JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 03, N0. 01, Tahun 2025, Hal. 103 - 125, ISSN: 3031-9498 (Online)

Implementasi Keamanan Server Aplikasi *E-Raport* SMK Negeri 1 Sinjai Menggunakan Wazuh

Mutawadiyah Mikyal[1], Mustari Lamada[2], Abdul Wahid[3]
[123]Universitas Negeri Makasssar
Email: mutawadiyahmikyal02@gmail.com

Article Info

Article history:

Received September 25, 2024
Revised October 06, 2024
Accepted October 13, 2024

Keywords:

Wazuh, server security, sysn flood slowris, low orbit ion cannon, monitoring server, e-raport.

ABSTRACT

Monitoring of the SYN flood Slowloris attack with 100,000 packets detected in /var/sys showed 52 events (9,175 bytes) between 09:53:57 and 10:06:58. Additionally, monitoring of 500,000 sockets by the Wazuh agent recorded 165 suspicious events with a total of 27,049 bytes. The monitoring of the Low Orbit Ion Cannon attack, sending 100,000 sockets, showed activity between 11:59:52 and 12:10:53, with 50 events (9,197 bytes). The attack using 300,000 sockets recorded between 11:59:52 and 12:22:53 showed 62 events (11,451 bytes), causing the E-Raport server to buffer, though connectivity remained stable. The attack with 500,000 sockets caused the server to time out, with 97 events (17,766 bytes). Overall analysis of the Slowloris attack with socket configurations of 100,000 and 500,000 showed that 100,000 sockets did not bring the server down, while 500,000 sockets with a payload of 120 bytes per packet and 64 TCP resulted in 100% packet loss. In the LOIC attack targeting IP 10.10.12.5, the researcher aimed at port 80 with 500,000 sockets per thread using the HTTP method, with monitoring times of 11:59:33 for 100,000 sockets, 11:59:52 for 100,000 sockets, 11:59:52 for 300,000 sockets, and 12:27:53 for 500,000 sockets.

Article Info

Article history:

Received September 25, 2024
Revised October 06, 2024
Accepted October 13, 2024

Keywords:

Wazuh, server security, syn flood slowris, low orbit ion cannon, monitoring server, e-raport

ABSTRACT

Pemantauan serangan SYN flood Slowloris dengan 100.000 packet terdeteksi di /var/sys, menunjukkan 52 event (9.175 bytes) antara 09:53:57 hingga 10:06:58. Selain itu, pemantauan 500.000 socket oleh Wazuh agent mencatat 165 event mencurigakan dengan ukuran 27.049 bytes. Hasil pemantauan pada serangan low orbit ion cannon mengirimkan 100.000 socket terlihat ada aktivitas dengan rentang waktu 11:59:52 hingga 12:10:53 terdapat 50 event dengan byte 9197 serangan socket 300.000 tercatat rentang waktu 11:59:52 hingga 12:22:53 tercatat sebanyak 62 event dengan total 11.451 byte menyebabkan server E-Raport menjadi buffering tetapi konektifitas tetap lancar dan serangan socket 500.000. socket menyebabkan server menjadi timed out terlihat adanya 97 event dengan total data sebesar 17.766 byte. Analisis hasil keseluruhan slowris dengan menerapkan beberapa socket yaitu 100.000, 500.000 pada socket 100.000 tidak menyebabkan server down ketika socket dikonfigurasi mengirimkan 500.000 paket dengan payload sebesar 120 byte per paket dengan tcp sebesar 64 mengindikasikan 100% packet loss. Pada serangan LOIC sebuah target, dalam hal ip 10.10.12.5 dalam konfigurasi ini, peneliti menargetkan port 80 dengan 500.000 socket per thread menggunakan metode http dengan monitoring time 11:59:33 socket 100.000, 11:59:52 socket 300.000 dan 12:2753 socket 500.000.

Corresponding Author:

Nama penulis: Mutawadiyahmikyal
Universitas Negeri Makassar
Email: mutawadiyahmikyal02@gmail.com

Pendahuluan

Perkembangan teknologi saat ini sudah sangat cepat dan pesat. Perkembangan teknologi diiringi dengan adanya perkembangan internet. Dengan perkembangan internet manusia mendapatkan informasi yang diinginkan dengan cepat dan mudah. Pemakaian teknologi informasi sudah berkembang dalam bidang pendidikan. Teknologi informasi menjadi salah satu aspek yang sangat mempengaruhi kehidupan sehari-hari[1].

Ada berbagai jenis sistem teknologi informasi seperti internet yang telah memungkinkan kita mengakses berbagai informasi dengan lebih mudah dan efisien. Dengan perkembangan internet manusia mendapatkan informasi yang diinginkan dengan cepat. Perkembangan teknologi informasi seperti ini terutama pada pengguna komputer yang meningkat dapat berdampak pada perkembangan dalam pengolahan data, dimana data akan dikirim dari tempat ke tempat melalui sarana telekomunikasi [2]. Seiring dengan kemajuan teknologi, muncul berbagai ancaman dan serangan keamanan dalam server aplikasi E-Raport. Sistem operasi yang terinfeksi perangkat lunak berbahaya dapat disusupi dan seorang penyerang akan menyerang sistem jaringan dengan maksud guna mengalahkan layanan keamanan pada fasilitas jaringan tersebut membuatnya lebih rentan terhadap penyusup, virus, dan bahkan data penting yang dapat dicuri [3].

Wazuh adalah platform keamanan yang terfokus pada deteksi ancaman dan pemantauan keamanan. Fitur utamanya adalah mampu memantau dari berbagai sumber termasuk server E-Raport untuk mendeteksi aktivitas mencurigakan atau perubahan konfigurasi yang tidak diinginkan dan dapat membantu mendeteksi serangan atau ancaman terhadap server. Wazuh akan memberikan peringatan jika ada perubahan atau aktivitas mencurigakan pada file. Dimana Wazuh akan mengumpulkan dari sumber-sumber khusus yang relevan dengan keamanan server E-Raport seperti aplikasi, sistem operasi, dan keamanan serta menganalisis 4 perilaku mencurigakan, tanda-tanda serangan atau aktifitas keamanan lainnya seperti serangan DoS (Denial of Service) [4].

Server merupakan kombinasi dari perangkat keras dan perangkat lunak yang dirancang untuk menyediakan layanan untuk client pada sebuah jaringan komputer[5]. Dalam konteks komputerisasi, server adalah gabungan dari perangkat keras dan perangkat lunak yang dirancang untuk memberikan layanan kepada client di jaringan komputer. Server menggunakan prosesor yang dapat diukur (scalable) dan memanfaatkan kapasitas RAM yang besar. Selain itu, server dilengkapi dengan sistem operasi khusus yang dikenal sebagai sistem operasi jaringan. Perangkat ini juga berfungsi untuk menjalankan perangkat lunak administratif yang mengendalikan akses terhadap jaringan dan sumber daya yang ada di dalamnya [6].Seperti yang dilakukan oleh Idrus dkk [7] yaitu *instrusion detection system* untuk keamanan *cloud* dengan

menggunakan sucirata untuk mencegah ancaman informasi yang terkait dengan komputasi awan

Distributed of Service (DDoS) merupakan salah satu serangan terhadap situs, jaringan, router dan server yang sangat sering terjadi termasuk pada router mikrotik. Serangan DDoS bertujuan untuk membuat jaringan router down sehingga tidak mampu melayani permintaan user yang memiliki hak akses yang sah [8]. Serangan DoS mirip dengan serangan DDoS. Secara garis besar, serangan DoS dibagi menjadi dua kelas yaitu *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS). Serangan DoS dilakukan oleh penyerang tunggal dan tujuannya adalah membuat aplikasi, layanan, atau mesin tidak tersedia. Hal ini dilakukan dengan cara membanjiri lebih banyak permintaan daripada yang dapat ditangani atau menggunakan sumber daya memproses sedemikian rupa sehingga permintaan yang sah atau legal tidak dapat ditangani [8].

Seperti yang dilakukan oleh nova dkk [9] yaitu wazuh sebagai *event management* dan deteksi celah keamananan pada server dari serangan Dos penelitian tersebut menggunakan salah satu aplikasi yaitu suricata yang di dalamnya terdapat metode IDS (*Instrusion Detection System)* yang berfungsi sebagai pendeteksi *attacker*.

Penelitian lain oleh Harahap dkk[10] yaitu *instrusion detection system and anomaly* menggunakan wazuh pada Universitas Muhammadiyah Palembang. Penelitian ini memanfaatkan firewall untuk keamanan sistem. Penggunaan firewall pada sistem tidak dapat memantau dan menganalisa traffic yang berada di dalam sebuah jaringan dan tidak memberikan peringatan ketika terjadi sebuah serangan. Adapun anomaly bisa saja bertujuan untuk menyerang, merusak, dan mengambil data atau informasi pada server.

Selanjutnya penelitian dari Rahmatullah dkk [11] tentang implmentasi SIEM dan IDS dalam monitoring terhadap ancaman serangan pada web server mengatakan bahwa ancaman serangan terhadap web server Dalam penelitian ini, cara mengatasi permasalahan tersebut melalui sistem informasi keamanan SIEM dengan platform Wazuh/Teler sebagai IDS yang akan diinstal pada web server untuk memvisualisasikan dan mendeteksi adanya ancaman pada lalu lintas jaringan dan metode yang digunakan dalam penelitian ini menggunakan Wazuh dan teler.

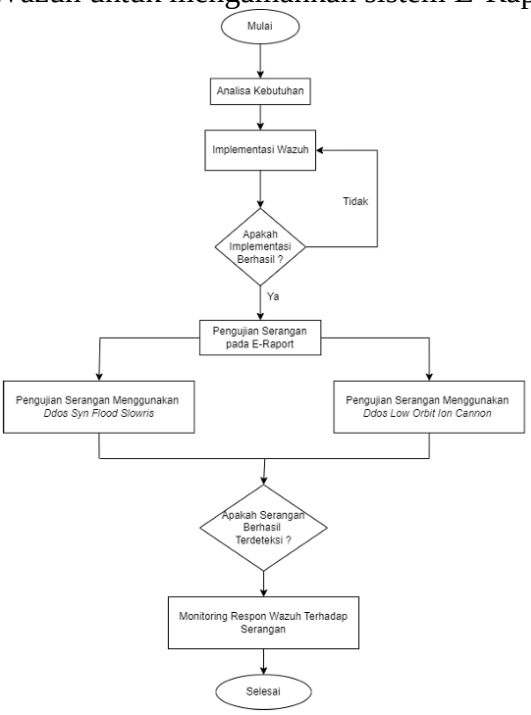
Penelitian ini memfokuskan pada upaya perlindungan data, peningkatan keamanan server, dan deteksi serta respons terhadap ancaman keamanan dalam konteks aplikasi E-Raport di SMK Negeri 1 Sinjai. Dengan menginstal Wazuh agent pada server E-Raport, penelitian ini bertujuan untuk memantau aktivitas secara real-time dan mendeteksi potensi ancaman yang dapat mengganggu integritas dan kerahasiaan data[12]. Selain itu, penelitian ini akan menganalisis konfigurasi server untuk memastikan bahwa langkah-langkah pengamanan yang tepat diterapkan, serta memberikan rekomendasi praktis untuk meningkatkan keamanan sistem informasi. Dengan pendekatan ini, diharapkan tercipta lingkungan yang lebih aman bagi pengelolaan data pendidikan dan meningkatkan kesadaran akan pentingnya keamanan siber di kalangan [13] seluruh smk negeri 1 sinjai

Metode

Metode penelitian yang digunakan yaitu metode eksperimen dimana dilakukan percobaan menggunakan sistem operasi Ubuntu dan kali linux yang melibatkan beberapa komponen utama yaitu server pusat, server E-Raport, Wazuh dashboard, Wazuh agent, switch, client, dan attacker yang terhubung melalui internet.

1. Tahapan Penelitian

Flowchart dibawa ini merupakan tahapan dari proses penelitian implementasi keamanan server aplikasi e-raport smk negeri 1 merupakan proses implementasi dan pengujian sistem keamanan menggunakan Wazuh untuk mengamankan sistem E-Raport dari serangan DDoS.



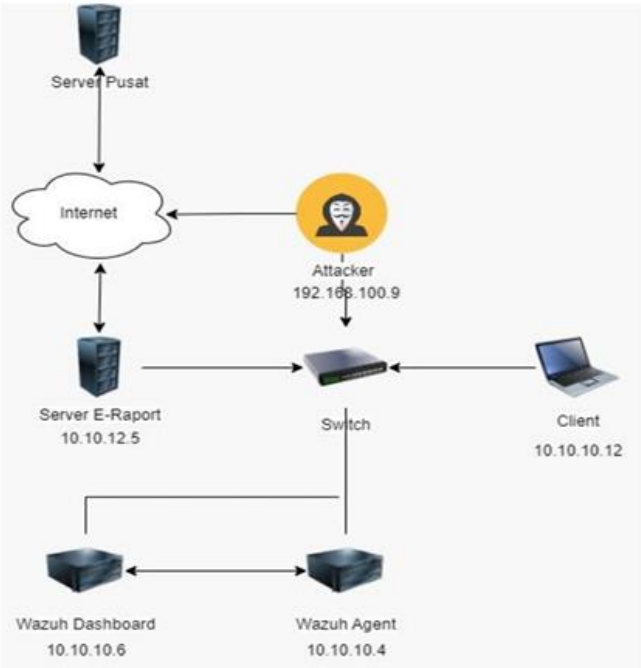
Gambar 1. Flowchart Penelitian

Pada Gambar 1 merupakan proses implementasi dan pengujian sistem keamanan menggunakan Wazuh untuk mengamankan sistem E-Raport dari serangan DDoS. Proses dimulai dari titik "Mulai," di mana dilakukan "Analisa Kebutuhan" untuk mengidentifikasi kebutuhan dan spesifikasi sistem keamanan yang harus dipenuhi. Setelah analisis kebutuhan, langkah berikutnya adalah "Implementasi Wazuh," Wazuh agent juga dipasang di berbagai endpoint untuk memastikan pemantauan dan pelaporan yang komprehensif. Setelah implementasi, yang melibatkan pemasangan dan konfigurasi Wazuh sebagai alat deteksi dan respon terhadap ancaman keamanan. Setelah implementasi, terdapat titik keputusan "Apakah Implementasi Berhasil?" Jika implementasi berhasil, proses berlanjut ke tahap "Pengujian Serangan pada E-Raport," di mana dua jenis serangan DdoS diuji: "Ddos Syn Flood Slowris" dan "Ddos Low orbit ion cannon." Kedua jenis serangan ini dilakukan secara terpisah untuk mengevaluasi efektivitas sistem dalam mendeteksi dan merespon ancaman. Selanjutnya, pada tahap keputusan "Apakah Serangan berhasil terdeteksi?", sistem mengevaluasi apakah serangan tersebut berhasil terdeteksi oleh Wazuh. Jika serangan berhasil terdeteksi, proses dilanjutkan ke tahap "Monitoring Respon Wazuh terhadap Serangan," di mana respon Wazuh terhadap serangan dianalisis untuk memastikan bahwa sistem memberikan respon yang tepat dan efektif. Akhirnya seluruh proses diakhiri dengan tahap "Selesai," menandakan selesainya siklus implementasi dan pengujian sistem keamanan ini.

2. Desain

Pada skema sistem Wazuh server dibawah menggambarkan sebuah sistem keamanan yang melibatkan beberapa komponen utama. Dalam jaringan ini, yaitu server pusat, server E-Raport, Wazuh dashboard, Wazuh agent, switch, client, dan attacker yang terhubung melalui

internet. Server pusat bertindak sebagai pusat pengelolaan data, sedangkan server E-Raport khusus menangani aplikasi E-Raport.



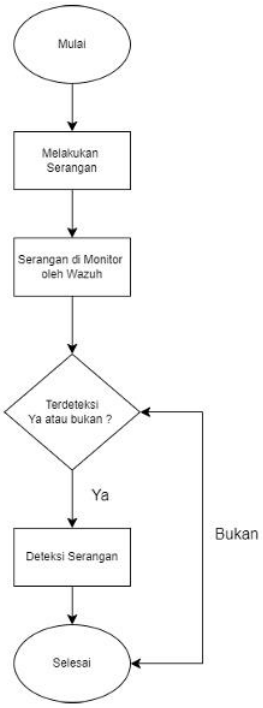
Gambar 2. Skema Sistem Wazuh Server

Pada Gambar 2 merupakan skema sistem wazuh server Wazuh dashboard dan Wazuh agent berperan dalam memonitor dan mendeteksi aktivitas mencurigakan atau serangan di jaringan. Switch digunakan untuk menghubungkan berbagai perangkat dalam jaringan lokal, sementara client adalah perangkat pengguna yang mengakses layanan E-Raport attacker yang terhubung melalui internet, merepresentasikan potensi ancaman eksternal terhadap sistem. Dalam skenario ini. Wazuh agent yang dipasang di server E-Raport mengirimkan dan data pemantauan ke Wazuh dashboard untuk dianalisis. Dashboard ini memberikan visualisasi dan laporan mengenai aktivitas jaringan dan potensi serangan yang terjadi. Jika attacker mencoba menyerang server E-Raport, Wazuh agent akan mendeteksi aktivitas tersebut dan mengirimkan informasi ke Wazuh dashboard untuk tindakan lebih lanjut. Implementasi ini menunjukkan bagaimana Wazuh dapat digunakan untuk meningkatkan keamanan jaringan dengan memonitor aktivitas secara real-time dan memberikan respon cepat terhadap ancaman, membantu menjaga integritas dan ketersediaan aplikasi E Raport di SMK Negeri 1 Sinjai.

3. Skenario Pengujian

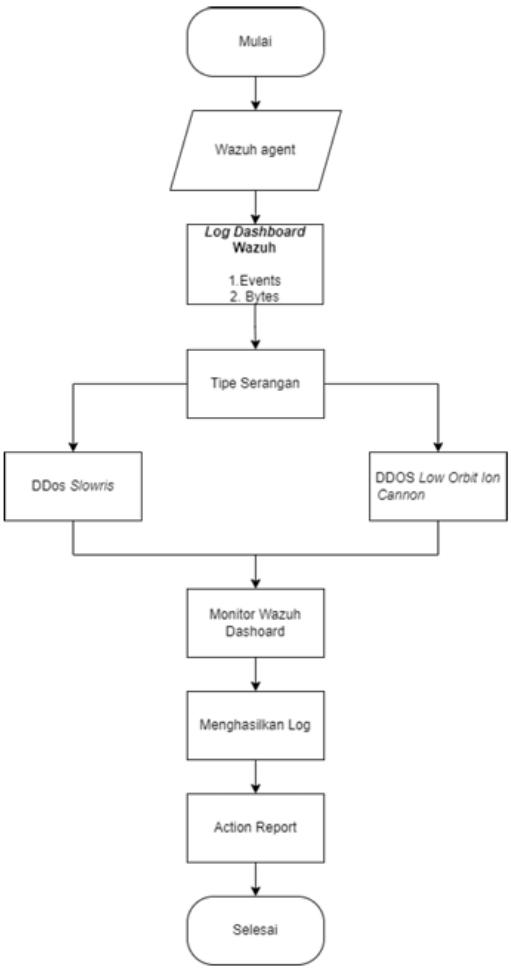
Pengujian dilakukan dengan salah satu perangkat sebagai pusat kontrol dan sebagai server tahap awal dari pengujian dilakukan dengan membuat satu network yang akan digunakan sebagai penghubung antara satu perangkat dengan perangkat lainya yaitu dengan cara menghubungkan server E-Raport di linux Ubuntu server. Setelah network penghubung terbuat, selanjutnya masuk ke dalam jaringan dengan melakukan login sebagai admin 34 dengan memasukkan username dan password yang sudah di buat sebelumnya masuk ke halaman Wazuh dengan menggunakan ip yang sudah di buat sebelumnya. pada Implementasi Keamanan

Server Aplikasi E-Raport SMK Negeri 1 Sinjai Menggunakan Wazuh juga terdapat flowchart yang dibuat seperti gambar 3 dibawah ini



Gambar 3. Flowchart Pemodelan Wazuh

Gambar 3. menjelaskan alur proses pemantauan dan deteksi serangan oleh sistem keamanan Wazuh dengan lebih rinci. Proses dimulai dari titik "Mulai," yang menandakan inisiasi prosedur pemantauan. Langkah berikutnya adalah "Melakukan Serangan," di mana sebuah serangan simulasi atau pengujian keamanan dilakukan terhadap sistem untuk menguji respon dan efektivitas Wazuh. Setelah serangan dilancarkan, tahap selanjutnya adalah "Serangan di Monitor oleh Wazuh," di mana Wazuh berfungsi sebagai sistem pemantauan keamanan yang terus mengawasi aktivitas jaringan dan mendeteksi adanya anomali atau indikasi serangan. Pada titik ini, sistem memasuki tahap keputusan "Terdeteksi Ya atau bukan?", di mana dilakukan evaluasi untuk menentukan apakah Wazuh berhasil mendeteksi serangan tersebut. Jika serangan terdeteksi, proses berlanjut ke langkah "Deteksi Serangan," yang mencakup identifikasi, pencatatan, dan analisis serangan oleh Wazuh untuk memastikan bahwa ancaman tersebut diakui dan ditangani dengan tepat. Akhirnya, alur proses diakhiri dengan tahap "Selesai," yang menandakan bahwa siklus pemantauan dan deteksi telah lengkap. Flowchart ini menggambarkan bagaimana Wazuh berperan dalam mendeteksi dan merespon ancaman keamanan secara sistematis dan efisien, memastikan bahwa setiap ancaman dapat diidentifikasi dan ditangani secepat mungkin untuk menjaga integritas dan keamanan sistem



Gambar 4. Flowchart Skenario Pengujian

Pada Gambar 4. menjelaskan proses pemantauan dan respon terhadap serangan DdoS menggunakan Wazuh dengan sangat rinci. Proses dimulai dari titik "Mulai," kemudian dilanjutkan dengan pemasangan "Wazuh agent" yang berfungsi sebagai komponen pemantauan di setiap endpoint dalam sistem. Setelah agent Wazuh diinstal, data aktivitas jaringan akan diteruskan ke " Dashboard Wazuh," di mana tentang "Events" (kejadian) dan "Bytes" (data yang diproses) dikumpulkan dan dianalisis. Selanjutnya, pada tahap "Tipe Serangan," sistem mengidentifikasi jenis serangan yang sedang terjadi, yang dapat berupa "DDos Slowris" atau "Ddos Low orbit ion cannon." Kedua jenis serangan ini diuji secara terpisah untuk mengevaluasi respon sistem terhadap masing-masing serangan. Proses kemudian berlanjut ke tahap "Monitor Wazuh Dashboard," di mana dashboard Wazuh digunakan untuk memantau aktivitas jaringan secara real-time dan mendeteksi anomali atau serangan yang sedang berlangsung. Informasi yang dikumpulkan kemudian digunakan untuk "Menghasilkan," yang mencatat semua aktivitas dan deteksi serangan secara rinci. Berdasarkan tersebut, dibuatlah "Action report," yang merupakan laporan tindakan yang diambil oleh sistem dalam merespon serangan, termasuk langkah-langkah mitigasi dan analisis dampak. Akhirnya, proses ini diakhiri dengan tahap "Selesai," yang menandakan bahwa seluruh siklus pemantauan, deteksi, dan respon terhadap serangan telah diselesaikan

4. Pengumpulan Data

Adapun pengumpulan data yang akan digunakan dengan cara melakukan observasi langsung untuk mengumpulkan data-data dari para siswa,guru, hak sekolah yang secara aktif menggunakan aplikasi E-Raport tersebut. Proses pengumpulan data akan melibatkan serangkaian langkah yang terdiri dari identifikasi kebutuhan pengguna aplikasi E-Raport, analisis performa sistem yang ada, serta wawancara dan diskusi dengan stakeholder terkait. Tujuan utama dari pengumpulan data ini adalah untuk memahami secara mendalam kebutuhan pengguna, mengevaluasi performa sistem yang ada, serta mengidentifikasi area area yang memerlukan perbaikan melalui penggunaan keamanan server aplikasi E Raport

Hasil

1. Analisa Kebutuhan

Dalam Implementasi Keamanan Server Aplikasi E-Raport SMK Negeri 1 Sinjai yang akan dilakukan terdapat beberapa kebutuhan, berikut detail spesifikasi perangkat keras maupun perangkat lunak yang di butuhkan :

a. Perangkat Keras

1. Laptop 1

Laptop 1 digunakan untuk membuat virtualisasi Wazuh dashboard untuk nantinya digunakan manajemen sistem memungkinkan pemantauan keamanan real-time, di mana administrator dapat dengan cepat melihat aktivitas dan status sistem. Selain itu, Wazuh dashboard menyediakan deteksi intrusi yang efektif, memungkinkan identifikasi upaya serangan dan aktivitas mencurigakan.

Tabel 1. Perangkat Keras Wazuh Dashboard

No	Spesikasi	Detail
1	Processor	*Intel® Core™ i7-1235G1*
2	RAM	12 GB
3	Penyimpanan	SSD 512GB
4	Grapics Cards	Intel® 23 Ghz

Berikut spesikasi dari virtual Machine (VM) Wazuh dashboard yang akan di virtualisasikan laptop 1 dengan virtual box ditunjukkan di Tabel 2

Tabel 2. Spesikasi Virtual Machine Wazuh Dashboard

No	Virtual Machine	Sistem Operasi	Ram	Peyimpanan
1	Wazuh Dasboard	Ubuntu 22.04	8 GB	100 GB
2	Wazuh Agent	Windows 11	8 GB	512 Gb

2. Komputer 2

Komputer 2 digunakan untuk membuat virtualisasi kali Linux sebagai attacker untuk mengirimkan serangan DdoS Tabel 3 menunnjukkan spesikasi dari komputer 2

Tabel 3. Spesikasi Komputer Attacker

No	Spesikasi	Detail
1	Sistem Operasi	Ubuntu 22.04
2	Processor	AMD Ryzen 5 5000 U
3	Peyimpanan	SSD 512GB

4	Ram	8 GB

b. Perangkat Lunak

Berikut ini beberapa nama dan versi perangkat lunak yang digunakan dalam implementasi ditunjukkan Tabel 4

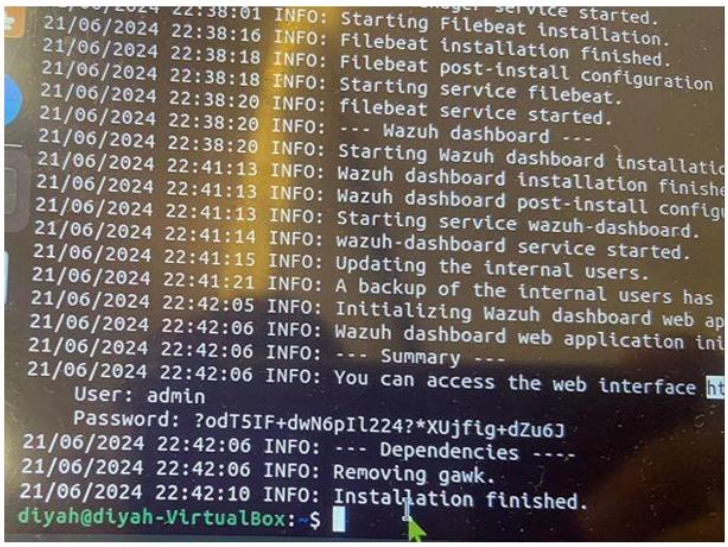
Tabel 4. Spesikasi Perangkat Lunak Wazuh Dashboard

No	Nama	Versi	Fungsi
1	Wazuh Dasboard	4.8.0	Tool untuk memonitoring aktifitas server
2	Wazuh Agent	4.8.1	Tool untuk mendeteksi serangan
3	Wazuh Manager	4.2.1	Aplikasi network monitoring
4	Filebeat	10.2	Mengirim data ke elasticsearch
5	Elastic search	7.10.2	Elasticsearch berkemampuan dalam pencarian dan analisis data secara realtime.
6	Kibana	7.10.2	Kibana memvisualisasikan data yang tersimpan pada elasticsearch.
7	Ubuntu	22.04	Sistem Operasi Wazuh dashboard dan agent
8	Kali Linux	2021.2	Sistem Operasi attacker
9	Loic	2.9.9.9.9	Tool untuk serangan DdoS
10	Slowris	1.8.2	Tool untuk serangan DdoS

2. Implmentasi

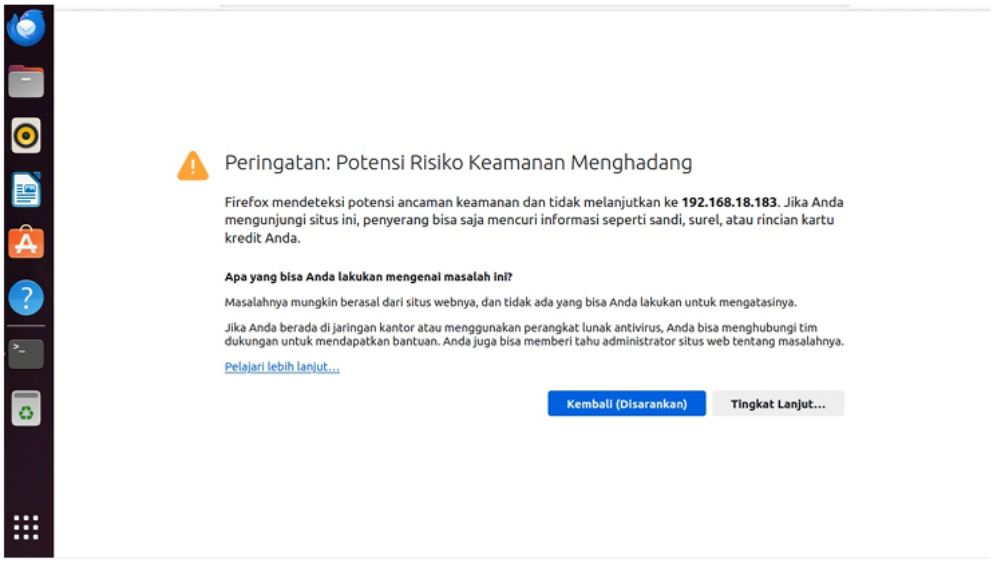
a. Konfigurasi Wazuh Dashboard

Pada penelitian ini di implementasikan di Ubuntu 22.04 dengan menggunakan Wazuh sebagai dashboard membantu visualisasi dan analisis data keamanan yang dikumpulkan dari berbagai sumber dan melakukan pengumpulan data , pemantauan integritas file, pemantauan registri windows, deteksi rootkit, deteksi anomali , malware, kerentanan, peringatan berbasis waktu dan respon aktif .tedapat beberapa komponen yaitu Wazuh indexer, Wazuh server dan Wazuh dashboard masing– masing komponen tersebut saling melengkapi, sehingga ketiga komponen harus terpasang dan dapat berkomunikasi agar sistem Wazuh bisa berjalan dengan normal. Untuk langkah awal dengan melakukan instalasi menggunakan wazuh dengan mengetikkan perintah Curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh install.sh -a seperti gambar 5



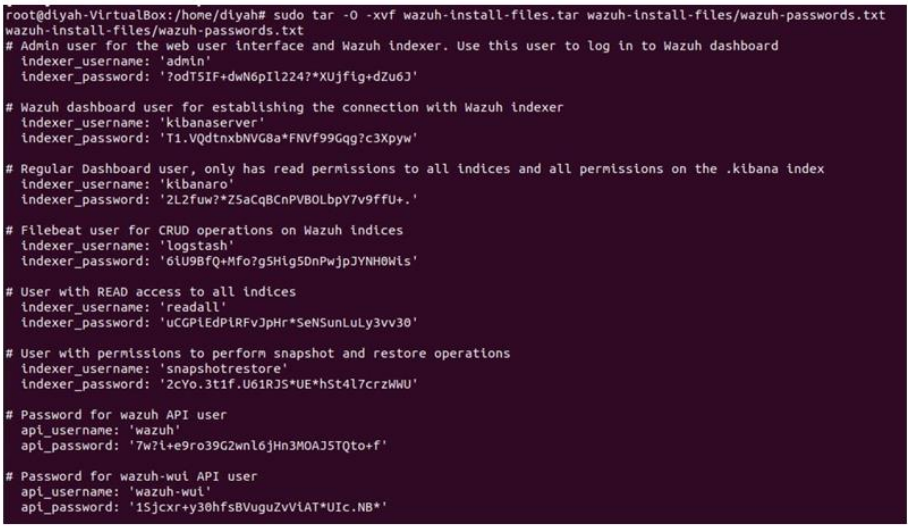
Gambar 5. Instalasi Wazuh Dashboard

Setelah itu, instalasi Wazuh dashboard dilakukan termasuk konfigurasi post-install dan memulai layanan Wazuh dashboard. Ada juga proses backup internal users dan inisialisasi aplikasi web Wazuh dashboard. menunjukkan bahwa proses instalasi selesai dengan memberikan informasi in, yaitu user: admin dan password: ?odT5IF+dWn6PlL224?*XUj5tig+dZu6J pada gambar 6 instalasi Wazuh central componets sudah berhasil, Pada Wazuh dashboard dapat di akses melalui dengan memasukkan ip server ke browser dan lanjutkan. Jika terdapat peringatan warning: Potensial security risk ahead bisa diabaikan dan klik advanced selajutnya pilih pada accept the risk and continue.



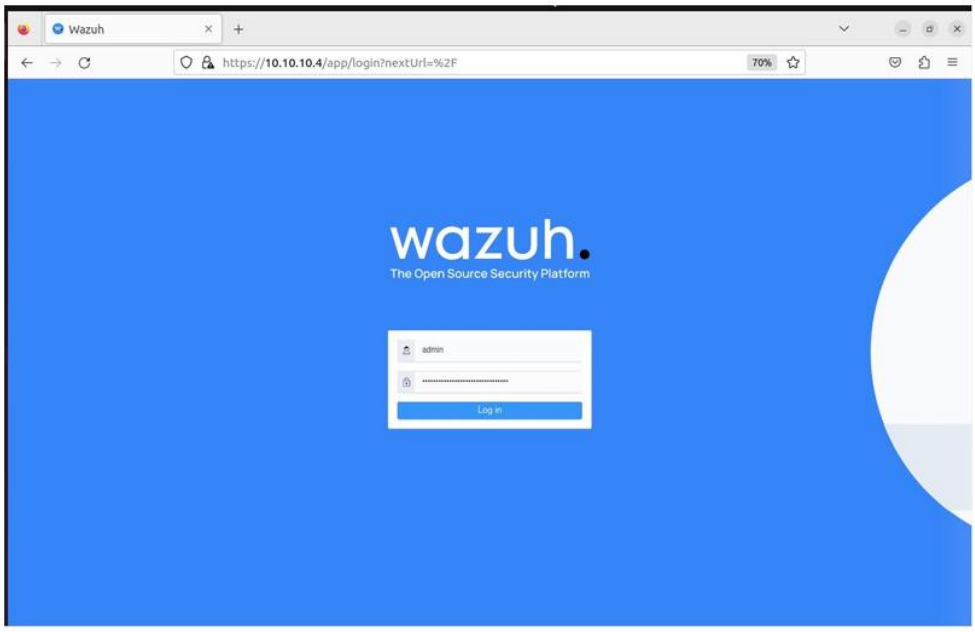
Gambar 6. Peringatan Sebelum Masuk di wazuh

Setelah menjalankan perintah untuk mendeteksi serangan melalui IDS/IPS *snort* 3 di dapatkan serangan berupa *alert* di *local.rules* yang sudah terlebih dahulu kita masukkan *alert. Alert* dapat dilihat pada gambar 7.



Gambar 7. Menampilkan Username dan Password Wazuh

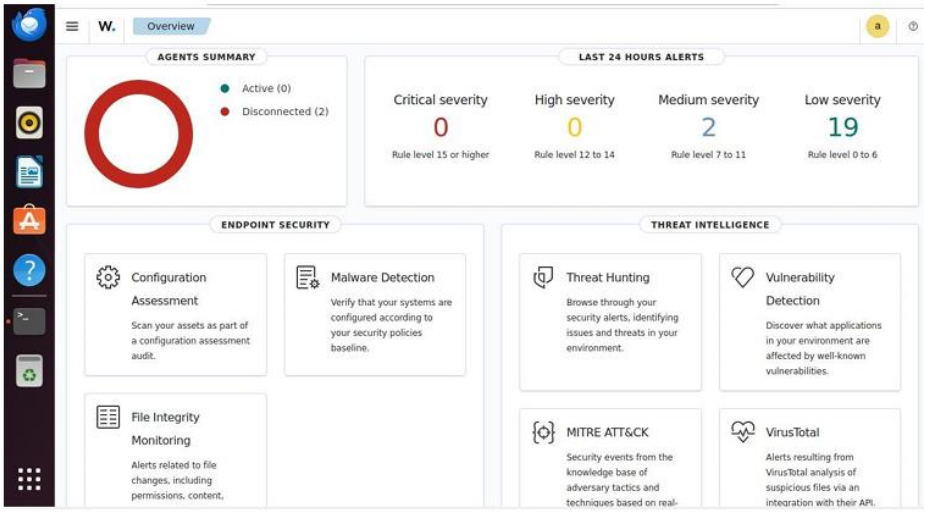
Selanjutnya pada gambar 8 untuk medapatkan username dan password default nya kita mengetikkan perintah sudo tar -O -xvf Wazuh-install-files.tar Wazuh-install-files/wazuh-passwords.txt



Gambar 8. Halaman l*ogin* Wazuh

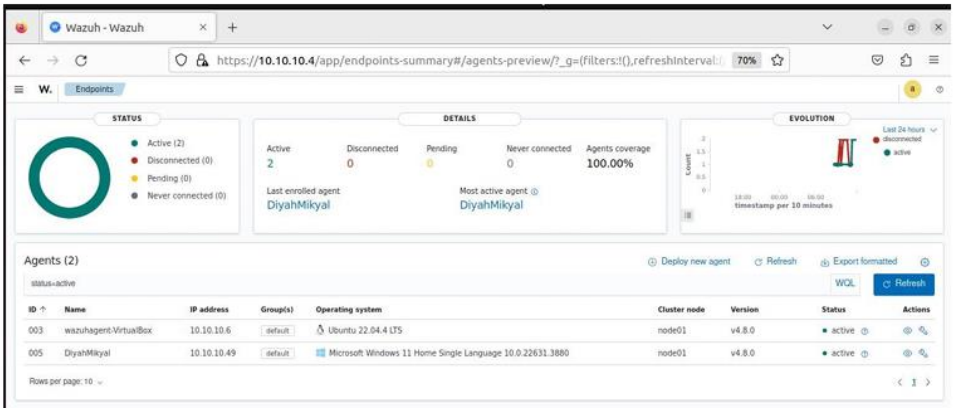
Pada gambar 4.4 menunjukkan antarmuka login dari platform keamanan open-source Wazuh. Halaman ini meminta pengguna untuk memasukkan kredensial login, yaitu nama pengguna (username) dan kata sandi (password). Pada gambar ini, terlihat bahwa username yang digunakan adalah "admin," dan kata sandi telah diisi, meskipun tidak terlihat karena disembunyikan oleh karakter mask (biasanya berupa titik atau bintang). Wazuh adalah alat untuk monitoring keamanan dan manajemen, yang sering digunakan untuk mendeteksi ancaman, monitoring sistem, dan mendukung kepatuhan terhadap kebijakan keamanan. URL di bagian atas browser menunjukkan bahwa antarmuka ini diakses melalui jaringan lokal

dengan alamat IP 10.10.10.4. Alamat ini biasanya digunakan dalam jaringan internal yang menunjukkan bahwa server Wazuh ini mungkin di-hosting secara lokal.



Gambar 9. Halaman Overview Wazuh

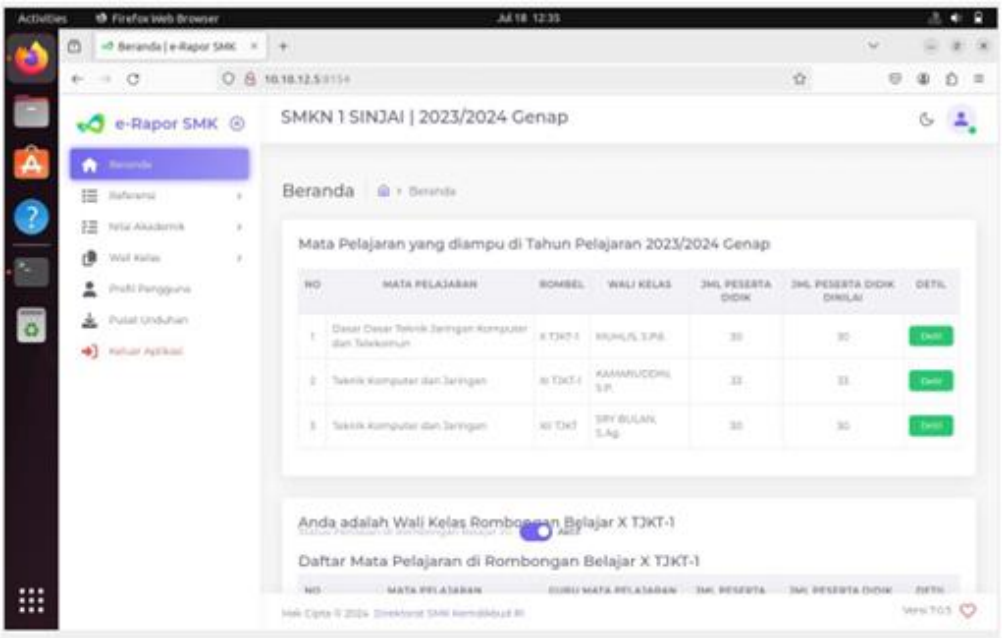
Gambar 9 menampilkan halaman "Overview" dari antarmuka Wazuh sebuah platform keamanan open-source. Di bagian atas, terdapat ringkasan status agent 47 dengan grafik donat menunjukkan bahwa tidak ada agent yang aktif (active) dan dua agent dalam status terputus (disconnected). Sebelah kanan grafik terdapat "Last 24 Hours Alerts" yang merinci jumlah peringatan keamanan yang dikategorikan berdasarkan tingkat keparahan tidak ada peringatan dengan tingkat "Critical severity" (kritis) atau "High severity" (tinggi), dua peringatan dengan tingkat "Medium severity" (sedang), dan 19 peringatan dengan tingkat "Low severity" (rendah).



Gambar 10. Halaman Antarmuka Endpoint Agen Wazuh

Pada gambar 10 menampilkan antarmuka dashboard Wazuh yang menunjukkan status agent yang terhubung ke server Wazuh. Pada bagian atas, 48 terdapat grafik donat yang menunjukkan status konektivitas agent dua agent dalam keadaan "Active" (aktif) dan tidak ada agent yang "Disconnected" (terputus), "Pending" (menunggu), atau "Never connected" (tidak pernah terhubung). Bagian detail mencantumkan agent terakhir yang didaftarkan dan agent paling aktif, yang keduanya adalah "DiyahMikyal." Pada tabel di bawahnya dua agent ditampilkan dengan informasi termasuk ID, nama, alamat ip, sistem operasi, dan status saat ini.

Agent pertama bernama "Wazuhagent-VirtualBox" dengan alamat IP 10.10.10.6 yang menjalankan Ubuntu 22.04.4 LTS, sedangkan agent kedua bernama "DiyahMikyal" dengan alamat IP 10.10.10.49 yang menggunakan Microsoft Windows 10 Home Single Language 10.0.22631.3880. Keduanya berada di cluster node01 dengan versi Wazuh 4.8.0 dan status aktif.

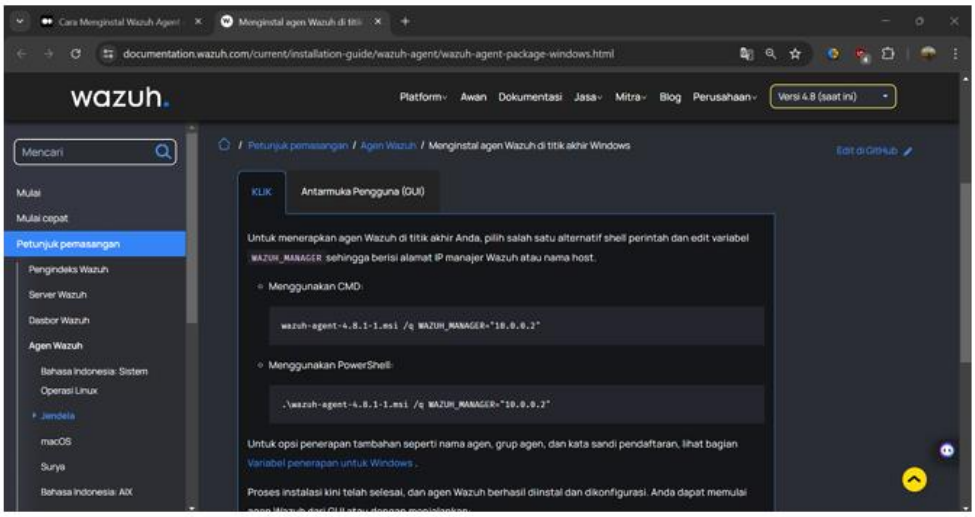


Gambar 11. Halaman Server E-Raport

Pada gambar 11 merupakan server E-Raport yang dihubungkan dengan Wazuh dashboard yang nantinya akan di monitoring ketika terjadinya serangan pada server E-Raport dengan ip 10.10.12.5 pada bagian utama layar menampilkan informasi tentang mata pelajaran yang diajarkan pada tahun pelajaran 2023/2024. Tabel tersebut mencantumkan nomor, nama mata pelajaran, rombel (rombongan belajar), wali kelas, jumlah peserta didik, jumlah peserta didik dinilai, dan tombol untuk melihat detail lebih lanjut.

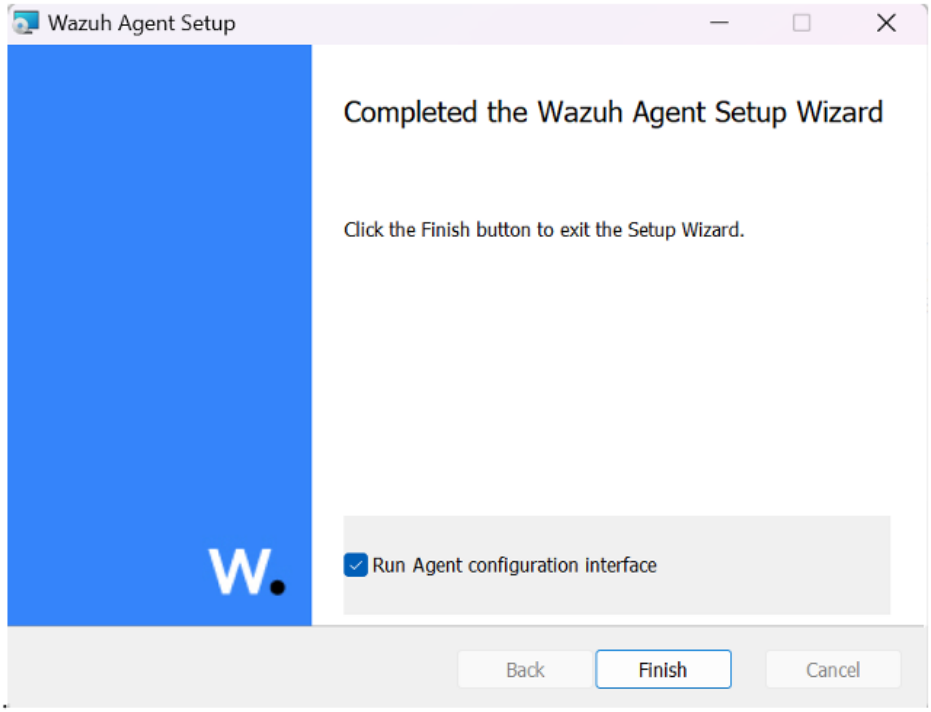
b. Konfigurasi Wazuh Agent

Wazuh Agent adalah komponen dari platform Wazuh yang dipasang pada endpoint seperti server, workstation, atau perangkat jaringan untuk memantau dan melaporkan berbagai aktivitas keamanan dan kepatuhan. Agent ini bertugas mengumpulkan data dari sistem operasi, aplikasi, dan keamanan, serta melakukan pemeriksaan integritas file, analisis kerentanan, dan pemantauan perilaku. Wazuh Agent mendukung berbagai sistem operasi termasuk Windows, Linux, dan macOS, serta dapat dikonfigurasi untuk berbagai kebutuhan keamanan spesifik. Untuk menginstall Wazuh agent yang pertama dilakukan unduh 50 Wazuh agent manager buka browser resmi wazuh.com di VM Windows 10 dan buka dokumentasi Wazuh untuk seperti gambar 4.8



Gambar 12. Halaman Resmi Wazuh Agent

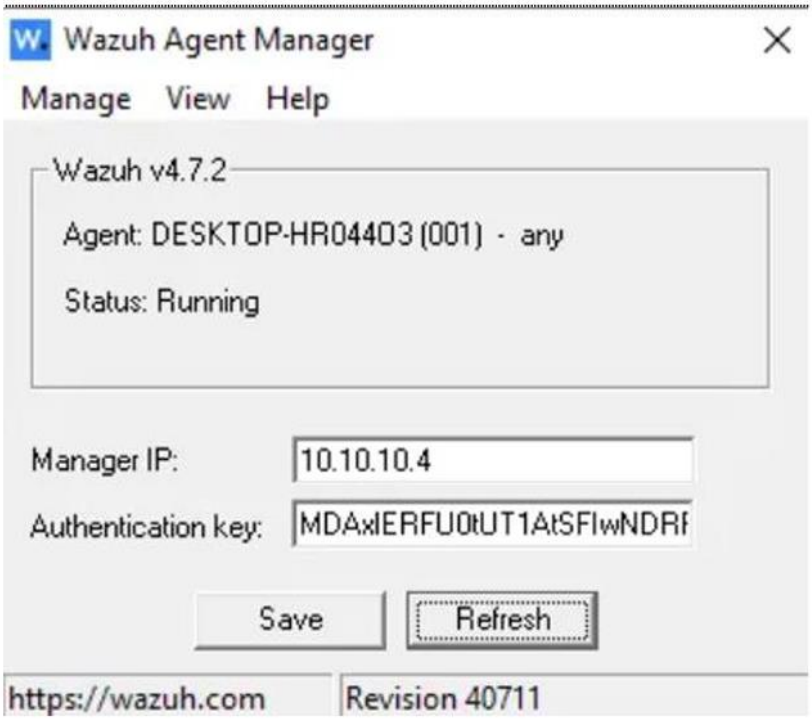
Opsi ini akan membuka antarmuka konfigurasi agent setelah mengklik tombol "Finish," memungkinkan pengguna untuk melakukan konfigurasi lebih lanjut pada Wazuh agent, seperti memasukkan alamat ip atau hostname Wazuh manager dan mengatur kunci autentikasi. Tombol 51 "Finish" di bagian bawah kanan akan mengakhiri proses instalasi dan memulai antarmuka konfigurasi agent jika opsi tersebut tetap dicentang. Tombol "Back" dan "Cancel" juga terlihat, namun pada tahap ini hanya tombol "Finish" yang relevan untuk menyelesaikan proses gambar 13



Gambar 13. Wazuh Agent Setup

Gambar 13 menampilkan antarmuka dari "Wazuh Agent Manager," sebuah aplikasi yang digunakan untuk mengelola agent Wazuh. Pada bagian atas, terlihat bahwa perangkat lunak yang digunakan adalah Wazuh versi 4.7.2. agent yang terdaftar memiliki nama

"DESKTOP-HR04403" dengan ID (001) dan saat ini dalam status "Running," menandakan agent sedang aktif dan berfungsi.



Gambar 14. Antarmuka Wazuh Agent Manager

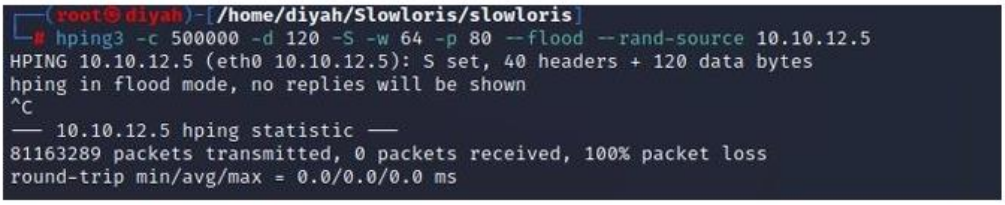
Setelah manager ip Wazuh agent dimasukkan kita cek di terminal Ubuntu Wazuh dashboard apakah status Wazuh agent aktif, menampilkan output dari terminal Linux, di mana perintah sudo systemctl status Wazuh-agent dijalankan untuk memeriksa status layanan Wazuh Terdapat juga aktivitas yang menunjukkan berbagai proses terkait Wazuh agent, termasuk penghapusan file PID, memulai proses eksekusi, dan menjalankan berbagai modul. Informasi ini berguna untuk diagnostik dan memastikan bahwa agent berfungsi sesuai harapan. Dapat di lihat pada Gambar 12

3. Pengujian Serangan Ddos Syn Flood Slowris

```
┌──(root㉿diyah)-[/home/diyah/Slowloris/slowloris]
└─# hping3 -c 100000 -d 120 -S -w 64 -p 80 --flood --rand-source 10.10.12.5
HPING 10.10.12.5 (eth0 10.10.12.5): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.12.5 hping statistic ---
293451 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

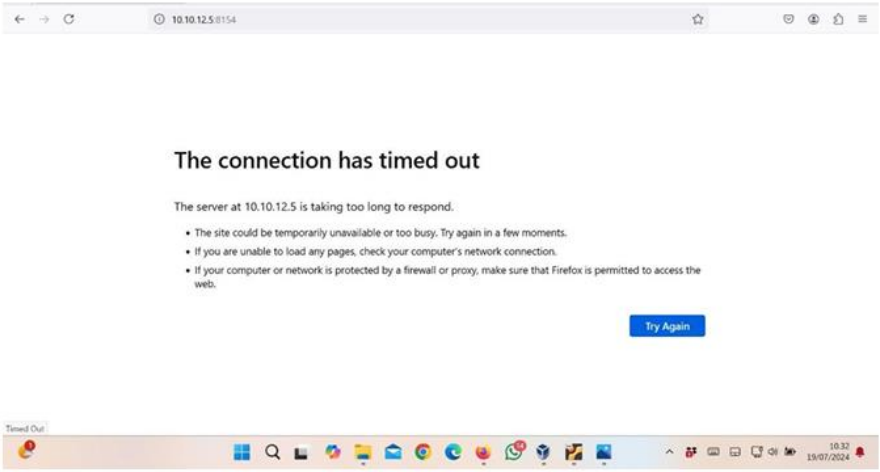
Gambar 15. Pengujian Serangan Ddos Hping 100000

Gambar 15 tersebut menunjukkan penggunaan perintah hping3 untuk melakukan serangan SYN Flood sebagai bagian dari pengujian keamanan. Perintah ini mengirimkan 100.000 paket SYN ke alamat IP 10.10.12.5 pada port 80, dengan ukuran jendela 64 byte dan payload data 120 byte, menggunakan alamat sumber acak (--rand-source). Gambar 13. Dashboard Melihat Status Wazuh Agent di dapatkan hasil 293.451



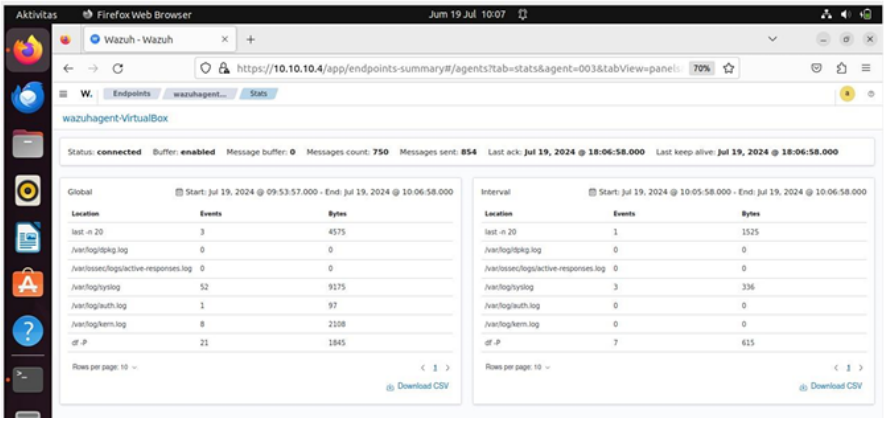
Gambar 16. Pengujian Serangan Ddos Hping 500000

Pada gambar 16 Pengujian serangan 500000 menunjukkan penggunaan perintah hping3 untuk melakukan simulasi serangan DDoS SYN Flood terhadap alamat ip 10.10.12.5 di port 80. Parameter yang digunakan meliputi -c 500000 yang berarti mengirimkan 500.000 paket; -d 120 untuk mengatur payload data sebesar 120 byte; -S untuk menandakan paket SYN; -w 64 untuk ukuran jendela sebesar 64 58 byte; -p 80 untuk target port 80; dan --Flood untuk mengirim paket secepat mungkin. Perintah ini juga menggunakan alamat sumber acak (--rand-source) untuk menaburkan asal serangan.



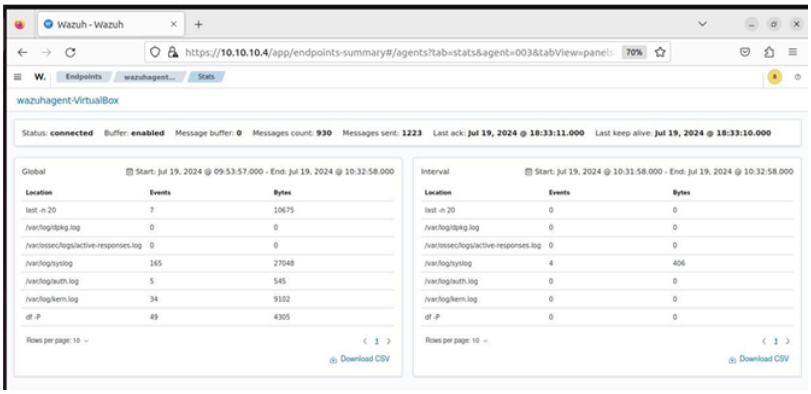
Gambar 17. Kondisi Server E-Raport 500000

Pada hasil monitoring wazuh hasil di dapatkan ketika terjadinya serangan hping3 yaitu 100000, dan 500000.



Gambar 17. Hasil Pemantauan Serangan Hping 3 100000

Selanjutnya pada gambar 17 Merupakan hasil pemantauan pada serangan hping 3 dengan mengirimkan 100000 packet berhasil terdeteksi Pada kolom "/var//sys," terlihat bahwa selama periode monitoring dari 09:53:57 hingga 10:06:58 pada tanggal 19 Juli 2024, terdapat 52 event dengan total 9175 bytes sys mencatat berbagai jenis sistem pesan seperti adanya packet yang banyak di server E-Raport atau informasi lainnya dari kernel dan aplikasi.



Gambar 17. Hasil Pemantauan Serangan Hping 3 50000

Pada Gambar 4.19 Hasil pemantauan serangan hping 500000 menunjukkan hasil pemantauan dari Wazuh pada agent "Wazuhagent-VirtualBox," yang sedang menggabungkan beberapa sistem file untuk mendeteksi aktivitas yang mencurigakan. Pada kolom "Global," yang mencakup periode monitoring dari 09:53:57 hingga 10:32:58 pada tanggal 19 Juli 2024, terlihat bahwa "/var//sys" mencatat 165 event dengan total 27048 bytes, menunjukkan aktivitas sistem yang signifikan lainnya seperti "/var//auth."

Tabel 5. Pengujian Keseluruhan Serangan Hping 3

No	*Location*	Jumlah Serangan *Socket Slowris*	*Events*	*Bytes*
1.	/var//sys	100.000	52	9175
2.	/var//kern.	100.000	8	2108
3.	df -p	100.000	21	1845
4.	*Last* -n 20	100.000	3	4575
5.	/var//auth.	100.000	1	97
6.	/var//sys	500.000	165	27048
7.	/var//kern.	500.000	5	545
8.	df -p	500.000	49	4305
9.	*Last* -n 20	500.000	7	10675
10.	/var//auth.	500.000	5	545

Pada tabel 4.5 menjelaskan hasil pemantauan serangan socket slowris menggunakan Hping 3, dengan dua skenario serangan satu dengan 100.000 serangan dan satu lagi dengan 500.000 serangan tercatat di berbagai sistem. Setiap entri dalam tabel ini mencantumkan lokasi, jumlah serangan socket slowris, events, dan total bytes yang tercatat. Pada skenario serangan 100.000, /var//sys mencatat 52 events dengan total 9175 bytes, menunjukkan bahwa ini sangat

informatif dalam mendokumentasikan serangan. /var//kern mencatat 8 events dengan 2108 bytes, sedangkan df -p mencatat 21 events dengan 1845 bytes. Last -n 20 mencatat 3 events dengan 4575 bytes, dan /var//auth hanya mencatat 1 event dengan 97 bytes, menunjukkan relevansi yang lebih rendah dalam mendeteksi serangan ini. Pada skenario serangan 500.000, /var//sys mencatat 165 events dengan total 27048 bytes, menunjukkan tingkat aktivitas yang sangat tinggi dalam mencatat serangan ini. Sebaliknya, /var//kern. dan /var//auth. masing-masing hanya mencatat 5 events 63 dengan total 545 bytes, menunjukkan bahwa kedua ini kurang sensitif terhadap serangan dalam jumlah besar.

4. Pengujian Serangan Ddos Low Orbit Ion Cannon

Low orbit ion cannon (LOIC) adalah alat sumber terbuka yang digunakan untuk melakukan serangan Distributed Denial of Service (DDoS). LOIC bekerja dengan membanjiri target dengan sejumlah besar permintaan HTTP, UDP, atau TCP dengan tujuan membuat layanan target tidak dapat diakses. Pengujian serangan DdoS menggunakan LOIC dapat dilakukan dengan menjalankan alat ini pada beberapa komputer yang terhubung ke internet, yang kemudian secara bersamaan mengirimkan permintaan ke server target. Pada gambar 18 pengujian pertama ini, serangan DdoS dilakukan dengan menggunakan Low Orbit Ion Cannon (LOIC) untuk mengirimkan 100.000 socket ke server target yang beralamat ip 10.10.12.5. Pada tampilan LOIC, terlihat bahwa mode pengujian yang digunakan adalah "Manual Mode (Do it yourself)" dengan metode serangan melalui protokol HTTP pada port 80. Jumlah thread yang digunakan untuk mengirim permintaan adalah 25, dengan masing-masing thread mengirimkan 100.000 permintaan socket.

Gambar 18. Pengujian Serangan Loic 10000

Pada gambar 19 kedua ini, serangan DdoS dilakukan menggunakan Low Orbit Ion Cannon (LOIC) dengan peningkatan intensitas serangan. Konfigurasi pengujian menunjukkan bahwa alamat ip target tetap sama, yaitu 10.10.12.5. Kali ini, jumlah permintaan socket yang dikirimkan dinaikkan menjadi 300.000 per thread, dengan total 25 thread yang digunakan untuk melakukan serangan. Metode serangan masih menggunakan protokol HTTP pada port 80, dengan timeout setiap permintaan ditetapkan selama 30 detik.

Gambar 19. Pengujian Serangan Loic 30000

Pada Gambar 20 pengujian ketiga ini, serangan DdoS dilakukan dengan menggunakan Low Orbit Ion Cannon (LOIC) dengan intensitas yang jauh lebih tinggi dibandingkan pengujian sebelumnya. Alamat IP target tetap 10.10.12.5, 71 namun kali ini jumlah permintaan socket yang dikirimkan dinaikkan menjadi 500.000 per thread, dengan total 25 thread.

Gambar 20. Pengujian Serangan Loic 10000

Tabel 6. Pengujian Keseluruhan Serangan LOIC

No	*Location*	Jumlah Serangan *Socket* LOIC	*Events*	*Bytes*
1.	/var//sys	100.000	50	9197
2.	/var//kern.	100.000	10	2614
3.	df -p	100.000	14	1230
4.	*Last* -n 20	100.000	2	3052
5.	/var//auth.	100.000	1	97
6.	/var//sys	300.000	62	11451
7.	/var//kern.	300.000	15	3899
8.	df -p	300.000	28	2460
9.	*Last* -n 20	300.000	4	6104
10.	/var//auth.	500.000	3	321
11.	/var//sys	500.000	97	17766
12.	/var//kern.	500.000	24	6304
13.	df -p	500.000	35	3075
14.	last -n 20	500.000	5	7630
15.	/var//auth.	500.000	4	406

Pada tabel 6 diatas menampilkan sebuah tabel yang memberikan rincian hasil pengujian serangan menggunakan LOIC (Low Orbit Ion Cannon) pada berbagai lokasi di sistem. Tabel ini terdiri dari lima kolom: Kolom pertama, "No", 77 berisi nomor urut dari 1 hingga 15, yang mengidentifikasi setiap entri secara unik. Kolom kedua, "Location ", menunjukkan lokasi atau perintah tempat disimpan, seperti `/var//sys`, `/var//kern., `/var//auth.`, `df -p`, dan `Last -n 20`. Lokasi ini merupakan tempat di mana data mengenai serangan disimpan untuk analisis lebih lanjut. Kolom ketiga, "Jumlah Serangan Socket LOIC", mencatat jumlah serangan yang dilakukan, yang secara konsisten diukur dalam satuan 100.000, 300.000, dan 500.000. Kolom ini memberikan gambaran tentang skala serangan yang diuji pada sistem. Kolom keempat, "Events", menunjukkan jumlah kejadian atau event yang tercatat di masing-masing lokasi . Angka-angka di kolom ini bervariasi, mulai dari 1 hingga 97, mencerminkan frekuensi kejadian yang dicatat pada setiap lokasi sebagai akibat dari serangan tersebut.

Pembahasan

Pada penelitian ini dilakukan implementasi keamanan server aplikasi E Raport SMK Negeri 1 sinjai menggunakan Wazuh yang dimana proses pengujian serangan DdoS menggunakan alat Slowris dan Low Orbit Ion Cannon (LOIC) serta analisis hasil monitoring yang dilakukan menggunakan Wazuh. Pengujian ini bertujuan untuk mengevaluasi kemampuan Wazuh dalam mendeteksi dan mencatat aktivitas serangan DdoS secara real-time. Pengujian dilakukan dengan menjalankan "/var//kern." juga mencatat sejumlah event dengan ukuran byte yang 61 berbeda. Pada kolom "Interval" yang mencakup periode waktu yang lebih pendek (dari 10:31:58 hinggan 10:32:58), "/var//sys" mencatat 4 event dengan total 406 byte sehingga pada serangan 500000 slowris menyebabkan server menjadi down dan server E-Raport tidak dapat diakses.

Pada hasil serangan Slowris yang didapatkan oleh monitoring Wazuh dilakukan analisis hasil keseluruhan serangan DdoS Slowloris terhadap ip target 192.168.100.9 dengan berbagai jumlah socket serangan (100,000 dan 500,000) serta hasil monitoring yang dilakukan menggunakan Wazuh. Tabel mencatat dua sesi pengujian, di mana setiap sesi menunjukkan peningkatan jumlah events dan bytes yang dicatat oleh Wazuh seiring dengan meningkatnya jumlah socket yang digunakan dalam serangan. Pada serangan dengan 100,000 socket, terdapat 52 events dan 9175 bytes tercatat. Pada puncaknya, dengan 500,000 socket, Wazuh mencatat 165 events dan 27048 bytes. Data ini menunjukkan bahwa semakin besar jumlah socket yang digunakan dalam serangan, Di bagian "Interval", yang menunjukkan data yang lebih granular dalam jangka waktu yang lebih pendek dari 88 monitoring, terlihat bahwa aktivitas pada interval tersebut lebih rendah dengan var//sys mencatat 4 event dan 406 bytes dan jumlah total pesan yang didapatkan 1223 ,buffer pesan 930 pesan yang mengindikasikan adanya banyak aktifitas dan yang ditangkap oleh Wazuh agent.

Pada hasil serangan Low Orbit Ion Cannon yang didapatkan oleh monitoring Wazuh dilakukan analisis hasil keseluruhan menggunakan Low Orbit Ion Cannon dengan menargetkan IP 10.10.12.5 (IP address E-Raport) pada pengujian dengan menerapkan beberapa socket yaitu 100000,300000 dan 500000 pada socket 100000 dan 300000 tidak menyebabkan down pada server ketika socket pada serangan LOIC sebuah target ip 10.10.12.5. Dalam konfigurasi ini, penguji menargetkan port 80 dengan 500,000 socket per thread menggunakan metode HTTP. Pengaturan ini bertujuan untuk mengirimkan sejumlah besar permintaan HTTP ke server dalam waktu singkat, membanjiri bandwidth dan sumber daya server sehingga menyebabkan overload. Timeout diatur selama 30 detik, memberikan cukup waktu bagi setiap permintaan untuk menunggu respon sebelum dianggap gagal. Dalam tes ini, serangan menghasilkan 25 thread aktif yang terus menerus mengirimkan permintaan HTTP ke server target tanpa menunggu respon, menghasilkan beban yang sangat besar. Di dapatkan hasil monitoring bahwa selama rentang waktu 11:59:52 hingga 12:27:53 total 839 pesan.

Perekaman log Wazuh selama serangan menunjukkan efektivitas yang bervariasi tergantung pada 89 intensitas serangan. Pada serangan DdoS menggunakan Slowloris, dengan peningkatan jumlah socket dari 100.000 hingga 500.000, Wazuh mencatat jumlah event dan ukuran byte yang meningkat secara signifikan. Untuk serangan dengan 100.000 socket, tercatat 49 event dengan 8.839 byte, sedangkan untuk 500.000 socket, tercatat 80 event dengan 32.123 byte. Perekaman log ini mengindikasikan bahwa Wazuh dapat menangkap aktivitas serangan secara detail, meskipun ada indikasi false negative pada serangan dengan jumlah socket yang lebih rendah, seperti yang terlihat pada pengujian 100.000 socket di mana server E-Raport tidak down meskipun ada aktivitas yang tercatat. Sebaliknya, pada serangan DdoS menggunakan Low Orbit Ion Cannon (LOIC), perekaman log Wazuh menunjukkan hasil yang konsisten dengan deteksi yang baik pada berbagai intensitas serangan. Untuk pengujian dengan 500.000 socket, Wazuh mencatat 97 event dengan total 17.766 byte, yang mengindikasikan respon sistem terhadap beban yang sangat tinggi.

Kesimpulan

Berdasarkan hasil pengujian dari Implementasi Keamanan Server Aplikasi E-Raport SMK Negeri 1 Sinjai Menggunakan Wazuh sebagai berikut :

1. Pada implementasi Wazuh untuk memonitor serangan DdoS Slowloris menunjukkan hasil yang efektif dalam mendeteksi dan mencatat aktivitas serangan.

2. Pada efisiensi penggunaan Wazuh dalam pemantauan serangan DdoS dapat diukur dari kemampuannya dalam mendeteksi dan merespon ancaman secara tepat waktu serta dampaknya terhadap kinerja aplikasi dan keamanan data. Implementasi yang efektif dari sistem monitoring ini memungkinkan Wazuh untuk memberikan peringatan pada Wazuh dashboard tentang aktivitas mencurigakan, mengidentifikasi pola serangan dengan akurasi tinggi, dan mengurangi false negatif.

3. Wazuh secara efektif menyimpan informasi atau data yang teridentifikasi selama kejadian serangan dengan cara yang terstruktur dan terorganisir. Selama serangan DdoS, Wazuh berhasil merekam berbagai detail terkait aktivitas serangan, termasuk jumlah event, ukuran byte, dan timestamp. Pada serangan DdoS Slowloris dan Low Orbit Ion Cannon (LOIC) menunjukkan kemampuan sistem dalam merekam, mendeteksi dan mencatat aktivitas serangan secara efektif. Pada serangan Slowloris terhadap ip 192.168.100.9, jumlah events dan bytes yang tercatat meningkat seiring dengan bertambahnya jumlah socket: 52 91 events dan 9175 bytes pada 100.000 socket dan 165 events dan 27048 bytes pada 500.000 socket. Data ini menunjukkan hubungan langsung antara jumlah socket dan intensitas aktivitas yang tercatat.

Daftar Pustaka

[1] S. Kramer and J. C. Bradfield, “A general definition of malware,” *J. Comput. Virol.*, vol. 6, no. 2, pp. 105–114, May 2010, doi: 10.1007/s11416-009-0137-1.
[2] I. B. A. I. Iswara and I. P. P. K. Yasa, “Analisis Dan Perbandingan Quality Of Service Video Conference Jitsi Dan Bigbluebutton Pada Virtual Private Server,” *J. Resist. Rekayasa Sist. Komput.*, vol. 4, no. 2, pp. 192–203, Oct. 2021, doi: 10.31598/jurnalresistor.v4i2.794.
[3] M. R. Ramadhani and A. R. Pratama, “Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia”.
[4] D. B. Rendro, W. N. Aji, J. R. Serang, C. Km, and T. Drangong, “Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang),” vol. 7, no. 2, 2020.
[5] A. G. S. Harahap, “Intrusion Detection And Anomaly Menggunakan Wazuh Pada Universitas Muhammadiyah Palembang”.
[6] F. Muhammad, I. Wahidah, and A. I. Irawan, “Analisis Pendeteksian Serangan Denial Of Service (DOS) Menggunakan Logika Fuzzy Metode Mamdani Pada Jaringan Internet Of Things (IOT)”.
[7] M. Nas, F. Ulfiah, and U. Putri, “Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan,” *J. Teknol. Elekterika*, vol. 20, no. 2, p. 92, Nov. 2023, doi: 10.31963/elekterika.v20i2.4536.
[8] 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. JBegaTI*, vol. 3, no. 2, Sep. 2022, doi: 10.29303/jbegati.v3i2.752.
[9] I. W. Sinaga, I. Saputra, and T. Zebua, “Pengamanan Data Nilai Pada Aplikasi E-Raport Berdasarkan Algoritma 2DES,” *KOMIK Konf. Nas. Teknol. Inf. Dan Komput.*, vol. 3, no. 1, Nov. 2019, doi: 10.30865/komik.v3i1.1604.

[10] B. Jaya, Y. Yuhandri, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. Dan Teknol.*, pp. 115–123, Dec. 2020, doi: 10.37034/jsisfotek.v2i4.32.

[11] Moh Sulthan Arief Rahmatullah, Andyana Muhandhatul Nabila, Salmaa Satifha Dewi, Vira Datry, and Fathika Afrine Azaruddin, "Implementasi SIEM dan IDS Dalam Monitoring Terhadap Ancaman Serangan Pada WEB Server," *SABER J. Tek. Inform. Sains Dan Ilmu Komun.*, vol. 2, no. 1, pp. 130–137, Dec. 2023, doi: 10.59841/saber.v2i1.666.

[12] E. Erawan and M. Salman, "Penguatan Keamanan Otomatis pada Sistem Operasi Ubuntu berbasis Image Mesin Virtual menggunakan solusi Packer," *Cakrawala Repos. IMWI*, vol. 6, no. 4, pp. 1089–1097, Aug. 2023, doi: 10.52851/cakrawala.v6i4.451.

[13] A. P. Armadhani, D. Nofriansyah, and K. Ibnutama, "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP," *J. SAINTIKOM J. Sains Manaj. Inform. Dan Komput.*, vol. 21, no. 2, p. 80, Aug. 2022, doi: 10.53513/jis.v21i2.6119.