SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MENGGUNAKAN WAZUH PADA PESANTREN TEKNOLOGI INFORMASI DAN KOMUNIKASI JOMBANG

TUGAS AKHIR

Faruq Aziz Saputra

0110220287

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

2023

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MENGGUNAKAN WAZUH PADA PESANTREN TEKNOLOGI INFORMASI DAN KOMUNIKASI JOMBANG

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer Pada Program Studi Teknik Informatika

Faruq Aziz Saputra

0110220287

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

2023

HALAMAN PERNYATAAN ORISINALITAS

Skripsi/Tugas Akhir ini adalah hasil karya penulis, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Faruq Aziz Saputra

NIM : 0110220287

HALAMAN PENGESAHAN

Skripsi/Tugas Akhir ini diajukan oleh :

Nama : Faruq Aziz Saputra

NIM : 0110220287

Program Studi : Teknik Informatika

Judul Skripsi : Implementasi Security Information and Event Management (SIEM) Menggunakan Wazuh Pada Pesantren Teknologi Informasi dan Komunikasi Jombang.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri.

DEWAN PENGUJI

Pembimbing	Penguji
Tubagus Rizky Dharmawan, S.T., M.Sc.	April Rustianto, S.Komp., M.T.
NIDN : 0410089103	NIDN : 0426048703

Ditetapkan di : Depok

Tanggal : 24 Februari 2024

KATA PENGANTAR

Alhamdulillahi Rabbil 'Aalamiin, segala puji bagi Allah SWT, atas limpahan rahmat karunia dan izin-Nya, kita mendapatkan kesehatan, umur panjang dan nikmat mengecap pendidikan. Sehingga dengan ini penulis dapat menyelesaikan Tugas Akhir ini. Penulisan Tugas Akhir ini dilakukan untuk memenuhi salah satu persyaratan untuk memperoleh gelar Sarjana komputer Program Studi Teknik Informatika pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, mulai dari proses perkuliahan hingga penyusunan skripsi ini, akan sulit bagi penulis untuk berhasil menyelesaikan Tugas Akhir ini. Oleh karena itu, dalam kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT.
2. Orang tua dan semua keluarga yang telah memberikan dukungan baik secara moril maupun materil dalam penyelesaian tugas ini.
3. Bapak Dr. Lukman Rosyidi, M.T, M.M. selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Ibu Tifani Nabarian, S.Kom, M.T.i selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
5. Bapak Nasrul, S.Kom, M.Kom selaku Dosen Pembimbing Akademik yang telah membimbing penulis selama berkuliah di Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Bapak Tubagus Rizky Dharmawan, S.T., M.Sc. selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
7. Bapak April Rustianto, S.Komp., M.T. selaku Dosen Penguji Tugas Akhir penulis dalam sidang tugas akhir ini.
8. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
9. Bapak Dedy Widjaya selaku Pimpinan Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang.

10. Rekan-rekan Mahasiswa seperjuangan yang telah sama sama berjuang dan memberikan support.

Dalam penulisan laporan ilmiah ini, penulis menyadari banyaknya kekurangan baik dalam menyampaikan teori maupun kaidah penulisan. Walaupun demikian, penulis telah berusaha menyelesaikan penulisan ilmiah ini sebaik mungkin. Oleh karena itu, apabila terdapat kekurangan di dalam penulisan ilmiah ini, dengan rendah hati penulis menerima kritik dan saran yang bersifat membangun dari pembaca.

Penulis berharap semoga kebaikan yang diberikan menjadi amal jariyah dan Semoga mendapatkan balasan terbaik dari Allah SWT. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 24 Februari 2024

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini:

Nama : Faruq Aziz Saputra

NIM : 0110220287

Program Studi : Teknik Informatika

Jenis karya : Tugas Akhir

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STT-NF **Hak Bebas Royalti Non Eksklusif (Non-exclusive Royalty - Free Right)** atas karya ilmiah saya yang berjudul :

IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MENGGUNAKAN WAZUH PADA PESANTREN TEKNOLOGI INFORMASI DAN KOMUNIKASI JOMBANG.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non Eksklusif ini STT-NF berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada tanggal : 24 Februari 2024

Yang menyatakan

(Faruq Aziz Saputra)

ABSTRAK

Nama : Faruq Aziz Saputra

NIM : 01101220287

Program Studi : Teknik Informatika

Judul : Implementasi Security Information and Event Management (SIEM) Menggunakan Wazuh Pada Pesantren Teknologi Informasi dan Komunikasi Jombang.

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 handal 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 merespon 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 : Security Information and Event Management (SIEM), Wazuh, Keamanan Informasi, Bot Telegram, Visualisasi Log, Alert Sistem.

ABSTRACT

Name : Faruq Aziz Saputra

NIM : 0110220287

Study Program : Informatics Engineering

Title : Implementation of Security Information and Event Management (SIEM) Using Wazuh at Pesantren Information and Communication Technology Jombang.

Information security is an important aspect for organizations and companies in the current era of digital transformation. Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang, as a technology-oriented education, requires a reliable security system considering the increasing information 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 terms of 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, and shows 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 shows results that are still within normal limits when an attack occurs.

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

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 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, 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 dihosting 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 menganalisa data atau informasi yang masuk ke dalam server yang diakses dengan izin maupun tanpa izin [2]. Data yang terkumpul akan dianalisa 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 memonitoring dan mendeteksi serangan secara realtime dengan melihat laporan event atau aktifitas pada aplikasi tersebut.

Pada penelitian ini, tools yang akan digunakan sebagai solusi adalah SIEM aplikasi Wazuh yang terintegrasi dengan aplikasi chatbot Telegram. Wazuh adalah aplikasi SIEM berbasis *Open Source* yang berfungsi sebagai sistem deteksi intrusi berbasis host (HIDS), yaitu suatu sistem yang mampu mendeteksi dan mengidentifikasi ancaman yang terjadi pada sistem komputer dengan mengidentifikasi setiap jenis serangan yang dilakukan oleh intruder [7]. Wazuh dapat mendeteksi ancaman jaringan dan memantau keamanan sebuah server secara real-time. Selain itu, Wazuh juga dapat melakukan pemindaian keamanan, pemindaian log, deteksi kerentanan dan respons insiden. Wazuh menggunakan *Elastic stack (Elasticsearch, Kibana)* sebagai media untuk menyimpan log dan alert [7].

Wazuh dipilih sebagai optimasi dashboard sistem pencatatan log karena memiliki *built-in log*, bersifat *open source,* mudah dalam penggunaannya, serta memiliki suatu komunitas sebagai wadah untuk bertanya dan berdiskusi perihal pemanfaatannya. Selain itu, Wazuh adalah aplikasi yang dimanfaatkan sebagai *log grabber* yang berfungsi mengubah log tidak beraturan menjadi suatu informasi yang mudah dipahami oleh manusia, serta menyediakan interface yang lebih menarik karena dilengkapi dengan diagram dan traffic.

Dalam menerapkan alert sistem, sebaiknya informasi alert dapat diimplementasikan secara mobile guna menyediakan akses informasi kapan dan dari mana saja, sehingga adiministrator 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 menganalisa keamanan sistem informasi data di PeTIK Jombang dengan harapan sistem ini dapat membantu mendeteksi, menganalisa, dan memonitor sistem data informasi secara real-time, serta mempermudah dalam manajemen insiden resiko di PeTIK Jombang.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan diatas, maka perumusan masalah yang menjadi fokus dalam penelitian ini adalah:

1. Bagaimana implementasi wazuh untuk melakukan pengelolaan dan monitoring keamanan pada sebuah jaringan?
2. Bagaimana visualisasi yang dihasilkan berdasarkan log pada insiden yang terjadi pada jaringan?
3. Bagaimana alert sistem pada log monitoring Wazuh dan bot telegram bekerja?
4. Bagaimana kinerja CPU dan memory pada server Wazuh?

1.3 Batasan Masalah

Batasan masalah yang ditetapkan pada penelitian ini adalah sebagai berikut:

1. Tool SIEM yang digunakan pada penelitian yaitu Wazuh.
2. Implementasi diterapkan di Pesantren Teknologi Informasi dan Komunikasi (PeTIK) Jombang.
3. Sistem operasi yang digunakan adalah Ubuntu.
4. Pengujian dilakukan dengan menggunakan Virtual Machine (VM) Virtual Box terhubung dengan jaringan PeTIK Jombang.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang akan diselesaikan, maka tujuan dari penelitian ini adalah:

1. Melakukan implementasi wazuh untuk melakukan pengelolaan dan monitoring keamanan pada sebuah jaringan.
2. Menampilkan visualisasi berdasarkan log yang dihasilkan berdasarkan log pada insiden yang terjadi pada jaringan menggunakan Wazuh.
3. Membangun sistem alert pada wazuh yang diintegrasikan dengan Telegram Bot.
4. Memantau kinerja CPU dan memory pada server Wazuh.

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah:

1. Menawarkan kemudahan pada administrator dalam membaca informasi serta melakukan monitoring traffic jaringan berdasarkan visualisasi yang dihasilkan dari Wazuh.
2. Memberikan kemudahan dalam memperoleh serta mengumpulkan informasi traffic jaringan karena Wazuh menghasilkan visualisasi berdasarkan pantauan log jaringan secara real time.
3. Memberikan inspirasi PeTIK Jombang untuk mengaplikasikan teknologi keamanan siber, khususnya penggunaan log yang ada pada aplikasi wazuh untuk mengambil keputusan dan Tindakan yang tepat.

1.6 Sistematika Penulisan

Sistematika penulisan pada laporan tugas akhir ini terbagi menjadi 5 (lima) bab. Adapun masing-masing bab merincikan intisari sebagai berikut:

BAB I PENDAHULUAN

Bab I merupakan penjabaran umum penelitian tugas akhir yang dilaksanakan. Bab ini meliputi latar belakang yang menjadi landasan dalam melakukan penelitian, rumusan

masalah, batasan masalah, tujuan penelitian serta manfaat yang diharapkan.

BAB II LANDASAN TEORI

Pada Bab II merupakan penjabaran secara rinci dasar teori yang digunakan sebagai landasan berpikir dalam pelaksanaan serta penulisan yang terdiri atas definisi keilmuan yang bersumber dari buku, jurnal dan penelitian terdahulu yang relevan.

BAB III METODOLOGI PENELITIAN

Pada Bab III merupakan rincian pekerjaan yang dilakukan dan menjelaskan rencana dan langkah-langkah dalam penelitian, seperti rancangan topologi, tabel pengalamatan, kebutuhan perangkat, metode pengujian dan skenario pengujian dan analisis.

BAB IV HASIL DAN PEMBAHASAN

Pada Bab IV meliputi perancangan Wazuh, pengujian serangan dan performance, analisis dalam setiap pengujian, dan analisis hasil yang diperoleh.

BAB V PENUTUP

Bab V merupakan uraian kesimpulan dari rangkaian penelitian yang dilakukan serta memuat saran untuk diberikan kepada peneliti lebih lanjut.

BAB II
KAJIAN LITERATUR

2.1. Landasan Teori

Suatu organisasi atau perusahaan membutuhkan infrastruktur teknologi informasi dalam menjalankan berbagai kegiatan operasionalnya. Salah satu bentuk pemanfaatan IT adalah mengumpulkan informasi dan data penting lainnya yang menjadi aset dari sebuah organisasi tersebut. Aset dan informasi tersebut memiliki nilai yang kemudian harus dilindungi keamanannya. Semakin besar skala suatu perusahaan atau organisasi, maka semakin besar pula skala pemanfaatan IT yang dibutuhkan. Hal ini kemudian menjadikan sistem IT tersebut sangat kompleks, dan tak jarang menjadi permasalahan tersendiri bagi departemen IT karena sulitnya melakukan pengelolaan dan monitoring. Teknologi mutakhir menjadi alternatif bagi perusahaan atau organisasi untuk menjaga keamanan aset informasinya, dan memudahkan departemen IT dalam melakukan pekerjaannya.

2.2. 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.

Cyber security sangat penting untuk mengantisipasi ancaman yang dapat mengganggu kinerja suatu sistem atau perangkat. Berikut beberapa kategori yang termasuk *cyber security*, yaitu:

a. *Network Security* (Keamanan Jaringan)

Tindakan untuk mengamankan jaringan komputer dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah. Network security mencakup berbagai teknologi dan praktik, seperti *firewall, intrusion detection system* (IDS), *intrusion prevention system* (IPS), *virtual private network* (VPN), dan lainnya.

b. *Aplication Security* (Keamanan Aplikasi)

Tindakan untuk melindungi aplikasi perangkat lunak dari ancaman dan serangan keamanan serta mencegah pencurian dan perubahan data yang tidak sah. *Application security* mencakup berbagai kegiatan, seperti analisis kode sumber, pengujian penetrasi, dan manajemen kerentanan.

c. *Cloud Security* (Keamanan Cloud)

Tindakan untuk melindungi data dan sumber daya yang berada pada layanan cloud computing sehingga dapat memitigasi kerahasiaan dan ketersediaan informasi yang disimpan dan diproses dalam cloud. Cloud security mencakup berbagai teknologi dan praktik, seperti enkripsi, kontrol akses, dan manajemen risiko.

2.3. 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. Gambar 2.1 merupakan gambaran hubungan CIA.

Gambar 2. 1. CIA Triad

a. *Confidentiality* (Kerahasiaan)

Suatu organisasi atau perusahaan dituntut memiliki kebijakan dalam menjaga datanya agar tetap rahasia, atau menjadi privasi. Hal ini meliputi kebijakan menentukan hak akses pada data. Kemudian melakukan enkripsi, menggunakan ID dan kata sandi, menerapkan otentikasi dua faktor guna menghindari penyebaran data dan informasi yang sensitif, serta melarang akses data oleh pihak yang tidak berwenang.

b. *Integrity* (Integritas)

Komponen integritas memastikan bahwa data dan informasi yang dimiliki suatu perusahaan atau organisasi adalah akurat, konsisten dan andal selama data tersebut diperlukan. Data yang dikirimkan tidak boleh berubah ataupun diubah oleh entitas yang tidak memiliki wewenang. Penggunaan perizinan pada file serta kontrol akses pengguna adalah solusi untuk menjaga integritas suatu data atau informasi tersebut. Selain itu, kontrol versi juga digunakan untuk meminimalisir perubahan pada data akibat human error dan ketidaksengajaan saat menggunakannya. Selain membatasi hak akses, memiliki cadangan data juga bagian dari menjaga integritas.

Cadangan data akan membantu apabila suatu data ingin dipulihkan, serta menghindari resiko kerusakan dari data secara keseluruhan. Kemudian hashing pada checksum dimanfaatkan untuk melakukan verifikasi sebuah data selama proses transfer data berlangsung.

c. *Availability* (Ketersediaan)

Ketersediaan atau availability menjamin bahwa setiap aplikasi, sistem, jaringan dapat diakses apabila dibutuhkan, serta dapat berfungsi sebagaimana mestinta. Komponen ini juga meliputi proses pemeliharaan peralatan, perawatan perangkat keras, perawatan software, memastikan ketersediaan jaringan dan data bagi pihak berwenang.

2.4. 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

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

b. Phising

Phising adalah jenis serangan yang digunakan untuk memanipulasi psikologis korban. Penyerang biasanya akan membuat email ataupun halaman website palsu dengan tujuan menipu agar korban menyerahkan informasi sensitifnya seperti username dan password. *Phising* termasuk serangan yang mudah dilakukan dan efektif terhadap korbannya.

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.

d. Malware

Malware adalah bentuk serangan yang dikemas menjadi perangkat lunak berbahaya bagi komputer, server dan jaringan komputer. Malware dapat merusak sistem informasi, mencuri data dari sistem, bahkan mengambil alih kontrol suatu komputer. Beberapa jenis malware yang sering dijumpai adalah *virus, worm, trojan horse, spyware* dan juga *ransomware*.

2.5. 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 resiko 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.

2.6. Intrusion Detection System (IDS)

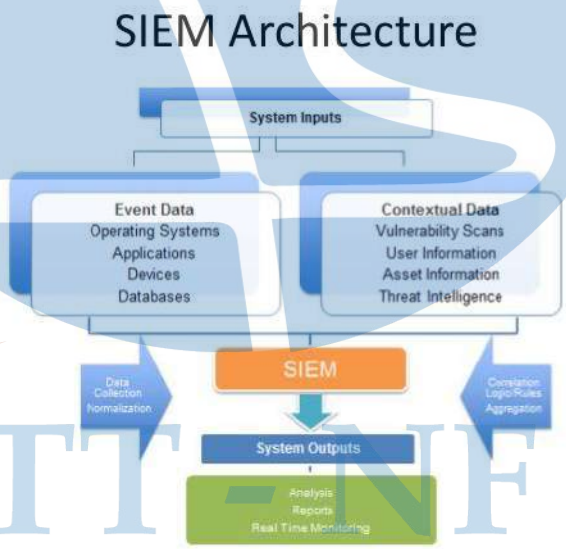
Intrusion Detection System (IDS) adalah aplikasi perangkat lunak atau perangkat yang memantau sistem atau aktivitas jaringan untuk pelanggaran kebijakan atau aktivitas jahat dan menghasilkan laporan ke sistem manajemen [12]. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam 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 didalam sebuah jaringan. Beberapa jenis IDS adalah sebagai berikut :

a. NIDS (*Network Intrusion Detection System*) IDS jenis ini ditempatkan di sebuah titik yang strategis untuk melakukan pengawasan terhadap traffic yang menuju berasal dari semua alat-alat (devices) dalam jaringan. Jenis IDS yang memantau lalu lintas jaringan secara real-time dan mendeteksi aktivitas mencurigakan atau serangan berbasis jaringan yang dapat mengancam keamanan sistem dan jaringan. NIDS bekerja pada lapisan jaringan dengan menganalisis paket data yang melewati titik pemantauan di jaringan
b. HIDS (*Host Intrusion Detection System*) IDS jenis ini berjalan pada host yang berdiri sendiri dalam sebuah jaringan. HIDS berfungsi untuk melakukan

pengawasan terhadap paket-paket yang berasal dari dalam maupun dari luar. HIDS hanya berfungsi pada satu alat saja, ketika ada kegiatan-kegiatan yang mencurigakan HIDS langsung memberikan peringatan kepada user. Jenis IDS yang memantau dan mendeteksi aktivitas atau serangan yang mencurigakan pada satu atau lebih host di dalam jaringan. HIDS bekerja pada level sistem operasi host/server dengan menganalisis aktivitas host, seperti perubahan pada sistem, aktivitas proses dan event lainnya yang terjadi pada host.

2.7. 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 aktifitas dan melakukan analisis Log keamanan dari berbagai jenis Log yang berasal dari berbagai perangkat yang terhubung di jaringan [13]. Gambar 2.2 merupaka



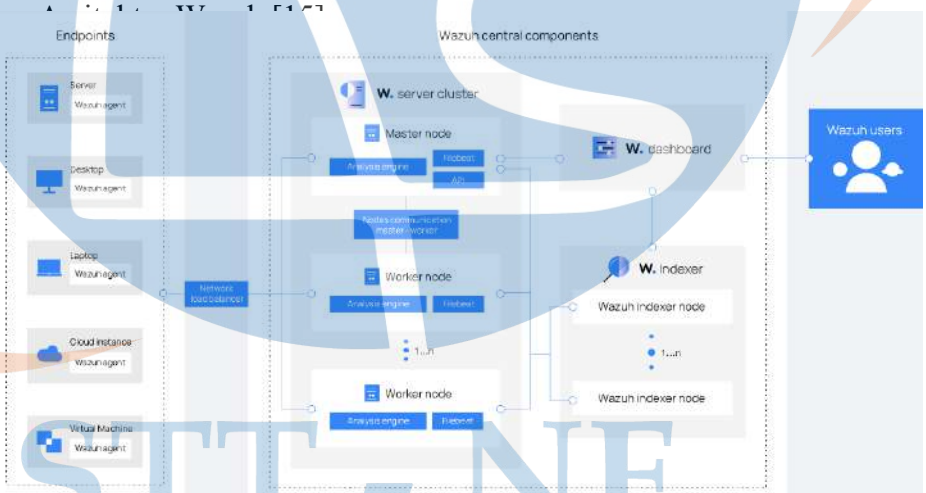
Gambar 2. 2. SIEM Archiecture

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]

2.8. 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*, *intrusion*, maupun log. Sedangkan Wazuh agent merupakan perangkat yang diinstall pada perangkat endpoint untuk melakukan pembacaan sistem, pengumpulan log serta mengirimkan ke Wazuh server [14]. Gambar 2.3 merupakan gamba



Gambar 2. 3. Architecture Apilkasi Wazuh

Pada penelitian ini, Wazuh memiliki peran paling penting dari penelitian. Berikut 4 fungsi komponen utama yang terdapat dalam Wazuh [15]:

a. Wazuh Indexer

Mesin analitik dan pencarian teks lengkap yang sangat *scalable*. Komponen ini berfungsi untuk mengindeks dan menyimpan peringatan yang dihasilkan oleh server Wazuh.

b. Wazuh Server

Memiliki fungsi untuk menganalisa data yang didapat dari agent, lalu melakukan decoder dan menyesuaikan dengan aturan standar keamanan, dengan menggunakan *threat intelligence* untuk mencari *indicators of compromise* (IOC) yang terkenal. Satu server dapat menganalisis data dari ratusan atau ribuan agen, dan memperluas secara horizontal Ketika disiapkan dalam sebuah lingkungan. Komponen sentral ini juga digunakan untuk mengelola agen, mengkonfigurasikan dan melakukan upgrade dari jarak jauh bila diperlukan.

c. Wazuh Dashboard

Wazuh Dashboard adalah antarmuka pengguna web untuk visualisasi dan analisis data. Ini mencakup seluruh dasbor yang siap digunakan untuk perihal keamanan, pemenuhan terhadap peraturan, aplikasi yang terdeteksi kerentanan, pemantauan integritas file, hasil penilaian konfigurasi, pemantauan infrastruktur cloud, dan lain-lain. Ini juga digunakan untuk mengelola konfigurasi Wazuh dan untuk memantau statusnya.

d. Wazuh Agent

Wazuh Agent diinstal pada endpoint seperti laptop, desktop, server, cloud, ataupun virtual. Mereka menyediakan kemampuan pencegahan, deteksi, dan respons ancaman. Wazuh Agent dapat dioperasikan di berbagai sistem operasi, antara lain Linux, Windows, macOS, Solaris, AIX, dan HP-UX.

2.9. Linux Ubuntu

Linux adalah sistem operasi yang bersifat open source dan memiliki lisensi *GNU General Public License* (GPL). Kode sumber yang merupakan bagian penting dari program disertakan dalam program tersebut sehingga dapat diakses oleh siapa saja

tanpa perlu mengikuti suatu perjanjian tertentu. Kata free menunjukkan kebebasan bukan gratis. Linux dapat dipublikasikan, dimodifikasi, dan didistribusikan secara bebas. Ubuntu merupakan sistem operasi yang terkenal di dunia dan menggunakan kernel Linux yang bersifat open source, yang berarti kode sumbernya dapat diakses dan diubah oleh siapa saja sesuai dengan lisensi *GNU General Public License* (GPL). Ubuntu dikembangkan oleh perusahaan Canonical Ltd dan dipelopori oleh *Mark Shuttleworth* yang tujuannya adalah menyediakan operasi sistem yang mudah digunakan, stabil, aman dan dapat diakses secara bebas untuk semua pengguna [16].

2.10. Virtualbox

VirtualBox adalah aplikasi *hypervisor* tipe 2 yang dapat menjalankan beberapa sistem operasi tamu di dalamnya sehingga dapat melakukan percobaan dengan beberapa tools sesuai dengan keperluan. Saat menggunakan VirtualBox, sistem operasi utama tidak akan berpengaruh. OS Host dan sistem operasi yang digunakan di VirtualBox masih dapat berkomunikasi satu sama lain.

2.11. Kali Linux

Menurut (Pritchett & Smet, 2013) Kali Linux adalah gudang pengujian penetrasi berbasis Linux yang membantu profesional keamanan dalam melakukan penilaian di lingkungan asli yang didedikasikan untuk hacking. Kali Linux adalah distribusi berbasis distribusi Debian GNU / Linux yang ditujukan pada forensik digital dan penggunaan pengujian penetrasi [12].

2.12. 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 [17].

2.13. Penelitian Terkait

Penelitian ini mengacu pada beberapa penelitian terkait yang disajikan dalam tabel. Tabel tersebut mempermudah dalam memahami ringkasan penelitian, kesamaan dan perbedaan pada penelitian yang ada dengan masalah yang ditemukan. Berikut adalah ikhtisar beberapa referensi penelitian terkait yang penulis dapatkan..

Tabel 2. 1. Penelitian Terkait

No.	Peneliti	Uraian Penelitian	Persamaan Penelitian	Perbedaan Penelitian
1	Muhammad Alfian Fahrudi, I Made Suartana (2023)	Penelitian ini menawarkan sebuah sistem integrasi antara endpoint security dengan bot messenger Telegram untuk mengawasi dan memonitor serangan terhadap web server secara langsung. Sistem integrasi akan menghemat biaya perusahaan dan meningkatkan kinerja SOC dalam mengawasi web server. Wazuh sebagai aplikasi endpoint security yang terhubung dengan bot Telegram. Dari hasil penelitian yang dilakukan dapat disimpulkan bahwa integrasi sistem monitoring Wazuh dengan bot messenger Telegram berhasil mengirim pesan secara langsung.	Penggunaan Wazuh sebagai aplikasi end-point dan terhubung dengan chatbot Telegram.	Tidak menampilkan visualisasi dashboard berdasarkan log yang event.
2	Nazar Firman Pratama (2023)	Perancangan sistem deteksi dini keamanan informasi di Dinas Komunikasi Informatika Statistik dan Persandian Kabupaten Bandung. Menggunakan Aplikasi Security Information Event Management (SIEM) Wazuh untuk memonitoring dan mendeteksi serangan secara realtime dengan melihat laporan	Penerapan SIEM Wazuh untuk monitoring log, dan menampilkan visualisasi dashboard	Penerapan integrasi Aplikasi Wazuh dan Telegram Chatbot untuk memudahkan monitoring secara realtime dan fleksibel.

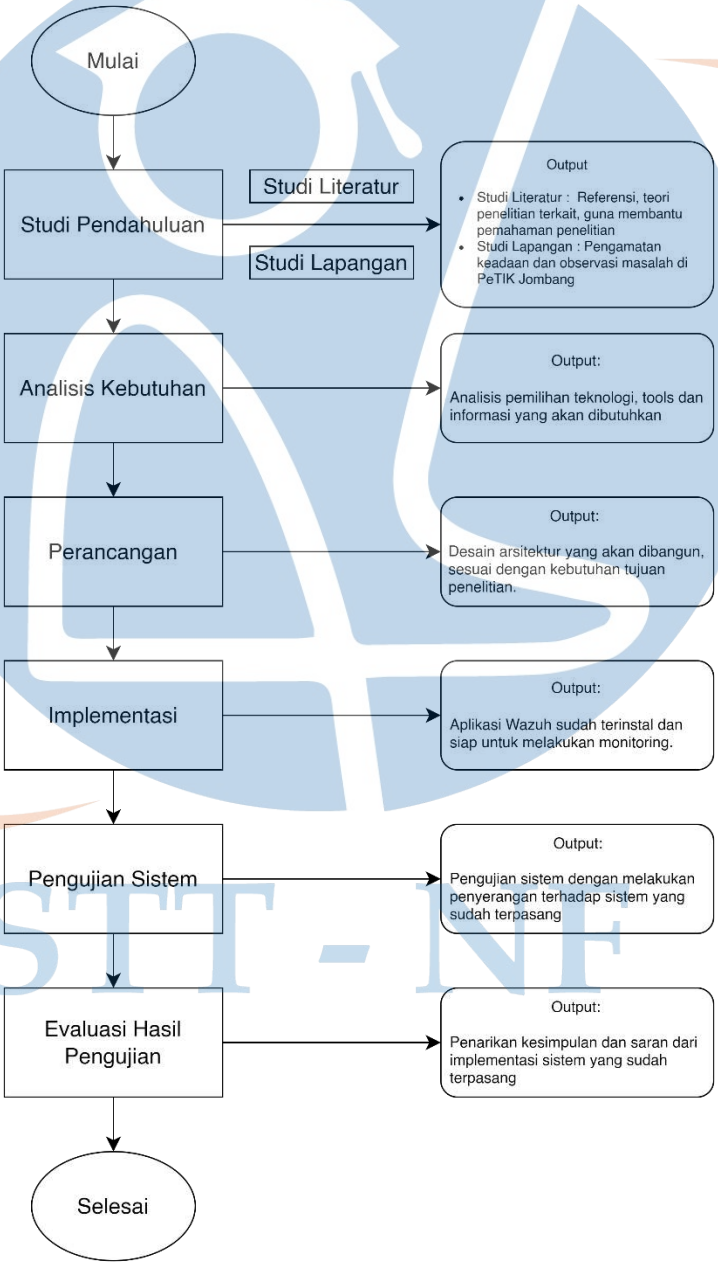
		event atau aktifitas pada aplikasi tersebut.	report Wazuh	
3	Muhammad Alfandi (2022)	Melakukan Analisa SIEM menggunakan Elastic Stack dan Splunk. Melakukan serangan fingerprinting, SQL Injection, DoS, dan Port Scanning. Hasil pengujian tersebut mampu mendeteksi semua serangan yang masuk ke web server secara realtime dan mengirimkan email notifikasi kepada administrator mengenai serangan yang terjadi.	Implementasi SIEM Splunk untuk mendeteksi serangan.	Penerapan Aplikasi SIEM Wazuh untuk mendeteksi serangan.
4	Muhammad Dehan Pratama Fitri Nova Deddy Prayama (2022)	Penelitian ini melakukan penelitian wazuh sebagai log event management dan deteksi celah keamanan pada server dari serangan DoS dan menggunakan Suricata untuk mendeteksi serangan DoS. Hasil dari penelitian ini adalah Wazuh manager mendapat informasi berupa log mengenai aktivitas yang dilakukan oleh agent. Suricata dapat mendeteksi adanya serangan DoS. Kemudian alert dari suricata tersebut diteruskan Wazuh agar ditampilkan pada web interface Wazuh. Kemudian log tersebut dapat divisualisasikan oleh Wazuh dengan beragam bentuk statistik agar mudah dipahami Alert dari Wazuh akan dikirimkan kepada administrator melalui e-mail.	Penerapan Wazuh sebagai Log Event Management	Penerapan integrasi Aplikasi Wazuh dan Telegram Chatbot untuk memudahkan monitoring secara realtime dan fleksibel.
5	Mustafa Dzul Akmal, Kartina Diah Kusuma Wardhani dan Muhammad Arif Fadhly Ridha (2018)	Dalam penelitian ini melakukan Implementasi Security And Event Management (SIEM) Menggunakan OSSIM. Melakukan pengujian serangan berupa DoS Attack, Brute Force, SQL Injection. Dengan hasil penelitian yaitu OSSIM dapat	Penerapan SIEM OSSIM untuk menganalisa kerentanan pada	Penerapan SIEM Wazuh untuk mendeteksi serangan dan melakukan integrasi dengan

		melakukan Analisa data yang dihasilkan dari penyerangan yang terjadi dalam bentuk grafik maupun diagram.	jaringan dan menampilkan dashboard visualisasi.	telegram untuk mendapatkan informasi secara realtime.

BAB III
METODOLOGI PENELITIAN

3.1. Tahapan Penelitian

Pada Gambar 3.1 dijelaskan bagaimana tahapan penelitian secara umum yang akan dilakukan oleh penulis.



Gambar 3. 1. Metodologi 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.

3.2. 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.

3.2.1 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 dilapangan (*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, menganalisa, dan memonitor sistem data informasi secara real-time, serta mempermudah dalam manajemen insiden resiko di Pesantren Pesantren Teknologi Informasi Komunikasi (PeTIK) Jombang.

3.2.2 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.

3.2.3 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.

3.2.4 Lingkungan Pengembangan

Framework/tools/laptop/server yang digunakan, lokasi penelitian, alat yang digunakan.

a) Wazuh Server

Tabel 3. 1. Spesifikasi Wazuh Server

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

b) Wazuh Agent

Tabel 3. 2. Spesifikasi Wazuh Agent

Spesifikasi	
Processore	Intel i7 Gen 11th
Storage	SSD 256 GB
Memory	16 GB
Operating System	Windows 11
Software	Wazuh Agent

c) PC Admin

Tabel 3. 3. Spesifikasi PC Admin

	Spesifikasi
Processore	Intel i7 Gen 11th
Storage	SSD 256GB
Memory	16 GB
Operating System	Windows 11
Software	Browser

3.2.5 Metode Pengujian

Berikut beberapa pengujian yang dilakukan, seperti:

3.2.5.1 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 menungkinkan 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.

3.2.5.2 Pengujian Performance

Parameter pengujian performance yang terapkan dalam penelitian ini adalah:

a) CPU

Perhitungan kinerja CPU dilakukan dengan menggunakan tools SNMP untuk memantau penggunaan CPU yang sudah diinstal wazuh pada server.

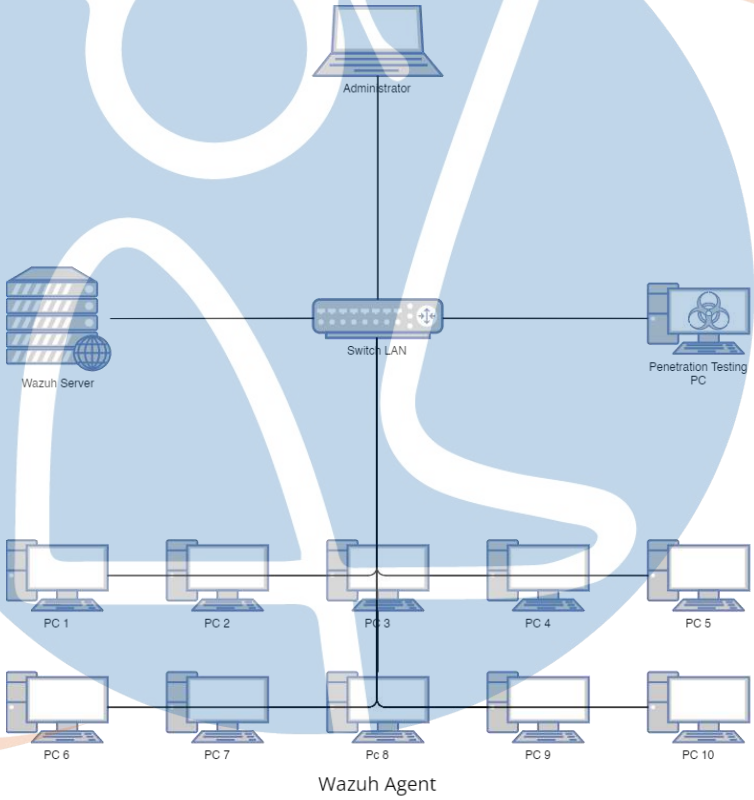
b) Memory

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

BAB IV
IMPLEMENTASI DAN EVALUASI

4.1 Rancangan Penelitian

Pada Simulasi penelitian ini dirancang server menggunakan *virtual machine* dengan sistem operasi Ubuntu Server 22.04. Topologi yang digunakan terdiri dari Server yang di-install *SIEM Wazuh Server*, *administrator*, *PC client* (*Wazuh Agent*), dan *PC attacker* (*penetration testing*).

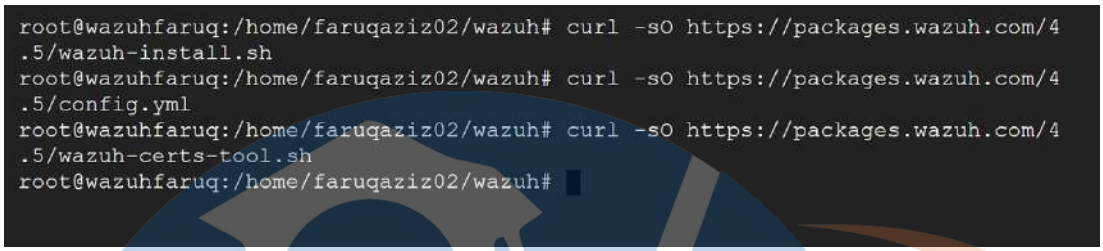


Gambar 4. 1. Desain Topologi Jaringan

Berdasarkan gambar 4.1, simulasi menggunakan jaringan LAN (*Local Area Network*) sederhana untuk mensimulasikan 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*.

4.1.1 Wazuh Indexer

Lakukan penginstalan server *Wazuh Indexer* yang bertindak sebagai penyimpan dan pengolah data keamanan dan log yang diperoleh dari *Wazuh Server*.



Gambar 4. 2. Initial Configuration

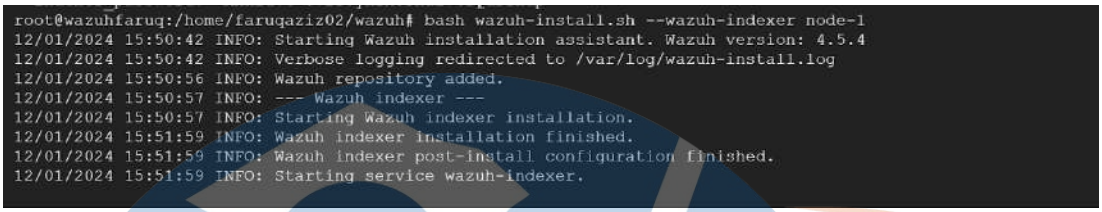
Lakukan pengubahan file konfigurasi *Wazuh Indexer* yaitu config.yml dengan mengubah network host menjadi IP address server, uncomment node name "node-1" lalu ganti node-1-ip menjadi IP address server dengan menggunakan perintah:

nano config.yml

Gambar 4. 3. Konfigurasi IP Wazuh Indexer

Aktifkan dan mulailah untuk menjalankan *Wazuh Indexer* dengan menggunakan perintah:

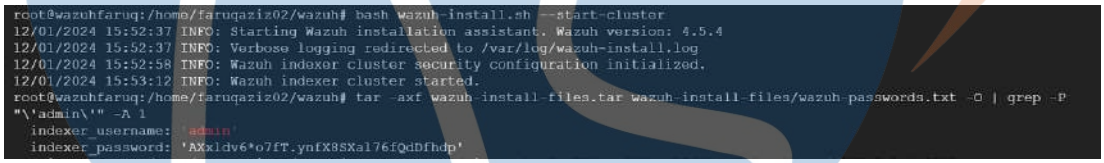
bash wazuh-install.sh --wazuh-indexer node-1



Gambar 4. 4. Running Wazuh Indexer

Lakukan inisialisasi klaster untuk pada node pengindeks Wazuh mana pun untuk memuat informasi sertifikat baru dan memulai klaster.

bash wazuh-install.sh --start-cluster



Gambar 4. 5. Inisialisasi Klaster

4.1.2 Wazuh Server

Jalankan asisten dengan opsi –wazuh-server diikuti dengan nama node untuk menginstal server Wazuh. Nama node harus sama dengan yang digunakan pada file config.yml di konfigurasi awal.

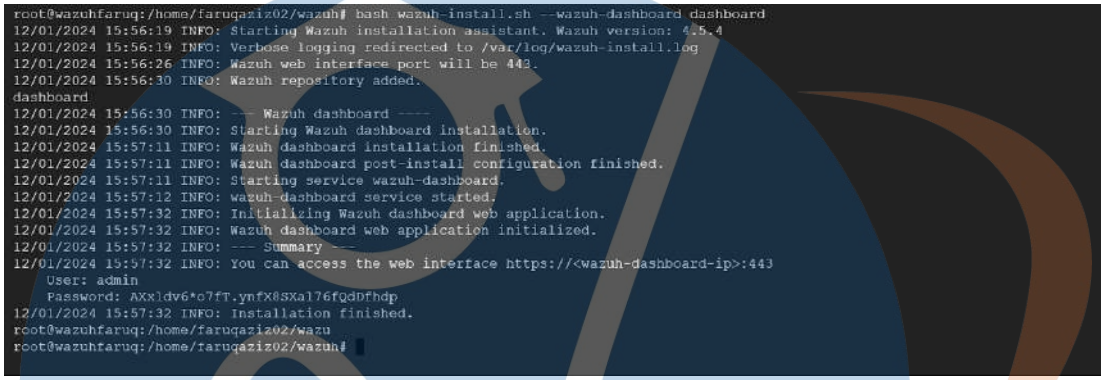
bash wazuh-install.sh --wazuh-server wazuh-1

Gambar 4. 6. Install Wazuh Server

4.1.3 Wazuh Dashboard

Lakukan penginstalan Wazuh Dashboard sebagai user interface untuk menampilkan laporan data keamanan yang diperoleh dari *Wazuh Indexer* dan dianalisis oleh *Wazuh Server*.

bash wazuh-install.sh --wazuh-dashboard dashboard



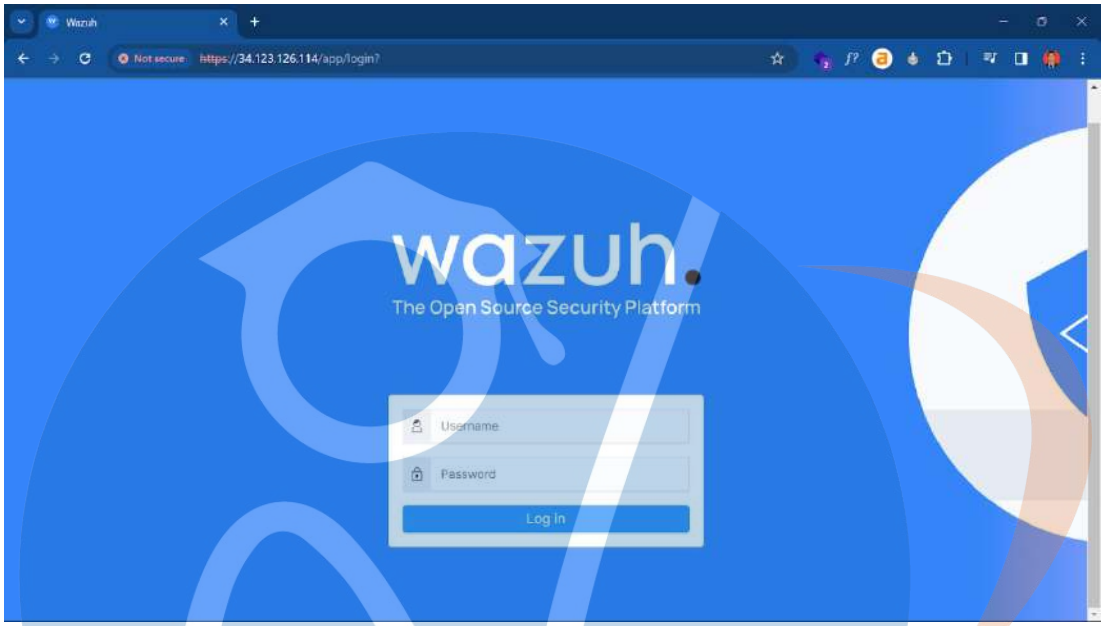
Gambar 4. 7. Instalasi Wazuh Dashboard

Aktifkan dan mulailah menjalankan *Wazuh Dashboard* dengan menggunakan perintah:

https://<wazuh-dashboard-ip>

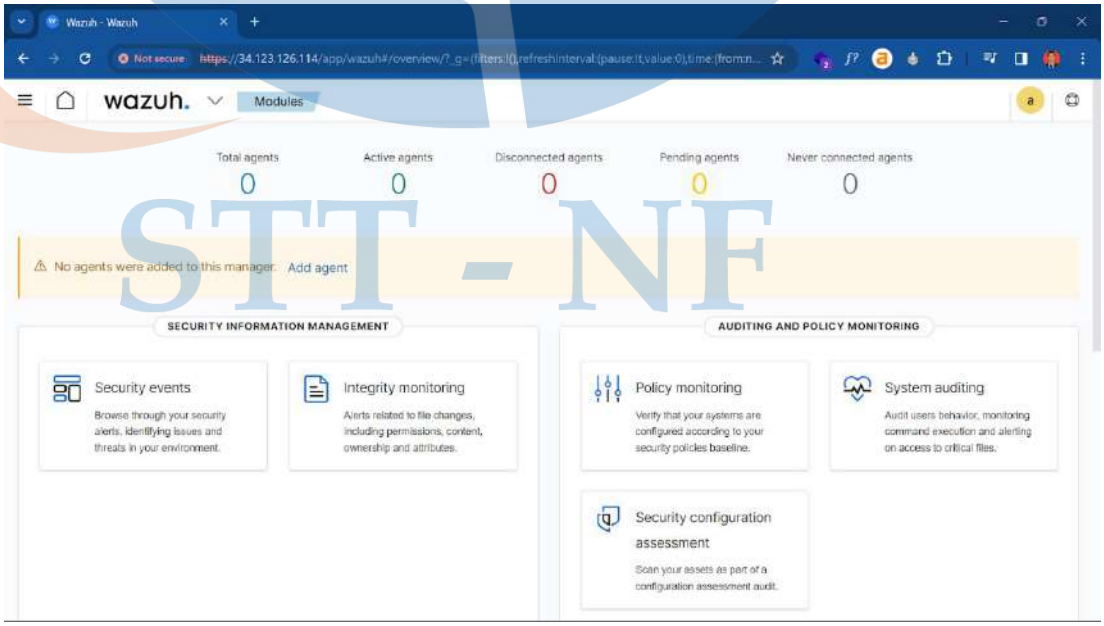
Gambar 4. 8. Running Wazuh Dashboard

Akseslah Wazuh Dashboard menggunakan alamat IP dari server yang telah di konfigurasi sebelumnya.



Gambar 4. 9. Halaman Login Wazuh

Berikut tampilan Wazuh Dashboard:

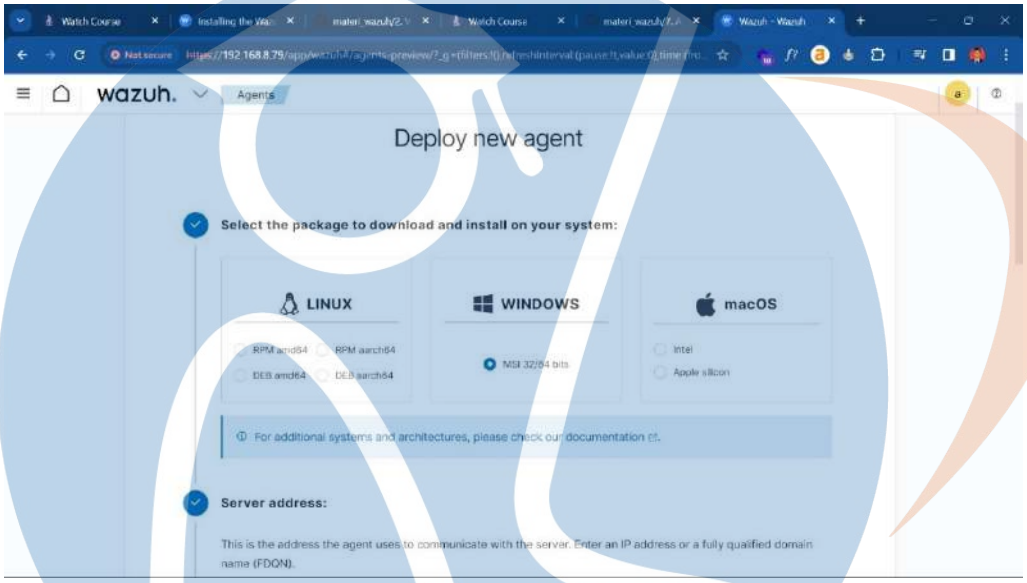


Gambar 4. 10. Tampilan Wazuh Dashboard

4.1.4 Wazuh Agent

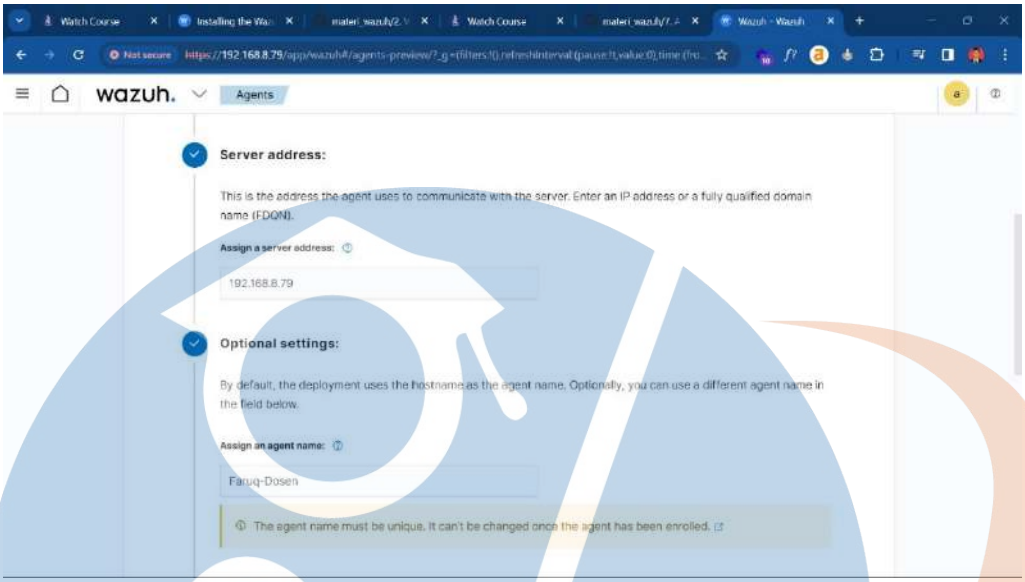
Melakukan penginstalan Wazuh Agent pada server yang dipantau sehingga didapatkan data keamanan, seperti log, aktivitas sistem dan informasi keamanan lainnya. Berikut tahapan menginstall Wazuh Agent pada endpoint Windows 11:

Pertama, memilih sistem operasi yang akan dipasang wazuh agent.



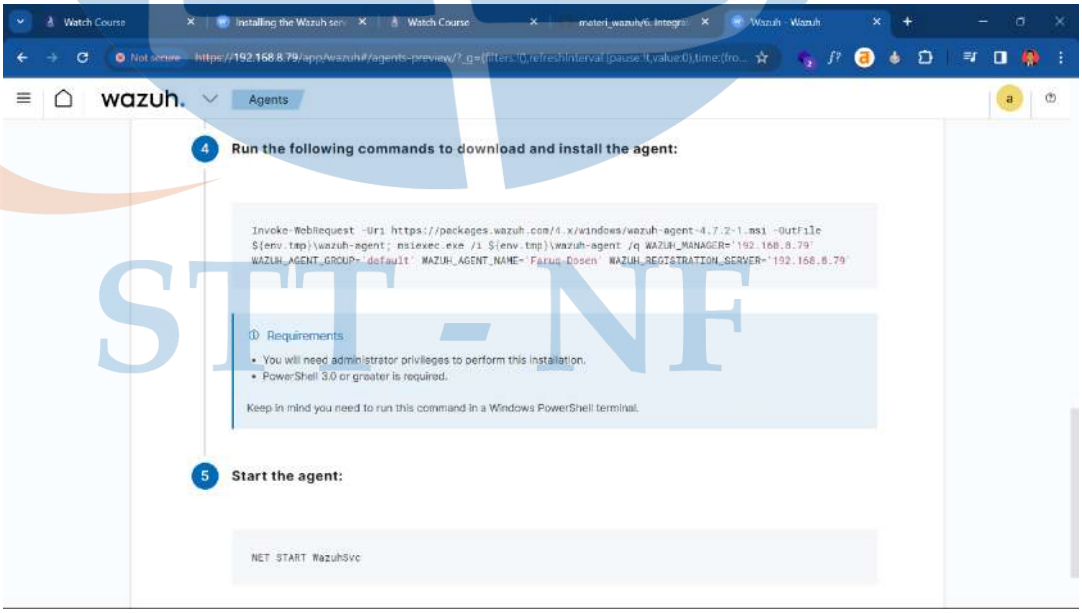
Gambar 4. 11. Tampilan Deploy Wazuh Agent

Kemudian, memasukkan IP address server wazuh dan nama agent wazuh



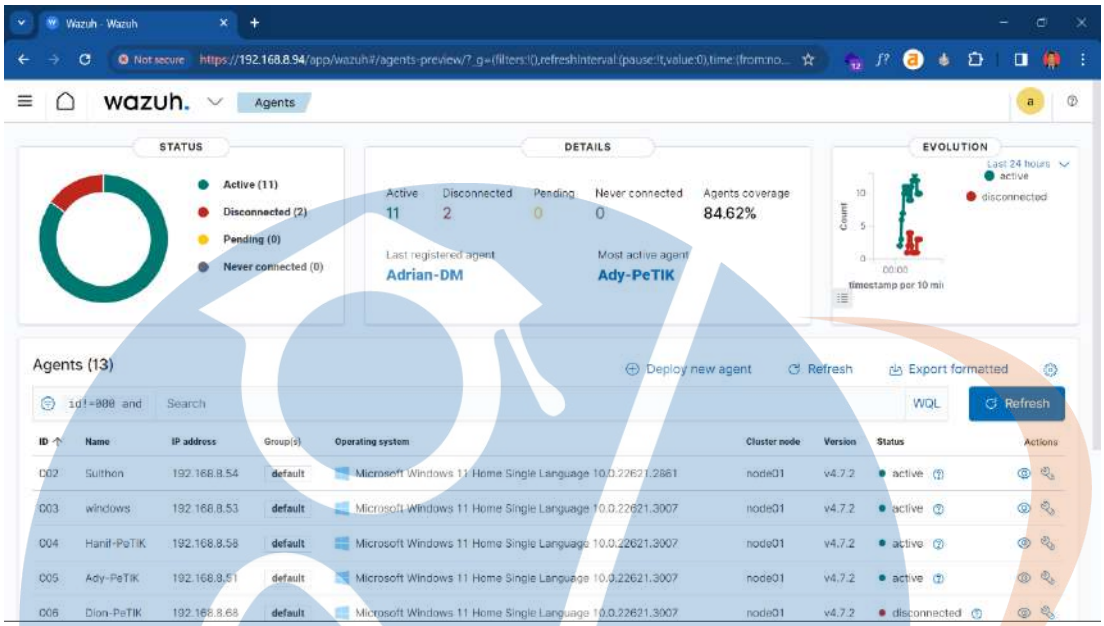
Gambar 4. 12. Masukkan Server Address

Selanjutnya, wazuh dashboard akan memberikan perintah untuk melakukan instalasi wazuh agent. Copy perintah dan jalankan di PowerShell Administrator.



Gambar 4. 13. Perintah Jalankan Instalasi Wazuh Agent

Setelah selesai dan berhasil maka wazuh agent akan tampil pada wazuh dashboard.

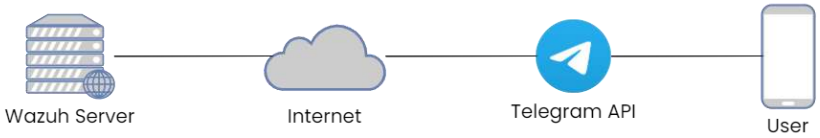


Gambar 4. 14. Tampilan Agent Yang Sudah Terinstall

Setelah pemasangan Wazuh Agent pada sebuah server berhasil, maka Wazuh Agent 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.

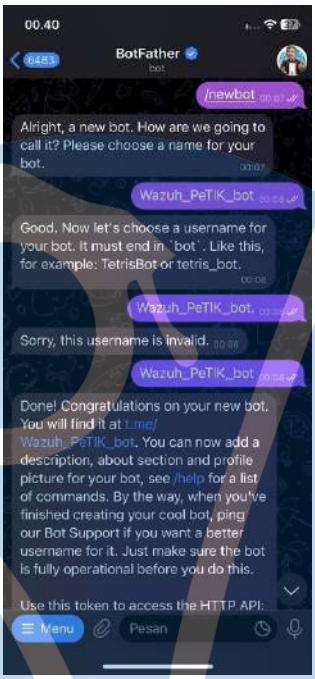
4.1.5 Integrasi Wazuh dengan Telegram

Untuk mempermudah administrator sistem maka dibuatlah notifikasi serangan menggunakan chatbot telegram untuk mengirimkan notifikasi ketika serangan terjadi secara realtime. Berikut tahapan dalam integrasi wazuh ke Chatbot Telegram.



Gambar 4. 15 Sistem Integrasi Bot Telegram

Pertama, membuat Telegram Bot dengan menggunakan API KEY dan CHAT ID menggunakan *BotFather Telegram.*



Gambar 4. 16. BotFather Telegram

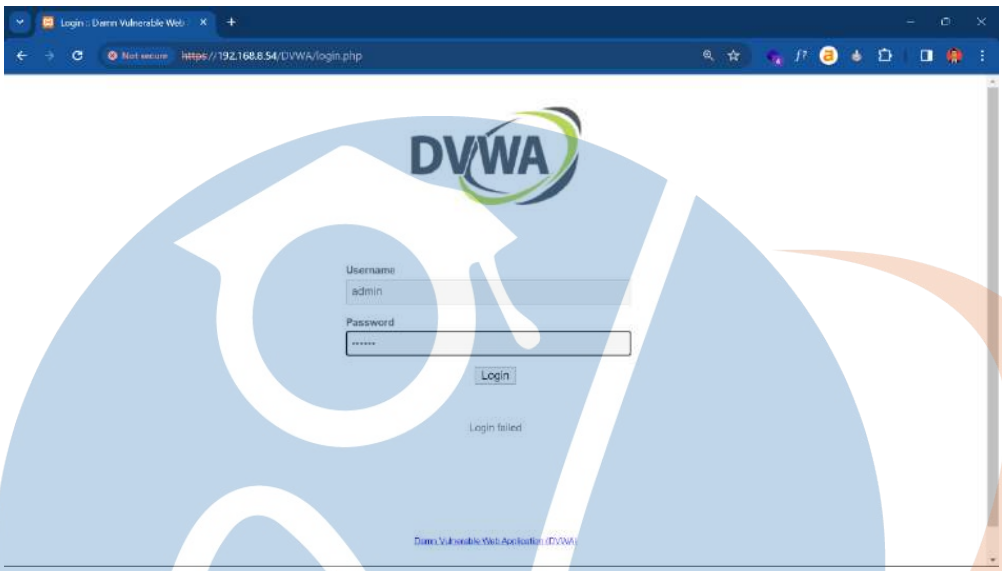
Mulai chat *BotFather* dengan perintah /start kemudian BotFather akan membalas chat dengan meminta nama untuk bot yang akan dibuat. Setelah nama sesuai dan disetujui maka BotFather akan mengirimkan API KEY yang nanti akan kita gunakan untuk integrasi wazuh server.

4.2 Pengujian Serangan Security

4.2.1 *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 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 masuk seperti username atau password.



Gambar 4. 17. Website DVWA Pada Agent

Selanjutnya, Wazuh Dashboard mendeteksi aktivitas serangan bruteforce yang dilakukan attacker terhadap Web pada Wazuh Agent.

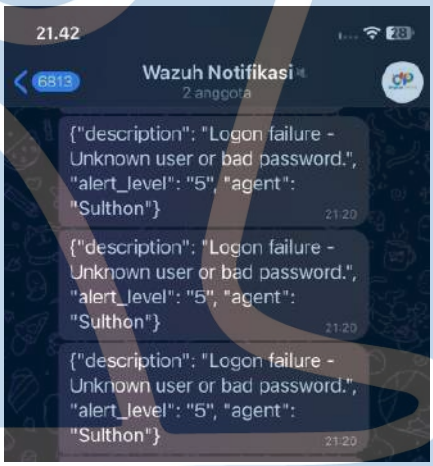
Gambar 4. 18 Hasil Pengujian Bruteforce

Pada Gambar 4. 18 menunjukkan hasil pengujian serangan bruteforce, yaitu adanya upaya login yang gagal menggunakan username atau password yang tidak valid.

›	Jan 20, 2024 @ 20:48:27.189	Logon failure - Unknown user or bad password.	5
›	Jan 20, 2024 @ 20:48:25.851	Logon failure - Unknown user or bad password.	5
›	Jan 20, 2024 @ 20:48:23.773	Logon failure - Unknown user or bad password.	5
›	Jan 20, 2024 @ 20:48:18.501	Logon failure - Unknown user or bad password.	5

Gambar 4. 19 Hasil Pengujian Request Time Out (RTO)

Pada Gambar 4.19 menunjukkan hasil pengujian yang menunjukkan adanya Request Time Out (RTO), yang merupakan kondisi dimana koneksi internet terganggu saat user mencoba mengakses server.



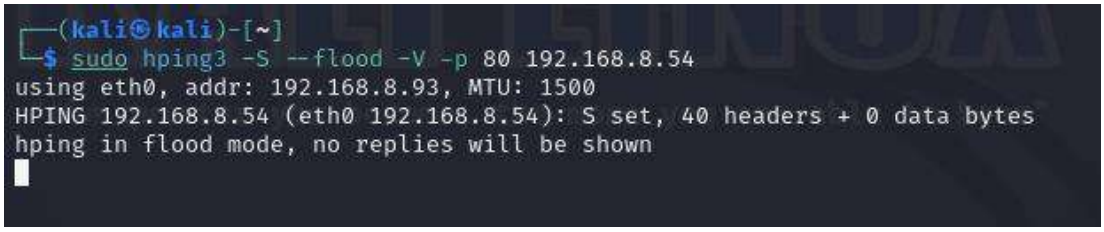
Gambar 4.20 Notifikasi Bot Wazuh Telegram

Pada Gambar 4.18 menunjukkan hasil notifikasi pada bot telegram yang sudah diintegrasikan dengan wazuh.

4.2.2 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 ini dilakukan menggunakan kali Linux dengan menggunakan perintah:

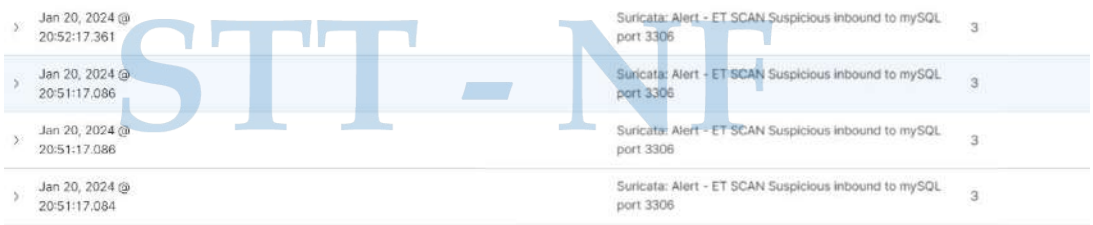
sudo hping3 -S –flood -V -p 80 192.168.8.54



Gambar 4. 23 Serangan SYN Flood

Berikut terdapat beberapa penjelasan mengenai fungsi dari setiap kata dalam perintah tersebut:

a. "sudo" adalah perintah untuk memberikan izin akses kepada superuser untuk mengeksekusi perintah.
b. "hping3" adalah digunakan untuk mengirim paket jaringan dan menguji serangan pada jaringan.
c. "-S" digunakan untuk mengirimkan paket bertanda SYN pada protocol TCP. Perintah ini dapat pula digunakan untuk melakukan serangan SYN flooding.
d. "--flood" adalah perintah untuk mengaktifkan mode flooding pada hping3 yang mengirimkan paket jaringan dalam jumlah tinggi dengan kecepatan tinggi pula pada target yang telah ditentukan.
e. "-V" adalah perintah untuk menampilkan rincian informasi setiap paket yang dikirim dan diterima.
f. "-p 80" adalah perintah untuk menentukan port target sasaran serangan.
g. *"192.168.8.54"* adalah alamat IP wazuh agen yang menjadi target serangan.



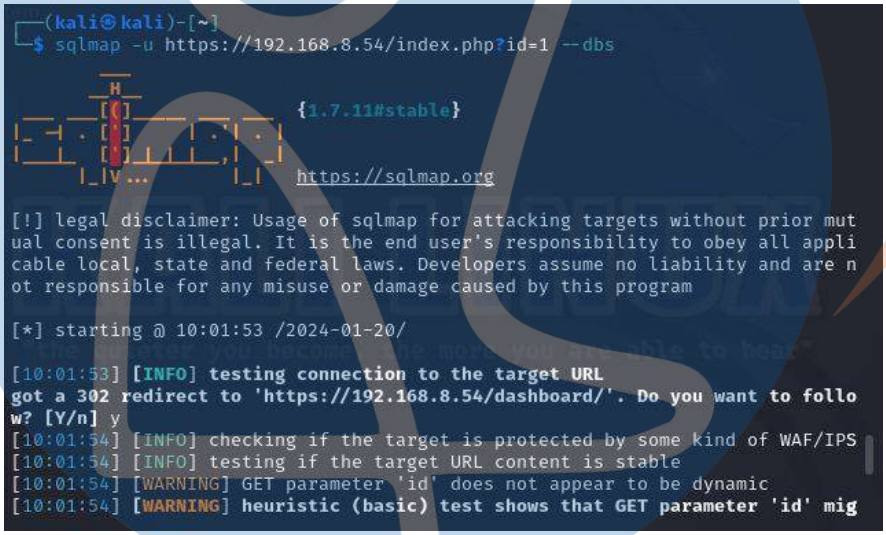
Gambar 4. 24 Hasil Pengujian SYN Flood

Pada Gambar 4. 22. menggambarkan hasil pengujian bahwa pada *Wazuh Dashboard* telah terdeteksi serangan *DoS Attack* yang mendeteksi serangan terhadap mySQL pada port 3306.

4.2.3 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 menungkinkan 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 dengan menggunakan perintah:

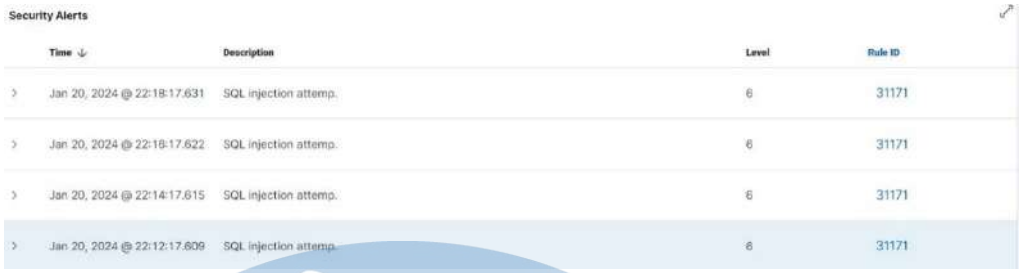
Sqlmap -u https://192.168.8.54 --dbs



Gambar 4. 25 Serangan SQL Injection

Berikut terdapat beberapa penjelasan mengenai fungsi dari setiap kata dalam perintah tersebut:

a. “Sqlmap” adalah perintah untuk melakukan eksploitasi kerentanan SQL Injection secara otomatis.
b. “-u” adalah perintah untuk menetapkan Alamat URL.
c. " *https://192.168.8.54*" adalah alamat URL situs web yang ingin diuji.
d. “–dbs” adalah perintah untuk menghitung database yang tersedia.



Gambar 4. 26 Hasil Pengujian SQL Injection

Pada Gambar 4. 24 menunjukkan hasil pengujian yang menyatakan bahwa pada *Wazuh Dashboard* telah terdeteksi serangan *SQL Injection*.

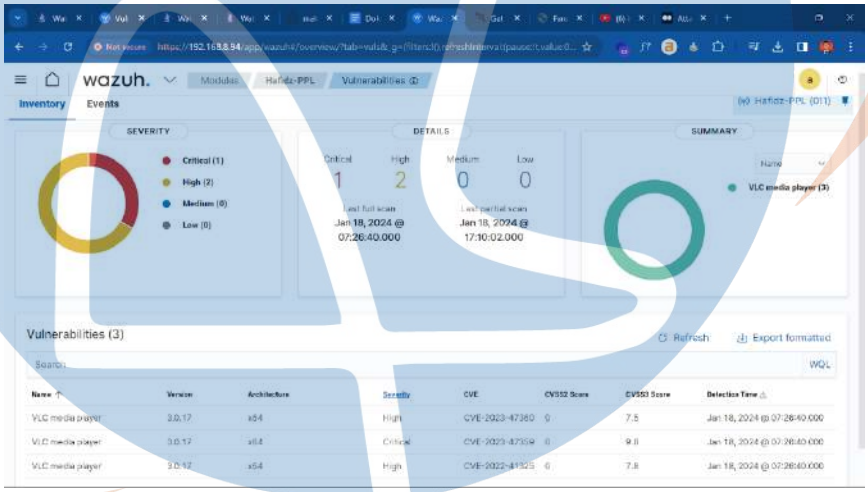
Tabel 4. 1. Hasil Pengujian Serangan

No	Pengujian Serangan	Ekspektasi	Hasil	Ket
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.
		Notifikasi Alert Telegram Bot	Tidak Sesuai Harapan	Tidak muncul notifikasi atau keterangan alert system pada telegram bot
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 4.1. 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 bruteforce, sementara untuk 2 serangan lainnya perlu dilakukan konfigurasi lebih lanjut.

4.2.4 Vulnerabilities Software



Gambar 4. 27. Vulnerabilities Software

Pada Gambar 4. 25 menunjukkan hasil vulnerabilities software yang menyatakan bahwa pada *Wazuh Dashboard* terdeteksi software yang memiliki kerentanan yaitu VCL media player yang memiliki kerentanan *high/critical* dengan skor CVSS (*Common Vulnerability Scoring System*) paling tinggi 9.8.

4.3 Pengujian Performance

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.

4.3.1 Kinerja CPU

Pertama, pengujian dilakukan terhadap kinerja CPU. Hasil pengujian diwakili oleh persentase yang ditunjukkan pada Tabel 4.2.

Tabel 4. 2. Hasil Pengujian CPU

Server	Persentase Sebelum Serangan	Persentase Sesudah Serangan
Agent	0.0% - 15%	0.0% - 60%

Berdasarkan Tabel 4.2, 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.

4.3.2 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 4.3.

Tabel 4. 3. Hasil Pengujian Memory

Server	Persentase Sebelum Serangan	Persentase Sesudah Serangan
Agent	0.0% - 40.0%	0.0% - 40.0%

Berdasarkan Tabel 4.3, 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.

4.3.3 Analisis

Dari hasil implementasi wazuh sampai dengan pengujian serangan yang dilakukan maka dilakukan analisis sebagai berikut:

1. Visualisasi Wazuh Dashboard memberikan pemahaman lebih baik dalam menghasilkan representasi grafis dari log insiden yang dapat membantu pengguna untuk mengidentifikasi ancaman keamanan dengan lebih efektif.
2. Integrasi aplikasi Wazuh dengan bot Telegram sebagai alert system memberikan respons real-time terhadap potensi ancaman keamanan. Dimana log yang ditangkap oleh Wazuh secara real-time dikirimkan ke Bot Telegram lengkap dengan keterangan dan tingkat alert-level tergantung potensi ancaman keamanan.
3. Pada pengujian pertama, jenis serangan yang dilakukan adalah BruteForce pada website DVWA yang sebelumnya telah diinstal pada Wazuh agent. Tujuan dari penyerangan ini adalah memecahkan username dan password login milik user. Penyerangan dilakukan sebanyak 4 kali, yaitu 2 kali serangan gagal login password, dan 2 kali serangan gagal login username. Keempat serangan tersebut berhasil dideteksi oleh Wazuh. Selain itu, penyerangan yang dilakukan juga terdeteksi sebagai Request Time Out (RTO) akibat gangguan koneksi internet user saat mengakses server pada agent.
4. Selanjutnya pada serangan kedua, dilakukan penyerangan DoS Attack dengan SYN Flood. SYN Flood akan melemahkan respon suatu server. Secara default, Wazuh tidak memiliki kemampuan mendeteksi serangan seperti ini. Sebagai solusinya, Wazuh membutuhkan Suricata sebagai network base yang dapat mengenali adanya serangan DoS. Cara kerja dari Suricata adalah

menyimpan log penyerangan yang dikenali sebagi DoS, kemudian mengirimkannya kepada Wazuh untuk diidentifikasi. Berdasarkan pengujian menggunakan serangan DoS dengan SYN Flood, diketahui bahwa Wazuh dapat memantau serta mengidentifikasi adanya serangan dengan bantuan Suricata.

5. Pengujian ketiga dilakukan dengan jenis serangan SQL Injection website DVWA yang sebelumnya telah diinstal pada Wazuh agent. Serangan SQL Injection bertujuan untuk menyalahgunakan keamanan pada database. Pada penelitian ini, serangan SQL Injection dilakukan pada kali Linux. Hasilnya menunjukkan bahwa Wazuh memiliki kemampuan mengenali seluruh serangan secara real time dari user maupun dari pihak luar.
6. Berdasarkan pemantauan pada kinerja CPU, diketahui bahwa CPU berada dalam kondisi normal saat persentasenya 0.0%-15%. Setelah dilakukan penyerangan terhadap agent (Gateaway dan Website), kinerja CPU diketahui mengalami peningkatan menjadi 0.0%-60%. Peningkatan kinerja CPU tersebut terjadi akibat Meningkatnya aktivitas pada server sehingga beban kerja CPU turut bertambah.
7. Selain mengukur kinerja CPU, selanjutnya dilakukan pengukuran kinerja memori. Memori dikatakan berada dalam keadaan normal apabila persentasenya adalah 0.0%-40.0%. Hasil pengukuran kinerja memori menunjukkan bahwa tidak ada peningkatan persentase sebelum penyerangan ataupun setelah penyerangan. Hal ini menunjukkan bahwa memori bekerja optimal dengan write speed memory yang sama terhadap kondisi sebelum dan sesudah serangan.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini bertujuan untuk melakukan implementasi Wazuh dalam pengelolaan dan pemantauan keamanan jaringan, menampilkan visualisasi berdasarkan log insiden, dan mengintegrasikan temuan aplikasi Wazuh dengan bot Telegram sebagai alert system. Dalam menjawab tujuan penelitian tersebut, dapat disimpulkan bahwa:

1. Penelitian ini berhasil mengimplementasikan Wazuh sebagai alat untuk efektif mengelola dan memonitor keamanan pada jaringan yang diteliti. Dengan menggunakan Wazuh, penelitian telah menunjukkan kemampuan sistem untuk mendeteksi dan merespon potensi ancaman keamanan. Beberapa serangan seperti *BruteForce, Dos Attack, dan SQL Injection* berhasil terdeteksi oleh Wazuh dan sesuai dengan harapan dalam penelitian ini.
2. Visualisasi berdasarkan log insiden pada jaringan memberikan pemahaman lebih baik terhadap pola keamanan. Dengan demikian, penelitian telah mencapai tujuan dalam menghasilkan representasi grafis dari log insiden yang dapat membantu pengguna untuk mengidentifikasi ancaman keamanan dengan lebih efektif.
3. Integrasi temuan aplikasi Wazuh dengan bot Telegram sebagai alert system memberikan respons real-time terhadap potensi ancaman keamanan. Hal ini meningkatkan efisiensi dalam tindakan tanggap terhadap insiden keamanan yang terdeteksi.
4. Saat dilakukan penyerangan, persentase kinerja CPU meningkat dari 0.0% - 15% menjadi 0.0% - 60%. Hal itu dipengaruhi oleh jumlah event aktivitas yang terjadi didalam server sehingga adanya penambahan beban kerja terhadap CPU. Sedangkan pengukuran kinerja memory dalam keadaan normal yaitu memiliki persentase 0.0% - 40.0%. Hal ini menunjukkan bahwa persentase kinerja memory tetap berjalan dengan normal dengan write speed memory yang sama terhadap kondisi server dalam keadaan apapun.

5.2 Saran

1. Peningkatan Fungsionalitas Wazuh: Untuk penelitian selanjutnya, disarankan untuk mengeksplorasi dan meningkatkan fungsionalitas Wazuh. Pengembangan fitur-fitur baru atau penyesuaian agar sesuai dengan kebutuhan spesifik lingkungan jaringan tertentu dapat menjadi fokus penelitian.
2. Optimasi Visualisasi Log: Perlu adanya penelitian lebih lanjut dalam mengoptimalkan visualisasi log insiden. Peningkatan dalam representasi grafis dan analisis data dapat membantu pengguna untuk lebih mudah memahami dan merespons ancaman keamanan.
3. Ekspansi Integrasi dengan Platform Lain: Penelitian dapat melibatkan eksplorasi lebih lanjut terkait integrasi Wazuh dengan platform lain selain Telegram. Mengintegrasikan sistem dengan berbagai platform dapat meningkatkan fleksibilitas dan kebergunaan aplikasi.
4. Studi Kasus Lanjutan: Sebagai saran tambahan, penelitian selanjutnya dapat melibatkan studi kasus lanjutan dengan skenario yang lebih kompleks atau jaringan yang lebih besar. Hal ini dapat membantu menguji dan mengembangkan aplikasi Wazuh dalam konteks yang lebih luas.

Dengan melanjutkan penelitian berdasarkan saran-saran diatas, diharapkan peneliti dapat berkontribusi lebih untuk pengembangan dan pemahaman keamanan jaringan menggunakan Wazuh.

DAFTAR REFERENSI

[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] Documentation Wazuh, “Wazuh Documentation.” Accessed: Nov. 06, 2023. [Online]. Available: Https://Documentation.Wazuh.Com/Current/Getting-Started/Components/Index.Html

[16] D. S. Sampurno, A. Noertjahyana, And A. Setiawan, “Implementasi Pembuatan Distro Linux Untuk Keperluan Laboratorium Informatika,” 2019.

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

STT - NF