Jurnal Studi Komputer dan Informatika
Vol. 9 No. 12, Desember 2025
ISSN : 21102133

DETEKSI DINI SERANGAN SIBER PADA SISTEM INFORMASI AKADEMIK BERBASIS WEB MENGGUNAKAN WAZUH

Fatullazi Abdul Haq[1], Mansur[2], Nurmi Hidayasari[3]
Politeknik Negeri Bengkalis
E-mail: fatullaziabdulhaq@gmail.com[1], mansur.polbeng82@gmail.com[2], nurmihidayasari@polbeng.ac.id[3]

Abstrak

Perkembangan teknologi informasi telah mendorong institusi pendidikan untuk memanfaatkan sistem informasi berbasis web sebagai sarana utama penyediaan layanan akademik dan penyebaran informasi. Namun, peningkatan pemanfaatan teknologi tersebut juga diiringi dengan meningkatnya ancaman serangan siber, seperti SQL Injection, Brute Force, dan Distributed Denial of Service (DDoS), yang berpotensi mengganggu ketersediaan layanan, merusak integritas data, serta menurunkan kepercayaan publik. Website Jurusan Teknik Informatika Politeknik Negeri Bengkalis sebagai pusat informasi akademik belum dilengkapi dengan sistem monitoring dan deteksi keamanan siber secara real-time, sehingga rentan terhadap serangan yang sulit terdeteksi secara dini.Penelitian ini bertujuan untuk merancang dan menerapkan sistem deteksi dini serangan siber pada sistem informasi akademik berbasis web menggunakan Wazuh sebagai Host-based Intrusion Detection System (HIDS) dan Security Information and Event Management (SIEM). Metode penelitian yang digunakan adalah pendekatan eksperimental melalui implementasi langsung sistem Wazuh pada server website jurusan. Sistem ini melakukan pemantauan dan analisis log secara real-time, dilengkapi dengan visualisasi dashboard berbasis web serta integrasi notifikasi otomatis melalui Telegram Bot. Pengujian dilakukan dengan mensimulasikan serangan siber berupa SQL Injection, Brute Force, dan DDoS sederhana untuk mengevaluasi kemampuan sistem dalam mendeteksi dan merespons ancaman. Hasil penelitian menunjukkan bahwa Wazuh mampu mendeteksi aktivitas mencurigakan secara real-time, mengklasifikasikan tingkat keparahan serangan, serta mengirimkan notifikasi secara cepat kepada administrator melalui Telegram. Implementasi sistem ini terbukti meningkatkan visibilitas keamanan, mempercepat respons terhadap insiden, dan memperkuat ketahanan keamanan website jurusan. Dengan demikian, penelitian ini diharapkan dapat menjadi referensi dalam penerapan sistem deteksi dini serangan siber berbasis open source pada lingkungan pendidikan tinggi, khususnya pada sistem informasi akademik berbasis web.

Kata Kunci — Keamanan Siber, Wazuh, IDS, SIEM, Website Akademik, Deteksi Dini Serangan Siber.

1. PENDAHULUAN

Perkembangan teknologi informasi yang begitu pesat telah memberikan berbagai kemudahan dalam penyebaran data dan informasi melalui jaringan internet. Namun, seiring kemudahan tersebut, muncul pula ancaman siber yang semakin kompleks. Laporan Data Breach Investigations Report (DBIR) 2021 dari Verizon menyebutkan bahwa terdapat lebih dari 29.000 insiden kebocoran data di seluruh dunia, dengan peningkatan signifikan pada sektor Pendidikan dan layanan publik [1]. Ancaman seperti SQL Injection, Brute Force, dan serangan Distributed denial of Service (DDoS) terus berkembang dan menyerang berbagai layanan web yang tidak memiliki sistem keamanan yang memadai [2].

Pada sistem informasi berbasis Web yang dimaksud adalah sistem informasi website Jurusan Teknik Informatika Politeknik Negeri Bengkalis yang dimana digunakan sebagai penyedia informasi akademik yang menjadi pusat komunikasi di ruang lingkup Jurusan Teknik Informatika. Dalam hal ini, website Teknik Informatika Politeknik Negeri Bengkalis

Vol. 9 No. 12, Desember 2025
ISSN : 21102133

berperan dalam menunjang kegiatan Pendidikan dan layanan informasi. Namun, pada website Teknik Informatika belum adanya sistem monitoring keamanan siber secara real-time yang membuat website teknik informatika berisiko menjadi target serangan siber kapan saja.

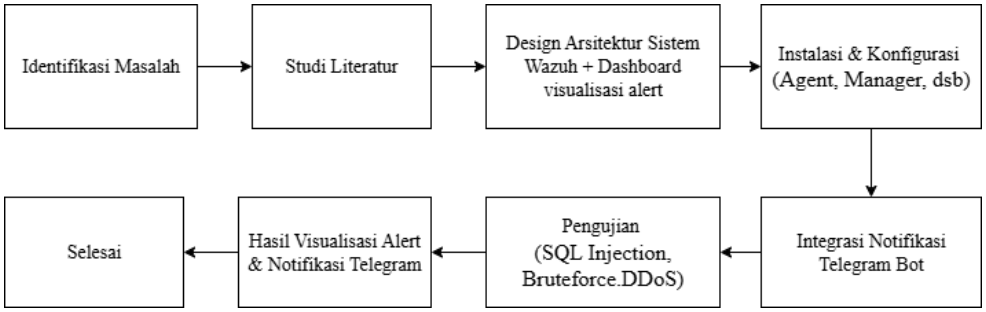
Sistem deteksi dini serangan siber merupakan pendekatan yang masih digunakan dalam dunia keamanan siber. Salah satu solusi opensource yang digunakan adalah Wazuh, yang dimana merupakan pengembangan dari OSSEC dengan kemampuan sebagai Host-based intrusion Detection System (HIDS) dan SIEM (Security information and Event Management). Wazuh dapat memantau log sistem secara real time untuk mendeteksi aktivitas yang mencurigakan, dan memberikan peringatan kepada administrator [3]. Wazuh juga mendukung integrasi dengan telegram atau kustom visualisasi dashboard sistem SIEM, yang menjadikannya fleksibel dan efisien untuk di implementasikan pada institusi dengan sumber daya terbatas.

Implementasi sistem deteksi dini menggunakan wazuh diharapkan mampu memberikan perlindungan terhadap website Teknik Informatika dari berbagai ancaman serangan siber. Melalui pengumpulan log, analisis aktivitas tidak wajar, dan pemberian notifikasi secara real time kepada administrator sehingga dapat segera merespons ancaman yang muncul. Hal ini tidak hanya membantu dalam pencegahan insiden siber, tetapi juga meningkatkan kesadaran keamanan siber dilingkungan kampus secara menyeluruh [1].

Dengan adanya sistem monitoring keamanan ini, diharapkan website jurusan dapat mengidentifikasi berbagai potensi ancaman siber yang dapat mengganggu ketersediaan informasi dan kepercayaan publik terhadap institusi. Penelitian ini menjadi langkah awal untuk meningkatkan ketahanan digital di sektor Pendidikan, khususnya di lingkungan Jurusan Teknik Informatika Politeknik Negeri Bengkalis.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental dengan metode implementasi langsung dan pengujian sistem keamanan pada website Jurusan Teknik Informatika Politeknik Negeri Bengkalis menggunakan Wazuh. Pendekatan ini dipilih untuk mengukur secara objektif kemampuan Wazuh dalam mendeteksi dan merespons serangan siber. Penelitian ini berfokus pada penerapan sistem deteksi dini serangan siber. Proses penelitian ini terdapat beberapa tahapan yang di lakukan, antara lain:



Gambar 1. Alur Penelitian yang akan dilakukan.

Vol. 9 No. 12, Desember 2025
ISSN : 21102133

3. HASIL DAN PEMBAHASAN

Eksperimen

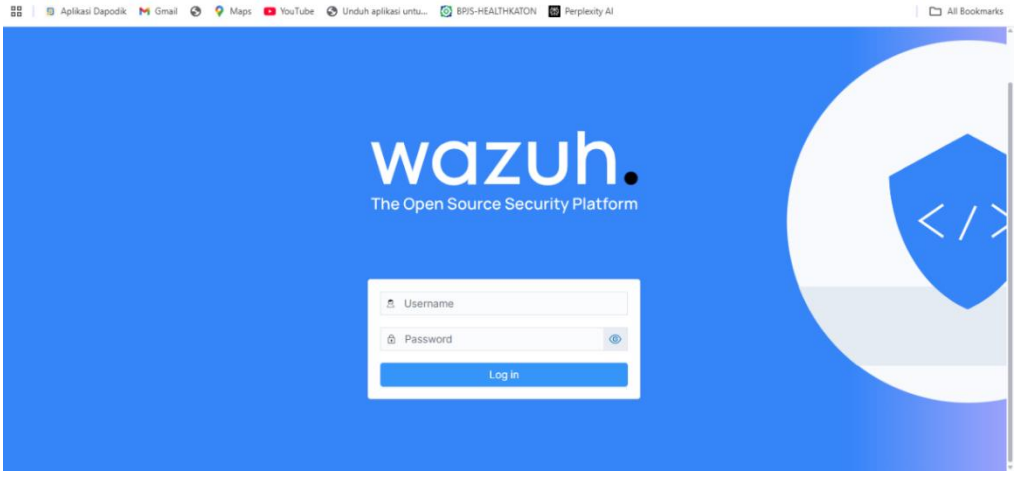
pada tahap ini merupakan bagian utama dari penelitian yang membahas hasil implementasi dan pengujian sistem deteksi dini serangan siber menggunakan wazuh yang bertujuan untuk menguji kemampuan sistem wazuh dalam mendeteksi berbagai jenis serangan siber pada website Jurusan Teknik Informatika Politeknik Negeri Bengkalis. Pengujian dilakukan pada lingkungan server vps berbasis linux ubuntu yang telah terpasang Wazuh manager dan Wazuh Agent, serta terintegrasi dengan dashboard kustom dan notifikasi Telegram. Sebelum melakukan pengujian, peneliti memastikan seluruh komponen sistem berada dalam kondisi siap pakai. Wazuh Manager dan Wazuh Agent telah terinstal dan terhubung dengan baik. Agent berjalan pada sistem operasi Ubuntu 22.04 LTS dan secara konsisten mengirimkan log aktivitas ke Wazuh Manager.

Implementasi Wazuh Manager dan Agent

Implementasi Wazuh merupakan tahap awal dalam proses eksperimen sistem deteksi dini serangan siber pada penelitian ini. Tahap awal eksperimen implementasi Wazuh diawali dengan proses instalasi layanan utama Wazuh beserta komponen pendukung lainnya, sehingga sistem dapat berjalan secara optimal setelah instalasi selesai. Tahap ini bertujuan untuk memastikan bahwa seluruh komponen utama sistem keamanan telah terpasang dengan terkonfigurasi dengan baik.

A. Wazuh Manager

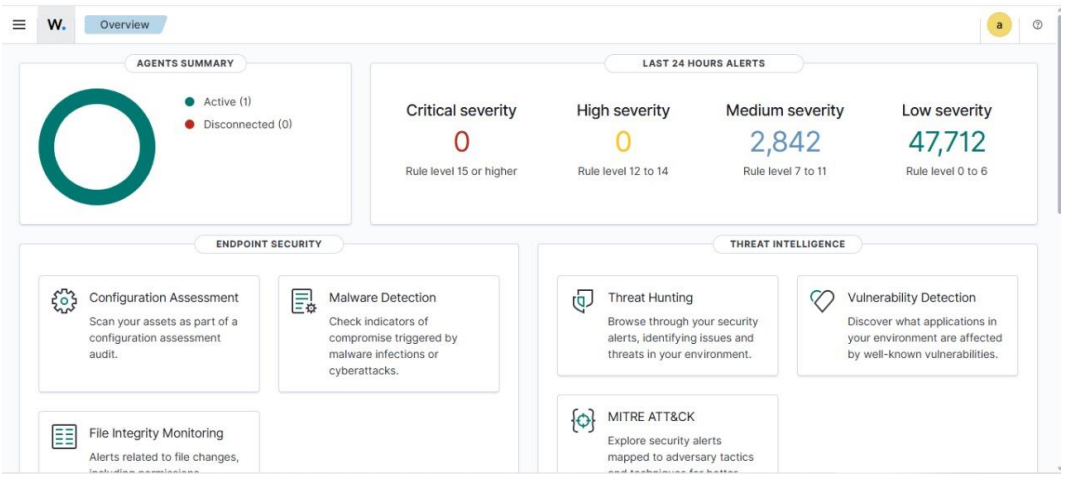
Wazuh Manager merupakan komponen utama dalam sistem deteksi dini serangan siber yang berfungsi sebagai pusat pengelolaan, analisis, dan korelasi data keamanan yang dikirimkan oleh Wazuh Agent. Pada penelitian ini, Wazuh diinstal pada server vps berbasis sistem operasi linux ubuntu dan dikonfigurasi untuk menerima serta memproses data log dari agent yang terpasang pada server website Jurusan Teknik Informatika



Gambar 2. Tampilan Wazuh

Dashboard wazuh ini merupakan titik awal menampilkan antarmuka utama dashboard Wazuh Manager yang berfungsi sebagai pusat pemantauan dan pengelolaan keamanan sistem.

Vol. 9 No. 12, Desember 2025
ISSN : 21102133

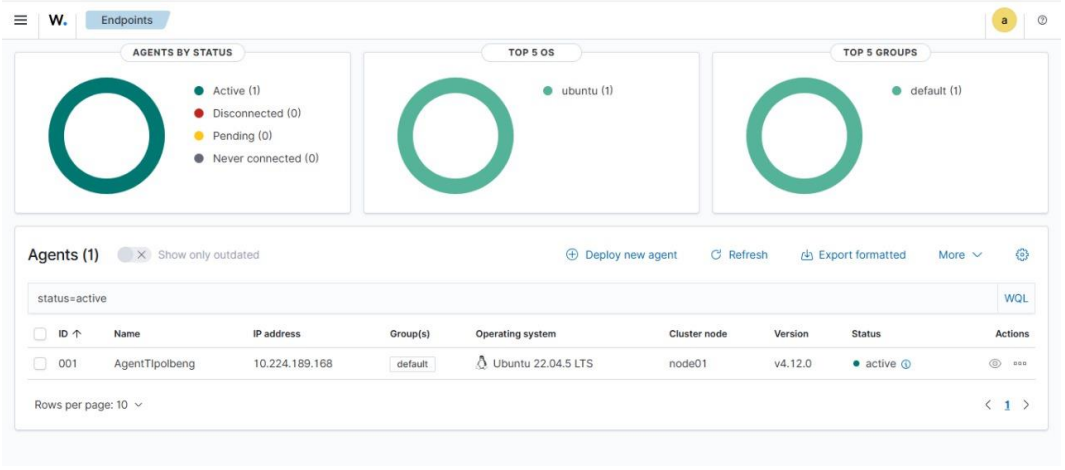


Gambar 3. Wazuh Manager

Tampilan wazuh manager menunjukan kondisi yang ditampilkan sudah berjalan dengan status aktif dengan meliputi informasi yang ditampilkan dengan status layanan utama Wazuh, penggunaan sumber daya sistem, serta kemampuan manager dalam menerima dan memproses data log dari agent sebagai pusat analisis keamanan.

B. Wazuh Agent

Wazuh Agent merupakan komponen sistem yang berfungsi sebagai pengumpul data log dan aktivitas pada server yang dimonitoring. Pada penelitian ini, agent diinstal pada server website Jurusan Teknik Informatika Politeknik Negeri Bengkalis yang menjadi objek penelitian. Agent bertugas mencatat aktivitas sistem yang berjalan pada server.



Gambar 4. Integrasi Wazuh Manager ke agent

Proses integrasi antara Wazuh agent dan Wazuh manager yang ditampilkan pada menu endpoints terlihat Agent berada dalam status aktif, yang menandakan proses instalasi, pendaftaran, dan koneksi agent ke manager telah berhasil dilakukan. Hasil ini menunjukan bahwa proses instalasi dan pendaftaran agent telah berjalan di wazuh manager. Agent mengirimkan seluruh aktivitas sistem ke Wazuh Manager, sehingga setiap event yang terjadi pada server dapat dimonitor secara real-time.

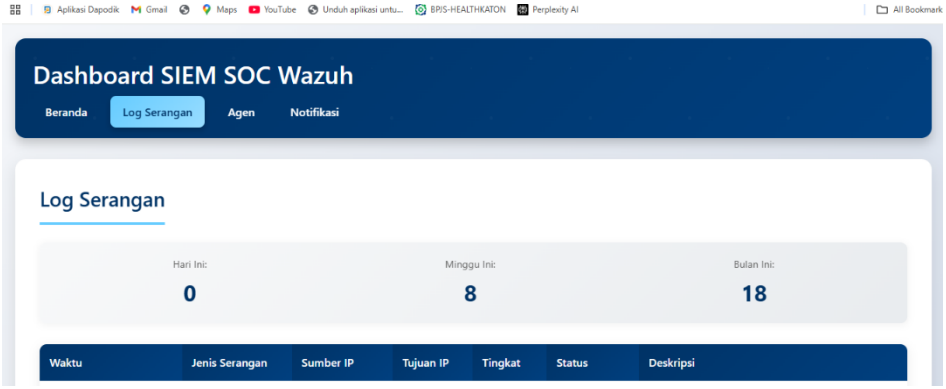
Vol. 9 No. 12, Desember 2025
ISSN : 21102133

Gambar 5. Website Teknik Informatika

Menampilkan website Jurusan Teknik Informatika Politeknik Negeri Bengkalis yang digunakan sebagai objek penelitian. Website ini menjadi target pengujian dalam eksperimen deteksi serangan siber, yang mana seluruh aktivitas akses permintaan HTTP, serta interkasi pengguna dipantau oleh Wazuh agent. Website ini merepresentasikan sistem informasi berbasis web yang umum digunakan di lingkungan kampus dan memiliki potensi kerentanan terhadap serangan siber.

Eksperimen Dashboard Kustom SIEM

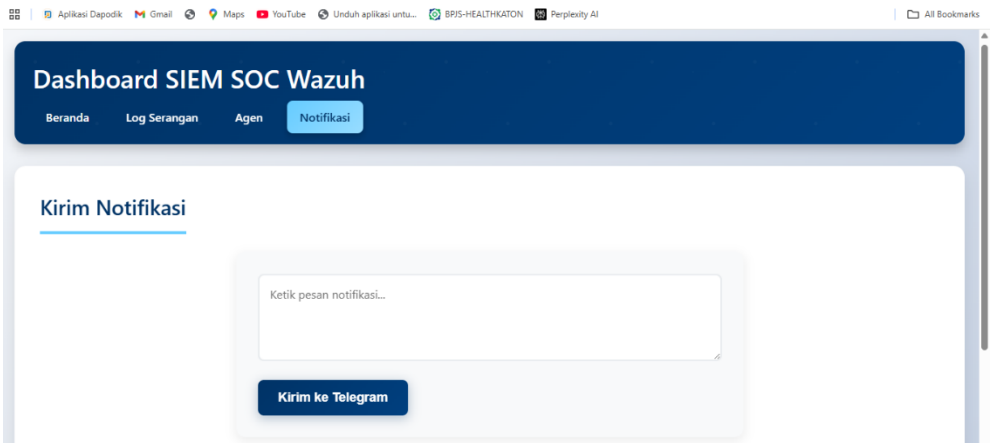
Eksperimen dashboard kustom dilakukan untuk menguji kemampuan sistem dalam menyajikan hasil deteksi keamanan secara visual dan terstruktur. Dashboard ini dirancang sebagai antarmuka pemantauan yang menampilkan data hasil analisis wazuh sehingga memudahkan administrator dalam memahami kondisi keamanan sistem secara menyeluruh.



Gambar 6. Dashboard Kustom SIEM

Hasil menunjukan bahwa dashboard kustom SIEM mampu menampilkan data keamanan secara real time dengan alert yang dihasilkan. Setiap serangan yang terdeteksi langsung terpantau pada visualisasi dashboard tanpa adanya keterlambatan yang signifikan.

Vol. 9 No. 12, Desember 2025
ISSN : 21102133

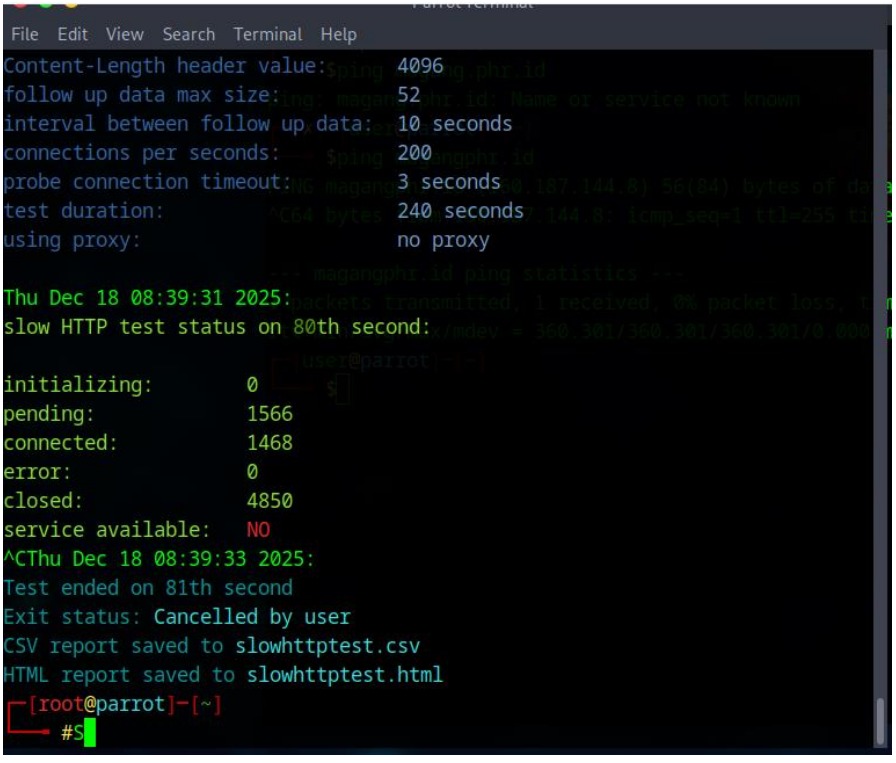


Gambar 7. Dashboard kustom SIEM

Dashboard kustom SIEM ini juga dirancang untuk mempermudah administrator dalam memantau kondisi keamanan pada sistem secara cepat dan terstruktur tanpa harus mengakses dashboard bawaan Wazuh secara langsung. Dashboard ini juga telah diintegrasi dengan Telegram Bot.

Eksperimen Deteksi Serangan DDoS

Eksperimen serangan pertama adalah dengan melakukan serangan Distributed Denial of service (DDoS) dengan mengamati respons sistem terhadap lonjakan trafik normal. Tujuan pengujian ini adalah untuk melihat kemampuan sistem dalam mendeteksi lonjakan trafik yang tidak normal. Setelah serangan dijalankan, Wazuh menghasilkan alert yang ditampilkan pada dashboard dan dikirimkan ke Telegram. Serangan DDoS dilakukan menggunakan tools Slowhttptest



Gambar 8. Serangan DDoS

Serangan DDoS menggunakan tools slowhttptest dilakukan untuk melihat aktivitas respon dari wazuh apakah bisa melakukan deteksi atau tidak dalam memantau log grafik

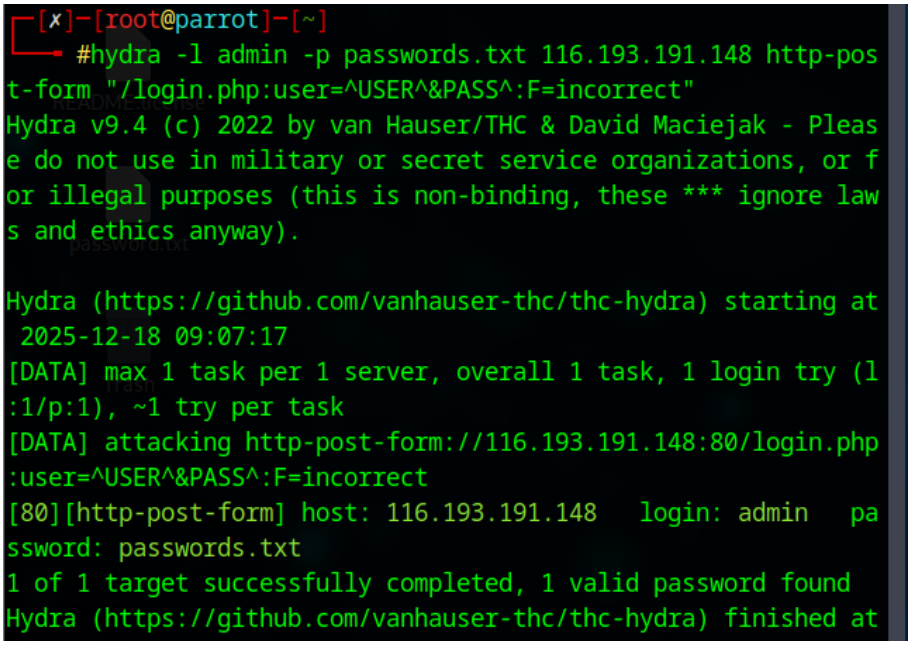
Vol. 9 No. 12, Desember 2025
ISSN : 21102133

Gambar 9. Hasil Deteksi Serangan DDoS

Hasil eksperimen menunjukan telah berhasil mendeteksi aktivitas serangan DDoS. Hasil ini menunjukan bahwa sistem berhasil mengenali adanya aktivitas jaringan yang tidak biasa dan mencatatnya sebagai anomali.Hasil eksperimen serangan DDoS yang secara otomatis dikirimkan ke Telegram administrator. Hal ini membuktikan bahwa sistem mampu mengenali pola serangan DDoS pada tahap awal.

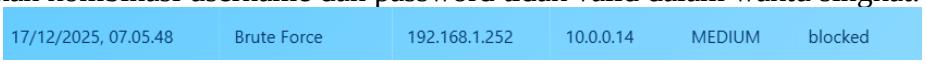
Eksperimen Deteksi Serangan Brute Force

Eksperimen deteksi serangan bruteforce dilakukan untuk menguji kemampuan sistem dalam mengenali percobaan akses tidak sah pada fitur autentikasi website. Pola serangan ini bertujuan untuk meniru upaya penyerang dalam menebak kredensial pengguna secara sistematis.



Gambar 10. Serangan Bruteforce

Serangan bruteforce dilakukan dengan melakukan percobaan login secara berulang menggunakan kombinasi username dan password tidak valid dalam waktu singkat.



Gambar 11. Hasil Deteksi Bruteforce

Hasil eksperimen menunjukan bahwa sistem berhasil mendeteksi serangan bruteforce dengan mencatat aktivitas percobaan login gagal pada server yang terjadi secara berulang. Data log yang tercatat pada sistem secara otomatis langsung dikirimkan ke notifikasi Telegram bot.

Eksperimen Serangan SQL Injection

Eksperimen deteksi serangan SQL Injection dilakukan untuk menguji kemampuan sistem dalam mengenali upaya manipulasi basis data pada aplikasi web. Tujuan dari pengujian ekperimen ini adalah untuk mengetahui apakah wazuh mampu mendeteksi pola akses yang mencurigakan pada aplikasi.

Vol. 9 No. 12, Desember 2025
ISSN : 21102133

Gambar 12. Serangan SQl Injection

Serangan SQL Injection dilakukan dengan menyisipkan query berbahaya pada parameter input aplikasi menggunakan tools pengujian keamanan web

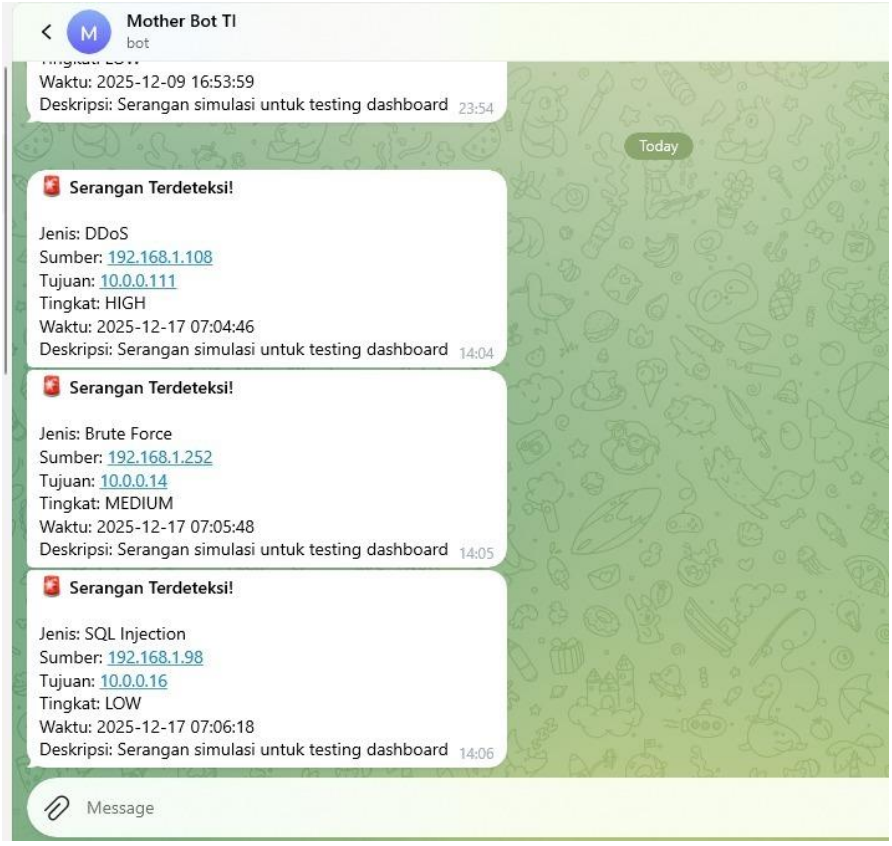
Gambar 13. Hasil Deteksi Serangan SQL Injection

Hasil pengujian menunjukkan bahwa sistem berhasil mengenali aktivitas mencurigakn dan menghasilkan alert. Selama eksperimen berlangsung, agent memantau log aplikasi web dan mencatat adanya permintaan HTTP yang mengandung pola query tidak normal.

Eksperimen Integrasi Notifikasi Telegram

Bagian dari sistem deteksi dini, peneliti menguji pengiriman notifikasi Telegram menggunakan bot yang telah dikonfigurasi dengan dashboard. Setiap alert yang terdeteksi akan langsung dikirimkan secara otomatis ke Telegram dalam format pesan yang informatif sesuai dengan alert yang terdeteksi.

Vol. 9 No. 12, Desember 2025
ISSN : 21102133



Gambar 14. Notifikasi Telegram

Hasil pengujian menunjukan bahwa notifikasi diterima secara otomatis dengan waktu yang sangat singkat setelah serangan terdeteksi. Informasi yang disampaikan mencakup jenis serangan, IP Sumber, tingkat keparahan, serta waktu kejadian

Analisis

Analisis ini bertujuan untuk mengevaluasi kinerja sistem dalam mendeteksi berbagai jenis serangan siber dengan menilai efektivitas visualisasi dashboard SIEM, dalam mengkaji peran notifikasi Telegram dalam mendukung proses peringatan dini. Hasil analisis dilakukan dengan mengaitkan temuan eksperimen dengan tujuan penelitian, yaitu membangun sistem deteksi dini yang mampu memberikan peringatan awal terhadap potensi serangan siber pada website Jurusan Teknik informatika Politeknik Negeri Bengkalis.

Analisis Kinerja Deteksi Wazuh

Berdasarkan hasil eksperimen yang telah dilakukan, Wazuh menunjukan Kinerja yang baik dalam mendeteksi berbagai Jenis serangan Siber. Hal ini terlihat dari keberhasilan sistem dalam mendeteksi serangan DDoS, bruteforce, dan SQl Injection yang disimulasikan selama pengujian. Kemampuan wazuh dalam mendeteksi serangan didukung mekanisme analisis log dan rule engine yang bekerja secara real-time. Setiap aktivitas yang mencurigakan dianalisis berdasarkan pola tertentu dan kemudian diklasifikasikan ke dalam tingkat keparahan yang sesuai. Alert yang dihasilkan berada pada kerentanan high, medium, dan low yang mengindikasikan bahwa serangan yang diuji masih berada pada tahap awal dan belum menimbulkan dampak signifikan terhadap sistem.

Analisis Visualisasi Dashboard SIEM

Dashboard SIEM berperan penting dalam menyajikan hasil deteksi Wazuh dalam bentuk visual yang mudah dipahami. Berdasarkan hasil pengamatan, Dashboard mampu menampilkan informasi penting seperti jumlah alert berdasarkan tingkat keparahan dan ringkasan aktivitas keamanan dalam periode tertentu. Visualisasi ini membantu administrator dalam memahami kondisi keamanan sistem secara keseluruhan dalam menganalisa statistik

Vol. 9 No. 12, Desember 2025
ISSN : 21102133

yang ditampilkan.

Dengan adanya dashboard SIEM, proses monitoring menjadi lebih efisien dan terstruktur sehingga administrator dapat dengan cepat mengidentifikasi potensi ancaman dan menentukan prioritas penanganan berdasarkan tingkat risikonya.

Analisis Efektivitas Notifikasi Telegram

Integrasi notifikasi Telegram memberikan kontribusi terhadap efektivitas sistem deteksi dini yang dibangun. Berdasarkan hasil eksperimen, setiap alert yang terdeteksi berhasil dikirimkan ke Telegram dalam waktu yang sangat singkat. Pesan notifikasi yang dikirimkan memuat informasi penting seperti jenis serangan, alamat IP sumber dan tujuan, tingkat keparahan, serta waktu kejadian. Informasi ini memberikan gambaran awal mengenai kondisi keamanan sistem tanpa harus membuka dashboard SIEM. Notifikasi Telegram membantu administrator dalam memberi informasi terkini serangan yang terjadi pada sistem secara real-time dan dapat segera melakukan respons lebih awal, sehingga potensi kerusakan pada sistem dapat diminimalkan.

Analisis Keterbatasan Sistem

Meskipun sistem deteksi dini yang dibangun telah berjalan dengan baik, penelitian ini masih memiliki beberapa keterbatasan. Salah satu keterbatasan utama adalah sistem hanya berfungsi sebagai alat deteksi dan notifikasi, belum dilengkapi dengan mekanisme pencegahan otomatis seperti pemblokiran alamat IP penyerang atau penghentian proses berbahaya secara langsung. Selain itu, pengujian serangan dilakukan dalam skala terbatas. Hal ini menyebabkan hasil eksperimen belum sepenuhnya merepsentasikan kondisi serangan siber dalam skala besar atau serangan yang lebih kompleks. Keterbatasan ini menjadi dasar bagi pengembangan sistem pada penelitian selanjutnya, baik dengan mengaktifkan fitur active response pada Wazuh maupun memperluas skenario pengujian.

4. KESIMPULAN

Berdasarkan proses implementasi, pengujian, serta analisis yang telah dilakukan pada penelitian ini, dapat disimpulkan bahwa sistem deteksi dini serangan siber berbasis Wazuh berhasil diterapkan pada website Jurusan Teknik Informatika Politeknik Negeri Bengkalis. Seluruh komponen utama yang digunakan, mulai dari Wazuh manager, Wazuh Agent, dashboard SIEM, hingga notifikasi Telegram, dapat bekerja secara terintegrasi dan menunjukan kestabilan selama proses pengujian berlangsung. Hasil eksperimen menunjukan bahwa Wazuh mampu mendeteksi beberapa jenis serangan siber pada sistem berbasis web, seperti serangan Distributed Denial of Service (DDoS), bruteforce, dan SQL Injection. Sebagian besar alert yang dihasilkan berada pada kategori high, medium, dan low. Kondisi ini menunjukan sistem memiliki sensitivitas yang baik terhadap aktivitas mencurigakan dan mampu memberikan peringatan sejak tahap awal serangan. Hal tersebut sejalan dengan tujuan utama penelitian ini, yaitu membangun sistem deteksi dini yang dapat membantu administator dalam mengenali potensi ancaman sebelum menimbulkan dampak yag lebih serius. Selain itu, dashboard SIEM juga memberikan kontribusi signifikan dalam mendukung sistem deteksi dini. Informasi serangan dapat diterima secara real-time oleh administrator, sehingga respons awal terhadap ancaman dapat diantisipasi dengan lebih cepat. Secara keseluruhan, penerapan Wazuh dalam penelitian ini dinilai efektif dan sesuai digunakan pada lingkungan kampus, khususnya pada sistem informasi berbasis web yang memiliki keterbatasan sumber daya dalam pengelolaan keamanan siber.

Saran

Berdasarkan hasil penelitian dan keterbatasan yang ditemukan selama proses eksperimen, peneliti memberikan beberapa saran yang dapat dijadikan bahan pertimbangan untuk pengembangan selanjutnya, antara lain:

1. Pengembangan sistem dapat dilakukan dengan mengaktifkan fitur active response pada Wazuh, sehingga sistem tidak hanya memberikan notifikasi tetapi juga dapat melakukan tindakan pencegahan otomatis seperti pemblokiran alamat IP penyerang.
2. Integrasi dengan layanan intelijen ancaman eksternal seperti database malware atau sistem threat intelligence yang dapat dipertimbangkan untuk meningkatkan akurasi dan efektivitas deteksi serangan

DAFTAR PUSTAKA

A. Firdaus, H. Sajati, and Y. Indrianingsih, "Penerapan Hids (Host Intrusion Detection System) Dalam Membangun Konfigurasi Firewall Secara Dinamik," Compiler, vol. 2, no. 2, pp. 53–58, 2013, doi: 10.28989/compiler.v2i2.46.

M. R. Kamal and M. A. Setiawan, "Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII," Automata, vol. 2, no. 2, pp. 1–6, 2021.

H. Khotimah, F. Bimantoro, and R. S. Kabanga, "Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat," J. Begawe Teknol. Inf., vol. 3, no. 2, pp. 213–219, 2022, doi: 10.29303/jbegati.v3i2.752.

Y. Daeng, J. Levin, M. Razzaq Prayudha, N. Putri Ramadhani, S. Imanuel, and A. Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng, "Analisis Penerapan Sistem Keamanan Siber TerhadapKejahatan Siber Di Indonesia," J. Soc. Sci. Res., vol. 3, no. 6, pp. 1135–1145, 2023.

D. A. S. Ilhami, "Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur," J. Sains, Nalar, dan Apl. Teknol. Inf., vol. 2, no. 1, pp. 51–60, 2022, doi: 10.20885/snati.v2i1.19.

A. Tedyyana, O. Ghazali, and O. W. Purbo, "Machine learning for network defense: automated DDoS detection with telegram notification integration," Indones. J. Electr. Eng. Comput. Sci., vol. 34, no. 2, pp. 1102–1109, 2024, doi: 10.11591/ijeecs.v34.i2.pp1102-1109.

N. Shafira Suryawatie Yomo, A. Zafrullah Mardiansyah, and I. Wayan Agus Arimbawa, "Deteksi Serangan SQL Injection Menggunakan Security Information and Event Management (SIEM) Wazuh (Sudi Kasus: Sistem Informasi Akademik Universitas Mataram) Detection of SQL Injection Attacks Using Security Information and Event Management (SIEM) Wazuh (," Univ. Mataram, pp. 1–9, 2022.

D. Luthfah, "Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law)," terAs Law Rev. J. Huk. Humanit. dan HAM, vol. 3, no. 1, pp. 11–22, 2021, doi: 10.25105/teras-lrev.v3i1.10742.

R. Hendra Wicaksana, A. Imam Munandar, P. L. Samputra, J. Salemba, R. No, and J. Indonesia, "Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic," J. Ilmu Pengetah. dan Teknol. Komun., vol. 22, no. 2, pp. 143–158, 2020, [Online]. Available: http://dx.doi.org/10.33164/iptekkom.22.2.2020.143-158

E. Dwi Setiawan and M. Raharjo, "Jurnal Informatika Terpadu," J. Inform. Terpadu, vol. 9, no. 1, pp. 34–39, 2023, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

A. Alhafidz and D. Haryanto, "Sistem Operasi Monitoring Server Menggunakan WAZUH," vol. 3, pp. 11513–11517, 2024.

M. A. Fahrudi and I. M. Suartana, "Integrasi End-point Security Berbasis Agent dan Bot Messenger untuk Deteksi dan Monitoring Serangan pada Web Server secara Real-time," J. Informatics Comput. Sci., vol. 04, pp. 275–282, 2023, doi: 10.26740/jinacs.v4n03.p275-282.

E. D. Madyatmadja, L. Kusumawati, S. P. Jamil, W. Kusumawardhana, S. Informasi, and U. B. Nusantara, "Infotech: journal of technology information," Raden Ario Damar, vol. 7, no. 1, pp. 55–62, 2021.

A. Hidayat, "Implementasi Intrusion Detection System Dalam Upaya Pencegahan Cyber Attack," vol. 10, no. 4, pp. 924–930, 2024.

M. R. Firmansyah, I. Kurniasari, and H. Kurniadi, "Implementasi SIEM Wazuh pada Server Rumah Sakit Islam Madinah Ngunut," vol. 8, no. 2, pp. 75–80, 2024.

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.

Y. Mulia, “IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER,” vol. 12, no. 2, pp. 1–23, 2016.

Gilang Patoni, Yusuf Muhyidin, and Dayan Singasatia, “Implementasi Wazuh Pada Ubuntu Server Untuk Mendeteksi Serangan Brute Force Hydra,” Merkurius J. Ris. Sist. Inf. dan Tek. Inform., vol. 2, no. 5, pp. 145–156, 2024, doi: 10.61132/merkurius.v2i5.290.

M. Daryuni, “Sistem Informasi Monitoring Data Persatuan Guru Republik Indonesia Kecamatan Bengkalis Menggunakan Metode Extreme Programming dan Framework Codeigniter,” vol. 12, no. x, pp. 46–58, 2021.