Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume xx Nomor x Edisi xxxx 20xx
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

EVALUASI KINERJA SISTEM ANCAMAN SIBER MELALUI INTEGRASI WAZUH DAN TELEGRAM DI PT. XYZ

Evaluating the Performance of a Cyber Threat Management System via Wazuh and Telegram Integration at PT. XYZ

Salwa Ardhana[1], **Muhammad Idris**[2]
Program Studi Rekayasa Keamanan Siber, Politeknik Negeri Batam, Batam, Indonesia
E-mail: salwaardhana0@gmail.com

Abstrak

Keamanan siber merupakan aspek krusial dalam menjaga keberlangsungan operasional sistem informasi perusahaan. PT. XYZ bagai entitas yang mengandalkan infrastruktur TI, memerlukan sistem deteksi dan respons ancaman yang efektif dan real-time. Penelitian ini bertujuan untuk mengevaluasi kinerja sistem keamanan berbasis Wazuh yang diintegrasikan dengan Telegram sebagai media notifikasi instan dalam merespons potensi ancaman siber. Metode yang digunakan meliputi instalasi dan konfigurasi Wazuh sebagai Security Information and Event Management (SIEM), integrasi dengan bot Telegram, serta pengujian melalui simulasi serangan seperti SQL Injection, Broken Access Control, Cryptographic Failures, dan Denial of Service (DoS). Evaluasi dilakukan berdasarkan parameter kecepatan deteksi, akurasi alert, serta efisiensi notifikasi kepada tim keamanan. Hasil penelitian menunjukkan bahwa integrasi Wazuh dengan Telegram mampu meningkatkan responsivitas sistem terhadap ancaman, dengan rata-rata waktu notifikasi di bawah 10 detik setelah deteksi serangan. Temuan ini membuktikan bahwa kombinasi Wazuh dan Telegram dapat menjadi solusi efektif dalam meningkatkan kapabilitas pemantauan dan respons keamanan siber di lingkungan perusahaan.Kata Kunci: Wazuh, Telegram, Keamanan Siber, SIEM, Evaluasi Kinerja, Deteksi Ancaman.

Abstract

Cybersecurity is a crucial aspect in ensuring the continuity of a company's information system operations. PT. XYZ, as an entity that relies heavily on IT infrastructure, requires an effective and real-time threat detection and response system. This research aims to evaluate the performance of a security system based on Wazuh integrated with Telegram as an instant notification medium in responding to potential cyber threats. The methodology includes the installation and configuration of Wazuh as a Security Information and Event Management (SIEM) system, integration with a Telegram bot, and testing through simulated attacks such as SQL Injection, Broken Access Control, Cryptographic Failures, and Denial of Service (DoS). The evaluation is based on parameters such as detection speed, alert accuracy, and notification efficiency to the security team. The results indicate that integrating Wazuh with Telegram significantly enhances system responsiveness to threats, with an average notification time of less than 10 seconds after an attack is detected. These findings demonstrate that the combination of Wazuh and Telegram can serve as an effective solution for improving cybersecurity monitoring and response capabilities within a corporate environment.

Keywords: Wazuh, Telegram, Cybersecurity, SIEM, Performance Evaluation, Threat Detection.

Naskah diterima xx Jan. 2024; direvisi xx Feb. 2024; dipublikasikan xx Apr. 2024.

I. PENDAHULUAN

Pada era pertumbuhan sistem informasi yang sangat cepat saat ini keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan, karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan[1]. Salah satu solusi penting dalam manajemen keamanan informasi adalah SIEM, yaitu sistem yang dapat memberikan analisis keamanan secara real-time melalui peringatan dari perangkat keras dan aplikasi jaringan, serta menyajikan data log dalam bentuk visualisasi untuk memudahkan analisis lalu lintas jaringan[2]. PT XYZ, sebagai perusahaan IT dan konsultan keamanan siber yang berdiri sejak 2022 dan berbasis di Bandung, saat ini belum memiliki

doi : 10.34010/jamika.v15i1.14190

sistem keamanan operasional internal, sehingga penerapan SIEM seperti Wazuh menjadi penting tidak hanya untuk perlindungan data perusahaan, tetapi juga sebagai nilai jual tambahan kepada klien, dengan integrasi ke saluran komunikasi demi pemantauan keamanan secara real-time dan peningkatan daya saing di bidang keamanan informasi.

Wazuh adalah perangkat lunak open source yang berfungsi sebagai sistem deteksi berbasis host (endpoint) yang menyatukan kemampuan XDR (Extended Detection and Response) dan SIEM (Security Information and Event Management), di antaranya menganalisis log, mendeteksi intrusi dan malware, memantau integritas file, melakukan penilaian konfigurasi sesuai standar industri, mendeteksi kerentanan, serta memberikan dukungan terhadap kepatuhan aturan. Wazuh juga mampu memberi peringatan berbasis waktu serta merespons secara aktif terhadap ancaman[3]. Perangkat ini dapat diintegrasikan dengan berbagai sistem keamanan lainnya seperti firewall dan antivirus, serta kompatibel dengan sistem operasi Windows, Linux, dan macOS. Wazuh memiliki fitur alert yang dapat mendeteksi berbagai jenis serangan, intrusi, penyalahgunaan perangkat lunak, kesalahan konfigurasi, kesalahan aplikasi, malware, rootkit, anomali sistem, serta pelanggaran kebijakan keamanan berdasarkan ruleset yang telah ditentukan [4]. Dalam konteks analisis log, Wazuh server bertindak sebagai pusat manajemen agent dan dashboard monitoring untuk integritas file, intrusi, dan analisis log, sedangkan Wazuh agent dipasang pada perangkat endpoint untuk membaca sistem, mengumpulkan log, serta mengirimkannya ke server untuk dilakukan analisis dan deteksi ancaman. Ancaman yang terdeteksi akan ditandai sebagai alert yang mencakup informasi seperti rule ID dan nama rule [5]. Peran Wazuh sangat signifikan dalam membantu mengidentifikasi berbagai kesalahan aplikasi maupun sistem, kesalahan konfigurasi, aktivitas jahat yang berhasil, pelanggaran kebijakan, dan permasalahan keamanan atau operasional lainnya.

Ancaman siber dapat ditujukan kepada siapa saja yang terhubung ke jaringan internet, dengan berbagai bentuk serangan seperti pencurian informasi, pemerasan, pembajakan, dan lain sebagainya [6]. Aktor yang melakukan serangan terhadap sistem atau jaringan organisasi dengan tujuan tertentu seperti pencurian data, sabotase, atau penyebaran malware dikenal sebagai *threat actor*. Wazuh memiliki kemampuan untuk mendeteksi aktivitas threat actor melalui pemantauan log, analisis perilaku, serta korelasi berbagai indikator ancaman (*Indicator of Compromise* / IOC). Aktivitas mencurigakan dapat berupa percobaan login tidak sah, pengumpulan informasi sistem, transfer data mencurigakan, hingga eksekusi perintah berbahaya atau malware.

Berbagai penelitian sebelumnya telah menunjukkan efektivitas Wazuh dalam meningkatkan keamanan sistem informasi. Chandra et al. (2024) [7] menunjukkan bahwa fitur *File Integrity Monitoring* (FIM) pada Wazuh mampu mendeteksi aktivitas mencurigakan terhadap file dan memberikan notifikasi kepada administrator secara efisien. Nova et al. (2022) [8] membahas penggunaan Wazuh untuk manajemen log dan deteksi celah keamanan, terutama dalam konteks serangan *Denial of Service* (DoS), serta menekankan fleksibilitas konfigurasi dan kecepatan respons sistem. Farrel et al. (2024) [9] juga memperlihatkan keberhasilan Wazuh dalam mendeteksi 100% percobaan serangan *brute force* melalui integrasi *active response* dan sistem notifikasi Telegram. Selain itu, Stanković et al. (2024)[10] melakukan tinjauan menyeluruh terhadap fitur-fitur Wazuh, termasuk pemantauan integritas file, analisis log, dan deteksi intrusi berbasis *SSH brute force*. Temuan-temuan ini menegaskan bahwa Wazuh merupakan solusi SIEM yang tangguh dan adaptif dalam berbagai konteks ancaman siber.

Penelitian ini bertujuan untuk mengevaluasi efektivitas Wazuh dalam konteks operasional keamanan informasi di lingkungan PT. XYZ. Fokus utama penelitian adalah mengukur kemampuan Wazuh dalam mendeteksi dan merespons ancaman siber secara akurat dan tepat waktu, serta menilai efisiensi pengiriman notifikasi melalui integrasi dengan platform komunikasi Telegram. Hasil penelitian diharapkan dapat memberikan gambaran komprehensif mengenai kinerja Wazuh dalam mendeteksi ancaman, sekaligus menjadi kontribusi praktis bagi PT. XYZ dalam membangun sistem keamanan yang proaktif dan andal.

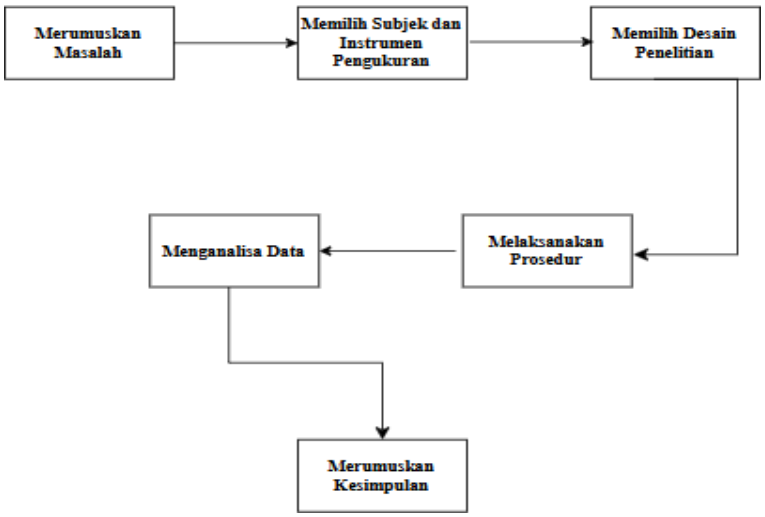
Penelitian ini dilakukan dalam bentuk pengembangan prototype dan belum diterapkan pada infrastruktur operasional PT. XYZ. Lingkup kajian dibatasi pada perancangan dan pengujian integrasi Wazuh dengan Telegram dalam lingkungan virtual untuk menilai kelayakan teknis solusi yang diusulkan. Implementasi penuh pada jaringan produksi perusahaan direncanakan sebagai langkah lanjutan apabila hasil pengujian prototype menunjukkan performa yang memadai dan sesuai kebutuhan operasional PT. XYZ.

II. METODE PENELITIAN

Dalam penelitian ini, saya menggunakan metode eksperimen, yang merupakan metode untuk mengetahui pengaruh dari perlakuan tertentu dalam kondisi yang terkendali [11]. Proses penelitian ini mengikuti tahapan-tahapan sebagaimana ditunjukkan pada Gambar 1. Tahap pertama adalah merumuskan masalah, yaitu kebutuhan perusahaan XYZ akan sistem monitoring keamanan yang mampu mendeteksi ancaman siber secara real-time. Oleh karena itu, dirumuskan permasalahan mengenai bagaimana mengimplementasikan solusi keamanan operasional menggunakan Wazuh sebagai sistem deteksi ancaman. Tahap kedua adalah memilih subjek dan instrumen pengukuran, di mana penelitian ini menggunakan Wazuh

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume xx Nomor x Edisi xxxx 20xx
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

sebagai alat utama untuk mengukur ketepatan dan kecepatan deteksi, mulai dari pengiriman log hingga notifikasi ke Telegram. Selanjutnya, desain penelitian ditentukan menggunakan pendekatan eksperimental, dengan skenario simulasi serangan siber untuk menguji performa sistem. Tahap berikutnya adalah melaksanakan prosedur, yaitu dengan mengonfigurasi Wazuh agar terintegrasi dengan Telegram, kemudian menjalankan simulasi serangan terhadap sistem. Setelah prosedur dijalankan, data yang diperoleh dianalisis untuk mengukur ketepatan dan waktu respons sistem terhadap ancaman. Terakhir, hasil analisis digunakan untuk merumuskan kesimpulan mengenai efektivitas Wazuh dalam mendeteksi dan merespons ancaman keamanan di lingkungan perusahaan XYZ.



Gambar 1. Metode Penelitian

Penelitian ini dilakukan secara mandiri oleh peneliti di lingkungan rumah dengan memanfaatkan dua unit perangkat komputer pribadi. Sistem diuji dan dibangun secara lokal menggunakan dua virtual machine (VM) untuk mensimulasikan fungsi sebagai Wazuh Server dan Wazuh Agent. Adapun spesifikasi perangkat keras yang digunakan dalam penelitian ditunjukkan pada Tabel 1:

TABEL 1
SPESIFIKASI LINGKUNGAN PENGUJIAN

Perangkat	Sistem Operasi	Spesikfikasi Umum	Fungsi
Laptop Pribadi	Ubuntu 22.04 LTS	2 vCPU, RAM 4 GB	Wazuh Server
VM	Ubuntu 22.04 LTS	2 vCPU, RAM 4 GB	Wazuh Agent

Sementara itu, perangkat lunak yang digunakan selama proses eksperimen dijelaskan pada Tabel 2:

TABEL 2
PERANGKAT LUNAK

Perangkat Lunak	Versi	Keterangan
Wazuh	v4.9	Sistem deteksi dan manajemen log
Telegram Bot API	Terbaru	Media notifikasi ancaman
Web Server	-	Endpoint untuk simulasi serangan

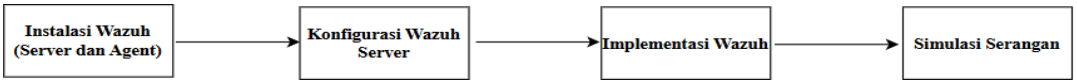
Desain eksperimen menggunakan pendekatan kuantitatif dengan metode eksperimen, untuk mengetahui pengaruh dari perlakuan berupa serangan siber terhadap sistem keamanan berbasis Wazuh. Instrumen utama dalam penelitian ini adalah Wazuh v4.9 yang digunakan sebagai sistem *Security Information and Event Management* (SIEM). Penelitian mengkaji efektivitas sistem dalam mendeteksi empat jenis serangan siber: SQL Injection, Broken Access Control, Cryptographic Failure, dan Denial of Service (DoS). Dua variabel utama digunakan dalam eksperimen ini, yaitu variabel bebas berupa jenis serangan, dan variabel terikat berupa ketepatan deteksi serta waktu respons sistem terhadap serangan. Indikator pengukurannya meliputi: (1) waktu yang dibutuhkan sejak serangan dijalankan hingga notifikasi diterima (kecepatan respons), dan (2) akurasi sistem dalam mengidentifikasi serangan berdasarkan rule yang telah diterapkan.

Ketepatan deteksi diukur untuk mengetahui sejauh mana sistem mampu mengenali ancaman yang muncul selama simulasi. Perhitungannya dilakukan dengan menggunakan rumus **Accuracy = (Jumlah Ancaman Teridentifikasi / Total**

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume xx Nomor x Edisi xxxx 20xx
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Ancaman) × 100%, di mana hasil akhir akan menunjukkan persentase deteksi berhasil terhadap total ancaman yang diuji. Selanjutnya, waktu respons dihitung untuk mengetahui seberapa cepat sistem memberikan reaksi setelah serangan dimulai. Rumus yang digunakan adalah **Waktu Respons = T respon – T serangan**, dengan *T serangan* menunjukkan waktu dimulainya serangan dan *T respon* adalah waktu saat Wazuh pertama kali memberikan respons atau mencatat ancaman. Indikator terakhir adalah kecepatan pengiriman notifikasi, yang menunjukkan seberapa cepat pesan peringatan diteruskan ke Telegram setelah ancaman terdeteksi. Pengukuran ini dilakukan dengan rumus **Kecepatan = T_notifikasi – T respon**, di mana *T notifikasi* merupakan waktu diterimanya pesan di Telegram, dan *T_respon* adalah waktu ketika ancaman berhasil diidentifikasi oleh Wazuh. Indikator ini digunakan sebagai dasar analisis dalam pembahasan untuk mengukur kinerja sistem secara menyeluruh, baik dari sisi akurasi pendeteksian, kecepatan respons, maupun efektivitas integrasi komunikasi melalui notifikasi real-time.

Adapun prosedur eksperimen dilakukan secara bertahap sesuai dengan alur yang ditunjukkan pada Gambar 2. Langkah pertama adalah melakukan instalasi Wazuh pada server dan agen menggunakan sistem operasi Ubuntu 22.04.1. Kedua, dilakukan konfigurasi Wazuh Server agar terhubung dengan saluran komunikasi Telegram untuk mengirimkan notifikasi secara otomatis saat terjadi insiden. Ketiga, proses implementasi dilakukan dengan mendepoy Wazuh Agent ke dalam Wazuh Server sehingga sistem dapat memantau aktivitas pada agen secara terpusat. Terakhir, melakukan simulasi serangan siber untuk menguji kinerja sistem dalam mendeteksi ancaman secara tepat dan cepat.



Gambar 2. Prosedur Eksperimen

III. HASIL DAN PEMBAHASAN

Dalam penelitian ini, deteksi terhadap empat jenis serangan siber dilakukan menggunakan aturan kustom yang disimpan di dalam file konfigurasi Wazuh, tepatnya pada local_rules.xml yang berada di direktori /var/ossec/etc/rules/. Semua aturan tersebut dikelompokkan ke dalam grup custom_rules_example, yang dibuat secara khusus untuk mendeteksi serangan SQL Injection, Broken Access Control, Cryptographic Failure, dan Denial of Service (DoS).

Pemilihan empat jenis serangan yang diuji dalam penelitian ini didasarkan pada kategori kerentanan yang termasuk dalam OWASP Top 10 (Open Web Application Security Project), yang menjadi standar internasional dalam klasifikasi risiko keamanan aplikasi. Serangan **SQL Injection** mewakili kategori *Injection* (A03:2021), karena eksploitasi ini masih sering ditemukan pada aplikasi web akibat input tidak tervalidasi. **Broken Access Control** dipilih karena berada pada peringkat pertama OWASP Top 10 (A01:2021), mengingat dampaknya yang kritis terhadap kerahasiaan dan integritas data apabila kontrol otorisasi gagal diterapkan. **Cryptographic Failures** mengacu pada kategori A02:2021, di mana praktik penggunaan algoritma kriptografi lemah (contohnya MD5) membuka peluang serangan kolisi dan pemalsuan data. Sedangkan **Denial of Service (DoS)** dipilih karena meskipun tidak secara eksplisit muncul dalam OWASP Top 10, serangan ini termasuk ancaman yang signifikan terhadap ketersediaan layanan, yang merupakan salah satu aspek utama dalam prinsip keamanan informasi (CIA Triad). Dengan demikian, keempat jenis serangan ini mencerminkan ancaman yang relevan terhadap keamanan web modern serta memberikan dasar kuat untuk menguji efektivitas sistem deteksi berbasis Wazuh.

SQL Injection: Rule dengan ID 100304 menggantikan rule default Wazuh (ID 31164) dan mendeteksi upaya SQL Injection melalui deskripsi "*SQL Injection attempt detected*" pada grup *attack, sqlinjection, web*. Kerentanan nyata tercermin pada **CVE-2024-8465**, yang menjelaskan serangan SQL Injection melalui parameter user_id pada endpoint /jobportal/admin/user/controller.php, memungkinkan penyerang untuk memperoleh seluruh data pengguna tanpa autentikasi. Skornya mencapai **High (CVSS 7.5)** oleh NVD dan **Critical (CVSS 9.8)** oleh INCIBE [12].

Gambar 3. Tampilan Rules Sql Injection

Broken Access Control: Rule ID 100301 mendeteksi percobaan akses tanpa otorisasi (Broken Access Control) dengan memantau log yang mengandung substring BrokenAccess: dan mengelompokkannya ke grup broken_access, web. Kasus nyata serupa terdapat pada CVE-2023-4018, yaitu kerentanan forced browsing di GitLab versi 16.2–16.3.x akibat improper permission validation, yang memungkinkan pembuatan eksperimen model oleh pengguna tanpa hak

Jurnal JAMIKA Manajemen Informatika
Jurnal Manajemen Informatika (JAMIKA)
Volume xx Nomor x Edisi xxxx 20xx
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Akses [13].

Gambar 4. Tampilan Rules Broken Access Control

Cryptographic Failure (Penggunaan MD5): Rule ID 100302 mendeteksi penggunaan algoritma kriptografi tidak aman (MD5) melalui kata kunci CryptoFail:. Hal ini sesuai dengan **CVE-2024-55885**, yang melaporkan MD5 digunakan dalam framework Go (beego < 2.3.4) untuk hashing cache key, dan rentan terhadap collision [14].

Gambar 5. Tampilan Rules Cryptographic Failures

Denial of Service (DoS): Rule ID 100303 mengidentifikasi "Possible DoS attack from" dalam log, masuk kategori dos, syslog, local, dan berkaitan dengan **CVE-2025-20139**, yang mendokumentasikan celah DoS yang dapat menyebabkan aplikasi tidak responsif atau crash [15].

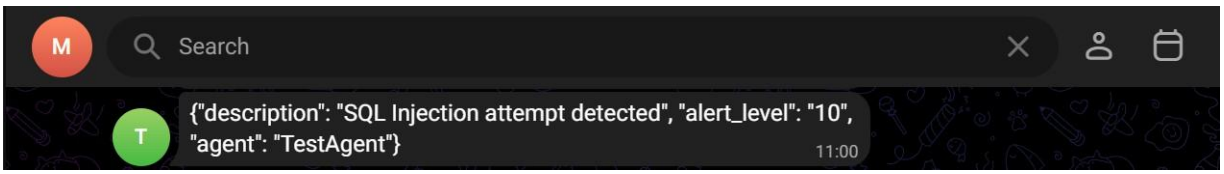
Gambar 6. Tampilan Rules DoS

Pengujian dalam penelitian ini difokuskan pada empat jenis serangan siber, yaitu SQL Injection, Broken Access Control, Cryptographic Failure, dan Denial of Service (DoS). Masing-masing serangan disimulasikan sebanyak tiga puluh kali untuk memperoleh hasil yang konsisten dalam pengukuran ketepatan deteksi, waktu respons, serta kecepatan pengiriman notifikasi dari sistem Wazuh ke saluran komunikasi Telegram.

Pada pengujian serangan SQL Injection, payload yang digunakan berupa ' OR '1'='1, yang disisipkan ke dalam parameter input seperti username melalui URL atau form login. Contoh permintaan (request) yang dikirimkan adalah: http://192.168.1.xx/admin.php?username=admin%27%20OR%20%271%27=%271&password=anything

Teknik ini bertujuan untuk mengeksploitasi kelemahan autentikasi dengan menyalahgunakan logika SQL, sehingga sistem menganggap input valid walaupun autentikasi tidak sah. Serangan ini juga memunculkan pola '1'='1 dalam log sistem, yang kemudian digunakan oleh Wazuh untuk memicu rule deteksi melalui konfigurasi <match>'1'='1</match>. Dengan demikian, sistem Wazuh dapat memberikan notifikasi ketika pola tersebut teridentifikasi dalam aktivitas log, yang menandakan adanya upaya serangan injeksi SQL.

Gambar 7. Tampilan Wazuh Berhasil Deteksi SQLi Gambar



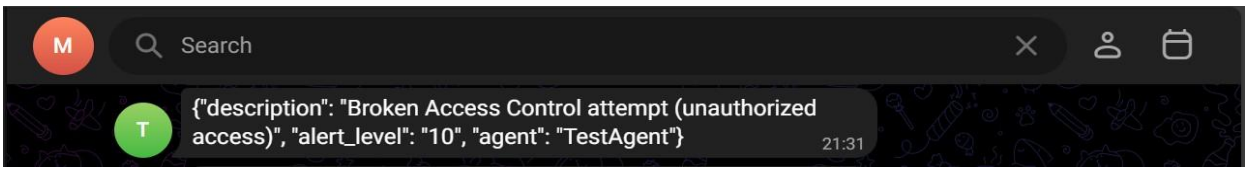
8. Tampilan Telegram Terima Notifikasi SQLi

doi : 10.34010/jamika.v15i1.14190

Jurnal Manajemen Informatika (JAMIKA)
Volume xx Nomor x Edisi xxxx 20xx
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

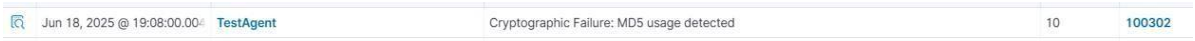
Untuk pengujian serangan Broken Access Control, metode yang digunakan adalah mencoba mengakses halaman admin secara langsung tanpa melalui proses otentikasi yang sah. Serangan ini mengeksploitasi kelemahan kontrol akses, di mana pengguna yang tidak berwenang mencoba mengakses sumber daya terbatas. Tujuan dari simulasi ini adalah menghasilkan entri log yang mengandung kata kunci "BrokenAccess: unauthorized" ketika sistem mendeteksi upaya akses tidak sah. Dengan rule tersebut, Wazuh mampu mendeteksi percobaan akses ilegal secara otomatis dan mengirimkan notifikasi kepada administrator melalui Telegram, sehingga efektivitas sistem dalam mengidentifikasi pelanggaran akses dapat diuji secara real-time.

Gambar 9. Tampilan Wazuh Berhasil Deteksi BAC

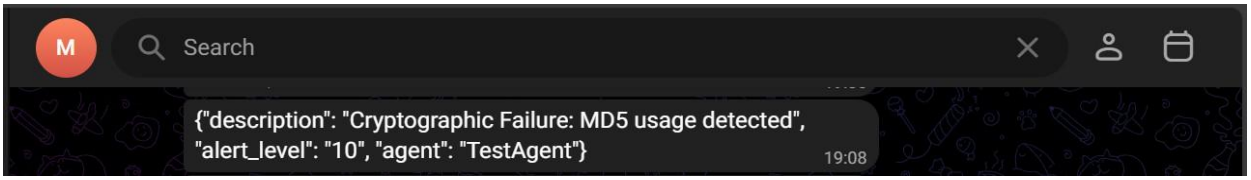


Gambar 10. Tampilan Telegram Terima Notifikasi BAC

Pada pengujian serangan *Cryptographic Failures*, simulasi dilakukan dengan menambahkan sebuah skrip PHP bernama md5test.php ke dalam sistem. Skrip ini secara sengaja menggunakan algoritma MD5 untuk melakukan proses hashing, yang dikenal sebagai algoritma kriptografi yang sudah usang dan rentan terhadap serangan kolisi. Setiap kali skrip tersebut dijalankan, maka log khusus akan dituliskan ke dalam file wazuh_crypto.log dengan format yang mengandung kata kunci **"CryptoFail:"** sebagai penanda bahwa telah terjadi praktik penggunaan algoritma kriptografi yang lemah.



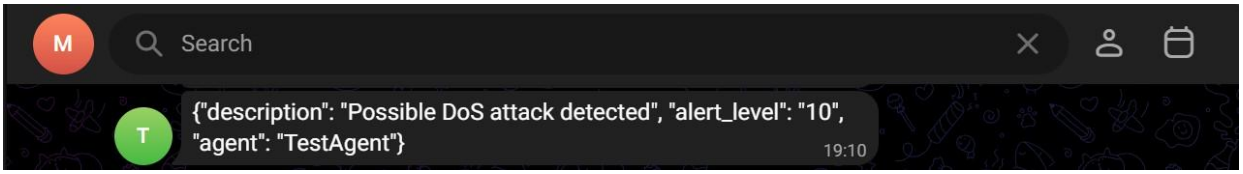
Gambar 11. Tampilan Wazuh Berhasil Deteksi Cryptographic Failures



Gambar 12. Tampilan Telegram Terima Notifikasi Cryptographic Failures

Pada pengujian serangan **Denial of Service (DoS)**, pendekatan yang digunakan tidak melibatkan penggunaan alat uji stres seperti ab, hping3, atau sejenisnya. Sebagai gantinya, simulasi dilakukan secara manual dengan cara menghasilkan log khusus yang merepresentasikan adanya upaya serangan DoS. Sebuah file log bernama **/var/log/wazuh_dos.log** dibuat di sisi agent, berfungsi sebagai tempat pencatatan aktivitas yang mencerminkan pola serangan. Untuk memicu isi log tersebut, digunakan skrip PHP bernama **doslog.php** yang dijalankan berulang kali dan menghasilkan entri log dengan pola tertentu

Gambar 13. Tampilan Wazuh Deteksi DoS



Gambar 14. Tampilan Telegram Terima Notifikasi DoS

Hasil pengujian ini kemudian diklasifikasikan ke dalam dua aspek utama, yaitu hasil deteksi ancaman oleh sistem dan kecepatan pengiriman notifikasi melalui integrasi dengan Telegram. Rangkuman hasil dari pengujian tersebut disajikan pada Tabel 3 dan Tabel 4 berikut :

doi : 10.34010/jamika.v15i1.14190

Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume xx Nomor x Edisi xxxx 20xx
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

TABEL 3
HASIL DETEKSI ANCAMAN

Jenis Serangan	Jumlah Percobaan	Rata-rata waktu respons (s)
Sql Injection	30	5.15
Broken Access Control	30	6.85
Cryptographic Failures	30	6.00
Denial of Service	30	4.00

TABEL 4
HASIL PENGIRIMAN NOTIFIKASI

Jenis Serangan	Jumlah Percobaan	Rata-rata waktu respons (s)
Sql Injection	30	5.25
Broken Access Control	30	6.95
Cryptographic Failures	30	6.10
Denial of Service	30	4.10

Ketepatan deteksi dalam penelitian ini menunjukkan hasil yang sangat memuaskan. Seluruh ancaman yang disimulasikan berhasil diidentifikasi dengan baik oleh sistem Wazuh, yaitu sebanyak 120 dari 120 percobaan. Hasil ini mencerminkan bahwa konfigurasi *custom rules* yang diterapkan telah berjalan secara efektif dalam mengenali pola ancaman yang diuji, baik dari jenis serangan SQL Injection, Broken Access Control, Cryptographic Failure, maupun Denial of Service (DoS). Tingkat akurasi yang dicapai mengindikasikan bahwa sistem mampu memberikan deteksi yang andal dalam skenario uji coba yang dilakukan.

Selain akurasi, waktu respons sistem terhadap serangan juga menjadi indikator penting dalam evaluasi kinerja karena menunjukkan seberapa cepat sistem mampu mengenali ancaman dan memberikan notifikasi kepada administrator. Hasil pengujian menunjukkan bahwa serangan Denial of Service (DoS) memiliki waktu deteksi dan notifikasi tercepat, masing-masing 4.00 detik dan 4.10 detik, karena disimulasikan melalui skrip doslog.php yang secara berulang mencatat log mencurigakan ke dalam file wazuh_dos.log, sehingga rule dapat langsung mencocokkannya tanpa korelasi tambahan. Sebaliknya, Broken Access Control (BAC) memerlukan waktu respons paling lama, yakni 6.85 detik untuk deteksi dan 6.95 detik untuk notifikasi, karena proses deteksinya membutuhkan korelasi beberapa event dalam log akses, termasuk pengecekan sesi pengguna, status autentikasi, serta upaya akses terhadap resource terbatas, yang menambah latensi. SQL Injection terdeteksi lebih cepat, dengan waktu deteksi 5.15 detik dan notifikasi 5.25 detik, karena pola serangannya khas dan langsung terbaca melalui parameter URL yang tercatat di log. Adapun Cryptographic Failures memiliki waktu respons menengah, dengan deteksi 6.00 detik dan notifikasi 6.10 detik, karena simulasi dilakukan melalui skrip md5test.php yang menulis log khusus ke file wazuh_crypto.log untuk mendeteksi penggunaan algoritma MD5 yang lemah. Perbedaan waktu ini mencerminkan efektivitas rules yang dibuat, di mana pola log yang eksplisit seperti DoS dan SQL Injection lebih cepat dikenali, sedangkan serangan yang membutuhkan analisis konteks seperti BAC memerlukan waktu lebih lama.

Meskipun demikian, seluruh notifikasi berhasil diterima melalui Telegram dalam waktu kurang dari 10 detik setelah ancaman terdeteksi, yang menunjukkan bahwa sistem notifikasi bersifat real-time dan responsif, memberikan nilai tambah dalam keamanan informasi karena memungkinkan tim keamanan segera melakukan mitigasi terhadap potensi ancaman. Dari sisi efektivitas integrasi, sistem monitoring Wazuh yang terhubung dengan Telegram terbukti berjalan dengan sangat baik. Seluruh pesan peringatan terkirim tanpa adanya keterlambatan maupun gangguan teknis seperti error pada sistem. Hal ini menandakan bahwa mekanisme integrasi antar komponen telah terkonfigurasi dengan tepat dan dapat diandalkan dalam lingkungan operasional yang sebenarnya. Selama keseluruhan proses pengujian, sistem Wazuh juga menunjukkan performa yang stabil. Dashboard berhasil mencatat seluruh log ancaman secara akurat, termasuk waktu deteksi dan pengiriman notifikasi, tanpa adanya kehilangan data. Hal ini menguatkan kesimpulan bahwa sistem mampu beroperasi secara konsisten dan dapat diandalkan untuk kebutuhan deteksi dini terhadap ancaman keamanan siber.

Studi ini belum mengimplementasikan Wazuh di infrastruktur produksi PT. XYZ, melainkan dilakukan melalui simulasi pada lingkungan virtual terbatas. Oleh karena itu, hasil pengujian yang diperoleh hanya menggambarkan potensi performa sistem dalam skenario laboratorium. Tahap implementasi nyata akan dipertimbangkan setelah dilakukan analisis kelayakan teknis dan evaluasi kebutuhan keamanan informasi perusahaan.

IV. KESIMPULAN

Penelitian ini bertujuan untuk mengevaluasi efektivitas Wazuh sebagai solusi keamanan operasional dalam mendeteksi dan merespons ancaman siber di lingkungan perusahaan XYZ. Berdasarkan latar belakang yang menunjukkan pentingnya

doi : 10.34010/jamika.v15i1.14190

pengelolaan keamanan informasi secara real-time, Wazuh dipilih sebagai platform SIEM open-source yang dapat diandalkan dalam proses monitoring, analisis log, serta integrasi dengan media notifikasi seperti Telegram.

Metode yang digunakan adalah pendekatan eksperimental, dengan langkah sistematis mulai dari instalasi dan konfigurasi Wazuh server dan agent, implementasi, hingga simulasi empat jenis serangan siber: SQL Injection, Broken Access Control, Cryptographic Failure, dan Denial of Service (DoS). Penelitian dilakukan dalam lingkungan virtual dengan spesifikasi terbatas namun cukup untuk merepresentasikan skenario keamanan jaringan lokal. Pengujian dilakukan dengan menjalankan serangan secara terkontrol dan mencatat ketepatan deteksi, waktu respons sistem, serta kecepatan pengiriman notifikasi dari Wazuh ke Telegram.

Hasil pengujian menunjukkan bahwa Wazuh berhasil mendeteksi seluruh serangan yang disimulasikan berdasarkan custom rule yang telah dibuat. Sistem mampu mengenali pola serangan seperti '1'='1 untuk SQL Injection, log akses ilegal untuk Broken Access Control, penggunaan MD5 untuk Cryptographic Failure, serta pola trafik mencurigakan untuk DoS. Seluruh notifikasi juga terkirim secara otomatis dan cepat ke Telegram, yang menandakan integrasi komunikasi berjalan efektif. Temuan ini membuktikan bahwa Wazuh tidak hanya mampu mendeteksi ancaman secara akurat, tetapi juga merespons dengan cepat, sehingga dapat meningkatkan kesiapan dan pertahanan keamanan informasi perusahaan.

Berdasarkan hasil simulasi tersebut, integrasi Wazuh dan Telegram memiliki prospek positif sebagai sistem deteksi ancaman dan notifikasi real-time. Namun, untuk penerapan pada infrastruktur PT. XYZ, diperlukan analisis kelayakan lebih lanjut terkait kompatibilitas, skalabilitas, dan kebijakan operasional. Implementasi penuh akan dilaksanakan apabila hasil evaluasi menunjukkan bahwa solusi ini dapat berjalan efektif dalam lingkungan produksi.

DAFTAR PUSTAKA

[1] Stallings, "Keamanan Sistem Informasi," *Semin. Nas. Inform. 2008 (semnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008*, vol. 2008, no. semnasIF, pp. 379–386, 2017.

[2] I. F. S. and A. A. T. J. V. S. Sipayung, "Analysis of SIEM Implementation in Open Source SIEM Tools: Study Case Wazuh and OSSIM Alien Vault," 2021.

[3] R. A. P. Azzah Shafiyyah1*, Gigih Forda Nama2, "IMPLEMENTASIWAZUHMENGGUNAKAN METODE PPDIOODISISTEM KEAMANAN JARINGANPSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER," *J. Inform. Tek. Elektro Terap.*, vol. 12, no. 2, pp. 1–23, 2016, [Online]. Available: https://journal.eng.unila.ac.id/index.php/jitet/article/view/4074/1680

[4] M. S. H. D. A. P. Putri, "IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) UNTUK DETEKSI DAN ANALISA INSIDEN KEAMANAN PADA WEB SERVER," *Corresp. Análisis*, no. 15018, pp. 1–23, 2016, [Online]. Available: https://eprints.ums.ac.id/116796/2/Naskah Publikasi_L200190199_Muhammad Sofiyan Hadi 2.pdf

[5] M. Dehan Pratama, F. Nova, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos." [Online]. Available: http://jurnal-itsi.org

[6] A. H. Amarullah, A. J. S. Runturambi, and B. Widiawan, "Analisis Ancaman Kejahatan Siber Bagi Keamanan Nasional Pada Masa Pandemi COVID-19," *J. Kaji. Strat. Ketahanan Nas.*, vol. 4, no. 2, pp. 17–28, 2021, doi: 10.7454/jkskn.v4i2.10052.

[7] B. Haryanto and D. W. Chandra, "Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW," *J. Indones. Manaj. Inform. dan Komun.*, vol. 5, no. 1, pp. 183–192, 2024, doi: 10.35870/jimik.v5i1.447.

[8] Fitri Nova, M. D. Pratama, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 3, no. 1, pp. 1–7, 2022, doi: 10.30630/jitsi.3.1.59.

[9] F. I. Farrel, I. Mardianto, A. S. Qamar, I. Systems, S. Program, and I. S. Program, "MANAGEMENT (SIEM) WAZUH WITH ACTIVE RESPONSE BRUTE FORCE ATTACKS ON THE GT-I2TI USAKTI," vol. 4, no. 1, pp. 1–7, 2024.

[10] Stefan Stanković, Slavko Gajin, and Ranko Petrović, "A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis," *Int. Conf. IcETRAN*, vol. IX, no. 6, pp. 1–5, 2022.

[11] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif Dan R&D*. 1967. [Online]. Available: https://www.academia.edu/118903676/Metode_Penelitian Kuantitatif_Kualitatif_dan_R_and_D_Prof_Sugiono

[12] National Vulnerability Database, "CVE-2024-8465 Detail," NVD – NIST, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2024-8465. [Accessed: 23-Jun-2025].

[13] National Vulnerability Database, "CVE-2023-4018 Detail," NVD – NIST, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-4018. [Accessed: 23-Jun-2025].

[14] National Vulnerability Database, "CVE-2024-55885 Detail," NVD – NIST, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2024-55885. [Accessed: 23-Jun-2025].

[15] National Vulnerability Database, "CVE-2025-20139 Detail," NVD – NIST, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-20139. [Accessed: 23-Jun-2025].

Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume xx Nomor x Edisi xxxx 20xx
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

doi : 10.34010/jamika.v15i1.14190