Analisa Deteksi Insiden Keamanan Jaringan menggunakan Wazuh Sebagai *Security Information and Event Management (SIEM)* pada Medianusa Permana

Muhammad Imam Gumilang[1], Atthariq[2], Guntur Syahputra[3]

[1,2,3] *Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA
[1]gumilang.imam@gmail.com (penulis korespondensi)
[2]attharig.huzaifah@pnl.ac.id
[3]guntursyahputra@pnl.ac.id

***Abstrak*— *Security Information and Event Management (SIEM)* adalah teknologi yang dirancang untuk menyatukan infomasi dari berbagai sumber keamanan untuk dilakukan analisis yang menghasilkan pelaporan yang efektif. *Platform* Wazuh menawarkan teknologi *SIEM* yang memberikan solusi bermanfaat untuk keamanan jaringan pada perusahaan penyedia layanan internet seperti PT. Medianusa Permana. *Platform* Wazuh mampu mendeteksi berbagai jenis serangan seperti *Denial of Service (DoS)* yang dibuktikan dengan percobaan serangan sebanyak 5 serangan dengan beban 20, 40, 60, 80, dan 100, yang menghasilkan peningkatan nilai pada fitur *Threat Hunting* sebesar 642 dan *Event* sebanyak 705. *SQL Injection* juga dilakukan sebanyak 5 serangan yang menghasilkan peningkatan nilai rata-rata pada fitur *Mittre Attack* sebanyak 400 dan pada fitur *Threat Hunting* juga terdapat lonjakan nilai dari nilai awal 163 menjadi 54.325 setelah dilakukan serangan *SQL Injection* sebanyak 5 kali serangan. Teknologi *Monitoring* pada PT. Medianusa Permana terdapat peningkatan ketika telah dilakukan implementasi *SIEM*, yang sebelumnya hanya terdapat *monitoring resource* dari sistem *server* perusahaan tersebut, kini teknologi *monitoring* pada perusahaan tersebut sudah mampu mendeteksi berbagai jenis serangan jaringan yang dapat meminimalisir resiko ancaman insiden keamanan jaringan menggunakan *Platform* Wazuh.**

***Kata kunci*— *Monitoring*, *Server*, Wazuh, *Security Information and Event Management*, *Denial of Service*, *SQL Injection*.**

Abstract*— *Security Information and Event Management (SIEM) is a technology designed to unify information from multiple security sources to perform analyzes that produce effective reporting. The Wazuh platform offers SIEM technology which provides useful solutions for network security for internet service provider companies such as PT. Medianusa Permana. The Wazuh platform is able to detect various types of attacks such as Denial of Service (DoS) as proven by 5 attack attempts with loads of 20, 40, 60, 80, and 100, which resulted in an increase in the value of the Threat Hunting feature by 642 and Event by 705. SQL Injection was also carried out in 5 attacks which resulted in an increase in the average value for the Mitre Attack feature by 400 and for the Threat Hunting feature there was also a score gain from the initial value of 163 to 54,325 after carrying out 5 SQL Injection attacks. Monitoring Technology at PT. Medianusa Permana saw improvements when SIEM was implemented, where previously there was only resource monitoring from the company's server system, now the company's monitoring technology is able to detect various types of network attacks which can minimize the risk of threats to network security incidents using the Wazuh Platform.

Keywords*— *Monitoring, Server, Wazuh, Security Information and Event Management, Denial of Service, SQL Injection.

I. Pendahuluan

Dalam era digital saat ini, keamanan jaringan menjadi salah satu bagian yang sangat krusial dalam operasional teknologi informasi. Perusahaan menghadapi berbagai ancaman keamanan yang terus berkembang, mulai dari serangan siber, *malware*, hingga pencurian data. Insiden keamanan jaringan dapat menyebabkan kerugian finansial yang signifikan, kerusakan reputasi, dan pelanggaran privasi data yang dapat berdampak jangka panjang.

PT. Medianusa Permana sebagai perusahaan yang bergerak di bidang teknologi informasi dan penyedia layanan internet, sangat menyadari pentingnya menjaga keamanan jaringan. Sebagai langkah pr*event*if, perusahaan ini membutuhkan sistem yang mampu mendeteksi, menganalisis, dan merespons insiden keamanan jaringan secara real-time. Salah satu solusi yang dapat diimplementasikan adalah penggunaan *Security Information and Event Management (SIEM)* yang menggabungkan pengelolaan informasi keamanan dan manajemen insiden keamanan dalam satu *platform*.

Security Information and Event Management (SIEM) adalah teknologi yang dirancang untuk menyatukan informasi dari berbagai sumber keamanan untuk analisis dan pelaporan yang lebih efektif. *SIEM* mengumpulkan data dari sumber log keamanan, aktivitas jaringan, data sistem, dan informasi yang berkaitan, *SIEM* juga menggunakan aturan dan skenario untuk menganalisis data yang dikumpulkan dengan tujuan mendeteksi aktivitas yang mencurigakan, hal ini melibatkan pemantauan pola dan tanda-tanda yang berpotensial dari serangan keamanan. *SIEM* menggabungkan informasi dari berbagai sumber untuk mencoba mengaitkan

kejadian-kejadian yang terkait, membentuk gambaran lengkap tentang potensi ancaman atau serangan yang sedang berlangsung, kemudian *SIEM* akan memberikan peringatan atau notifikasi [12].

Wazuh merupakan salah satu *platform Security Information and Event Management (SIEM)* yang open source. Wazuh menawarkan solusi yang sangat bagus dan bermanfaat bagi sebuah instansi atau perusahan yang melakukan implementasi *platform* ini dalam pengelolaan dan pemantauan terhadap sistem jaringan mereka. Wazuh menyediakan deteksi dini untuk aktivitas yang mencurigakan atau abnormal yang melibatkan pemantauan pada sistem *log* aktivitas, melakukan analisis terhadap keamanan, dan melaporkan terkait serangan atau sebuah insiden keamanan. Wazuh juga menyediakan fitur pelaporan dan dapat melakukan visualisasi yang memudahkan perusahaan untuk memahami data keamanan dan membuat laporan keamanan yang terstruktur.

Tinjauan teoritis membahas secara mendalam teori-teori yang relevan, seperti Jaringan Komputer, Internet, *Server*, Sistem Operasi Ubuntu, Keamanan Jaringan, Sistem *Monitoring*, yang akan digunakan untuk menganalisis data dan menjawab permasalahan penelitian.

A. Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas beberapa unit komputer yang didesain sedemikian rupa sebagaimana tujuan utamanya yakni untuk dapat berbagi sumber daya, berkomunikasi, dan dapat mengakses informasi. Jaringan komputer adalah dua atau lebih komputer yang terhubung satu sama lain dan digunakan untuk berbagi data. Jaringan komputer dibangun dengan kombinasi *hardware* dan software [6].

B. Internet

Internet adalah wujud dari perpaduan jaringan komputer-komputer dunia, internet perlu juga dipandang serius sebagai gudang informasi. Internet menjadi salah satu sumber daya informasi yang sangat potensial untuk mempermudah sistem kehidupan. Bayangkan saja, kehadiran internet telah mampu melahirkan sebuah sistem kehidupan baru yang lain, atau diistilahkan dengan dunia maya. Dunia maya memiliki kemiripan yang sangat jelas dengan kehidupan nyata. Apa yang Anda lakukan di dunia nyata, saat ini bisa juga kita lakukan di dunia maya [4].

C. Server

Server adalah suatu sistem komputer yang menyediakan jenis layanan tertentu untuk client dalam suatu jaringan komputer. Server dilengkapi dengan sistem operasi khusus untuk mengontrol akses dan sumber daya yang ada di dalamnya biasanya sistem operasi khusus tersebut disebut sistem operasi jaringan atau *Network Operating System*. Selain itu server didukung dengan RAM yang besar dan prosesor yang bersifat scalable [6].

D. Sistem Operasi Ubuntu

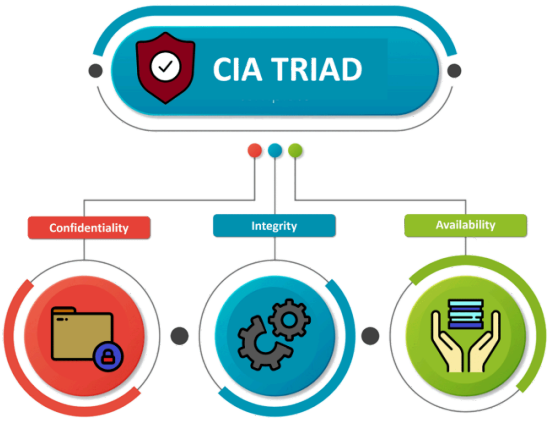
Ubuntu merupakan sistem operasi yang berbasis atau distribusi Linux (atau sering dikenal sebagai “distro”) berbasis Debian dan kaya akan fitur di dalamnya. Sistem operasi Ubuntu bersifat open-source sehingga bisa digunakan oleh siapa saja dengan gratis.

Ubuntu berasal dari filosofi Afrika Selatan yang berarti ”*humanity to others*” di mana harapannya sistem operasi Ubuntu ini dapat menghubungkan interaksi manusia di seluruh belahan dunia. Sistem operasi tersebut pertama kali dirilis pada 2004 oleh Mark Shuttleworth, seorang pebisnis dari Afrika Selatan di bawah perusahaan Canonical. Sebagai pengelola Ubuntu, Canonical bertugas untuk merilis versi Ubuntu yang baru setiap enam bulan untuk yang reguler dan dua tahun sekali untuk versi *Long Term Service (LTS)*. Alhasil, Ubuntu menjadi sistem operasi yang stabil dan berkualitas.

E. Keamanan Jaringan

Keamanan Jaringan atau *Cyber Security* adalah suatu kegiatan yang dilakukan oleh sistem dalam rangka menjaga, melindungi sistem dan jaringan komputer dari suatu serangan ilegal dari seseorang. Perlindungan pada sistem jaringan ini dapat berupa perangkat lunak (*Software*), aplikasi atau perangkat lain yang berhubungan dengan sistem komputer. Dengan adanya sistem ini, pihak- pihak yang memiliki data dapat menanggulangi ancaman di sistem jaringan komputer.

Dalam definisi lain, keamanan jaringan juga dapat diartikan sebagai suatu praktik atau bidang yang melindungi sistem, jaringan, dan program dari serangan digital. Serangan yang dimaksud adalah serangan siber (*cyber attack*). Serangan siber adalah suatu tindakan jahat dan disengaja oleh seseorang atau organisasi untuk mencoba meretas sistem informasi dari orang lain atau organisasi lain. Serangan ini dilakukan biasanya dikarenakan ingin mendapatkan keuntungan dari korban berupa mengakses data, mengubah data, menghancurnya informasi yang sensitif, mengambil uang melalui ransomware, atau mengganggu kegiatan bisnis yang berjalan normal. Untuk memahami keamanan siber lebih lanjut, terdapat 3 prinsip dasar dalam keamanan informasi yang perlu dipahami, yaitu Kerahasiaan, Integritas, dan Ketersediaan atau lebih sering dikenal CIA Triad [8].

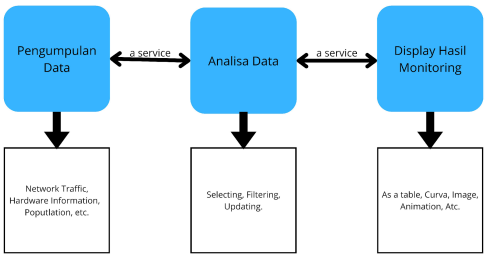


Gambar 1 *CIA TRIAD*

1) *Confidentiality*, merupakan karakteristik utama untuk sistem yang aman. Kerahasiaan ini memastikan bahwa data dan informasi hanya tersedia untuk orang-orang yang memiliki akses untuk mengaksesnya atau dengan kata lain informasinya tidak disebarluaskan kepada individu yang tidak berwenang.
2) *Integrity*, merupakan suatu karakteristik yang mana informasi yang ada mengacu kepada fakta bahwa informasi yang disimpan tidak diubah dengan cara yang berbeda dari data yang sebelumnya ada atau dengan kata lain data telah diubah oleh pihak yang tidak berwenang.
3) *Availability*, mengacu kepada kebutuhan untuk dapat menggunakan layanan atau *software* bila diperlukan dengan cara yang memungkinkan untuk melakukan fungsi yang dirancang. Ketersediaan memastikan bahwa setiap klien bisa mengakses informasi yang mereka inginkan sesuai dengan hak akses dan kebutuhan mereka.

F. Sistem *Monitoring*

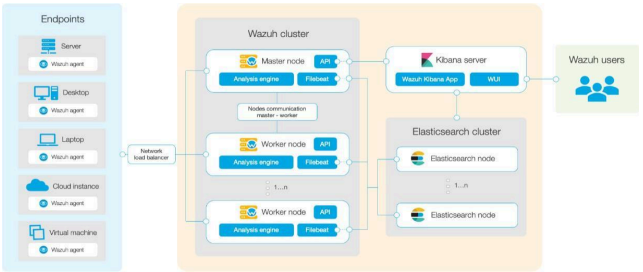
Sistem *Monitoring* merupakan suatu proses untuk mengumpulkan data dari berbagai sumber daya, biasanya data yang dikumpulkan merupakan data yang *real time*. Sistem *monitoring* adalah bagian yang tidak terpisahkan dari sebuah infrastruktur jaringan/sistem yang merupakan kebutuhan yang tidak boleh ditunda-tunda. Sistem *monitoring* akan melakukan sistem deteksi dini berguna memonitor kesehatan dari sisem dan jaringan [4].



Gambar 2 Sistem *Monitoring*

G. *SIEM*

Security Information and Event Management (SIEM) merupakan sistem *monitoring* yang mampu mendeteksi serangan dan respons sistem keamanan terhadap serangan melalui analisis log dari berbagai *event*-log yang bersumber dari data secara real-time. Log merupakan informasi dari perangkat yang berisi kegiatan dari log tersebut, mulai dari lalu lintas jaringan, status dari perangkat dan lainnya.



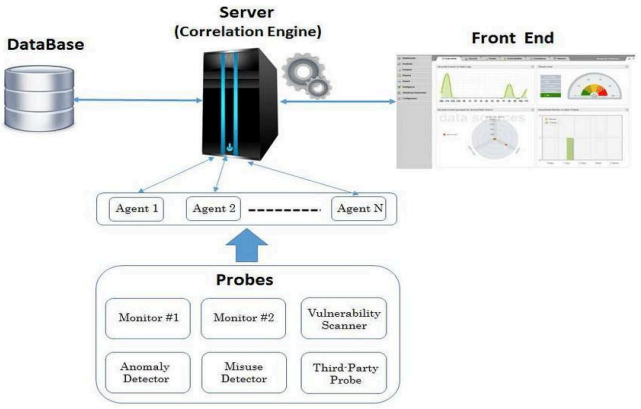
Gambar 3 *SIEM*

Sistem SIEM bekerja dengan mengumpulkan data dari berbagai sumber dalam infrastruktur jaringan, termasuk dari jaringan, security, server, database, dan aplikasi untuk mengidentifikasi potensi ancaman, baik yang berasal dari eksternal ataupun internal. Perangkat-perangkat pemberi input SIEM dianggap sebagai sensor yang menangkap kejadian sesuai dengan tempatnya berada. Data yang berhasil dikumpulkan akan ditampilkan pada dashboard dalam bentuk chart sehingga lebih mudah dibaca dan dimengerti, ataupun lebih mudah menemukan suatu pola khusus. SIEM menyediakan penyimpanan jangka panjang, sehingga dapat dilakukan korelasi data dalam jangka waktu yang cukup lama. Teknologi SIEM dapat melakukan teknik korelasi yang terintegrasi dengan berbagai sumber data, sehingga data dapat diproses menjadi informasi yang bermanfaat [2].

H. Wazuh

Wazuh merupakan *platform* open source yang berfungsi sebagai sistem deteksi ancaman, pemantauan keamanan dan respon insiden. *Platform* Wazuh merupakan implementasi dari *Security Information and Event Management* (SIEM). Wazuh menyediakan berbagai fitur yang dapat menganalisis data log, instruksi dan deteksi malware, pemantauan integritas file, penilaian konfigurasi dan deteksi kerentanan sistem. Wazuh memiliki 3 buah komponen yaitu :

1) Wazuh Agent, merupakan sebuah endpoints seperti desktop, server, instans cloud atau mesin virtual, yang dapat melakukan pencegahan, deteksi, dan response.
2) Wazuh Server, merupakan server yang bertugas menganalisis data yang diterima oleh agent dan memprosesnya melalui decoder dan aturan.
3) Elastic Stack , digunakan untuk melakukan pencarian dan analisis.



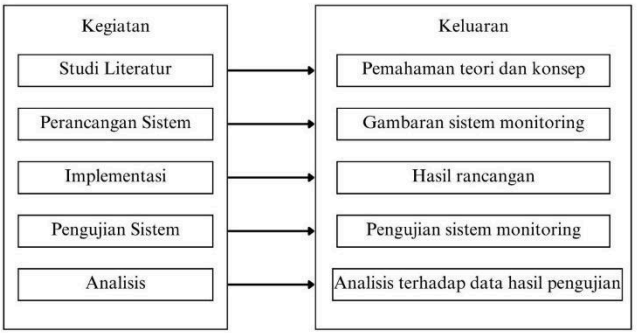
Gambar 4 Arsitektur Wazuh

II. Metodologi Penelitian

A. Tahapan Penelitian

Dalam penyusunan penelitian ini diperlukan sebuah sususan tahapan penelitian yang terstruktur agar dapat membantu dalam penyusunan penelitian. Tahapan penelitian ini terdiri langkah-langkah yang akan dilakukan dalam

penyelesaian masalah yang akan dibahas. Adapun tahapan penelitian yang akan dilakukan dapat dilihat pada gambar 1 berikut.



Gambar 5 Tahapan Penelitian

Penjelasan dari tahapan metode yang akan dilakukan ini :

Pada tahapan awal melakukan studi literatur, mencari berbagai referensi dari berbagai sumber seperti buku, jurnal ilmiah, referensi yang bersumber dari perpustakaan maupun internet dan lainnya yang berhubungan dengan judul penelitian yang akan dilakukan.

1) Perancangan system pada penelitian ini menjelaskan perancangan system yang akan dibangun yaitu system *monitoring* yang menggunakan *Platform* Wazuh.
2) Tahapan implementasi merupakan kegiatan instalasi berbagai kebutuhan untuk melakukan *monitoring* pada server PT. Medianusa Permana, hal yang dibutuhkan untuk proses ini seperti Wazuh Server, Wazuh Indexer, Wazuh Dashboard, dan Wazuh Agent.
3) Tahapan lanjutan setelah implementasi yaitu tahapan pengujian. Tahapan ini bertujuan untuk memastikan hasil dari sebuah sistem yang telah dibuat berjalan dan sesuai dengan perancangan sistem sebelumnya.
4) Kemudian akan dilakukan analisa terhadap aktivitas *monitoring* dan deteksi ancaman keamanan jaringan yang ditawarkan oleh *platform* Wazuh.

B. Rancangan Sistem

Adapun tahapan perancangan sistem merupakan tahap setelah menganalisis masalah yang terjadi, maka aktivitas perancangan dimulai dengan mendesain dan merencanakan dimana sistem tersebut harus diletakkan dengan memperhitungkan beberapa kondisi dan peralatan yang harus diperhatikan agar sistem mampu berjalan dengan baik.

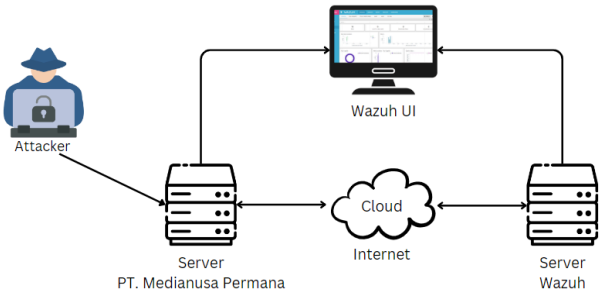
Agar sistem mampu berjalan sesuai dengan yang diharapkan, maka hardware yang akan digunakan juga harus diperhatikan. Meskipun sebenarnya tidak ada persyaratan tertentu mengenai spesifikasi hardware minimum yang harus dipenuhi dalam menjalankan sistem *monitoring* jaringan, khususnya Wazuh beserta plugins tambahan apabila dibutuhkan, namun berdasarkan data dari penelitian terkait dapat disimpulkan bahwa spesifikasi hardware atau komputer yang paling baik digunakan yaitu :

- Memiliki Processor 2 Core
- Menggunakan RAM 2 GB
- Menyediakan Storage 60 GB

Tahap selanjutnya yaitu merancang kebutuhan software yang dibutuhkan untuk menjalankan sistem *monitoring* agar mendapatkan data yang dibutuhkan yang nantinya data tersebut digunakan untuk kebutuhan analisa, adapun software yang akan digunakan yaitu :

- Sebuah Sistem Operasi Ubuntu
- Wazuh Indexer
- Wazuh Server
- Wazuh Dashboard
- Wazuh Agent

Dapat dilihat pada gambar 2 yang merupakan gambaran rancangan sistem *monitoring* yang akan dibuat.



Gambar 6 Rancangan Sistem

1) Arsitektur Wazuh

Arsitektur Wazuh didasarkan pada Wazuh Agent, yang berjalan pada endpoint yang dipantau dan meneruskan data keamanan ke server pusat. Perangkat tanpa Wazuh Agent seperti firewall, Switch, Router, dan Acces Point didukung dan dapat secara aktif mengirim data log melalui Syslog, SSH, atau API. Server pusat menerjemahkan dan menganalisis informasi yang diterima dan meneruskan hasilnya ke Wazuh Indexer untuk proses analisa dan penyimpanan.

Wazuh Indexer Cluster adalah kumpulan dari satu atau lebih node yang berkomunikasi satu sama lain untuk membaca dan menulis ke indeks. Penerapan Wazuh yang lebih kecil dan tidak memerlukan pemrosesan data dalam jumlah besar dapat dengan mudah ditangani oleh cluster node tunggal. Kluster multi-node direkomendasikan jika memantau banyak endpoint, ketika data dalam jumlah besar, maka perlu penyimpanan yang besar pula.

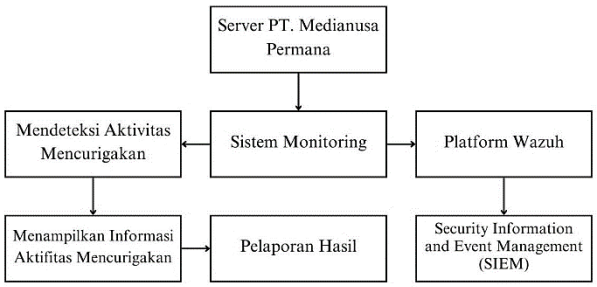
Diagram berikut mewakili arsitektur implementasi Wazuh dan menunjukkan komponen solusi dan bagaimana Wazuh Server dan node Wazuh Indexer dikonfigurasi sebagai cluster untuk menahan beban yang berlebih.

PT. Medianusa Permana sebagai perusahaan yang bergerak di bidang teknologi informasi dan penyedia layanan internet, menyadari pentingnya menjaga keamanan jaringan. Sebagai langkah pr*eventi*f, perusahaan ini membutuhkan sistem yang mampu mendeteksi, menganalisis, dan merespons insiden keamanan jaringan secara real-time. *Platform* Wazuh menawarkan semua hal yang dibutuhkan oleh perusahaan

tersebut, maka pada penelitian ini dilakukan implementasi Wazuh pada PT. Medianusa Permana.

2) Blok Diagram

Pada bagian ini akan menggambarkan sistem yang akan dianalisis serta bagaimana SIEM diterapkan. Penjelasan akan diberikan melalui diagram blok untuk memudahkan pemahaman. Berikut adalah diagram blok yang digunakan dalam perancangan sistem yang akan dibuat.



Gambar 7 Rancangan Diagram Blok

C. Teknik Pengujian

Tahapan teknik pengujian pada sistem deteksi ancaman keamanan jaringan pada PT. Medianusa Permana menggunakan Wazuh. Adapun tahapan teknik pengujian-nya, sebagai berikut :

1) *Penetration Testing* (Pengujian Penetrasi)

Pada pengujian ini dilakukan percobaan serangan siber terhadap salah satu Wazuh Agent atau client daripada Wazuh. Serangan yang dilakukan meliputi *Denial of Service (DoS), Dirsearch,* dan *SQL Injection*. Hal ini dilakukan untuk dapat menentukan akurasi kinerja *platform* Wazuh dalam mendeteksi insiden keamanan jaringan.

2) *Comparison Testing* (Pengujian Perbandingan)

Perbandingan dilakukan guna untuk mengetahui perbedaan performa sebelum dan sesudah dilakukan implementasi *monitoring* jaringan menggunakan *platform* Wazuh, dengan membandingkan fitur dan kemampuan dari *platform* tersebut.

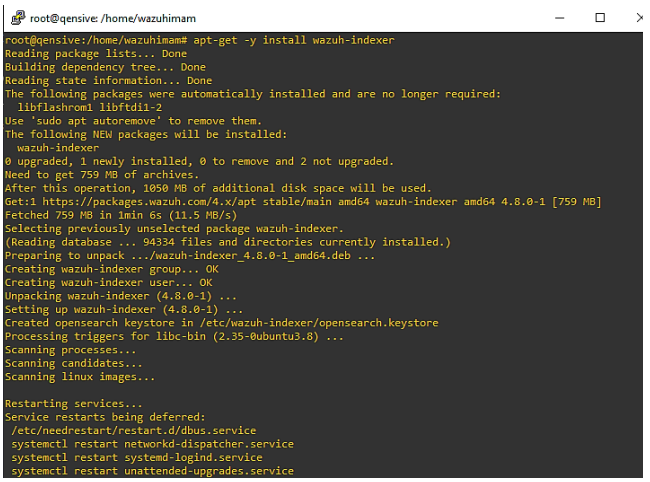
III. Hasil dan Pembahasan

A. Implementasi Wazuh Server

Berikut ini adalah bagaimana tahapan implementasi *monitoring* jaringan menggunakan *platform* Wazuh dengan metode *Security Information and Event Management* yang akan diterapkan pada PT. Medianusa Permana. Adapun tahapan untuk melakukan implementasi *platform* wazuh pada sebuah server dibutuhkan beberapa tahapan seperti, instalasi Wazuh-Indexer, Wazuh- Manager, dan Wazuh-Dashboard.

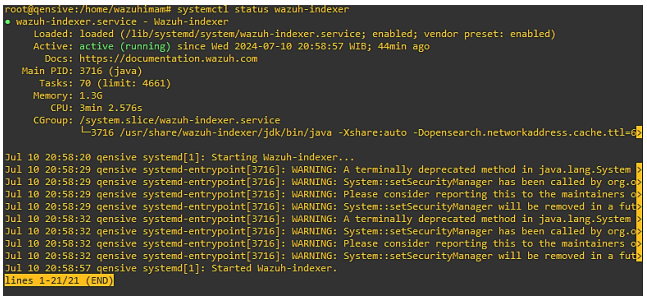
1) Wazuh Indexer

Berikut ini merupakan langkah instalasi Wazuh Indexer.



Gambar 8 Instalasi Wazuh Indexer

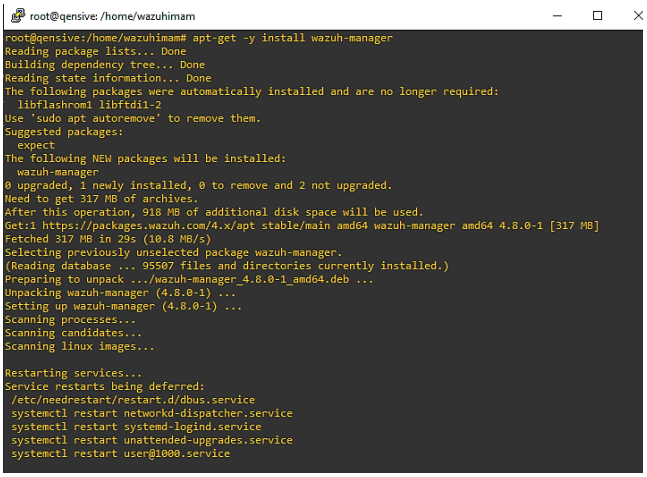
"apt-get -y install wazuh-indexer" merupakan perintah linux untuk mendapatkan *package* Wazuh Indexer sebesar 759 MB, proses pada gambar 1 menunjukkan instalasi telah berhasil dijalankan. Kemudian memastikan Wazuh Indexer telah aktif, dengan melakukan perintah "systemctl status wazuh-indexer", seperti gambar 2.



Gambar 9 Status Wazuh Indexer

2) Wazuh Server

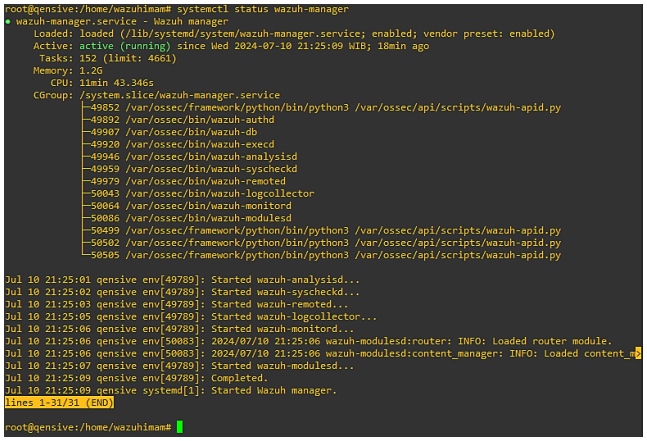
Berikut ini merupakan langkah instalasi Wazuh Server.



Gambar 10 Instalasi Wazuh Server

"apt-get -y install wazuh-manager" merupakan perintah linux untuk mendapatkan package Wazuh Server sebesar 317

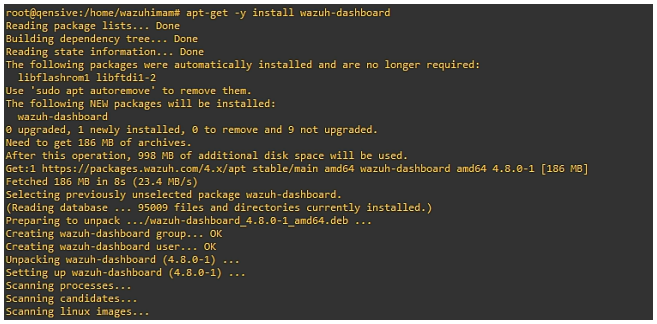
MB, proses pada gambar 3 menunjukkan instalasi telah berhasil dijalankan. Kemudian memastikan Wazuh Server telah aktif, dengan melakukan perintah "systemctl status wazuh-manager", seperti gambar 4.



Gambar 11 Status Wazuh Server

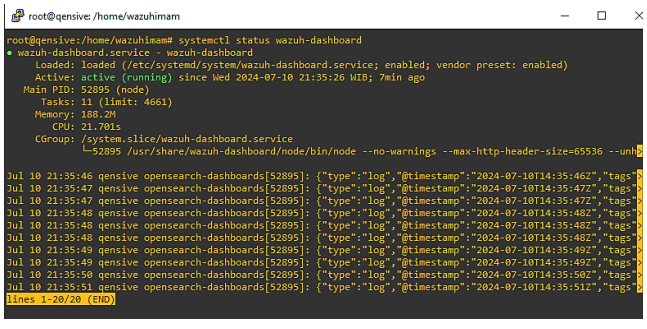
3) Wazuh Dashboard

Berikut ini merupakan langkah instalasi Wazuh Dashboard.



Gambar 12 Instalasi Wazuh Dashboard

"apt-get -y install wazuh-manager" merupakan perintah linux untuk mendapatkan package Wazuh Server sebesar 317 MB, proses pada gambar 4.5 menunjukkan instalasi telah berhasil dijalankan. Kemudian memastikan Wazuh Server telah aktif, dengan melakukan perintah "systemctl status wazuh-manager", seperti gambar 6.

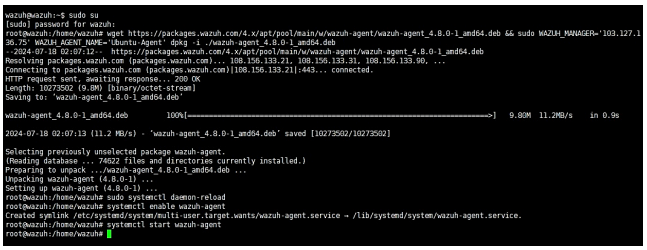


Gambar 13 Status Wazuh Dashboard

B. Wazuh Agent

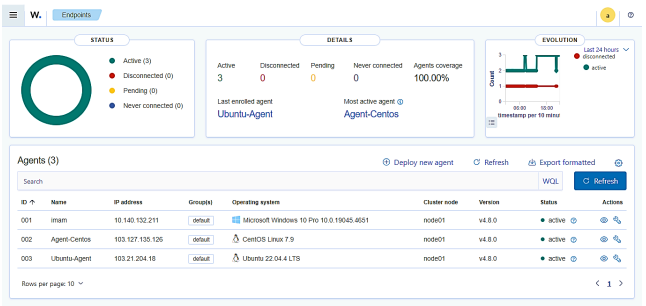
Wazuh Agent bersifat multi-*platform* dan berjalan pada endpoint yang ingin di *monitoring*. Wazuh Agent berkomunikasi dengan Wazuh Server, mengirimkan data secara real-time melalui channel yang terenskripsi dan terautentikasi.

Pada penelitian ini, Wazuh Agent akan di install pada server PT. Medianusa Permana guna untuk melakukan deteksi insiden keamanan jaringan pada perusahaan tersebut. Adapun langkah awal untuk menambahkan Wazuh Agent pada server PT. Melakukan implementasi Wazuh Agent langsung pada server PT. Medianusa Permana dengan menjalankan perintah yang terdapat pada gambar 14.



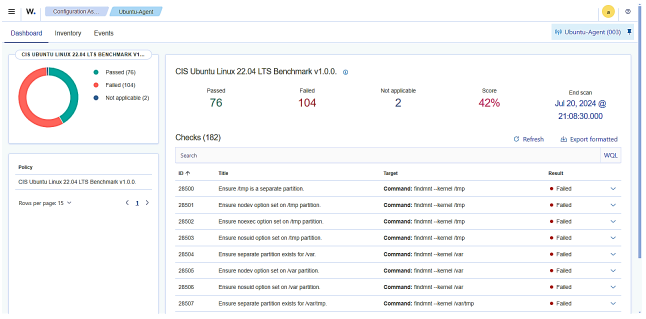
Gambar 14 Instalasi Wazuh Agent

Wazuh Agent sudah berhasil berjalan pada server PT. Medianusa Permana, untuk memastikan hal tersebut dapat dilihat pada halaman endpoints summary pada gambar 8.



Gambar 15 Endpoint Summary

Ketika Wazuh Agent telah berjalan pada server PT. Medianusa Permana, terdapat proses *Benchmark* yang dilakukan, hal ini berfungsi untuk menilai kualitas yang terdapat pada sistem dengan menunjukkan nilai persentase dari sistem tersebut, hasil dari *CIS* Ubuntu Linux 22.04 LTS *Benchmark* v1.0.0 dapat dilihat pada gambar 9.



Gambar 16 Hasil *Benchmark*

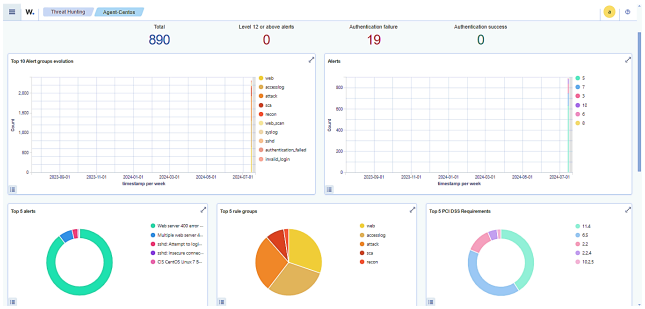
C. Percobaan Penyerangan Menggunakan *DoS*

Pada tahapan ini penguji akan melakukan pengujian berupa mencoba menyerang client atau Wazuh Agent, adapun jenis serangan yang dilakukan adalah *Denial of Service* (*DoS*), dengan tujuan untuk melihat kemampuan *platform* Wazuh mampu mendeteksi secara akurat penyerangan yang dilakukan. Adapun kondisi dari client sebelum dilakukan penyerangan *DoS* dapat dilihat pada tabel 1.

TABEL I
SEBELUM DILAKUKAN PENYERANGAN *DoS*

Location	*Events*	*Bytes*
last -n 20	43	69058
/var/log/messages	14	975
/var/ossec/logs/active-responses.log	0	0
/var/log/secure	156	15277
/var/log/maillog	0	0
/var/log/audit/audit.log	926	283998
/var/log/nginx/error.log	3	853
netstat listening ports	43	23392
/var/log/nginx/access.log	757	166654
df -P	280	24191

Sebelum dilakukan penyerangan, total *event* yang telah terjadi ialah sebanyak 2.222 dan ukuran data total 584.398 *Bytes*. Total *Threat Hunting* sebelum dilakukan serangan *DoS* dapat dilihat pada gambar 10.



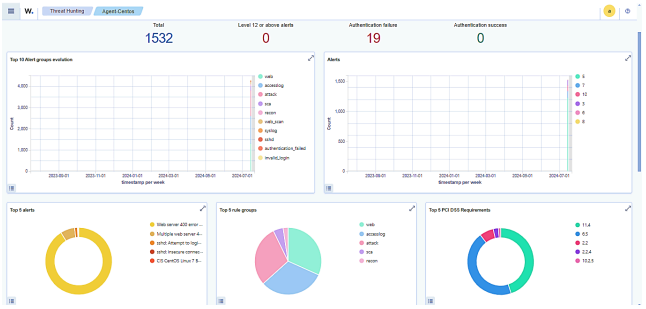
Gambar 17 *Threat Hunting* Sebelum *DoS*

Sebelum dilakukan serangan, total *Threat Hunting* yang terjadi adalah 890. Kemudian dilakukan serangan *DoS* terhadap salah satu client dari Wazuh sebanyak 5 percobaan dengan beban yang berbeda yaitu 20, 40, 60, 80, dan 100. Didapatkan peningkatan setelah dilakukan serangan *DoS* yang dapat dilihat pada tabel 2 berikut.

TABEL II
SESUDAH DILAKUKAN PENYERANGAN *DoS*

Location	*Events*	*Bytes*
last -n 20	48	77088
/var/log/messages	17	1184
/var/ossec/logs/active-responses.log	0	0
/var/log/secure	158	15481
/var/log/maillog	0	0
/var/log/audit/audit.log	948	290146
/var/log/nginx/error.log	3	853
netstat listening ports	48	26112
/var/log/nginx/access.log	1395	304106
df -P	310	26766

Setelah dilakukan penyerangan *DoS*, total *event* yang terjadi telah meningkat menjadi sebanyak 2.927 dan ukuran data total juga terjadi peningkatan menjadi 741.736 *Bytes*. Total *Threat Hunting* sesudah dilakukan serangan *DoS* dapat dilihat pada gambar 11.



Gambar 18 *Threat Hunting* Sesudah *DoS*

Setelah dilakukan penyerangan *DoS* kelima dengan beban yang bertambah menjadi 100, terdapat peningkatan terhadap *Threat Hunting* menjadi 1.532.

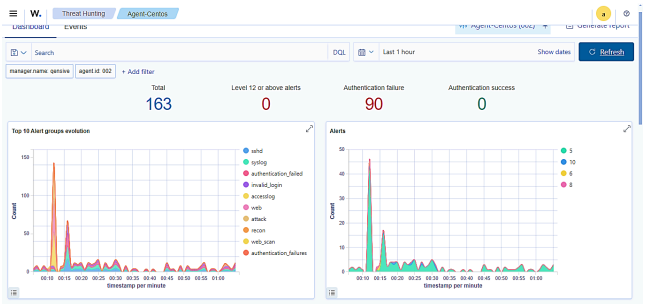
D. Percobaan Penyerangan Menggunakan SQLMap

Pada pengujian selanjutnya dilakukan penyerangan *SQL Injection* terhadap salah satu client yang telah menjadi Wazuh Agent. Adapun kondisi dari client sebelum dilakukan penyerangan *SQL Injection* dapat dilihat pada tabel 3.

TABEL III
SEBELUM DILAKUKAN PENYERANGAN *SQL INJECTION*

Location	*Events*	*Bytes*
last -n 20	1267	2034802
/var/log/messages	71	5081
/var/ossec/logs/active-responses.log	0	0
/var/log/secure	7782	794456
/var/log/maillog	25741	7996447
/var/log/audit/audit.log	6	2235
/var/log/nginx/error.log	271	47646
netstat listening ports	1267	689248
/var/log/nginx/access.log	21	1346
df -P	7656	657434

Adapun *event* yang telah terdeteksi sebelum dilakukan *SQL Injection* adalah 44.082 *event* dan total ukuran total data yaitu 12.228.695 *Bytes*. Total *Threat Hunting* sebelum dilakukan serangan *DoS* dapat dilihat pada gambar 12.



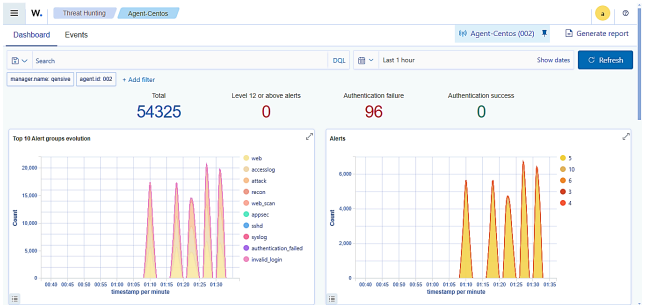
Gambar 19 *Threat Hunting* sebelum *SQL Injection*

Nilai total dari *Threat Hunting* sebelum dilakukan *SQL Injection* adalah 163. Kemudian dilakukan serangan *SQL Injection* terhadap salah satu client dari Wazuh sebanyak 5 percobaan. Didapatkan peningkatan setelah dilakukan serangan *SQL Injection* yang dapat dilihat pada tabel IV berikut.

TABEL IV
SEBELUM DILAKUKAN PENYERANGAN *SQL INJECTION*

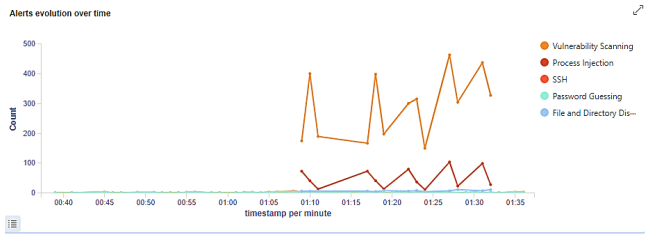
Location	*Events*	*Bytes*
last -n 20	1271	2041226
/var/log/messages	72	5153
/var/ossec/logs/active-responses.log	0	0
/var/log/secure	8187	834185
/var/log/maillog	29288	9094950
/var/log/audit/audit.log	57	13920
/var/log/nginx/error.log	57819	12164233
netstat listening ports	1271	691424
/var/log/nginx/access.log	22	1411
df -P	7680	659494

Setelah dilakukan penyerangan kelima menggunakan SQL Map dan Dirsearch, total *event* yang terjadi telah meningkat menjadi sebanyak 105.667 *event* dan ukuran data total juga terjadi peningkatan menjadi 25.505.996 *Bytes*. Grafik pada fitur *Threat Hunting* juga mengalami peningkatan yang sangat signifikan, total *Threat Hunting* setelah melakukan *SQL Injection* sebanyak 5 percobaan adalah 54.325.



Gambar 20 *Threat Hunting* sebelum *SQL Injection*

Terdapat juga fitur *Mittre Attack* yang mampu mendeteksi kelima serangan tersebut yang dapat dilihat dalam bentuk grafik pada gambar 14.



Gambar 21 *Mittre Attack*

E. *Comparison Testing*

Untuk mengetahui pengaruh penerapan deteksi insiden keamanan jaringan menggunakan *platform* Wazuh setelah dilakukan implementasi, perubahan yang terjadi dalam hal *monitoring* pada PT. Medianusa Permana menjadi acuan sebagai perbandingan sebelum dan sesudah dilakukan implementasi *platform* Wazuh.

TABEL V
SEBELUM DILAKUKAN PENYERANGAN *SQL INJECTION*

Fitur dan Kemampuan	Sebelum *Platform* Wazuh	Setelah *Platform* Wazuh
Status Up Time	Ya	Ya
CPU Usage	Ya	Tidak
Memory Usage	Ya	Tidak
Disk Usage	Ya	Tidak
Event Count Evolution	Tidak	Ya
Threat Hunting	Tidak	Ya
Vulnerability Detection	Tidak	Ya
Mittre Attack	Tidak	Ya
Security Operation	Tidak	Ya
Configuration Assessment	Tidak	Ya
Malware Detection	Tidak	Ya
Cloud Security	Tidak	Ya
Event Count Stats	Tidak	Ya

Dari tabel V dapat diketahui bahwa sistem *monitoring* yang terdapat pada PT. Medianusa Permana sebelum dilakukan implementasi hanya dapat melakukan *monitoring resource* pemakaian server. Setelah dilakukan implementasi *platform* Wazuh, PT. Medianusa Permana kini telah memiliki teknologi *Security Information and Event Management* untuk memastikan keamanan server pada perusahaan tersebut.

IV. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian pada penelitian Analisa Deteksi Insiden Keamanan Jaringan Menggunakan Wazuh Sebagai *Security Information and Event Management* (*SIEM*) Pada PT. Medianusa Permana dapat disimpulkan bahw hasil pengujian penetration testing menggunakan *Denial of Service* dengan jumlah pengujian sebanyak 5 serangan, dengan beban 20, 40, 60, 80, dan 100 dilakukan dengan bertahap. Dari keseluruhan percobaan yang dilakukan maka didapatkan peningkatan dari total *event* yang terjadi ialah 705. Kemudian dari pengujian *Denial of Service*

(*DoS*) juga didapati kenaikan nilai pada fitur *Threat Hunting*, dari keseluruhan serangan *DoS* yang dilakukan sebanyak 5 serangan, nalai *Threat Hunting* terjadi peningkatan sebanyak 642. Serangan ditingkatkan dengan menggunakan SQLMap yang melakukan penyerangan *SQL Injection* sebanyak 5 kali pada client, antara lain seperti *Mittre Attack* yang terjadi peningkatan grafik dengan nilai rata-rata peningkatan 400 sebanyak 5 kali. Pada *Threat Hunting* juga terdapat lonjakan nilai total yang dideteksi, dari nilai awalnya 163 menjadi 54.325, kenaikan tersebut didapat dari pengujian serangan yang dilakukan sebanyak 5 kali.

Hasil perbandingan antara sebelum dilakukan implementasi sistem *monitoring* jaringan menggunakan *platform* Wazuh dan ketika sudah dilakukan implementasi, terdapat peningkatan dalam hal *monitoring* terhadap *Security Information and Event Management* yang terdapat pada *platform* Wazuh, dibandingkan dengan sebelum dilakukan implementasi, PT. Medianusa Permana hanya memiliki sistem *monitoring* yang hanya menghasilkan nilai *resource* seperti penggunaan CPU, Memory, dan Penyimpanan.

Referensi

[1] P. M. Dehan, F. Nova, D. Prayama, "Wazuh sebagai Log *Event* Management dan Deteksi Celah Keamanan pada Server dari Serangan *DoS*," J. Teknol. Inf. Politeknik Negeri Padang, vol. 3, no. 1, ISSN 2722-4600, 2022.

[2] K. Husnul, dkk, "Implementasi *Security Information and Event Management* (SIEM) pada Aplikasi SMS Center Pemerintah Daerah Provinsi Nusa Tenggara Barat," Dept. Inf. Eng. Mataram University, vol. 3, no. 2, ISSN 2746-0983, 2022.

[3] Arif Gilang Surya, Hutrianto, "Intrusion Detection And Anomaly Menggunakan Wazuh pada Universitas Muhammadiyah Palembang," F. T. Ilmu Kom., ISSN 2685-2683.

[4] H. Muhammad Aliyul, P. Rosyani, "Implementasi Sistem *Monitoring* Jaringan dan Server Menggunakan Zabbix yang Terintegrasi dengan Grafana dan Telegram," vol. 8, no. 6, ISSN 2715-7393, 2021, doi: 10.30865/jurikom.v8i6.3631.

[5] R. Dwi Risza Budi, Periyadi, A. Sularsa, "Implementasi *Monitoring* Jaringan Menggunakan Cacti dan Web Authentication Menggunakan Karberos pada MAN 1 Bojonegoro," F. Ilmu Ter. Universitas Telkom, vol. 1, no. 3, ISSN 2442-5826, 2015.

[6] D. Setiawan, "Buku Sakti Pemrograman Web: HTML, CSS, PHP, MYSQL & Javascript," p. 216, 2017.

[7] Wazuh Documentation, "Wazuh Architecture" https://documentation.wazuh.com/current/getting-started/architecture.html (diakses 8 Des. 2024).

[8] Ary Adianto, "Mengenal 14 Jenis Serangan Siber dan Cara Mencegahnya," 13 april, 2022. https://www.helios.id/id/blog-id/detail/mengenal-14-jenis serangan-siber-dan-cara-mencegahnya (diakses 3 Des. 2023).

[9] PT. Biznet Gio Nusantara, "Mengenal apa itu Ubuntu, Jenis, dan Kelebihannya," https://www.biznetgio.com/news/apa-itu-ubuntu (diakses 8 Des. 2023).

[10] P. Reza, A. Affandi, E. Setijadi, "Rancang Bangun Aplikasi *Monitoring* Jaringan dengan Menggunakan Simple Network Management Protocol," J. T. Elektro ITS., vol. 2, no. 1, ISSN 2337-3539, 2013.

[11] Adi Widodo, "Implementasi *Monitoring* Jaringan Komputer Menggunakan Dude," STMIK. Insan Pembangunan, vol. 11, no. 1, ISSN 1979-1496, 2015.

[12] Nurul Huda, "SIEM : Pengertian, Cara Kerja , serta Perbedaannya dengan SOAR," https://www.dewaweb.com/blog/pengertian-siem/ (diakses 9 Des. 2023).

[13] N. Furqan, I. Suandi, Muhammad, "Implementasi Intrusion Detection System (IDS) Pada Sistem Keamanan Jaringan Menggunakan Telegram Sebagai Media Notifikasi," J. T. Elektro Politeknik Negeri Lhokseumawe, vol. 7, no. 1, 2023.