Jurnal Informatika Terpadu

https://journal.nurulfikri.ac.id/index.php/JIT
ISSN ONLINE : 2460-8998

IMPLEMENTASI WAZUH SIEM UNTUK MANAJEMEN *LOG EVENT* DI PESANTREN TEKNOLOGI INFORMASI DAN KOMUNIKASI JOMBANG

Faruq Aziz Saputra[1], Tubagus Rizky Dharmawan[2], April Rustianto [3]

[1,2,3]Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri
Depok, Jawa barat, Indonesia 16451
faruqaziz02@gmail.com, tubagus@nurulfikri.ac.id, april.rustianto@dosen.nurulfikri.ac.id

Abstract

Information Security is essential for organizations and companies in the current digital transformation era. As a technology-oriented education, Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang requires a reliable security system, considering the increasing security risks. This research proposes the implementation of Wazuh as a Security Information And Event Management (SIEM) integrated with Telegram Bot for real-time system security detection and analysis. Wazuh was chosen because it has advantages in log management, ease of use, and strong community support. This research describes the implementation process of Wazuh, incident log visualization, and integration with Telegram Bot as an alert system. It tests attacks such as Bruteforce, DoS *Attack (SYN Flood), and SQL Injection, showing that Wazuh effectively detects and responds to potential threats. Log visualization provides benefits in terms of efficiency and effectiveness in handling security incidents. In addition, Wazuh's integration with Telegram can provide notifications via Telegram Bot in real-time. This research also involves performance testing by monitoring the CPU and memory of the Wazuh server, and results show that the CPU and memory are still within normal limits when an attack occurs.*

Keywords: *Alert System, Information Security, Log Visualization, Security Information and Event Management (SIEM), Wazuh*

Abstrak

Keamanan informasi merupakan aspek penting bagi organisasi dan perusahaan di era transformasi digital saat ini. Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang, sebagai pendidikan yang berorientasi pada teknologi, memerlukan sistem keamanan yang andal mengingat risiko keamanan informasi yang terus meningkat. Penelitian ini mengusulkan implementasi Wazuh sebagai *Security Information And Event Management (SIEM)* yang terintegrasi dengan *Telegram Bot* untuk deteksi dan analisis keamanan sistem secara *real-time*. Wazuh dipilih karena memiliki keunggulan dalam hal *log management*, kemudahan penggunaan, dan dukungan komunitas yang kuat. Penelitian ini menguraikan proses implementasi Wazuh, visualisasi log insiden, dan integrasi dengan *Telegram Bot* sebagai *alert system.* Pengujian serangan seperti *Bruteforce*, DoS *Attack (SYN Flood)*, dan *SQL Injection*, dan menunjukkan bahwa Wazuh efektif mendeteksi dan merespons ancaman potensial. Visualisasi log memberikan manfaat dalam hal efisiensi dan efektivitas dalam menangani insiden keamanan. Selain itu, integrasi Wazuh dengan Telegram dapat memberikan notifikasi melalui Telegram Bot secara *real-time*. Penelitian ini juga melibatkan pengujian kinerja dengan memantau CPU dan *memory server* Wazuh, dan menunjukkan hasil yang masih dalam batas normal saat terjadi serangan.

Kata kunci: *Alert* Sistem, Keamanan Informasi, *Security Information And Event Management* (SIEM), Visualisasi Log, Wazuh

1. PENDAHULUAN

Pada era transformasi digital saat ini, keamanan informasi menjadi hal yang sangat diperlukan bagi setiap orang maupun organisasi. Akses internet yang berkembang sangat luas memberikan akses lebih untuk memperoleh data Informasi secara cepat, mudah, dan praktis. Hal tersebut mendorong instansi maupun perusahaan untuk memanfaatkan internet agar dapat meningkatkan kinerja dan efektivitas dalam mencapai tujuan organisasi [1]. Kemudahan akses terhadap data dan informasi tanpa kesadaran yang baik akan keamanan informasi dapat menimbulkan ancaman yang dapat muncul sewaktu-waktu pada *server* yang dioperasikan oleh manajemen individu maupun organisasi, seperti pada *server* di pemerintahan, pendidikan, dan dunia usaha. [2]. Data dan informasi mempunyai hubungan yang sangat erat satu sama lain, tanpa

Diterima 22 Oktober 2024, Direvisi 25 Oktober 2024, Diterima untuk publikasi 28 Oktober 2024

data maka informasi tidak dapat tercipta dan tanpa informasi maka data tidak berguna. Oleh karena itu, perlindungan data dan informasi di dalam perusahaan merupakan hal yang penting [3].

Menurut Peraturan Menteri Komunikasi dan Informatika No.4 Tahun 2016 tentang Standar Sistem Manajemen Keamanan Informasi (SMKI), bahwa setiap penyelenggara sistem elektronik harus mematuhi SMKI dengan memegang nilai CIA (*Confidentiality, Availability, and Integrity*) [4]. Pesantren Teknologi Informasi Komunikasi (PeTIK) Jombang yang merupakan lembaga pendidikan berbasis teknologi yang memanfaatkan berbagai *resource* teknologi untuk memaksimalkan kinerja agar dapat mencapai tujuan dengan efektif. Oleh karena itu, sistem dan teknologi informasi yang ada di Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang harus mampu untuk menyediakan informasi yang cepat dan akurat.

Keamanan dari sistem dan teknologi harus dilindungi untuk menjaga aset informasi dari serangan atau penyalahgunaan. Kemudahan akses informasi dapat menimbulkan permasalahan baru yaitu ancaman, serangan, dan pencurian data oleh pihak-pihak yang tidak beretika. Data informasi yang penting sering kali dicuri oleh peretas melalui web *server* yang memiliki kelemahan keamanan yang signifikan. Untuk itu, diperlukan upaya perbaikan sistem keamanan siber mencegah penyalahgunaan data secara ilegal [5].

Berdasarkan hasil observasi di lapangan, banyaknya aktivitas yang dilakukan oleh mahasantri dalam menggunakan komputer untuk mengakses internet, memungkinkan adanya permasalahan yang muncul terkait sistem keamanan jaringan di Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang. Diantaranya, adanya indikasi serangan *ssh password guessing* untuk mengakses *user*, melakukan *request* akses ke web *server* secara berlebihan sehingga menyebabkan *website* mahasantri yang di*host*ing menjadi *down*, dan adanya indikasi penggunaan *software* aplikasi yang terindikasi *malware*. Berdasarkan hal tersebut, maka solusi yang dapat dimanfaatkan yaitu menggunakan *system information and event management* (SIEM) yang dapat memberikan informasi log yang terjadi di jaringan untuk menjaga keamanan informasi pada jaringan di lingkungan Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang dan visualisasi Log *monitoring* lebih mudah dipahami. *Security Information And Event Management* (SIEM) termasuk salah satu teknologi keamanan informasi yang mengadopsi metodologi untuk membaca dan menganalisis data atau informasi yang masuk ke dalam *server* yang diakses dengan izin maupun tanpa izin [2]. Data yang terkumpul akan dianalisis secara *realtime* dan terpusat yaitu berupa log dari berbagai *event* log berbagai aplikasi dan perangkat keamanan seperti *server*, *network*, *firewall*, dan sebagainya [6].

Beberapa pemanfaatan SIEM telah dibuktikan berdasarkan penelitian terdahulu dan memberikan dampak yang positif. Pada tahun 2018, Mustafa Dzul Akmal, dkk melakukan penelitian dengan judul Implementasi *Security Information And Event Management* (SIEM). Menggunakan OSSIM, dengan hasil OSSIM dapat melakukan analisa data yang dihasilkan dari setiap penyerangan yang terjadi dalam bentuk grafik maupun diagram. Selanjutnya pada tahun 2021, Wahluf Abidian melakukan penelitian serupa menggunakan *framework* Splunk untuk membangun SIEM berdasarkan log *firewall traffic* jaringan UII. Hasil dari penelitian ini adalah visualisasi non-*cluster*, visualisasi *with-cluster* serta sistem peringatan yang terintegrasi dengan bot Telegram. Visualisasi *cluster* tersebut memudahkan administrator untuk memahami informasi pada *traffic* jaringan UII. Kemudian pada bulan Maret tahun 2023, Nazar Firman Pratama melakukan penelitian yang bertujuan untuk membangun Sistem Deteksi Dini Keamanan Informasi DISKOMINFO Kabupaten Bandung menggunakan Wazuh, hasilnya adalah Wazuh dapat memonitor dan mendeteksi serangan secara *realtime* dengan melihat laporan *event* atau aktivitas pada aplikasi tersebut [7].

Dalam menerapkan *alert* sistem, sebaiknya informasi *alert* dapat diimplementasikan secara mobile guna menyediakan akses informasi kapan dan dari mana saja, sehingga administrator mempunyai kebebasan dalam *monitoring* untuk mencapai efisiensi yang maksimal. Oleh karena itu dibutuhkan integrasi antara *alert* sistem pada Wazuh dengan menggunakan aplikasi Telegram. Telegram merupakan sebuah aplikasi yang dapat diakses pada *smartphone* ataupun perangkat komputer. Pada Telegram, terdapat fitur bot yang dapat diintegrasikan dengan Wazuh melalui API untuk membantu menerima informasi secara real time saat *alert* muncul.

Berdasarkan temuan masalah di Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang, serta merujuk pada penelitian terdahulu, maka penelitian ini fokus dalam implementasi Wazuh sebagai *Security Information And Event Management* (SIEM) sebagai solusi untuk mendeteksi dan menganalisis keamanan sistem informasi data di PeTIK Jombang dengan harapan sistem ini dapat membantu mendeteksi, menganalisis, dan memonitor sistem data informasi secara *real-time*, serta mempermudah dalam manajemen insiden risiko di PeTIK Jombang.

Cyber Security

Cyber Security adalah berbagai alat, kebijakan, konsep keamanan, perlindungan keamanan, proses manajemen risiko, pelatihan praktik, dan teknologi yang dapat digunakan untuk memberikan perlindungan terhadap lingkungan, organisasi dan aset pengguna dalam menjamin keamanan *cyber* [8]. Tanggung jawab dalam *Cyber Security* terbagi menjadi beberapa tingkatan, mulai dari tanggung jawab pribadi hingga tingkat kenegaraan. Pada tingkat pribadi, setiap orang bertanggung jawab menjaga keamanan identitasnya, data dan perangkatnya. Kemudian di tingkat korporat, setiap orang bertanggung jawab menjaga reputasi perusahaan, data dan keamanan pelanggan. Selanjutnya, di tingkat tertinggi atau negara, tanggung jawabnya menjaga

keamanan di tingkat nasional, menjaga kesejahteraan dan keselamatan seluruh warga negara.

Information Security

Keamanan informasi adalah tindakan untuk menjaga aset informasi dari ancaman potensial. Keamanan informasi secara tidak langsung menjamin kelangsungan usaha, mengurangi risiko yang timbul, dan memungkinkan meningkatkan keuntungan atas investasi. Sesuai dengan ISO/IEC 17799:2005 tentang Sistem Manajemen Keamanan Informasi, keamanan informasi mengatasi berbagai ancaman untuk menjamin kelangsungan usaha, meminimalkan risiko usaha, serta meningkatkan investasi dan peluang usaha [9]. Keamanan informasi bertanggung jawab dalam mengamankan informasi pada infrastruktur IT dari berbagai ancaman yang mungkin terjadi. Organisasi perlu menerapkan *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) atau biasa disebut sebagai CIA Triad. *Confidentiality* adalah memastikan privasi terhadap data terjaga serta membatasi akses dengan menerapkan metode enkripsi yang terotentikasi. Kemudian *Integrity* menjamin sebuah informasi akurat dan kredibel. Sedangkan *Availability* menjamin setiap informasi dapat selalu diakses pihak yang memiliki otoritas.

Ancaman Jaringan (*Network Threat*)

Jaringan komputer pada sebuah organisasi atau perusahaan menghubungkan berbagai perangkat dan layanan IT yang ada di dalam instansi. Berbagai perangkat IT yang dimiliki oleh organisasi atau Perusahaan merupakan sebuah *value* yang harus dijaga dari berbagai ancaman yang dapat merugikan. Sehingga sebuah instansi harus memiliki sistem untuk mencegah terjadinya serangan yang dapat mengganggu keamanan jaringan pada sebuah instansi [11]. Berikut beberapa contoh serangan yang sering digunakan untuk menyerang berbagai infrastruktur jaringan, diantaranya:

a. *Bruteforce*

Brute force adalah ancaman jaringan untuk meretas *password*. Ancaman ini dilakukan dengan cara mencoba semua kemungkinan dari kombinasi yang umum digunakan sebagai *password*.

b. SQL *Injection*

SQL *Injection* merupakan metode injeksi dan penyalahgunaan keamanan *database* yang digunakan untuk memasukkan sebuah parameter pada *website* ataupun sebuah *statement query* secara sengaja dengan tujuan untuk mendapatkan data *user*.

c. DDoS *Attack*

Distributed Denial of Service (DDoS) adalah serangan yang ditujukan pada organisasi maupun perusahaan. Bentuk serangan ini adalah membanjiri sumber daya jaringan korban dengan melakukan mengirimkan banyak *packet* sehingga infrastruktur jaringannya tidak mampu memproses *traffic* yang sah pada jaringannya.

Risk Assessment

Risk Assessment adalah proses identifikasi penilaian risiko untuk menentukan bahaya dan risiko apa saja yang mungkin terjadi pada sistem TI. Hasil dari *risk assessment* digunakan untuk membantu identifikasi kontrol yang sesuai, dan meminimalisir dampak yang ditimbulkan selama proses *risk mitigation*. Dalam *risk assessment*, terdapat empat tahap utama, yaitu:

a. *Threat Identification* (Identifikasi Risiko Ancaman)

Ancaman atau *threat* adalah kemungkinan yang dapat menimbulkan kerugian dan biasanya berasal dari suatu *threat source* yang melakukan serangan ke dalam sistem. Ancaman atau *threat* ini tidak dapat menghasilkan risiko ancaman apabila tidak terdapat celah yang terbuka pada suatu sistem.

b. *Risk Mitigation* (Mitigasi Risiko)

Tahap ini meliputi akses prioritas, evaluasi dan implementasi sistem guna meminimalisir risiko dari proses *risk assessment*. Tahap mitigasi risiko bertujuan memahami kemungkinan dan dampak dari setiap risiko yang teridentifikasi.

c. *Evaluation and Monitoring* (Evaluasi dan Pemantauan)

Tahap evaluasi dan pemantauan bertujuan untuk menilai tingkat risiko, kemudian memutuskan tindakan apa yang perlu diputuskan untuk mengelola risiko tersebut. Tahap ini, sistem, komponen dan *software* yang dimiliki akan diperbarui atau update dengan versi terbaru.

d. *Security Strategy Defence in Depth* (Pertahanan Strategi Keamanan Secara Mendalam)

Ketika menerapkan sistem keamanan informasi, organisasi biasanya menggunakan strategi *defence in depth* yang memandang keamanan dari berbagai sudut. *Defence in depth* adalah sebuah konsep keamanan yang memiliki banyak lapisan perlindungan untuk meningkatkan keamanan sistem secara keseluruhan.

Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah aplikasi perangkat lunak atau perangkat yang memantau sistem atau aktivitas jaringan untuk pelanggaran kebijakan atau aktivitas jahat dan menghasilkan laporan ke sistem manajemen [12]. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, dengan melakukan analisis dan mencari bukti dari percobaan. IDS sendiri muncul dengan beberapa jenis dan pendekatan yang berbeda akan tetapi tetap dengan tujuan yang sama yaitu

mendeteksi *traffic* yang mencurigakan di dalam sebuah jaringan.

Security Information And Event Management (SIEM)

SIEM diperkenalkan pertama kali oleh Mark Nicolett dan Amrit Williams dari Garnet pada tahun 2005. SIEM merupakan sebuah teknologi yang berfungsi untuk mendeteksi berbagai ancaman dan insiden dengan cara mengumpulkan Log *real-time* dari sebuah aktivitas dan melakukan analisis Log keamanan dari berbagai jenis Log yang berasal dari berbagai perangkat yang terhubung di jaringan [13]. SIEM diperlukan untuk pengumpulan dan analisis data otomatis. Data berasal dari berbagai sumber diantaranya sistem *Intrusion Detection Systems* (IDS), *Data Loss Prevention* (DLP) *router*, *firewall*, *server*, *user workstation* dan lainnya. Ketika suatu *event* terjadi, maka log akan muncul dari perangkat yang terhubung ke SIEM. Log yang dikirim tersebut merupakan data yang sangat sulit untuk dibaca dan dianalisis, dengan menggunakan SIEM kita dapat dengan mudah menganalisis log yang dikirim dari perangkat-perangkat tersebut. Dengan demikian memungkinkan bagi kita untuk mengontrol jaringan dengan cepat dan secara terpusat. [13]

Wazuh

Wazuh merupakan sebuah *tools* SIEM Open *Source* yang berfungsi sebagai sistem deteksi intrusi yang berbasis *host* (*endpoint*). Wazuh merupakan sebuah aplikasi *monitoring* yang berfungsi untuk mendeteksi ancaman pada *server*, memonitor integritas *server*, hingga melaporkan insiden yang ada pada *server*. Wazuh terdiri dari 2 (dua) bagian yaitu Wazuh-*Server* dan Wazuh *Agent*. Wazuh *server* merupakan perangkat yang digunakan sebagai manajemen agen dan *dashboard* sistem *monitoring* baik *file integrity*, intrusi, maupun log. Sedangkan Wazuh *agent* merupakan perangkat yang di-*install* pada perangkat *endpoint* untuk melakukan pembacaan sistem, pengumpulan log serta mengirimkan ke Wazuh *server* [14].

Telegram

Telegram adalah layanan perpesanan yang sangat populer, dengan opsi untuk berbicara dengan orang-orang dalam grup atau secara pribadi di *cloud*. Bot merupakan salah satu fitur telegram yang paling banyak digunakan, dan API Telegram bot ini dapat dibuat oleh siapa saja dan dipakai untuk integrasi dengan sistem lainnya. Telegram Bot API adalah sebuah perangkat lunak yang digunakan untuk berinteraksi dengan pengguna dan sebuah sistem yang membutuhkan sebuah *Application Programming Interface* (API). Integrasi sistem wazuh dengan bot telegram berfungsi untuk menampilkan hasil data *alert* dari data wazuh ke Telegram bot. Sistem integrasi menggunakan API yang sudah disediakan oleh BotFather Telegram untuk menghubungkan Wazuh dan Telegram [15].

2. METODE PENELITIAN

2.1 Rancangan Penelitian

Rancangan penelitian ini dibuat sebagai langkah awal untuk menguraikan lebih detail tentang apa yang akan dilakukan dalam penelitian mencakup jenis penelitian, metode analisis, metode pengumpulan data, lingkungan pengembangan, , metode pengujian dan analisis.

2.1.1 Jenis Penelitian

Dalam Proses penelitian ini menggunakan jenis penelitian deskriptif observasional. Metode penelitian deskriptif observasional adalah penelitian dengan menggambarkan suatu keadaan atau masalah yang digali melalui pengamatan yang terjadi di lapangan (*Field Research*) secara objektif. Jenis penelitian deskriptif yang digunakan dalam penelitian ini adalah studi kasus (*Case Study*), yaitu implementasi SIEM Wazuh di Pesantren Teknologi Informasi Komunikasi (PeTIK) Jombang dengan harapan sistem ini dapat membantu mendeteksi, menganalisis, dan memonitor sistem data informasi secara *real-time*, serta mempermudah dalam manajemen insiden risiko di Pesantren Pesantren Teknologi Informasi Komunikasi (PeTIK) Jombang.

2.1.2 Metode Analisis

Peneliti menggunakan metode analisis kuantitatif dalam penelitian ini. Metode kuantitatif digunakan ketika menguji sistem dengan pengujian kerentanan. Pendekatan kuantitatif membantu untuk memahami secara mendalam evaluasi desain sistem yang telah dibuat.

2.1.3 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini menggunakan metode observasi, dimana peneliti melakukan pengamatan secara langsung terhadap situasi dan peristiwa yang ada di lapangan. Dalam studi kasus ini, observasi dilakukan peneliti adalah observasi sistematik dimana peneliti melakukan pengamatan dan pengumpulan data secara sistematis di lapangan.

2.1.4 Lingkungan Pengembangan

a) Wazuh *Server*

Spesifikasi Wazuh *Server* dapat dilihat pada tabel 1 berikut.

Tabel 1. Spesifikasi Wazuh *Server*

	Spesifikasi
Processor	4 vCPU
Hard Disk	50 GB
Memory	8 GB
Operating System	Ubuntu-22.04LTS
Software	Wazuh 4.7.2

b) Wazuh *Agent*

Tabel 2 di bawah menunjukkan spesifikasi Wazuh *Agent*.

Tabel 2. Spesifikasi Wazuh *Agent*

Spesifikasi	
Processor	Intel i7 Gen 11th
Hard Disk	SSD 256 GB
Memory	16 GB
Operating System	Windows 11
Software	Wazuh *Agent*

c) PC Admin

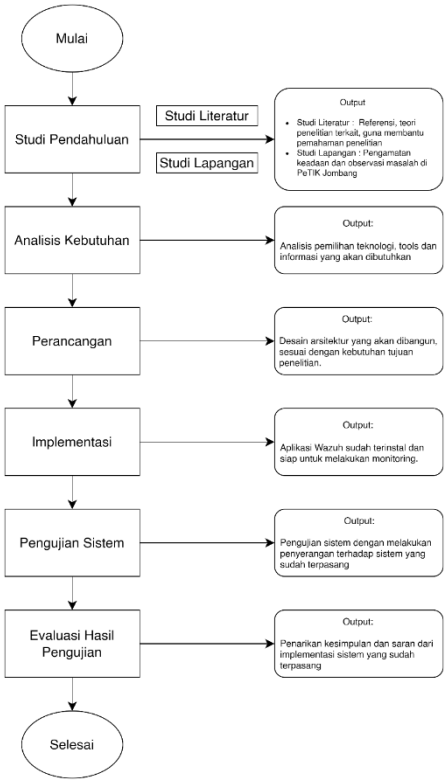
Tabel 3 berikut menunjukkan spesifikasi untuk PC Admin.

Tabel 3. Spesifikasi PC Admin

Spesifikasi	
Processor	Intel i7 Gen 11th
Hard Disk	SSD 256GB
Memory	16 GB
Operating System	Windows 11
Software	Browser

2.2 Tahapan Penelitian

Pada bagian ini dijelaskan bagaimana tahapan penelitian secara umum yang dilakukan. Tahapan penelitian dapat dilihat pada gambar 1.



Gambar 1. Tahapan Penelitian

a. Studi Pendahuluan

Tahap ini melibatkan pengumpulan informasi dan pemahaman awal tentang topik penelitian, studi literatur, mencari referensi penelitian terkait guna membantu dalam pemahaman penelitian, dan melakukan studi lapangan untuk melakukan pengamatan dan memahami objek penelitian.

b. Analisis Kebutuhan

Tahap analisis kebutuhan melibatkan identifikasi dan pemahaman terhadap kebutuhan dan masalah yang akan diselesaikan dalam penelitian ini. Melakukan identifikasi tujuan utama penelitian, kebutuhan, serta kendala yang mungkin dihadapi dalam implementasi solusi. Analisis ini membantu dalam merumuskan strategi dan pendekatan yang tepat untuk menyelesaikan masalah yang diteliti.

c. Perancangan

Pada tahap ini, Anda akan merancang solusi SIEM menggunakan Wazuh berdasarkan hasil analisis kebutuhan. Ini mencakup desain infrastruktur, integrasi dengan sistem yang ada, pengaturan konfigurasi, perencanaan implementasi dan simulasi serangan.

d. Implementasi

Tahap implementasi melibatkan penerapan solusi SIEM Wazuh ke dalam lingkungan pesantren PeTIK Jombang. Ini bisa melibatkan instalasi perangkat lunak, konfigurasi sistem, pengaturan aturan dan kebijakan keamanan, serta integrasi dengan infrastruktur TI yang ada.

e. Pengujian Sistem

Setelah implementasi, tahap pengujian sistem dilakukan untuk memastikan bahwa solusi SIEM berfungsi sebagaimana mestinya. Ini mencakup pengujian fungsionalitas, keandalan, kinerja, dan keamanan sistem.

f. Evaluasi Hasil

Tahap terakhir adalah evaluasi hasil dari implementasi SIEM Wazuh. Mengevaluasi sejauh mana solusi tersebut memenuhi tujuan yang ditetapkan, mengidentifikasi kekurangan atau masalah yang mungkin muncul, dan merumuskan rekomendasi untuk perbaikan atau peningkatan selanjutnya.

2.3 Metode Pengujian

2.3.1 Pengujian Serangan *Security*

Serangan yang akan diuji dalam penelitian ini adalah:

a) DoS *Attack* (*denial-of-service*)

*Denial-of-Service (*DoS*) Attack* merupakan bentuk serangan siber yang bertujuan untuk membuat layanan, atau jaringan tidak tersedia bagi pengguna. Tujuan utama dari serangan DoS adalah menghabiskan *bandwitch*, mengganggu koneksi antar *server* dan mengganggu kinerja sistem. Salah satu

sasaran utama serangan DoS adalah mengganggu layanan yang dijalankan oleh *host* yang terhubung ke internet.

b) SQL *Injection*

SQL *Injection* adalah serangan yang digunakan untuk memasukkan sebuah perintah SQL *query* secara sengaja dengan tujuan untuk mendapatkan data dari *database*. Untuk meningkatkan efisiensi serangan, penyerang biasanya menggunakan alat bantu seperti Sqlmap yang tersedia dalam sistem operasi Kali Linux, yang memungkinkan melakukan serangan SQL *injection* secara otomatis.

c) *Bruteforce*

Pengujian *bruteforce* diterapkan pada *Wazuh Agent* dengan tujuan menyerang kombinasi *username* dan *password* (*login failure*). Proses *login failure* dilakukan dengan mengubah *username* dan *password* secara *random* melakukan *trial* dan *error*, yang berakibat kegagalan akses pengguna ke *server*. Demikian juga dengan membatasi akses ke akun tertentu melalui perintah yang salah diberikan kepada *server*.

2.3.2 Pengujian Performance

Parameter pengujian yang terapkan dalam penelitian ini adalah:

a) CPU

Perhitungan kinerja CPU dilakukan dengan menggunakan *tools* SNMP untuk memantau penggunaan CPU yang sudah di-*install* wazuh pada *server*.

b) *Memory*

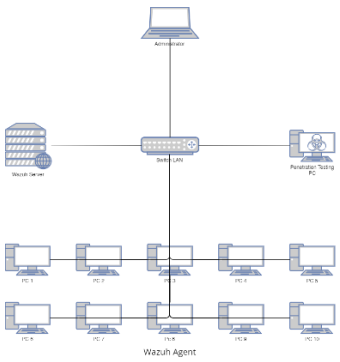
Perhitungan kinerja memori dilakukan dengan menggunakan *tools* SNMP untuk menghitung jumlah total memori yang tersedia seta besar penggunaan memori yang terpakai.

3. HASIL DAN PEMBAHASAN

Hasil penelitian dan pembahasan penelitian menjelaskan tentang hasil implementasi sistem yang dirancang berdasarkan masalah dan tujuan penelitian yang telah dirumuskan.

3.1 Implementasi Sistem

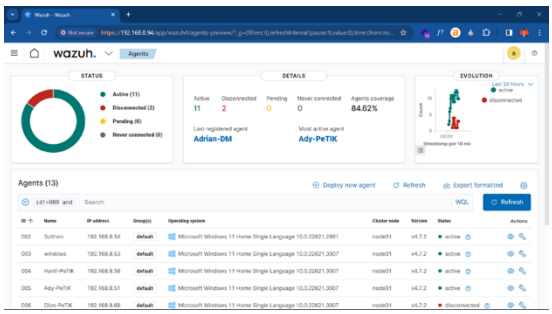
A. Desain Topologi Jaringan



Gambar 2. Desain Topologi Jaringan

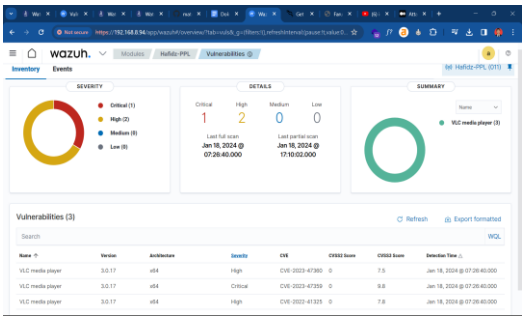
Berdasarkan gambar 2, simulasi menggunakan jaringan LAN (*Local Area Network*) sederhana untuk menstimulasikan Komunikasi yang terjadi antara *host* dan *server* dimana *host* dan *server* terhubung pada suatu jaringan yang sama. Pada simulasi ini terdapat *host* yang di *install* web *server* sebagai *client* dan *host* yang melakukan penyerangan dengan menggunakan sistem operasi *Kali Linux*.

B. Tampilan Wazuh



Gambar 3. Tampilan *Dashboard* Wazuh

Pada gambar 3, tampilan wazuh *dashboard* dan *list Agent* wazuh yang sudah terhubung dengan wazuh *server*. Kemudian Wazuh *server* mengumpulkan informasi dan data dari aktivitas sistem dan jaringan pada *server* tersebut. Informasi yang dikumpulkan dapat meliputi log sistem, *file*, *port* yang terbuka, aktivitas *user*, dan lain sebagainya kemudian ditampilkan pada halaman wazuh *dashboard*.



Gambar 4. Tampilan *Dashboard Vulnerabilities*

Pada gambar 4, tampilan *dashboard vulnerabilities* pada *agent* wazuh yang terhubung dengan wazuh. *Agent* Wazuh akan menarik data inventaris perangkat lunak dan mengirimkan informasi ke *server*, di mana informasi tersebut dikorelasikan dengan basis data CVE (*Common Vulnerabilities and Exposure*) yang terus diperbarui, untuk mengidentifikasi tingkat kerentanan perangkat lunak yang digunakan.

C. Integrasi Bot Telegram

Gambar 5. Sistem Integrasi Bot Telegram

Pada gambar 5, proses Wazuh mengirimkan notifikasi ketika terjadi serangan secara *realtime*. Wazuh mengirimkan deskripsi *alert* pada telegram bot dengan memanfaatkan API KEY dan CHAT ID yang didapat dari Telegram BotFather, kemudian diintegrasikan dengan pemrograman python yang dibuat pada sistem wazuh *server*. Selanjutnya akan muncul deskripsi *alert* pada Telegram *user* sesuai dengan kode program python yang dibuat.

3.2 Pengujian Sistem

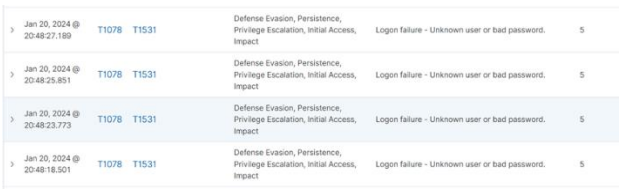
A. *Vulnerabilities Assessment*

a. *Brute force*

Pengujian *bruteforce* diterapkan pada *Wazuh Agent* dengan tujuan menyerang kombinasi *username* dan *password* (*login failure*). Proses *login failure* dilakukan dengan mengubah *username* dan *password* secara *random* melakukan trial dan eror, yang berakibat kegagalan akses pengguna ke *server*. Pada pengujian ini, serangan *bruteforce* dilakukan terhadap gateway salah satu agen yang sudah dipasang web *server*. Langkah Pertama adalah membuka web DVWA yang sebelumnya sudah di pasang pada agen Wazuh dan mencoba *login* dengan mencoba berbagai kombinasi akses masuk seperti *username* atau *password*, yang dapat dilihat pada gambar 6.

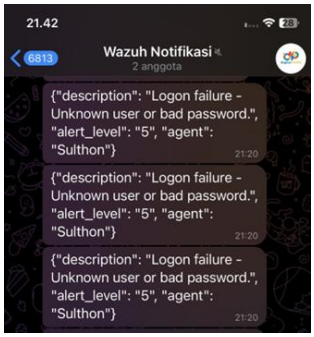
Gambar 6. *Website* DVWA Pada *Agent*

Selanjutnya, Wazuh *Dashboard* mendeteksi aktivitas serangan *bruteforce* yang dilakukan *attack*er terhadap Web pada Wazuh *Agent*.



Gambar 7. Hasil Pengujian *Bruteforce*

Pada gambar 7 menunjukkan hasil pengujian serangan *bruteforce*, yaitu adanya upaya *login* yang gagal menggunakan *username* atau *password* yang tidak valid.



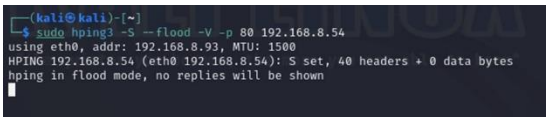
Gambar 8. Notifikasi Bot Wazuh Telegram

Pada gambar 8 menunjukkan hasil notifikasi *login failure* pada bot telegram yang sudah diintegrasikan dengan wazuh.

b. DoS *Attack* (SYN *Flood*)

SYN *Flood* adalah salah satu serangan DoS *Attack* yang bertujuan untuk mengganggu kinerja *server* dengan mengirimkan permintaan SYN palsu. Dalam pengujian ini, dilakukan serangan SYN *Flood* terhadap Wazuh *Agent* yang ada di Pesantren PeTIK Jombang. Serangan yang ditunjukkan pada gambar 9 dilakukan menggunakan kali Linux dengan menggunakan perintah sebagai berikut

sudo hping3 -S –flood -V -p 80 192.168.8.54



Gambar 9. Serangan SYN *Flood*

Gambar 10. Hasil Pengujian SYN *Flood*

Pada gambar 10 menggambarkan hasil pengujian bahwa pada *Wazuh Dashboard* telah terdeteksi serangan DoS *Attack* yang mendeteksi serangan terhadap mySQL pada *port* 3306.

c. SQL *Injection*

SQL *Injection* adalah serangan yang digunakan untuk memasukkan sebuah perintah SQL *query* secara sengaja dengan tujuan untuk mendapatkan data dari *database*. Untuk meningkatkan efisiensi serangan, penyerang biasanya menggunakan alat bantu seperti Sqlmap yang tersedia dalam sistem operasi Kali Linux, yang memungkinkan melakukan serangan SQL *injection* secara otomatis. Pada pengujian ini, dilakukan serangan terhadap *Wazuh Agent* yaitu *website* DVWA yang dipasang pada *server local* https://192.168.8.54/DVWA menggunakan perintah yang dapat dilihat pada gambar 11.

Sqlmap -u https://192.168.8.54 –dbs

Gambar 11. Serangan SQL *Injection*

Kemudian pada Wazuh *Dashboard* akan mendeteksi tindakan serangan SQL *Injection* yang dilakukan *attack*er terhadap Wazuh *Agent* (*website* milik *agent*).

Gambar 12. Serangan SQL *Injection*

Pada gambar 12 menunjukkan hasil pengujian yang menyatakan bahwa pada Wazuh *Dashboard* telah terdeteksi serangan SQL *Injection*.

Tabel 4. Hasil Pengujian Serangan

No	Pengujian	Pengujian	Hasil	Keterangan
1	*Bruteforce*	Menampilkan Log di Wazuh *Dashboard*	Sesuai Harapan	*Dashboard* wazuh memunculkan hasil *alert system* yaitu *login failure* atau terdeteksi kesalahan *login* dalam menggunakan *user* atau *password* yang salah.
		Notifikasi *Alert* Telegram Bot	Sesuai Harapan	Menunjukkan hasil notifikasi pada bot telegram yaitu keterangan dengan deskripsi "*login failure*-Unkown *user* or bad *password*" dengan *alert* level 5 dan nama agen Sulthon.
2	DoS *Attack* (SYN *Flood*)	Menampilkan Log di Wazuh *Dashboard*	Sesuai Harapan	*Dashboard* wazuh memunculkan hasil *alert system* yaitu terdeteksi melakukan scan susspicious inbound to mySQL pada *port* 3306.
3	SQL *Injection*	Menampilkan Log di Wazuh *Dashboard*	Sesuai Harapan	*Dashboard* wazuh memunculkan hasil *alert system* yaitu SQL *injection* attemp dengan level kerentenan yaitu 6.
		Notifikasi *Alert* Telegram Bot	Tidak Sesuai Harapan	Tidak muncul notifikasi atau keterangan *alert system* pada telegram bot

Pada tabel 4, menunjukkan hasil pengujian serangan secara keseluruhan dan hasil yang didapat untuk menampilkan log di wazuh *dashboard* sesuai harapan ekspektasi peneliti, dan untuk notifikasi *alert* telegram dari 3 serangan yang diuji hanya 1 yang masuk ke dalam notifikasi telegram bot yaitu serangan *brute force*, sementara untuk 2 serangan lainnya perlu dilakukan konfigurasi lebih lanjut.

B. Performance *Assessment*

Pengujian performa dilakukan untuk mengukur keadaan perangkat saat menerima serangan, dan membandingkannya dengan keadaan sebelum perangkat menerima serangan. Pengujian performa dilakukan terhadap dua perangkat berbeda, yaitu CPU dan *Memory*.

a. Kinerja CPU

Pertama, pengujian dilakukan terhadap kinerja CPU. Hasil pengujian diwakili oleh persentase yang ditunjukkan pada tabel 5.

Tabel 5. Hasil Pengujian CPU

Server	Sebelum Pengujian	Setelah Pengujian
Agents	0.0% - 15%	0.0% - 60%

Berdasarkan tabel 5, kinerja CPU pada kondisi normal atau sebelum terjadinya serangan berada pada *range* 0.0% hingga 15%, persentase ini menunjukkan bahwa CPU berada dalam kondisi normal. Kemudian, setelah dilakukan beberapa kali percobaan serangan berbeda, persentase penggunaan CPU diketahui meningkat menjadi 60%. Hal ini menunjukkan bahwa kinerja CPU bertambah akibat adanya aktivitas serangan dari *user*. Penambahan beban CPU terjadi mengikuti banyaknya jumlah *event* (serangan) yang terjadi dalam satu waktu terhadap *agent* termasuk beberapa serangan dari publik yang terdeteksi berdasarkan hasil pemantauan pada *agent* Wazuh dan mempertimbangkan beberapa faktor lainnya yang mungkin terjadi pada sistem operasi.

b. *Memory*

Setelah melakukan analisis perbandingan kinerja pada CPU, selanjutnya dilakukan pula analisis perbandingan kinerja pada perangkat memori. Hasil pengujian diwakili oleh persentase yang ditunjukkan pada Tabel 6.

Tabel 6. Hasil Pengujian *Memory*

Server	**Sebelum Pengujian**	**Setelah Pengujian**
Agents	0.0% - 40.0%	0.0% - 40.0%

Berdasarkan tabel 6, diketahui bahwa kinerja memori tidak mengalami peningkatan atau perubahan pada saat terjadinya serangan. Persentase penggunaan memori sebelum terjadi serangan adalah 0.0% hingga 40.0% atau dalam keadaan normal. Setelah dilakukan beberapa kali serangan, persentase penggunaan memori tetap berada pada *range* 0.0% hingga 40.0%. Hal ini menunjukkan bahwa kinerja memori tetap berjalan normal dengan *write speed memory* yang sama terhadap kondisi sebelum serangan ataupun setelah terjadi serangan.

3.3 Analisis

Dari hasil implementasi Wazuh hingga pengujian serangan yang dilakukan, dilakukan analisis sebagai berikut. Pertama, visualisasi pada Wazuh *Dashboard* memberikan pemahaman yang lebih baik dalam menghasilkan representasi grafis dari log insiden, yang membantu pengguna mengidentifikasi ancaman keamanan dengan lebih efektif. Kedua, integrasi aplikasi Wazuh dengan bot Telegram sebagai sistem peringatan memberikan respons *real-time* terhadap potensi ancaman keamanan. Log yang ditangkap Wazuh secara *real-time* dikirimkan ke bot Telegram lengkap dengan keterangan dan tingkat level peringatan sesuai dengan potensi ancaman keamanan. Ketiga, pada pengujian pertama, serangan *Brute force* dilakukan pada situs web DVWA yang sebelumnya di-*install* di Wazuh *agent*. Serangan ini bertujuan untuk membobol *username* dan *password login* pengguna. Serangan dilakukan empat kali: dua kali serangan gagal *login password* dan dua kali serangan gagal *login username*. Keempat serangan tersebut berhasil dideteksi oleh Wazuh, dan serangan ini juga terdeteksi sebagai *Request Time Out* (RTO) akibat gangguan koneksi internet saat pengguna mengakses *server* pada *agent*.

Selanjutnya, pada pengujian serangan kedua, dilakukan DoS *Attack* menggunakan SYN *Flood*, yang melemahkan respons *server*. Secara *default*, Wazuh tidak mendeteksi jenis serangan ini, sehingga Suricata diperlukan sebagai *network base* yang dapat mengenali DoS. Suricata bekerja dengan menyimpan log serangan DoS yang kemudian dikirim ke Wazuh untuk diidentifikasi. Berdasarkan pengujian ini, Wazuh mampu memantau dan mengidentifikasi serangan DoS dengan bantuan Suricata. Kemudian, pada pengujian ketiga, serangan SQL *Injection* dilakukan pada situs web DVWA yang di-*install* di Wazuh *agent*, bertujuan menyalahgunakan keamanan *database*. Pengujian ini menunjukkan bahwa Wazuh mampu mengenali semua serangan secara *real-time*, baik dari pengguna maupun dari luar.

Berikutnya, pemantauan kinerja CPU menunjukkan bahwa CPU berada dalam kondisi normal pada kisaran 0.0%-15%. Setelah serangan pada *agent* (*Gateway* dan *Website*), kinerja CPU meningkat hingga 0.0%-60%, yang disebabkan oleh peningkatan aktivitas pada *server* yang menambah beban kerja CPU. Terakhir, selain pengukuran kinerja CPU, juga dilakukan pengukuran kinerja memori. Memori dikatakan normal pada kisaran 0.0%-40.0%, dan hasil pengujian menunjukkan tidak ada peningkatan persentase sebelum maupun setelah serangan, menandakan memori bekerja optimal dengan kecepatan tulis yang sama baik sebelum maupun sesudah serangan.

4. KESIMPULAN

Penelitian ini bertujuan untuk mengimplementasikan Wazuh dalam pengelolaan dan pemantauan keamanan jaringan, menampilkan visualisasi berdasarkan log insiden, serta mengintegrasikan aplikasi Wazuh dengan bot Telegram sebagai sistem peringatan (*alert system*). Berdasarkan hasil yang diperoleh, penelitian ini berhasil mengimplementasikan Wazuh sebagai alat yang efektif dalam mengelola dan memonitor keamanan pada jaringan yang diteliti. Dengan menggunakan Wazuh, penelitian menunjukkan bahwa sistem mampu mendeteksi dan merespons berbagai potensi ancaman keamanan, seperti serangan *Brute force*, DoS *Attack*, dan SQL *Injection*, sesuai dengan harapan penelitian. Visualisasi yang dihasilkan dari log insiden pada jaringan juga memberikan pemahaman yang lebih baik terhadap pola keamanan, sehingga tujuan penelitian dalam menciptakan representasi grafis yang membantu pengguna mengidentifikasi ancaman keamanan tercapai dengan baik. Integrasi aplikasi Wazuh dengan bot Telegram sebagai *alert system* terbukti memberikan respons *real-time* terhadap potensi ancaman keamanan, yang meningkatkan efisiensi dalam tindakan tanggap terhadap insiden yang terdeteksi.

Selama uji serangan, persentase kinerja CPU meningkat dari 0.0%-15% menjadi 0.0%-60% akibat jumlah aktivitas di dalam *server* yang menambah beban kerja pada CPU, sedangkan kinerja memori tetap dalam keadaan normal dengan persentase 0.0%-40.0%, menunjukkan *write speed memory* yang sama pada kondisi *server*, baik sebelum maupun sesudah serangan. Untuk saran, penelitian selanjutnya disarankan meningkatkan fungsionalitas Wazuh, terutama melalui eksplorasi dan pengembangan fitur-fitur baru yang sesuai dengan kebutuhan jaringan tertentu. Selain itu, pengoptimalan visualisasi log insiden melalui peningkatan representasi grafis dan analisis data juga perlu diteliti untuk membantu pengguna dalam memahami dan merespons ancaman keamanan. Integrasi Wazuh dengan platform selain Telegram akan meningkatkan fleksibilitas dan kegunaan aplikasi. Terakhir,

studi kasus yang lebih kompleks atau jaringan yang lebih besar dapat menjadi fokus penelitian untuk menguji dan mengembangkan aplikasi Wazuh dalam konteks yang lebih luas.

DAFTAR PUSTAKA

[1] N. Firman Pratama, "Perancangan Sistem Deteksi Dini Keamanan Informasi Diskominfo Kabupaten Bandung," *Jurnal Teknik Informatika Dan Sistem Informasi*, Vol. 10, No. 1, Pp. 808–820, 2023, [*Online*]. Available: Http://Jurnal.Mdp.Ac.Id

[2] Muhammad Alfandi, "Analisa Security Information And Event Management (Siem) Menggunakan Elastic Stack Siem Dan Splunk," Pekanbaru, 2022.

[3] T. Suryantoro And D. F. Sari, "Analisa Serangan Terhadap Port 80 Webserver Dengan Siem Wazuh Menggunakan Metode Deteksi Dan Oscar," 2022.

[4] Kemenkominfo, "Peraturan Menteri Komunikasi Dan Informatika Indonesia (Pp Nomor 4 Tahun 2016)," 2016. [*Online*]. Available: Www.Peraturan.Go.Id

[5] 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," *Journal Of Informatics And Computer Science*, Vol. 04, 2023.

[6] Bojana Vilendečić, Ratko Dejanović, And Predrag Ćurić, "The Impact Of Human Factors In The Implementation Of Siem Systems," *J. Of Electrical Engineering*, Vol. 5, No. 4, Pp. 196–203, Jul. 2017, Doi: 10.17265/2328-2223/2017.04.004.

[7] Stefan Stanković, Slavko Gajin, And Ranko Petrović, "A Review Of Wazuh Tool Capabilities For Detecting Attacks Based On Log Analysis," 2022.

[8] H. Ardiyanti, "Cyber-Security Dan Tantangan Pengembangannya Di Indonesia," 2014. [*Online*]. Available: Http://Kominfo.Go.Id/Index.Php/Content/Detail/3980/

[9] A. N. Puriwigati, "Sistem Informasi Manajemen-Keamanan Informasi," 2020. [*Online*]. Available: Https://Www.Researchgate.Net/Publication/341293613

[10] Cisco, "Building Blocks Of Information Security." Accessed: Nov. 09, 2023. [*Online*]. Available: Https://Www.Learncisco.Net/Courses/Iins/Common-Security-Threats/Information-Security-And-Common-Threats.Html

[11] W. Abidian, "Implementasi Splunk Dalam Membangun Security Information And Event Management Berdasarkan Log Firewall Traffic Type (Studi Kasus: Jaringan Uii)," 2021.

[12] M. D. Akmal Et Al., "Implementasi Security Information And Event Management (Siem) Menggunakan Ossim," *Jurnal Aksara Komputer Terapan Politeknik Caltex Riau*, Vol. 7, No. 2, P. 1, 2018.

[13] G. González-Granadillo, S. González-Zarzosa, And R. Diaz, "Security Information And Event Management (Siem): Analysis, Trends, And Usage In Critical Infrastructures," *Sensors*, Vol. 21, No. 14, Jul. 2021, Doi: 10.3390/S21144759.

[14] M. Dehan Pratama, F. Nova, And D. Prayama, "Wazuh Sebagai Log Event Management Dan Deteksi Celah Keamanan Pada Server Dari Serangan DoS," Wazuh Sebagai Log Event Management Dan Deteksi Celah Keamanan Pada Server Dari Serangan DoS Jitsi : *Jurnal Ilmiah Teknologi Sistem Informasi*, Vol. 3, No. 1, Pp. 1–7, 2022, [*Online*]. Available: Http://Jurnal-Itsi.Org

[15] R. H. Susanto, "Implementasi Bot Telegram Untuk Monitoring Jaringan Mikrotik Router Os Menggunakan Aplikasi The Dude Pada Kantor Balas Ksda Riau," 2021.