Implementasi Log Analysis dan Real-Time Intrusion Detection System (IDS) Berbasis Wazuh pada Aplikasi Web Berbasis Laravel

Petra Narwastu Panjaitan[1], Andy Triwinarko, S.T., M.T.[2]
1Mahasiswa Program Studi Rekayasa Keamanan Siber, Politeknik Negeri Batam
2Dosen Pembimbing, Program Studi Rekayasa Keamanan Siber, Politeknik Negeri Batam
Proyek Pembelajaran Rekayasa Keamanan Siber, Politeknik Negeri Batam
1petranwp29@gmail.com, 2andy@polibatam.ac.id

Informasi Artikel
Riwayat artikel:
Diterima: -
Direvisi: -
Disetujui: -

ABSTRAK

Aplikasi web menjadi salah satu target utama serangan siber karena sifatnya yang dapat diakses secara luas melalui internet, termasuk aplikasi yang dibangun menggunakan framework Laravel. Berbagai serangan seperti SQL Injection, Cross-Site Scripting (XSS), brute force login, port scanning, dan akses tidak sah mengancam keamanan aplikasi web, sementara deteksi ancaman pada banyak sistem masih mengandalkan pemeriksaan log secara manual sehingga lambat dan rentan terhadap keterlambatan penanganan. Penelitian ini menerapkan Wazuh, yaitu platform Security Information and Event Management (SIEM) sekaligus Intrusion Detection System (IDS) open-source, untuk melakukan analisis log (log analysis) dan mendeteksi serangan secara real-time terhadap aplikasi web bantuan hukum berbasis Laravel yang diberi nama Go Hukum. Wazuh Agent dipasang pada server yang menjalankan aplikasi Go Hukum untuk mengumpulkan log aplikasi, log web server, dan log autentikasi, kemudian Wazuh Manager menganalisis serta mendeteksi indikasi serangan berdasarkan rules, dan hasilnya dipantau melalui Wazuh Dashboard. Penelitian ini menggunakan jenis penelitian terapan dengan model pengembangan Network Development Life Cycle (NDLC) yang meliputi tahapan analisis, desain, simulasi prototipe, implementasi, monitoring, dan manajemen. Pengujian dilakukan melalui simulasi serangan terkendali terhadap aplikasi Go Hukum untuk mengukur akurasi deteksi dan response time. Hasil yang diharapkan adalah terwujudnya sistem monitoring keamanan berbasis Wazuh yang mampu mendeteksi serangan terhadap aplikasi web Laravel secara cepat dan akurat, sehingga meningkatkan efektivitas pengawasan keamanan dan mempercepat respons terhadap insiden.

Kata kunci: *sistem deteksi intrusi, keamanan aplikasi web, Laravel, analisis log, waktu nyata, SIEM, Wazuh*

I. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong hampir semua organisasi untuk mengadopsi sistem berbasis web untuk menjalankan proses bisnis mereka. Salah satu kerangka kerja pembuatan aplikasi web yang populer adalah Laravel, sebuah kerangka kerja PHP yang dikenal karena kemudahan pengembangannya, keamanan bawaan, dan ekosistem yang matang. Namun, karena aplikasi web Laravel dapat diakses secara luas di internet, aplikasi tersebut rentan terhadap serangan siber.

Injeksi SQL, cross-site scripting (XSS), serangan brute-force, pemindaian port, dan upaya akses tidak sah hanyalah beberapa dari berbagai jenis serangan yang menimbulkan ancaman nyata bagi keamanan aplikasi web. Semua aktivitas yang terjadi pada aplikasi atau server biasanya dicatat, seperti log aplikasi Laravel, log server web (Apache/Nginx), dan log otentikasi sistem. Log ini menyimpan informasi penting, seperti waktu akses, alamat IP, jenis permintaan, status HTTP, dan pesan kesalahan. Dengan analisis yang tepat, log ini dapat berfungsi sebagai sumber data penting untuk mendeteksi tanda-tanda serangan.

Masalahnya adalah banyak administrator masih meninjau log satu per satu secara manual, sehingga deteksi ancaman menjadi lambat, tidak efisien, dan rentan terhadap keterlambatan respons. Semakin lama serangan tidak terdeteksi, semakin besar potensi kerusakannya, baik itu pelanggaran data, gangguan layanan, atau kerusakan reputasi organisasi.

Salah satu solusi untuk masalah ini adalah menggunakan platform Security Information and Event Management (SIEM) [1]. Wazuh adalah platform SIEM dan XDR (Extended Detection and Response) sumber terbuka yang menyediakan analisis log terpusat, deteksi intrusi berbasis aturan, pemantauan integritas file, dan kemampuan respons proaktif [2], [3]. Dengan Wazuh, log yang

dihasilkan oleh aplikasi web dapat dikumpulkan, dianalisis, dan dilihat secara terpusat dan secara real-time tanpa peninjauan manual.

Studi ini menggunakan Wazuh sebagai sistem analisis log dan deteksi intrusi (IDS) untuk memantau dan mendeteksi serangan terhadap aplikasi web bantuan hukum berbasis Laravel yang selanjutnya disebut Go Hukum. Wazuh Agent diinstal pada server yang menjalankan aplikasi Go Hukum untuk mengumpulkan log. Wazuh Manager menganalisis dan mendeteksi sinyal serangan berdasarkan aturan, termasuk aturan bawaan dan aturan yang dirancang untuk pola serangan aplikasi web. Hasil deteksi ditampilkan secara real-time melalui Dasbor Wazuh, memungkinkan administrator untuk segera mengidentifikasi dan menanggapi serangan.

Penelitian sebelumnya sebagian besar telah mengeksplorasi topik yang berkaitan dengan analisis log dan sistem deteksi intrusi (IDS) [4]–[8]. Studi-studi ini sebagian besar berfokus pada mesin deteksi mandiri atau IDS jaringan. Studi ini mengambil pendekatan yang berbeda, menggunakan platform SIEM/IDS Wazuh yang sudah mapan dan berstandar industri untuk secara langsung memantau dan mendeteksi serangan terhadap aplikasi web Go Hukum berbasis Laravel.

Log adalah catatan yang secara otomatis dihasilkan oleh program, aplikasi, atau perangkat jaringan untuk mendokumentasikan semua aktivitas atau peristiwa. Analisis log mengacu pada proses pengumpulan, analisis, dan interpretasi data log untuk mengidentifikasi pola, anomali, atau informasi penting bagi keamanan sistem. Sistem deteksi intrusi (IDS) adalah program yang dirancang untuk memantau lalu lintas data atau aktivitas pada sistem atau jaringan untuk mendeteksi aktivitas mencurigakan.

Wazuh adalah platform keamanan sumber terbuka yang menyediakan fungsionalitas SIEM dan XDR. Wazuh dapat melakukan pengumpulan dan analisis log, deteksi intrusi, pemantauan integritas file, deteksi kerentanan, dan respons proaktif [2]. Komponen utamanya meliputi Wazuh Agent, Wazuh Manager (server), Wazuh Indexer, dan Wazuh Dashboard. Dalam penelitian ini, aplikasi web Go Hukum berbasis Laravel adalah objek yang dipantau, dan log yang dihasilkannya berfungsi sebagai sumber data untuk analisis Wazuh.

II. METODE

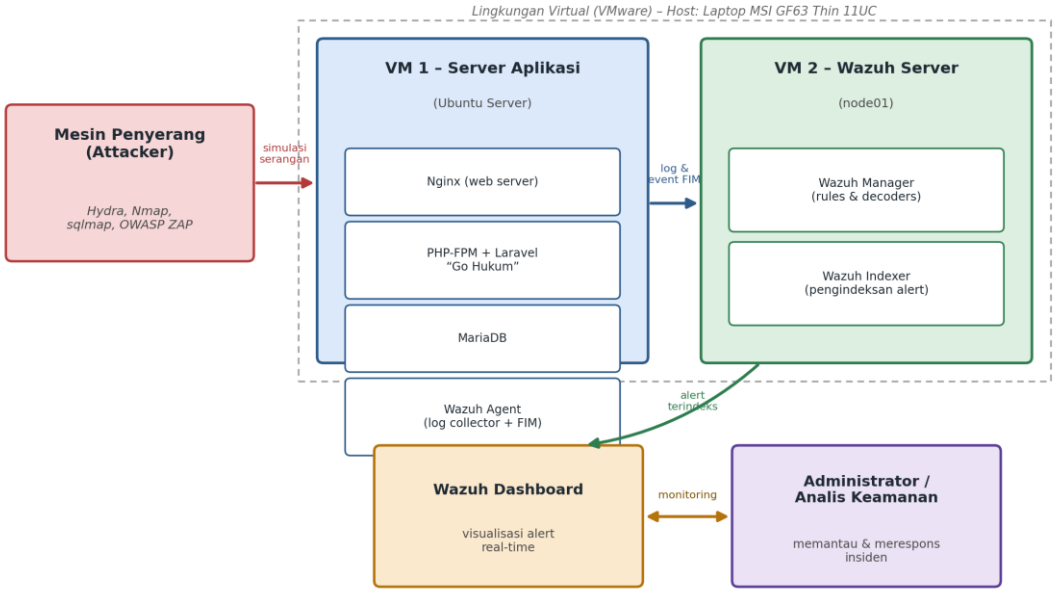
A. Gambaran Umum Sistem

Secara umum, sistem yang dibangun pada penelitian ini terdiri atas empat komponen utama, yaitu (1) server aplikasi, (2) server keamanan (Wazuh Manager beserta Indexer), (3) mesin penyerang (attacker), dan (4) Wazuh Dashboard yang diakses oleh administrator, sebagaimana digambarkan pada Gambar 1.

Server aplikasi menjalankan aplikasi web bantuan hukum Go Hukum yang dibangun dengan framework Laravel, dilayani oleh web server Nginx, dan menggunakan basis data MariaDB. Pada server ini dipasang Wazuh Agent yang bertugas mengumpulkan tiga sumber log, yaitu log akses Nginx, log kesalahan (error) Nginx, dan log aplikasi Laravel, serta memantau integritas berkas (File Integrity Monitoring/FIM) pada direktori aplikasi secara real-time.

Wazuh Agent meneruskan seluruh data yang terkumpul ke Wazuh Manager yang berjalan pada mesin virtual terpisah. Wazuh Manager menganalisis data tersebut menggunakan rules dan decoder, baik bawaan maupun yang disesuaikan, untuk mendeteksi pola serangan pada aplikasi web. Hasil analisis selanjutnya diteruskan ke Wazuh Indexer untuk diindeks, sehingga dapat divisualisasikan secara real-time melalui Wazuh Dashboard.

Untuk menguji efektivitas sistem, sebuah mesin penyerang yang terhubung pada jaringan virtual yang sama digunakan untuk melancarkan simulasi serangan (brute force SSH menggunakan Hydra, serta pemindaian/enumerasi jalur aplikasi web) terhadap server aplikasi. Administrator memantau seluruh notifikasi dan alert yang dihasilkan melalui Wazuh Dashboard untuk melakukan analisis dan pengambilan keputusan terhadap insiden yang terdeteksi. Seluruh lingkungan pengujian dijalankan di atas VMware yang di-hosting pada satu unit laptop (spesifikasi lengkap pada Tabel 4), sebagaimana ditunjukkan pada Gambar 1 berikut.



Gambar 1. Arsitektur sistem penelitian

B. Tahapan Penelitian (NDLC)

Studi ini merupakan proyek percontohan yang menggunakan teknologi Wazuh sebagai sistem analisis log dan sistem deteksi intrusi (IDS) untuk memantau aplikasi web Go Hukum berbasis Laravel. Pendekatan deskriptif digunakan, mengukur kinerja sistem berdasarkan data uji numerik (accuracy, precision, recall, dan waktu respons). Model pengembangan mengikuti Network Development Life Cycle (NDLC) [9], yang berfokus pada implementasi dan penyebaran sistem pemantauan keamanan. NDLC dipilih karena tahapannya sesuai dengan karakteristik penelitian ini, yaitu membangun dan menguji sebuah sistem monitoring keamanan pada lingkungan server, mulai dari analisis kebutuhan hingga pengelolaan pascaimplementasi.

Penelitian ini dilakukan berdasarkan enam tahapan NDLC [9], yaitu:

1. Analisis: Mengidentifikasi masalah dan kebutuhan dalam sistem pemantauan keamanan, serta menganalisis item log yang perlu dipantau (log aplikasi, log web server, log otentikasi).

2. Desain: Merancang topologi dan arsitektur pemantauan, proses pengumpulan log, aturan dan decoder, serta merancang skenario uji serangan.

3. Simulasi Prototipe: Membangun lingkungan uji coba menggunakan VMware dan menguji konektivitas antara Wazuh Agent dan Wazuh Manager.

4. Implementasi: Melakukan instalasi dan konfigurasi Wazuh secara lengkap, serta menyesuaikan decoder dan rules untuk mendeteksi pola serangan.

5. Monitoring: Menggunakan tools pihak ketiga seperti Hydra, sqlmap, Nmap, dan OWASP ZAP untuk melakukan simulasi serangan terkontrol, seperti brute force, injeksi SQL, XSS, pemindaian port, dan akses tidak sah.

6. Manajemen: Mengevaluasi hasil pengujian, menyempurnakan penyusunan rules untuk mengurangi false positive, serta memberikan rekomendasi.

Tes ini mensimulasikan serangan terkontrol pada aplikasi Go Hukum dan memeriksa apakah Wazuh berhasil mendeteksi ancaman tersebut. Efisiensi deteksi dievaluasi dengan menghitung jumlah true positive, false positive, true negative, dan false negative dari setiap kasus uji, kemudian kinerja sistem diukur menggunakan metrik accuracy, precision, recall, dan F1-Score. Selain itu, tes ini mencakup pengukuran waktu respons, yaitu waktu yang dibutuhkan dari inisiasi serangan hingga munculnya peringatan pada panel kontrol Wazuh.

Tabel 1
Kasus uji serangan

Jenis Serangan	Alat Pengujian	Indikator Deteksi
Brute force	Hydra	Peringatan beberapa upaya otentikasi gagal.
Injeksi SQL	SQLMap	Mendeteksi pola injeksi SQL dalam log server web.

Jenis Serangan	Alat Pengujian	Indikator Deteksi
Cross-Site Scripting (XSS)	OWASP ZAP	Mendeteksi pola skrip berbahaya dalam parameter aplikasi.
Pemindaian port	Nmap	Mendeteksi aktivitas pemindaian port di log sistem.

III. HASIL DAN DISKUSI

A. Lingkungan Implementasi

Sistem monitoring dibangun pada lingkungan tervirtualisasi menggunakan VMware, terdiri atas dua mesin virtual: satu mesin menjalankan Wazuh Manager, Indexer, dan Dashboard (Wazuh server), sedangkan mesin lainnya berperan sebagai server aplikasi web sekaligus tempat Wazuh Agent dipasang. Aplikasi web yang dipantau adalah aplikasi bantuan hukum berbasis Laravel bernama Go Hukum, yang dilayani oleh web server Nginx. Spesifikasi lingkungan pengujian ditampilkan pada Tabel 2, spesifikasi aplikasi Go Hukum ditampilkan pada Tabel 3, dan spesifikasi perangkat keras yang digunakan untuk menjalankan seluruh lingkungan virtual ditampilkan pada Tabel 4.

Tabel 2
Spesifikasi lingkungan pengujian

Komponen	Keterangan
Sistem operasi server	Ubuntu 26.04 LTS
Web server	Nginx 1.28
Runtime aplikasi	PHP 8.5 (PHP-FPM)
Basis data	MariaDB 11.8
Aplikasi yang dipantau	Aplikasi web bantuan hukum Go Hukum berbasis Laravel
Wazuh Agent	wazuh-GoHukum (ID 001), versi 4.14.6
Alamat IP agent	192.168.81.128
Wazuh Manager	wazuh-server (node01)
Sumber daya VM	2 vCPU, 7,2 GB RAM

Tabel 3
Spesifikasi aplikasi web Go Hukum

Komponen	Keterangan
Nama aplikasi	Go Hukum (aplikasi bantuan hukum)
Framework	Laravel 12
Starter kit autentikasi	Laravel Breeze
Antarmuka (frontend)	Tailwind CSS
Peran pengguna	Admin, Pengacara (Lawyer), Klien
Fitur utama	Manajemen pengaduan dan konsultasi hukum antara klien dan pengacara
Basis data (lingkungan pengujian)	MariaDB 11.8 (lihat Tabel 2)

Tabel 4
Spesifikasi perangkat pengujian (host)

Komponen	Keterangan
Perangkat	Laptop MSI GF63 Thin 11UC
Prosesor	Intel Core i5-11400H @ 2.70GHz (12 CPU logis)
Memori (RAM)	16 GB
Kartu grafis (VGA)	NVIDIA GeForce RTX 3050
Sistem operasi (host)	Windows 11 Home Single Language 64-bit
Perangkat lunak virtualisasi	VMware (menjalankan kedua mesin virtual penelitian)

Spesifikasi pada Tabel 4 diperoleh melalui DirectX Diagnostic Tool (dxdiag) pada perangkat yang digunakan untuk menjalankan seluruh lingkungan virtual penelitian.

B. Konfigurasi Pengumpulan Log dan FIM

Agar Wazuh dapat menganalisis aktivitas aplikasi web, berkas konfigurasi agent (ossec.conf) disesuaikan dengan menambahkan sumber log web server dan log aplikasi Laravel melalui direktif localfile. Selain itu, fitur File Integrity Monitoring (FIM) diaktifkan secara real-time pada direktori aplikasi untuk mendeteksi perubahan berkas yang tidak sah, seperti indikasi web defacement atau penanaman webshell. Direktori penyimpanan log aplikasi dikecualikan dari FIM agar tidak menghasilkan alert berlebih. Sumber log yang dipantau dirangkum pada Tabel 5.

Tabel 5
Sumber log dan objek yang dipantau

Objek	Lokasi	Metode
Log akses web	/var/log/nginx/access.log	localfile
Log error web	/var/log/nginx/error.log	localfile
Log aplikasi	/var/www/.../storage/logs/laravel.log	localfile
Integritas berkas	/var/www/bantuan-hukum	FIM realtime

C. Hasil Deteksi Serangan

Setelah konfigurasi selesai, Wazuh Agent berhasil terhubung ke Wazuh Manager dengan status aktif (Gambar 2), dan log web server berhasil

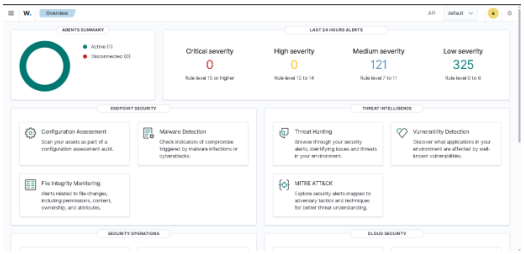
terbaca serta diklasifikasikan oleh decoder web-accesslog. Pengujian dilakukan melalui simulasi serangan terkendali dari mesin penyerang terhadap server aplikasi. Tiga kategori skenario diuji, yaitu brute force pada layanan SSH, pemindaian/enumerasi path pada aplikasi web, dan modifikasi berkas pada direktori aplikasi. Hasil deteksi ditampilkan pada Tabel 6.

Tabel 6
Hasil deteksi skenario pengujian

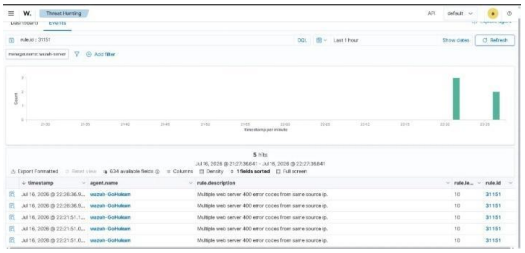
Skenario	Aturan · Level	Deskripsi Aturan	Status
Brute force SSH	2502 · 10	Pengguna gagal memasukkan kata sandi lebih dari satu kali	Terdeteksi
Brute force SSH (korelasi)	5763 · 10	sshd: upaya brute force untuk mendapatkan akses ke sistem	Terdeteksi
Scanning web	31101 · 5	Kode error 400 pada web server	Terdeteksi
Scanning web (korelasi)	31151 · 10	Beberapa kode error 400 web server dari alamat IP sumber yang sama	Terdeteksi
Integritas berkas (FIM)	554 · 5	Berkas baru ditambahkan ke dalam sistem	Terdeteksi

Catatan: deskripsi aturan merupakan terjemahan dari pesan rule bawaan Wazuh.

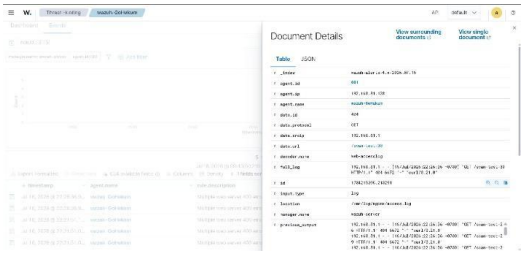
Hasil pada Tabel 6 menunjukkan pola deteksi berlapis. Untuk setiap kategori serangan, Wazuh tidak hanya mencatat kejadian tunggal (aturan level rendah seperti 2502 dan 31101), tetapi juga mengorelasikan kejadian berulang dari sumber yang sama menjadi indikasi pola serangan dengan tingkat keparahan lebih tinggi (aturan level 10 seperti 5763 dan 31151). Pada skenario brute force SSH, Wazuh secara otomatis memetakan kejadian ke kerangka MITRE ATT&CK [10] dengan taktik Password Guessing, SSH, dan Brute Force. Pada skenario scanning web, alert korelasi 31151 disertai identifikasi alamat IP sumber (data.srcip) sehingga penyerang dapat dikenali secara spesifik, sebagaimana ditunjukkan pada Gambar 3. Sementara itu, FIM berhasil mendeteksi penambahan berkas pada direktori aplikasi secara real-time dalam hitungan detik, dengan detail alamat IP sumber ditunjukkan pada Gambar 4.



Gambar 2. Status Wazuh Agent aktif pada dashboard



Gambar 3. Deteksi korelasi scanning web (rule 31151)



Gambar 4. IP sumber

D. Analisis Kinerja Deteksi

Kinerja deteksi sistem dievaluasi berdasarkan sepuluh kasus uji terkendali, terdiri atas lima kasus serangan (sesuai Tabel 6) dan lima kasus akses normal ke rute aplikasi yang sah sebagai pembanding (baseline). Dari sepuluh kasus tersebut diperoleh True Positive (TP) = 5, yaitu seluruh percobaan serangan berhasil memicu alert yang sesuai; False Negative (FN) = 0, karena tidak ada serangan yang lolos dari deteksi; False Positive (FP) = 0, karena tidak ada akses normal yang keliru dikategorikan sebagai serangan; dan True Negative (TN) = 5, yaitu seluruh akses normal dikenali dengan benar sebagai aktivitas yang sah.

Hasil ini dirangkum pada Tabel 7. Perlu digarisbawahi bahwa nilai 100% pada seluruh metrik ini diperoleh dari sepuluh kasus uji terkendali dalam skala kecil sehingga bersifat indikatif dan belum tentu merepresentasikan kondisi lalu lintas produksi yang jauh lebih beragam (lihat bagian Saran).

Selain akurasi deteksi, diukur pula waktu respons, yaitu selang waktu dari dilancarkannya serangan hingga munculnya alert. Pada sisi agent dan manager, alert terbentuk dalam hitungan detik setelah aktivitas terekam pada log. Waktu hingga alert tampil pada Wazuh Dashboard berkisar antara beberapa detik hingga sekitar satu sampai dua menit, terutama dipengaruhi oleh proses indexing pada Wazuh Indexer, bukan oleh keterlambatan agent dalam membaca log.

Tabel 7
Metrik kinerja deteksi

Metrik	Nilai
Accuracy	100%

Metrik	Nilai
Precision	100%
Recall	100%
F1-Score	100%

E. Pembahasan

Hasil pengujian membuktikan bahwa Wazuh mampu menggantikan pemeriksaan log manual dengan analisis terpusat dan deteksi otomatis secara real-time. Keunggulan utama yang teramati adalah mekanisme deteksi berlapis: kombinasi aturan tunggal dan aturan korelasi memungkinkan sistem membedakan kesalahan biasa (misalnya satu kegagalan login atau satu galat 404) dari pola serangan sesungguhnya (upaya brute force dan pemindaian berulang). Pemetaan otomatis ke kerangka MITRE ATT&CK serta identifikasi IP sumber turut mempercepat proses analisis dan pengambilan keputusan oleh administrator. Temuan ini sejalan dengan penelitian lain yang juga menunjukkan efektivitas Wazuh dalam mendeteksi serangan brute force menggunakan Hydra pada layanan SSH [12], serta dalam memonitor keamanan server secara terpusat melalui SIEM [11], [13].

Nilai metrik yang tinggi pada penelitian ini perlu dimaknai dalam konteks set uji terkendali yang terbatas. Pengujian difokuskan pada tiga kategori serangan (brute force SSH, scanning/enumerasi web, dan pelanggaran integritas berkas), sedangkan skenario lain seperti SQL Injection, Cross-Site Scripting (XSS), dan port scanning yang direncanakan pada Tabel 1 belum sepenuhnya diuji dan menjadi arah pengembangan selanjutnya. Untuk memperoleh evaluasi statistik yang lebih kuat, disarankan pengujian dengan volume dan variasi lalu lintas yang lebih besar, penggunaan alat serangan khusus (seperti Hydra, sqlmap, Nmap, dan OWASP ZAP), serta penyusunan aturan kustom untuk mengurangi potensi false positive pada lingkungan produksi.

IV. KESIMPULAN

Implementasi SIEM Wazuh terbukti sangat efektif untuk menggantikan pemantauan manual. Pendekatan ini esensial untuk mempercepat penanganan insiden dan menjaga keandalan aplikasi web Go Hukum berbasis Laravel.

V. SARAN

Berdasarkan hasil penelitian ini, beberapa saran dapat diberikan untuk pengembangan lebih lanjut:

1. Pengujian perlu diperluas untuk mencakup skenario serangan yang belum diuji pada penelitian ini, seperti SQL Injection, Cross-Site Scripting (XSS), dan port scanning menggunakan alat seperti sqlmap, OWASP ZAP, dan Nmap sebagaimana direncanakan pada Tabel 1.

2. Volume dan variasi data uji perlu ditingkatkan agar evaluasi kinerja sistem (accuracy, precision, recall) lebih representatif dan tidak hanya terbatas pada skenario terkendali dalam jumlah kecil.

3. Penyusunan custom rules dan decoder tambahan disarankan untuk mengurangi potensi false positive ketika sistem diterapkan pada lingkungan produksi dengan traffic yang lebih kompleks.

4. Integrasi Wazuh dengan mekanisme active response, seperti pemblokiran otomatis alamat IP penyerang, dapat dipertimbangkan untuk mempercepat mitigasi insiden.

5. Pengujian pada lingkungan produksi yang sesungguhnya (bukan hanya lingkungan virtual/simulasi) diperlukan untuk memvalidasi kinerja sistem dalam kondisi operasional nyata.

DAFTAR PUSTAKA

[1] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, 21(14), 4759. https://doi.org/10.3390/s21144759

[2] Wazuh Inc. (2026). Wazuh Documentation. Diakses dari https://documentation.wazuh.com/current/index.html

[3] Stanković, S., Gajin, S., & Petrović, R. (2022). A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. Proceedings, IX International Conference IcETRAN, Novi Pazar, Serbia, 6–9 Juni 2022, 1–5.

[4] Artika, D. D., Rumahorbo, D., Al-Majid, M. H., & Kiswanto, D. (2025). Implementasi Sistem Keamanan Website dengan Analisis Log dan Deteksi Aktivitas Anomali Menggunakan Isolation Forest. Jurnal Informatika dan Teknik Elektro Terapan (JITET), 13(3S1).

[5] Berutu, dkk. (2025). Pengembangan Sistem Logging Server Berbasis Website dengan Visualisasi Real-Time dan Alert Sederhana. Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI).

[6] Firdyanto, T., & Rushendra, R. (2024). Implementation of Intrusion Detection System with Rule-Based Method on Website. Journal of Computer Networks, Architecture and High Performance Computing, 6(3), 1245–1252. https://doi.org/10.47709/cnahpc.v6i3.4256

[7] Lestari, T., Riadi, I., & Umar, R. (2020). Analisis Keamanan Transaksi E-Commerce Menggunakan Intrusion Detection System (IDS) Berbasis Snort. Jurnal Ilmiah FIFO, 12(1).

[8] Riza, F. (2022). Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging. Jurnal Sistim Informasi dan Teknologi, 5(1), 7–15. https://doi.org/10.37034/jsisfotek.v5i1.161

[9] Kosasi, S. (2011). Penerapan Network Development Life Cycle untuk Pengembangan Teknologi Thin Client pada

Pendidikan KSM Pontianak. Jurnal Ilmiah Komputasi dan Elektronika (JIKE), 1(2), 125–141.

[10] MITRE Corporation. (2026). MITRE ATT&CK®. Diakses dari https://attack.mitre.org/

[11] Aditya, R., Muhyidin, Y., & Singasatia, D. (2024). Implementasi Security Information and Event Management (SIEM) untuk Monitoring Keamanan Server Menggunakan Wazuh. Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika, 2(5), 137–144. https://doi.org/10.61132/merkurius.v2i5.289

[12] Patoni, G., Muhyidin, Y., & Singasatia, D. (2024). Implementasi Wazuh pada Ubuntu Server untuk Mendeteksi Serangan Brute Force Hydra. Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika, 2(5), 145–156. https://doi.org/10.61132/merkurius.v2i5.290

[13] Saputra, F. A., Dharmawan, T. R., & Rustianto, A. (2024). Implementasi Wazuh SIEM untuk Manajemen Log Event di Pesantren Teknologi Informasi dan Komunikasi Jombang. Jurnal Informatika Terpadu, 10(2), 146–155. https://doi.org/10.54914/jit.v10i2.1435