupakan sistem monitoring dan manajemen log dari sumber data seperti jaringan, endpoint, firewall, dan sebagainya. Jika SIEM bertindak dalam pencegahan, maka dalam konteks keamanan siber yang diharapkan mampu mendeteksi ancaman dari lalu lintas jaringan yang mencurigakan, hal ini dilakukan oleh perangkat yang bernama IDS. Kedua hal

ini saling berkaitan di mana penggunaan IDS yang dapat mendeteksi lalu lintas mencurigakan dan kemudian akan mengirimkan alert sebagai peringatan ke sistem SIEM. Dari sini dapat dilakukan analisis apakah lalu lintas ini merupakan ancaman yang perlu dicegah atau tidak (Comodo, 2023).

Berdasarkan penelitian yang sudah dilakukan sebelumnya terdapat pendekatan yang berbeda. Perbedaan pada penelitian sebelumnya yaitu pada sisi integrasi endpoint jaringan. Dalam penelitian ini, SIEM dan IDS diintegrasi untuk monitoring pada suatu web server sedangkan pada penelitian sebelumnya belum terdapat integrasi pada sistem SIEM. Penggunaan IDS pada penelitian saat ini untuk memvisualisasikan log lalu akan dikirimkan ke Wazuh untuk sistem manajemennya.

Tujuan dari adanya penelitian ini adalah untuk mengimplementasikan SIEM dengan menggunakan Wazuh untuk memanajemen sistem serangan yang ada pada web server. Wazuh dikombinasikan dengan Teler sebagai IDS yang akan diinstal pada web server untuk memvisualisasikan log dan mendeteksi adanya ancaman pada lalu lintas jaringan khususnya yang mengarah ke web server. Wazuh akan memberikan peringatan ketika rules yang ada dipicu oleh suatu kondisi tertentu lalu akan mengirimkan sebuah sinyal peringatan pada suatu web server. Dengan adanya pengimplementasian SIEM dan IDS dalam monitoring terhadap ancaman serangan pada web server, diharapkan dapat mempermudah administrator untuk mengetahui serangan maupun ancaman yang sedang terjadi pada web server sehingga dapat mendeteksi lebih awal apabila terjadi suatu insiden, mempermudah dalam suatu sistem manajemennya, dan membantu dalam proses digital forensik.

METODE PENELITIAN

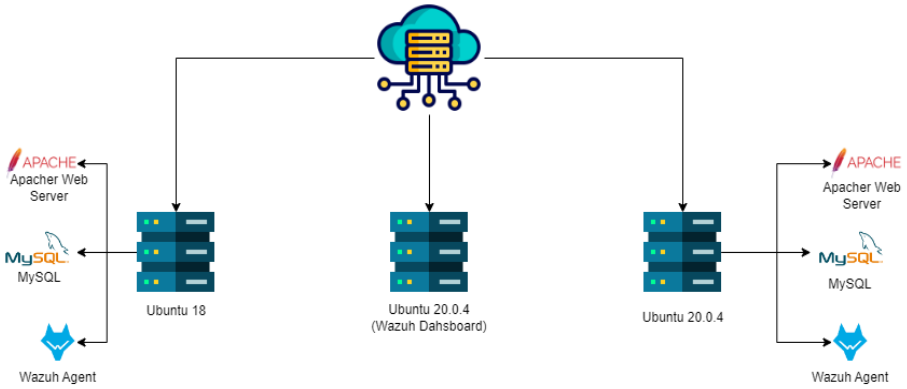
Pada penelitian ini digunakan metode dokumentasi dan investigasi Forensik dalam meneliti atau menganalisis data log server pada website menggunakan wazuh dan teler. Metadata log web server yang didapatkan kemudian akan dianalisis oleh Wazuh. Wazuh merupakan perangkat berbasis open source sebagai sistem deteksi intrusi berbasis endpoint, wazuh menyediakan fitur visibilitas keamanan yang lebih dalam ke sebuah infrastruktur dengan memantau host pada sistem operasi dan juga pada tingkat aplikasi (Pratama,2022). Dalam penelitian ini wazuh bertindak sebagai sebagai manajemen agen, dashboard sistem monitoring baik file integrity, intrusion, maupun log, serta untuk melakukan pembacaan sistem, pengumpulan log.

Sistem monitoring adalah suatu proses di mana data real-time dikumpulkan dari

berbagai sumber. Secara umum, sistem monitoring terdiri dari tiga tahap utama:

1. Pengumpulan data monitoring, di mana data diambil dari berbagai sumber.
2. Analisis data monitoring, dimana data tersebut dianalisis untuk mendapatkan wawasan dan informasi yang berguna.
3. Tampilan data hasil monitoring, di mana hasil analisis ditampilkan untuk pemantauan dan pengambilan keputusan.

Selama proses ini, berbagai tindakan atau layanan (service) dapat berjalan secara terus-menerus dengan interval waktu tertentu. Proses-proses dalam sistem monitoring dimulai dengan pengumpulan data seperti data lalu lintas jaringan (network traffic), informasi perangkat keras (hardware information), dan data lainnya. Data ini kemudian diolah dan dianalisis selama tahap analisis data, dan akhirnya hasilnya ditampilkan untuk penggunaan dan pemantauan yang lebih lanjut.



***Gambar** . Topologi Sistem*

HASIL DAN PEMBAHASAN (ABIS EAS)

Hasil

Integrasi Teler dan Wazuh dalam Sistem Intrusion Detection System (IDS) telah membuktikan peningkatan signifikan dalam efektivitas deteksi serangan siber. Keberhasilan ini dikaitkan dengan penggunaan database IDS yang lebih luas, memungkinkan pengenalan serangan yang lebih akurat. Serangan yang terdeteksi mencakup berbagai kategori, seperti "Common Web Attack", "CVE" (Common Vulnerabilities and Exposures), "Bad IP Address", "Bad Referrer", "Bad Crawler", dan "Directory Bruteforce". Sistem IDS yang memungkinkan penyesuaian aturan juga memberikan fleksibilitas untuk menyesuaikan deteksi serangan sesuai kebutuhan, meningkatkan adaptabilitas dan responsivitas terhadap ancaman keamanan siber yang dinamis.

Dalam pengujian penulis, penggunaan Nikto dan OWASP ZAP sebagai alat penyerang menunjukkan efektivitas Teler dan Wazuh dalam mengidentifikasi berbagai jenis serangan. Berikut adalah contoh serangan yang berhasil dideteksi oleh Teler:

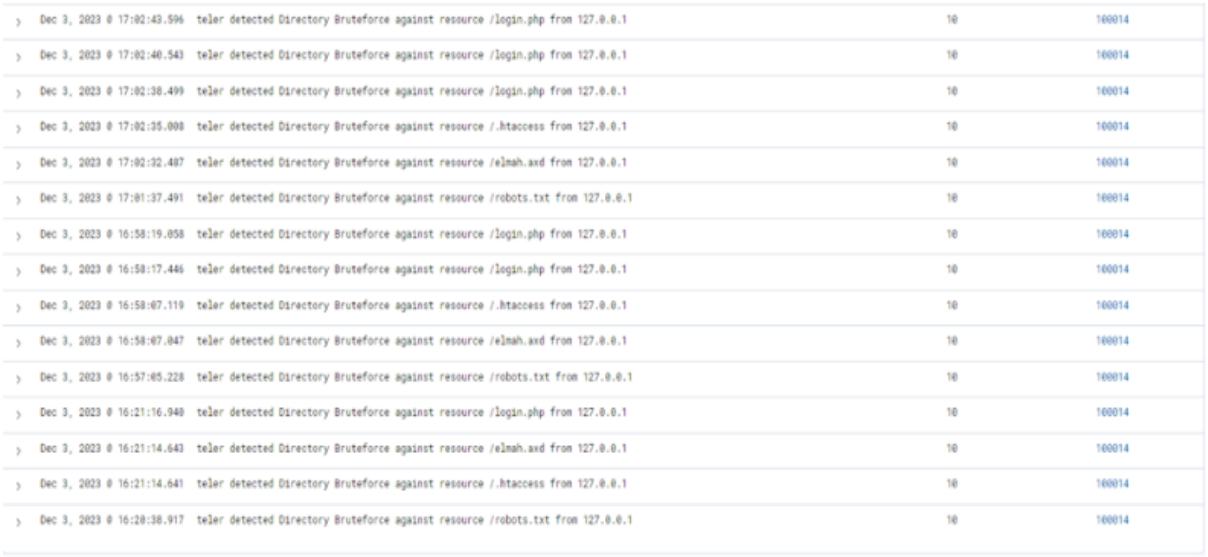
Common Web Attack

Dalam pengujian keamanan yang penulis lakukan, penulis menggunakan Nikto dan OWASP ZAP sebagai alat penyerangan untuk menguji efektivitas Teler dan Wazuh dalam mendeteksi serangan. Hasilnya menunjukkan bahwa kombinasi Teler dan Wazuh sangat efektif dalam mengidentifikasi berbagai jenis serangan web umum. Beberapa contoh serangan yang berhasil dideteksi termasuk injeksi HTML yang merusak, seperti penggunaan tag <img> dengan atribut onerror yang memicu alert JavaScript, serta deteksi elemen HTML yang mungkin berbahaya, termasuk tag <script> dan fungsi VBScript/JScript yang dienkripsi dan dikemas. Ini menegaskan bahwa gabungan antara Teler dan Wazuh, saat diuji dengan Nikto dan OWASP ZAP, dapat mendeteksi banyak sekali serangan web umum dengan efektif. Selain hasil diatas masih banyak juga Common Web Attack yang terdeteksi

Pada pengujian yang sama, Teler juga berhasil mendeteksi serangan yang berkaitan dengan kerentanan yang tercantum dalam Common Vulnerabilities and Exposures (CVE). Contoh serangan tersebut termasuk:

1. CVE-2021-42667: Teler berhasil mengidentifikasi beberapa upaya serangan terhadap sumber daya /login.php. Ini menunjukkan adanya upaya untuk mengeksploitasi kerentanan khusus pada halaman login, yang terjadi berulang kali dari alamat IP yang sama.
2. CVE-2021-28164: Demikian pula, Teler mendeteksi serangan terhadap sumber daya /WEB-INF/web.xml. Serangan ini bertujuan untuk mengeksploitasi kerentanan yang terkait dengan konfigurasi atau pengaturan web aplikasi.

Kedua jenis serangan CVE ini, yang terdeteksi berulang kali, menunjukkan efektivitas sistem deteksi Teler dalam mengidentifikasi upaya penyerangan yang spesifik terhadap kerentanan yang telah dikenali sebelumnya. Hal ini menegaskan pentingnya memperbarui dan memelihara keamanan sistem untuk melindungi terhadap kerentanan yang diketahui.Serangan *Directory Bruteforce* :



Selain deteksi serangan CVE, Teler juga berhasil mengidentifikasi serangan brute force direktori yang berulang kali terjadi. Serangan ini ditargetkan pada berbagai sumber daya penting, termasuk:

1. /login.php: Berulang kali, Teler mendeteksi upaya brute force terhadap halaman login, yang menunjukkan upaya untuk menebak atau memaksa masuk menggunakan berbagai kombinasi username dan password.

2. /.htaccess: Beberapa upaya brute force juga ditujukan pada file .htaccess, yang merupakan file konfigurasi penting pada server web dan berisi aturan untuk mengatur akses ke direktori.
3. /elmah.axd: File elmah.axd juga menjadi sasaran brute force, yang merupakan bagian dari ELMAH (Error Logging Modules and Handlers) dan sering digunakan dalam aplikasi web berbasis .NET untuk logging.
4. /robots.txt: Teler juga mendeteksi upaya brute force terhadap file robots.txt, file yang biasanya berisi petunjuk tentang bagaimana mesin pencari harus merayapi situs.

Serangan brute force ini, yang terjadi dari alamat IP yang sama, menunjukkan upaya yang terkoordinasi untuk mendapatkan akses tidak sah atau informasi penting dari server. Hal ini menegaskan perlunya keamanan yang kuat dan pemantauan yang terus-menerus untuk melindungi terhadap serangan yang bertujuan untuk mengkompromikan sumber daya web.

PENUTUP

Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan, dapat disimpulkan bahwa Teler, bersama dengan Wazuh, menunjukkan kemampuan yang sangat baik dalam mendeteksi berbagai jenis serangan web. Melalui penggunaan alat penyerangan seperti Nikto dan OWASP ZAP, Teler berhasil mengidentifikasi serangan yang berkaitan dengan kerentanan CVE, serangan web umum, serta upaya brute force terhadap direktori.

Teler secara efektif mengidentifikasi jenis serangan, alamat IP yang menyerang, dan sumber daya yang menjadi target. Hal ini mencakup deteksi injeksi HTML, elemen HTML yang berpotensi berbahaya, dan upaya brute force pada halaman login dan file konfigurasi penting seperti .htaccess. Kinerja ini menunjukkan pentingnya Teler dan Wazuh dalam sistem keamanan web, memberikan informasi real-time yang penting untuk pencegahan dan respons terhadap serangan.

Untuk penelitian masa depan, terdapat potensi pengembangan lebih lanjut pada Teler, seperti implementasi fungsi pencegahan serangan berdasarkan data yang dikumpulkan. Salah satu kemungkinannya adalah penerapan pembelajaran mesin untuk secara otomatis memasukkan IP tertentu ke dalam daftar hitam yang terdeteksi mencoba menyerang server. Ini akan meningkatkan keamanan server dan mengurangi risiko kerentanan terhadap serangan serupa di masa yang akan datang.

DAFTAR PUSTAKA

Comodo. (2023). DIFFERENCE BETWEEN SIEM AND IDS. Diakses dari https://www.comodo.com/difference-between-siem-and-ids.php pada tanggal 10 Oktober 2023

Hadi, M.S,& Devi A. (2023). IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) UNTUK DETEKSI DAN ANALISA INSIDEN KEAMANAN PADA WEB SERVER. Universitas Muhammadiyah Surakarta

Rizaty, M.A. (2023). Pengguna Internet di Indonesia Sentuh 212 Juta pada 2023. Diakses dari https://dataindonesia.id/internet/detail/pengguna-internet-di-indonesia-sentuh-212-juta-pada-2023 pada tanggal 10 Oktober 2023

Rouse, M. (2023). Web-Based Application. Diakses dari https://www.techopedia.com/definition/26002/web-based-application pada tanggal 1 0 Oktober 2023

Khotimah, H., Bimantoro, F., & Kabanga, R. S. (2022). Implementasi Security Information and Event Management (SIEM) Pada aplikasi SMS center Pemerintah Daerah Provinsi Nusa tenggara Barat. *Jurnal Begawe Teknologi Informasi (JBegaTI)*, *3*(2). https://doi.org/10.29303/jbegati.v3i2.752

Kusuma, G. (2022). Implementasi owasp zap Untuk Pengujian Keamanan Sistem informasi akademik. *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, *16*(2), 178–186. https://doi.org/10.47111/jti.v16i2.3995

Tedyyana, A., & Ghazali, O. (2021). Teler real-time HTTP intrusion detection at website with Nginx Web Server. *JOIV : International Journal on Informatics Visualization*, *5*(3), 327. https://doi.org/10.30630/joiv.5.3.510