Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika
Vol.2, No.5 September 2024
e-ISSN: 3031-8912; p-ISSN: 3031-8904; Hal 137-144
DOI: https://doi.org/10.61132/merkurius.v2i4.289
Available online at: https://journal.arteii.or.id/index.php/Merkurius/

Implementasi *Security Information And Event Management* (*SIEM*) Untuk Monitoring Keamanan Server Menggunakan *Wazuh*

Rangga Aditya[*1], Yusuf Muhyidin[2], Dayan Singasatia[3]

[1-2] Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Wastukancana, Indonesia
Korespondensi Penulis : rangga04102002@gmail.com

Abstract: *One form of utilizing technological advances is the application of web applications using web servers to share information, provide services, and store data. Behind the ease of use of web applications that can be accessed from anywhere, there is a considerable risk of cybersecurity threats where web applications can be targeted by cyber criminals who want to steal sensitive information or take over the system. These security problems can be overcome with a reactive approach, namely the implementation of a security system that is able to detect and analyze security incidents in web applications quickly and effectively. One solution that can be used is to implement Security Information and Event Management (SIEM). SIEM is a system that can be used to manage logs generated from various data sources such as endpoints, network devices, and firewalls, One SIEM application that is open source and can be used for detection and analysis of cyber attack incidents is Wazuh. Wazuh is open source software that functions as a host-based (endpoint) detection system that incorporates XDR (External Data Representation) capabilities. The method used in solving the problem uses the Experimental method, there are 5 stages in this experimental method, namely requirements analysis, design, implementation, testing, evaluation. The results of these tests can be detected by Wazuh as a SIEM for monitoring server security and attack detection.*
Keywords*: Web security, SIEM, Wazuh, Experimental.*

Abstrak. Salah satu bentuk dari pemanfaatan kemajuan teknologi berupa penerapan aplikasi web menggunakan web server untuk berbagi informasi, memberikan layanan, dan menyimpan data. Dibalik kemudahan dalam penggunaan aplikasi web yang dapat diakses darimana pun, terdapat risiko ancaman keamanan siber yang cukup besar dimana aplikasi web dapat menjadi target serangan oleh penjahat siber yang ingin mencuri informasi sensitif atau mengambil alih sistem. Masalah keamanan tersebut dapat diatasi dengan pendekatan reaktif yaitu penerapan sistem keamanan yang mampu mendeteksi dan menganalisa insiden keamanan pada aplikasi web secara cepat dan efektif. Salah satu solusi yang dapat digunakan adalah dengan mengimplementasikan *Security Information and Event Management (SIEM)*. *SIEM* adalah sistem yang dapat digunakan untuk mengelola log yang dihasilkan dari berbagai sumber data seperti endpoint, perangkat jaringan, maupun firewall, Salah satu aplikasi *SIEM* yang bersifat open source dan dapat digunakan untuk deteksi serta analisa insiden serangan siber adalah *Wazuh*. *Wazuh* adalah perangkat lunak open source yang berfungsi sebagai sistem deteksi berbasis host (endpoint) yang menyatukan kemampuan *XDR* (*External Data Representation*). Metode yang digunakan dalam penyelesaian masalah tersebut menggunakan metode Eksperimental, ada 5 tahapan dalam metode eksperimental ini yaitu analisis kebutuhan, desain, implementasi, pengujian, evaluasi. Hasil dari pengujian tersebut dapat di deteksi oleh *Wazuh* sebagai *SIEM* untuk memonitoring keamanan server dan deteksi penyerangan.
Kata kunci: *Keamanan web, SIEM, Wazuh, Eksperimental.*

LATAR BELAKANG

Kemajuan teknologi informasi dan komunikasi yang sangat pesat saat ini telah membawa perubahan besar di berbagai aspek kehidupan masyarakat. Akses internet yang berkembang cukup luas memberikan kemudahan dalam melakukan komunikasi ke berbagai tujuan dengan jangkauan yang sangat luas. Hal tersebut mendorong instansi maupun perusahaan untuk memanfaatkan internet agar dapat meningkatkan kinerja dan efektivitas dalam mencapai tujuan organisasi. Salah satu bentuk dari pemanfaatan

Received: Mei 12, 2024; Revised: Juni 18, 2024; Accepted: Juli 20, 2024; Published: Juli 29, 2024
* Rangga Aditya : rangga04102002@gmail.com

tersebut berupa penerapan aplikasi web menggunakan web server untuk berbagi informasi, memberikan layanan, dan menyimpan data.(Hadi Sofiyan Muhammad, 2023)

Dibalik kemudahan dalam penggunaan aplikasi web yang dapat diakses darimana pun, terdapat risiko ancaman keamanan siber yang cukup besar dimana aplikasi web dapat menjadi target serangan oleh penjahat siber yang ingin mencuri informasi sensitif atau mengambil alih sistem. Keamanan siber merupakan bidang yang berkaitan dengan melindungi sistem komputer, jaringan, dan data dari ancaman dan serangan yang dilakukan secara elektronik. Ancaman-ancaman dalam dunia maya dapat berasal dari berbagai pihak seperti hacker, *malware, phishing* dan masih banyak lagi. Maka dari itu, praktik-praktik keamanan siber seperti penggunaan *firewall*, enkripsi data sensitif, pemantauan aktivitas jaringan secara real-time, serta pelatihan kesadaran tentang keamanan bagi pengguna menjadi sangat penting untuk melawan ancaman-ancaman tersebut. Berdasarkan laporan tahunan monitoring keamanan siber BSSN tahun 2021, terdapat 332 aduan siber dengan target sektor pemerintah daerah, pemerintah pusat, ekonomi digital, IIVN, dan lainnya. Terdapat 3 jenis aduan siber tertinggi yang dilaporkan berdasarkan jumlah kasus sesuai pembagian sektor dimana jenis tersebut merupakan kerentanan yang dapat ditemukan pada aplikasi web diantaranya adalah *SQL Injection*, *cross-site scripting*(*XSS*), dan *information disclosure* (BSSN, 2022).

Masalah keamanan tersebut dapat diatasi dengan pendekatan reaktif yaitu penerapan sistem keamanan yang mampu mendeteksi dan menganalisa insiden keamanan pada aplikasi web secara cepat dan efektif. Salah satu solusi yang dapat digunakan adalah dengan mengimplementasikan *Security Information and Event Management (SIEM)*. *SIEM* adalah sistem yang dapat digunakan untuk mengelola log yang dihasilkan dari berbagai sumber data seperti endpoint, perangkat jaringan, maupun *firewall*, Salah satu aplikasi *SIEM* yang bersifat open source dan dapat digunakan untuk deteksi serta analisa insiden serangan siber adalah *Wazuh*. *Wazuh* adalah perangkat lunak open source yang berfungsi sebagai sistem deteksi berbasis *host* (*endpoint*) yang menyatukan kemampuan *XDR* (*External Data Representation*).

KAJIAN TEORITIS

1. Security Information and Event Management (*SIEM*)

SIEM adalah singkatan dari "Security Information and Event Management" SIEM diterjemahkan sebagai "Manajemen Informasi dan Keamanan Peristiwa." sistem yang digunakan untuk memantau dan mendeteksi serangan serta merespon keamanan melalui analisis log dari berbagai event yang diperoleh dari sumber data secara real-time. Teknologi ini memiliki jangkauan pengumpulan data yang luas dan dapat mengaitkan serta menganalisis event dari berbagai sumber dan menentukan apakah kejadian tersebut merupakan serangan atau tidak. Analisis SIEM mencakup semua aplikasi yang digunakan perusahaan, perangkat jaringan, perangkat keamanan, dan server. Sistem SIEM bekerja dengan mengumpulkan dan menganalisis data dari berbagai sumber dalam suatu infrastruktur IT, seperti log dari perangkat jaringan, sistem operasi, aplikasi, dan perangkat keamanan. Data ini kemudian diagregasi dan dianalisis untuk mendeteksi aktivitas yang mencurigakan atau ancaman keamanan.(Shafiyyah et al., 2024)

2. Cyber Security

Cyber security terdiri dari dua kata yaitu *cyber* yang berarti dunia maya dan security yang berarti keamanan sehingga jika digabungkan *cyber security* memiliki arti keamanan siber. *Cyber security* atau keamanan siber berperan dalam mendeteksi, memperbaiki, atau menurunkan tingkatan risiko dari ancaman siber (*cyber threat*) dan serangan siber (*cyber attack*) serta seluruh kegiatan yang memberi ancaman terhadap keamanan seluruh komponen sistem siber.(Khotimah et al., 2022)

3. Wazuh

Wazuh adalah perangkat lunak open source yang berfungsi sebagai sistem deteksi berbasis host (endpoint) yang menyatukan kemampuan XDR (External Data Representation) dan SIEM (Security Information and Event Management) diantaranya menganalisis log, deteksi intrusi dan malware, monitor file integrity, penilaian konfigurasi sesuai standar industri, deteksi kerentanan, dan dukungan kepatuhan terhadap aturan. Memberi peringatan berdasarkan waktu, dan merespons secara aktif. Wazuh memberikan fitur visibilitas keamanan yang lebih dalam pada infrastruktur dengan memantau host di sistem operasi dan tingkat aplikasi. Arsitektur Wazuh tersusun dari tiga

komponen pusat (Wazuh Indexer, Wazuh Server, Wazuh Dashboard) dan komponen endpoint (Wazuh Agent).(Shafiyyah et al., 2024)

a. Wazuh Indexter

Wazuh Indexer merupakan search engine untuk mengindeks dan menyimpan *alert* yang dihasilkan oleh *Wazuh Server* sehingga dapat memudahkan pencarian data dan kebutuhan analisis. Data disimpan dalam *JSON document* dimana kumpulan dari *document* yang memiliki korelasi disebut sebagai *index*.(Shafiyyah et al., 2024)

b. Wazuh Server

Wazuh Server menganalisis data yang diterima dari *Wazuh Agent*, memprosesnya melalui *decoders* dan *rules* menggunakan *threat intelligence* untuk mencari ancaman yang populer. Selain itu, *Wazuh Server* juga digunakan untuk mengelola *Wazuh Agent*, termasuk kebutuhan konfigurasi dan *upgrade*.(Shafiyyah et al., 2024)

c. Wazuh Dashboard

Wazuh Dashboard merupakan antarmuka web untuk visualisasi data dan kebutuhan analisis. Wazuh Dashboard menampilkan security events, regulatory compliance, kerentanan aplikasi yang terdeteksi, data hasil monitor file integrity, hasil penilaian konfigurasi, monitoring events pada infrastruktur cloud, dan informasi lainnya yang dapat digunakan untuk mendukung kebutuhan analisis. Selain itu, Wazuh Dashboard juga digunakan untuk mengelola konfigurasi Wazuh dan monitor statusnya.

d. Wazuh Agent

Wazuh Agent diimplementasikan pada perangkat endpoint (Linux, Windows, macOS, Solaris, AIX, dan OS lainnya) yang menyediakan kemampuan pencegahan, deteksi, dan respon terhadap ancaman. Agen Wazuh bersifat multi-platform dan berjalan pada titik akhir yang ingin dipantau pengguna. Ia berkomunikasi dengan server Wazuh, mengirimkan data hampir secara real-time melalui saluran terenkripsi dan terautentikasi.

METODOLOGI PENELITIAN

Metode yang digunakan dalam penyusunan penelitian ini adalah metode eksperimental. Metode eksperimental merupakan metode penelitian yang digunakan untuk mengetahui pengaruh perlakuan tertentu terhadap subyek yang sedang diteliti melalui pengujian dengan kondisi yang berbeda – beda dan terkendalikan. Adapun diagram alir penelitian ini dapat dilihat pada Gambar dibawah ini:

Gambar 1. Alur Metode Eksperimental

1. Analisis Kebutuhan

Analisis kebutuhan berguna untuk menentukan kebutuhan apa yang diperlukan dalam penelitian. Kemudian menganalisis permasalahan yang ada dan menentukan kebutuhan perangkat lunak yang akan digunakan untuk pengujian. Berdasarkan hasil analisis penulis, maka dibutuhkan perangkat keras dan perangkat lunak yang dibutuhkan dalam penelitian ini.

2. Desain

Desain merupakan tahapan kedua setelah analisis kebutuhan yang berguna untuk mengetahui gambaran dari alur penelitian agar dapat memperjelas bagaimana cara kerja dari wazuh yang diimplementasikan. Adapun desain yang telah dibuat oleh penulis sebagai berikut:

3. Implementasi

Pada tahap ini dilakukan implementasi keamanan jaringan dan penginstalan perangkat lunak yang digunakan dalam penelitian ini, seperti install apk Wazuh, Kali Linux dan Ubuntu.

4. Pengujian

Tahap keempat merupakan tahap pengujian terhadap Wazuh sebagai SIEM yang telah dirancang untuk mendeteksi dan memonitoring ketika terdapat insiden penyerangan terhadap web server. Website yang digunakan untuk pengujian merupakan website yang sengaja dibuat untuk kepentingan pengujian, dalam penelitian ini pengujian dilakukan dengan beberapa jenis serangan yang sering ditujukan terhadap web server. Penulis

menggunakan dua penyerangan yang sering terjadi pada web server yaitu *Sql Injection* dan *DDoS* dengan menggunakan *tools Loic*.

5. Evaluasi

Tahap evaluasi ini merupakan tahap pembahasan hasil dari kinerja Wazuh sebagai SIEM untuk mendeteksi serangan dan memonitoring serangan. Dalam tahap ini terdapat beberapa poin yang akan dibahas terkait hasil dari pengujian skenario penyerangan yang dilakukan.

HASIL DAN PEMBAHASAN

1. Pengujian Sql Injection

Pada hasil pengujian ini dilakukan dengan penyerangan Sql Injection terhadap website yang telah dibuat untuk pengujian. Pengujian Sql Injection menggunakan *tools* sqlmap dengan perintah *sqlmap –u* kemudian masukkan web yang dituju --*dbs.*

Gambar 2. Perintah *Sqlmap*

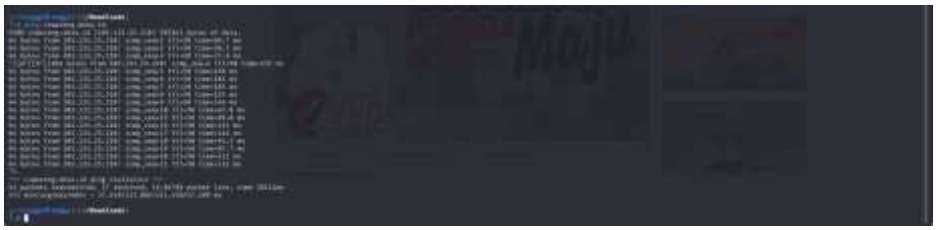
Pada gambar diatas terdapat parameter (-u) yaitu menunjukkan URL dari target pengujian beserta parameter *query* yang rentan, parameter (--dbs) menginstruksikan sqlmap untuk melihat *database* yang ada pada target. *Database* target bisa dilihat pada gambar dibawah ini.

Gambar 3. *Database* Target

Dapat dilihat terdapat dua database yang ada pada target, penulis ingin melihat tabel pada database acuart untuk melihat isi tabel pada database acuart bisa dilakukan dengan menggunakan perintah *sqlmap –u* kemudian masukkan web yang dituju *–D acuart --tables.*

2. *Pengujian DDoS*

Pengujian selanjutnya dilakukan dengan menggunakan penyerangan *DDoS* terhadap *website* yang akan digunakan untuk pengujian. Penyerangan *DDoS* dilakukan menggunakan *tools Loic* dengan menggunakan perintah *ping* pada web yang dituju.



Gambar 4. Perintah Ping

Perintah *ping* diatas digunakan untuk melihat *IP address* dari web Desa Ciwareng dan didapatkan *IP* tersebut yaitu 103.133.25.210. Setelah *IP* didapatkan, selanjutnya melakukan perintah *nmap 103.133.25.210*.

Tabel 1. Scannig

PORT	STATE	SERVICE
21/tcp	Open	Ftp
53/tcp	Open	Domain
80/tcp	Open	Http
433/tcp	Open	Https
2222/tcp	Open	EterNetLIP-1
10000/tcp	Open	Snet-sensor-mgmt
20000/tcp	Open	Dnp

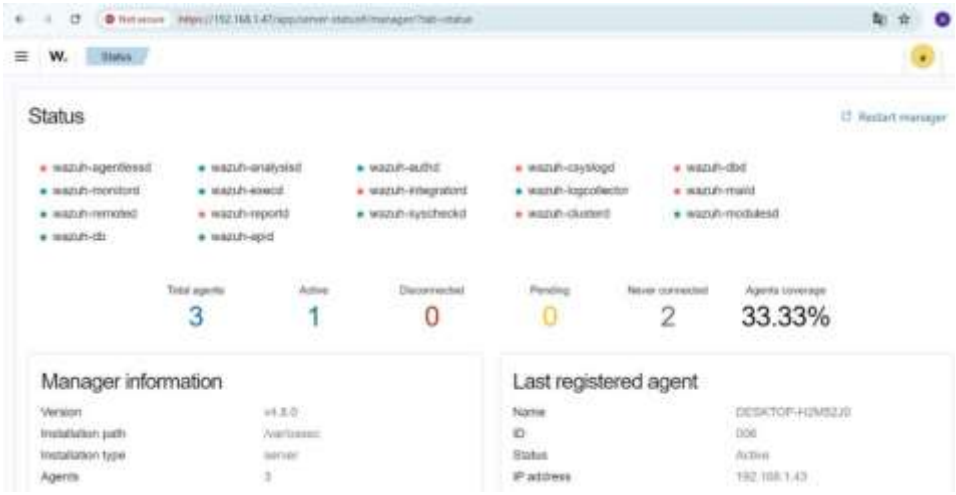
Setelah itu, melakukan penyerangan menggunakan *tools Loic* dengan perintah *sudo mono LOIC.exe*. Setelah tools Loic terbuka maka masukkan halaman URL dari target dan masukkan port yang terbuka untuk diserang, disini penulis menggunakan port 53/tcp. Setelah melakukan penyerangan, maka dapat dilihat hasil penyerangan tersebut pada web yang digunakan untuk pengujian ini.

Tabel 2. Hasil Uji Serangan

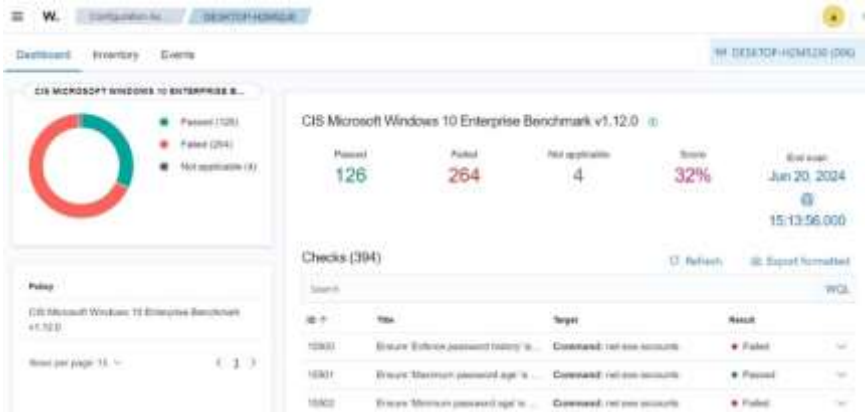
No	Uji Serangan	Keterangan	Koneksi
1	SQL	Terdeteksi	
2	DDOS	Tidak Terdeteksi	1000
		Tidak Terdeteksi	1500
		Tidak Terdeteksi	2000

3. Hasil *Evaluasi*

a. Hasil Wazuh



Gambar 5. Hasil Wazuh



Gambar 6. Hasil Pengujian

KESIMPULAN

Berdasarkan hasil pengujian dan hasil evalusi, pengujian penyerangan terhadap web server yang telah dilakukan dapat di deteksi oleh Wazuh namun hanya pada tingkat kerentanan yang rendah. Hasilnya dapat disimpulkan bahwa saja sql tidak dapat terdeteksi dan yg ddos dapat terdeteksi, yang menandakan bahwa pengecekkan pengujian penyerangan terhadap web server dapat terdeteksi pada kerentanan yang rendah. Berdasarkan hasil penelitian diatas, saran yang bisa disampaikan yaitu mencoba melakukan pengujian penyerangan dengan menggunakan penyerangan yang lain seperti *Dos*, *Brute Force* sehingga dapat diketahui bahwa pengujian penyerangan tersebut dapat terdeteksi oleh Wazuh pada tingkat kerentanan rendah, sedang, ataupun tinggi.

DAFTAR REFERENSI

Arief, M., Trisnawan, P. H., Data, M., Studi, P., Informatika, T., Komputer, F. I., & Brawijaya, U. (2024). *IMPLEMENTASI SISTEM DETEKSI SERANGAN SLOWLORIS PADA ARSITEKTUR JARINGAN SOFTWARE-DEFINED NETWORK*. *1*(1), 1–10.

Astuti, I. K. (2018). Fakultas Komputer INDAH KUSUMA ASTUTI Section 01. *Jaringan Komputer*, 8. https://id.scribd.com/document/503304719/jaringan-komputer

Bastian, A., Sujadi, H., & Abror, L. (2020). Analisis Keamanan Aplikasi Data Pokok Pendidikan (DAPODIK) Menggunakan Penetration Testing Dan SQL Injection. *INFOTECH Journal*, *6*(2), 65–70.

Hadi Sofiyan Muhammad, P. D. A. P. (2023). Implementasi Security Information and Event Management (Siem) Untuk Deteksi Dan Analisa Insiden Keamanan Pada Web Server. *Correspondencias & Análisis*, *15018*, 1–23.

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 210. https://doi.org/10.30998/string.v6i2.11477

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), 213–219. https://doi.org/10.29303/jbegati.v3i2.752

Shafiyyah, A., Elektro, J. T., Teknik, F., & Lampung, U. (2024). *Implementasi sistem keamanan jaringan di psdku universitas lampung waykanan menggunakan server wazuh untuk deteksi dan respon serangan siber*.

Stefan Stanković, Slavko Gajin, & Ranko Petrović. (2022). A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. *IX INTERNATIONAL CONFERENCE IcETRAN*, *IX*(june), 6–9.

Swami, R., Dave, M., & Ranga, V. (2019). Software-defined Networking-based DDoS Defense Mechanisms. *ACM Computing Surveys*, *52*(2). https://doi.org/10.1145/3301614

Umar, R., & Prasetyo Marsaid, A. (2023). Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing. *Jurnal Riset Komputer)*, *10*(1), 2407–389. https://doi.org/10.30865/jurikom.v10i1.5835