

***ANALISIS SECURITY INFORMATION AND EVENT MANAGEMENT  
(SIEM) BERBASIS WAZUH DALAM MENDETEKSI MALICIOUS  
SOFTWARE PADA SISTEM OPERASI LINUX***

**SKRIPSI**

**YOGA YOSEPINO SINAGA  
201401081**



**PROGRAM STUDI S-1 ILMU KOMPUTER  
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI  
UNIVERSITAS SUMATERA UTARA  
MEDAN  
2024**

**ANALISIS *SECURITY INFORMATION AND EVENT MANAGEMENT*  
(SIEM) BERBASIS WAZUH DALAM MENDETEKSI *MALICIOUS*  
*SOFTWARE* PADA SISTEM OPERASI LINUX**

**SKRIPSI**

**Diajukan untuk melengkapi tugas dan memenuhi syarat memperoleh ijazah  
Sarjana Ilmu Komputer**

**YOGA YOSEPINO SINAGA  
201401081**



**PROGRAM STUDI S-1 ILMU KOMPUTER  
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI  
UNIVERSITAS SUMATERA UTARA  
MEDAN  
2024**

**PERSETUJUAN**

**Judul** : ANALISIS *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) BERBASIS WAZUH  
DALAM MENDETEKSI *MALICIOUS SOFTWARE*  
PADA SISTEM OPERASI LINUX

**Kategori** : SKRIPSI

**Nama** : YOGA YOSEPINO SINAGA

**Nomor Induk Mahasiswa** : 201401081

**Program Studi** : SARJANA (S-1) ILMU KOMPUTER

**Fakultas** : ILMU KOMPUTER DAN TEKNOLOGI INFORMASI  
UNIVERSITAS SUMATERA UTARA

Medan, 27 Mei 2024

**Komisi Pembimbing** :

**Pembimbing 2**

Dewi Sartika Br Ginting S.Kom., M.Kom.  
NIP. 199005042019032023

**Pembimbing 1**

Dr. Ir. Elviawaty Muisa Zamzami  
S.T., M.T., M.M., IPU  
NIP.197510082008011011

**Diketahui/Disetujui Oleh**

**Program Studi S-1 Ilmu Komputer**

**Ketua,**

Dr. Amalia ST., M.T.  
NIP. 197812212014042001

**PERNYATAAN****ANALISIS *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM)  
BERBASIS WAZUH DALAM MENDETEKSI *MALICIOUS SOFTWARE* PADA  
SISTEM OPERASI LINUX****SKRIPSI**

Saya mengakui bahwa skripsi ini adalah hasil karya saya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing telah disebutkan sumbernya.

Medan, 13 Februari 2024



Yoga Yosepino Sinaga

201401081

## PENGHARGAAN

Segala puji syukur dipanjatkan kepada Tuhan Yang Maha Esa karena atas berkat dan rahmat karunia-Nya, penulis bisa berada di tahap penyusunan skripsi yang berjudul “Analisis *Security Information and Event Management (SIEM)* Berbasis Wazuh Dalam Mendeteksi *Malicious Software* Pada Sistem Operasi Linux”. Penulisan skripsi ini bertujuan untuk syarat mendapatkan gelar Sarjana Komputer di Fakultas Ilmu Komputer & Teknologi Informasi dengan Program Studi Ilmu Komputer, Universitas Sumatera Utara. Penulis menyadari bahwa karena keterbatasan dan kemampuan penulis, masih terdapat kesalahan maupun kekurangan dalam penulisan skripsi ini.

Penyusunan skripsi ini tidak terlepas dari bantuan, dukungan, dan bimbingan dari banyak pihak. Oleh karena itu, penulis mengucapkan banyak terima kasih kepada:

1. Kedua orang tua penulis yakni Bapak Henry Dunand Sinaga S.P. dan Ibu Agustina Aritonang S.P. atas kasih cinta yang begitu besar dan juga doa kepada penulis sedari kecil hingga bisa sampai tahap ini.
2. Bapak Prof. Dr. Muryanto Amin S.Sos., M.Si. selaku Rektor Universitas Sumatera Utara.
3. Ibu Dr. Maya Silvi Lydia B.Sc., M.Sc. selaku Dekan Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara.
4. Ibu Dr. Amalia, S.T., M.T. selaku Ketua Program Studi S-1 Ilmu Komputer Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara.
5. Kak Dr. Ir. Elviawaty Muisa Zamzami S.T., M.T., M.M., IPU selaku Dosen Pembimbing I yang telah memberi dukungan, motivasi, masukan, dan bimbingan spiritual yang membangun kepada penulis selama penyusunan skripsi ini.
6. Ibu Dewi Sartika Br Ginting S.Kom., M.Kom selaku Dosen Pembimbing II dan Dosen Pembimbing Akademik yang telah memberi banyak masukan yang berharga kepada penulis selama penyusunan skripsi ini, serta membimbing saya dari awal memasuki masa perkuliahan.
7. Bapak Dr. Mohammad Andri Budiman S.T., M.Comp.Sc., M.E.M selaku Dosen Penguji I yang telah memberi masukan, saran dan kritik yang membangun kepada penulis terhadap penyusunan skripsi ini.
8. Bapak Prof. Dr. Syahril Efendi S.Si., M.I.T. selaku Dosen Penguji II yang telah

memberi saran, masukan dan kritik yang membantu penulis dalam penyusunan skripsi.

9. Seluruh bapak dan ibu dosen dan staff Fasilkom-TI USU, khususnya dosen Program Studi S-1 Ilmu Komputer yang mendidik dan memberi wawasan serta moral yang berharga, baik di bangku perkuliahan maupun setelah lulus.
10. Kakak-kakak saya, Yola Yohanna Sinaga S.Kep., Ns. dan Yesi Sinaga S.Stat. yang telah membimbing dan membantu penulis secara moral, mendoakan, tempat keluh kesah serta sumber motivasi dan panutan bagi penulis.

Dan seluruh pihak yang telah memberi dukungan serta doa baik yang tidak bisa penulis cantumkan semuanya. Akhir kata penulis berharap besar semoga skripsi penulis bisa memberikan guna dan manfaat bagi pembaca.

Medan, 22 Oktober 2023

Penulis,



Yoga Yosepino Sinaga

**ANALISIS *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM)  
BERBASIS WAZUH DALAM MENDETEKSI *MALICIOUS SOFTWARE*  
PADA SISTEM OPERASI LINUX**

Abstrak

Saat ini perkembangan teknologi mengalami kemajuan yang sangat pesat, namun di balik layar terdapat ancaman dan serangan yang tidak diketahui kapan akan terjadi. Serangan dan ancaman tersebut dapat merusak sistem dan membahayakan data penting bagi segala aspek baik individual bahkan organisasi. Dengan ancaman dan serangan tersebut, keamanan informasi atau keamanan siber berperan penting dalam melindungi bahkan mencegah serangan dan ancaman yang terjadi. *Security Information and Event Management* (SIEM) yang merupakan satu dari banyak metode keamanan siber adalah alat yang digunakan untuk memantau lalu lintas jaringan dari ancaman yang memberikan analisis secara *real-time* dari log yang dihasilkan aplikasi atau perangkat. Pada penelitian kali ini SIEM yang digunakan adalah Wazuh, yang berguna untuk *memonitoring*, melakukan analisa, dan mengeksekusi terhadap log serangan yang masuk kedalam sistem atau agent. Serangan yang diuji pada penelitian kali ini adalah fokus dalam mendeteksi dan mengeksekusi *Malicious Software* pada Linux. Hasil dari pengujian tersebut Wazuh dengan bantuan integrasi dari VirusTotal dapat mendeteksi dan mencatat aktivitas serangan tersebut pada log secara akurat pada server dan melakukan pengeksekusian terhadap serangan secara *real-time*.

**Kata Kunci:** Keamanan Siber, *Security Information and Event Management*, Wazuh, *Malicious Software*, Linux, Wazuh.

## **ANALYSIS OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) BASED ON WAZUH IN DETECTING MALICIOUS SOFTWARE ON LINUX OPERATING SYSTEM**

### *Abstract*

*Currently, the development of technology is progressing very rapidly, but behind the scenes there are threats and attacks that are not known when they will occur. These attacks and threats can damage the system and endanger important data for all aspects of both individuals and organizations. With these threats and attacks, information security or cybersecurity plays an important role in protecting and even preventing attacks and threats that occur. Security Information and Event Management (SIEM), which is one of many cybersecurity methods, is a tool used to monitor network traffic for threats that provide real-time analysis of logs generated by applications or devices. In this research, the SIEM used is Wazuh, which is useful for monitoring, analyzing, and executing attack logs that enter the system or agent. The attack tested in this research is focused on detecting and executing Malicious Software on Linux. The results of the test, Wazuh with the help of integration from VirusTotal can detect and record the attack activity in the log accurately on the server and execute the attack in real time.*

**Keywords:** *Cyber Security, Security Information and Event Management, Malicious Software, Linux, Wazuh.*



## DAFTAR ISI

<b>PERSETUJUAN .....</b>	<b>ii</b>
<b>PERNYATAAN .....</b>	<b>iii</b>
<b>PENGHARGAAN.....</b>	<b>iv</b>
<b>ABSTRAK.....</b>	<b>vi</b>
<b>ABSTRACT .....</b>	<b>vii</b>
<b>DAFTAR ISI .....</b>	<b>viii</b>
<b>DAFTAR TABEL .....</b>	<b>x</b>
<b>DAFTAR GAMBAR.....</b>	<b>xi</b>
<b>BAB 1 PENDAHULUAN.....</b>	<b>1</b>
<b>1.1 Latar Belakang.....</b>	<b>1</b>
<b>1.2 Rumusan Masalah .....</b>	<b>3</b>
<b>1.3 Batasan Masalah.....</b>	<b>3</b>
<b>1.4 Tujuan Penelitian.....</b>	<b>3</b>
<b>1.5 Manfaat Penelitian.....</b>	<b>4</b>
<b>1.6 Metodologi Penelitian .....</b>	<b>4</b>
<b>1.7 Penelitian Relevan.....</b>	<b>5</b>
<b>1.8 Sistematika Penulisan .....</b>	<b>6</b>
<b>BAB 2 LANDASAN TEORI.....</b>	<b>8</b>
<b>2.1 Keamanan Siber.....</b>	<b>8</b>
<i>2.1.1 Definisi keamanan siber.....</i>	<i>8</i>
<i>2.1.2 Fungsi keamanan siber.....</i>	<i>9</i>
<i>2.1.3 Komponen keamanan siber.....</i>	<i>10</i>
<i>2.1.4 Jenis keamanan siber .....</i>	<i>11</i>
<b>2.2 Security Information and Event Management (SIEM) .....</b>	<b>12</b>
<b>2.3 Wazuh .....</b>	<b>12</b>
<b>2.4 Virtual Machine (VM) .....</b>	<b>12</b>
<b>2.5 Linux .....</b>	<b>13</b>
<b>2.6 Amazon Linux.....</b>	<b>13</b>

2.7	Ubuntu.....	14
2.8	Malicious Software .....	14
2.9	VirusTotal .....	15
2.10	Application Programming Interface (API) .....	15
2.11	File Integrity Monitoring (FIM) .....	15
2.12	European Institute for Computer Antivirus Research (EICAR) test file... .....	16
<b>BAB 3 ANALISIS DAN PERANCANGAN .....</b>		<b>17</b>
3.1	Analisis .....	17
3.1.1.	Analisis masalah.....	17
3.1.2.	Analisis kebutuhan.....	19
3.2	Perancangan Sistem.....	20
3.2.1.	Diagram umum penelitian.....	20
3.2.2.	Diagram umum SIEM .....	21
3.3	Flowchart (Diagram Alir) .....	23
3.3.1.	Flowchart analisis malware.....	23
3.3.2.	Flowchart penelitian.....	24
3.4	Sequence Diagram (Diagram Urutan) .....	25
<b>BAB 4 IMPLEMENTASI DAN PENGUJIAN.....</b>		<b>26</b>
4.1	Implementasi.....	26
4.1.1	Spesifikasi laptop dan virtual machine yang digunakan.....	27
4.1.2	Instalasi dan Konfigurasi Wazuh Server.....	29
4.1.3	Menghubungkan Wazuh Agent dengan Wazuh Server.....	37
4.1.4	Konfigurasi Untuk Deteksi dan Penghapusan Malicious Software .....	41
4.2	Pengujian.....	46
<b>BAB 5 PENUTUP .....</b>		<b>51</b>
5.1	Kesimpulan .....	51
5.1	Saran .....	51
<b>DAFTAR PUSTAKA .....</b>		<b>53</b>

**DAFTAR TABEL**

<b>Tabel 4.1</b> Spesifikasi Perangkat Lunak .....	26
<b>Tabel 4.2</b> Spesifikasi Laptop yang Digunakan .....	27
<b>Tabel 4.3</b> Spesifikasi Server .....	28
<b>Tabel 4.4</b> Spesifikasi Agent .....	29

## DAFTAR GAMBAR

<b>Gambar 2.1</b> Jenis-Jenis Keamanan Siber .....	11
<b>Gambar 3.1</b> Alur Penelitian .....	21
<b>Gambar 3.2</b> Alur Proses SIEM.....	22
<b>Gambar 3.3</b> Flowchart Analisis Malware .....	24
<b>Gambar 3.4</b> Flowchart Penelitian.....	25
<b>Gambar 3.5</b> Diagram urutan penelitian .....	25
<b>Gambar 4.1</b> Penambahan Repositori Wazuh .....	30
<b>Gambar 4.2</b> Penambahan Repositori Wazuh .....	30
<b>Gambar 4.3</b> Mengunduh Skrip dan Konfigurasi Wazuh .....	30
<b>Gambar 4.4</b> Konfigurasi Wazuh .....	31
<b>Gambar 4.5</b> Skrip Running dan Unduh Package Wazuh Indexer .....	31
<b>Gambar 4.6</b> Konfigurasi pada Wazuh Indexer.....	32
<b>Gambar 4.7</b> Status Wazuh Indexer.....	32
<b>Gambar 4.8</b> Instalasi Wazuh Manager.....	33
<b>Gambar 4.9</b> Pengaktifan Wazuh Manager.....	33
<b>Gambar 4.10</b> Memulai Wazuh Manager.....	33
<b>Gambar 4.11</b> Status Wazuh Manager.....	34
<b>Gambar 4.12</b> Instalasi Wazuh Dashboard.....	34
<b>Gambar 4.13</b> Pengaktifan Wazuh Dashboard .....	34
<b>Gambar 4.14</b> Wazuh Dashboard Dimulai.....	35
<b>Gambar 4.15</b> Konfigurasi Wazuh Dashboard .....	35
<b>Gambar 4.16</b> Halaman Login Wazuh Dashboard.....	35
<b>Gambar 4.17</b> Tampilan Depan Wazuh Dashboard.....	36
<b>Gambar 4.18</b> Instalasi Filebeat.....	36
<b>Gambar 4.19</b> Konfigurasi Filebeat .....	37
<b>Gambar 4.20</b> Menambahkan Repositori Wazuh .....	37
<b>Gambar 4.21</b> Menambahkan Repositori Wazuh .....	38
<b>Gambar 4.22</b> Menghubungkan Wazuh Manager dengan Wazuh Agent .....	38
<b>Gambar 4.23</b> Mengaktifkan Wazuh Agent .....	39
<b>Gambar 4.24</b> Starting Wazuh Agent .....	39
<b>Gambar 4.25</b> Edit konfigurasi pada server .....	40
<b>Gambar 4.26</b> Restart Wazuh Agent.....	41

<b>Gambar 4.27</b> Wazuh Running Realtime .....	42
<b>Gambar 4.28</b> Instalasi jq .....	43
<b>Gambar 4.29</b> Skrip Eksekusi .....	43
<b>Gambar 4.30</b> Perintah Izin dan Kepemilikan Skrip .....	44
<b>Gambar 4.31</b> Restart Wazuh Agent .....	44
<b>Gambar 4.32</b> Penambahan Rule di Server .....	44
<b>Gambar 4.33</b> File Konfigurasi pada Server .....	45
<b>Gambar 4.34</b> File Konfigurasi pada Server .....	45
<b>Gambar 4.35</b> Penambahan Rule pada Server .....	46
<b>Gambar 4.36</b> Restart Wazuh Manager .....	46
<b>Gambar 4.37</b> Tampilan Depan Wazuh Server .....	47
<b>Gambar 4.38</b> Tampilan Depan Agent .....	47
<b>Gambar 4.39</b> File Integrity Monitoring .....	48
<b>Gambar 4.40</b> Pengunduhan File Terdeteksi Malware .....	49
<b>Gambar 4.41</b> Respon Terhadap Perintah pada Terminal Agent .....	50
<b>Gambar 4.42</b> Hasil Monitoring pada Wazuh Dashboard atas File Terindikasi Malware .....	50

# **BAB 1**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Tahun 1970-an, keamanan siber muncul ketika Bob Thomas membuat program Creeper, yang memiliki kemampuan untuk berjelajah melalui ARPANET dan meninggalkan jejak remah di mana pun program itu pergi. Reaper, program yang bertujuan untuk membasmi Creeper, ditulis oleh penemu email Ray Tomlinson. Reaper merupakan contoh pertama dari perangkat lunak antivirus dan program yang mereplikasi diri sendiri, menjadikannya *worm* pertama.

Dunia saat ini sangat membutuhkan informasi. Internet dan teknologi berkembang begitu pesat membuat informasi dapat diakses dengan cepat, akurat, dan tepat dan sangat penting bagi berbagai hal, seperti membantu dalam pengambilan keputusan, membuat keputusan yang bijaksana, atau bahkan menjadi bagian dari gaya hidup yang kekinian. Saat ini, semakin banyak pemerintah, organisasi nirlaba, bisnis, dan individu yang sangat bergantung pada fenomena teknologi informasi. (Broto, 2013).

Selain kemajuan teknologi, ada ancaman dan serangan yang dapat terjadi kapan saja. Serangan ini dapat terjadi pada server atau pusat data yang dikendalikan individu atau organisasi, seperti server di sektor pemerintahan, pendidikan, dan bisnis. Keamanan informasi sangat penting dalam upaya melindungi informasi sensitif dan rahasia. Ini dilakukan untuk melindungi informasi sensitif dari ancaman dan serangan yang mungkin terjadi karena teknologi informasi semakin berkembang. Teknologi dalam keamanan informasi dapat membantu seorang administrator dalam melakukan monitoring dan analisa jaringan pada suatu perusahaan terhadap ancaman dan serangan yang terjadi (Rihal, 2010).

Menurut FBI, kejahatan dunia maya telah meningkat sebanyak tiga ratus persen sejak awal pandemi virus corona. Selain itu, lembaga pusat pelaporan kejahatan siber di Amerika Serikat yang disebut IC3 (Internet Crime Complaint Centre), yang dioperasikan oleh Federal Bureau of Investigation, melaporkan bahwa hanya pada tahun 2020, masyarakat Amerika Serikat mengajukan 791.790 pengaduan kepada lembaga tersebut, dengan kerugian yang dilaporkan melebihi \$4,1 miliar dan sektor tersebut didominasi oleh *malicious software*, perangkat lunak yang sengaja dirancang untuk mempengaruhi perangkat atau sistem komputer dengan cara yang merugikan atau tidak diinginkan. Ini menunjukkan peningkatan total pengaduan sebesar 69% dibandingkan tahun 2019. Namun, karena banyak kasus yang tidak sempat dilaporkan, data tersebut masih merupakan data kotor. Sangat sulit untuk menentukan semua bahaya dan serangan yang telah ataupun akan dilakukan. Ancaman serangan seperti itu menyebabkan kebocoran dan kehilangan data besar, yang dapat merugikan lembaga terkait. Oleh karena itu, teknologi keamanan yang dapat membaca dan mengevaluasi serangan diperlukan.

*Security Information and Event Management* (SIEM) merupakan sistem pemantauan yang dapat mendeteksi dan menanggapi serangan terhadap sistem khususnya sistem keamanan dengan menggunakan data *real-time* untuk menganalisis *log* peristiwa. Teknologi SIEM ini dapat mengumpulkan data dalam jumlah besar dan memiliki kemampuan untuk menganalisis kejadian dari berbagai sumber untuk menentukan serangan (Kamal & Setiawan, 2021). Sangat sulit untuk mengidentifikasi semua bahaya yang berasal dari pihak yang tidak bertanggung jawab. Ancaman dan serangan seperti itu menyebabkan kebocoran dan kehilangan data besar, yang dapat merugikan lembaga terkait. Oleh karena itu, teknologi keamanan yang dapat membaca dan mengevaluasi serangan diperlukan. Salah satu *tools* SIEM yang dapat digunakan ialah Wazuh.

Wazuh adalah *software* SIEM yang bertindak sebagai sistem pengenalan penyusupan berbasis endpoint. Analisa keamanan, pencegahan intrusi, analisis catatan data, respons aktif, dan pemantauan integritas *file* dilakukan oleh Wazuh. Wazuh adalah perangkat yang memantau host pada tingkat sistem operasi dan aplikasi, meningkatkan visibilitas keamanan infrastruktur (Pratama, Nova, & Prayama, 2022). Penelitian ini menguji salah satu *tools* SIEM yakni Wazuh

dalam mendeteksi dan mengeksekusi serangan *malicious software* yang dikhususkan pada sistem operasi linux.

## 1.2 Rumusan Masalah

Berdasarkan informasi latar belakang yang sudah dijelaskan, ancaman serangan siber semakin besar dan dapat menyerang semua aspek. Hal ini menuntut semua individu maupun bisnis berbasis teknologi untuk memperkuat sistem keamanannya, baik *website* maupun aplikasi. Sehingga *Security Information and Event Management* (SIEM) menjadi salah satu solusi demi menghindari potensi ancaman siber, seperti mengimplementasikan Wazuh dengan pemantauan terhadap jaringan agar meminimalisir terjadinya serangan.

## 1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Wazuh sebagai *tools* SIEM yang dipakai.
2. Menjalankan Wazuh Indexer, Wazuh Manager, Wazuh Dashboard, dan Wazuh Agent secara bersamaan menggunakan Amazon Linux Server dan Ubuntu Agent.
3. Pengujian dilakukan dalam satu jaringan yang sama.
4. Parameter pengujian adalah menganalisa *log* pada perangkat jika *malicious software* ada dan kecepatan dalam membersihkan file berbahaya tersebut.
5. Hanya mereka yang memiliki pengetahuan dasar tentang jaringan dan keamanan siber, seperti administrator, yang dapat memahami dan menganalisis hasil *log* dan simulasi dari penelitian skripsi berikut.

## 1.4 Tujuan Penelitian

Penelitian ini memiliki tujuan yakni mengevaluasi efektivitas kemampuan dari *Security Information and Event Management* (SIEM) berbasis Wazuh dalam mendeteksi perangkat lunak berbahaya pada sistem operasi linux. Lalu penelitian ini juga bertujuan untuk memahami sejauh mana SIEM Wazuh dapat



membantu dalam mengidentifikasi dan merespons ancaman keamanan terhadap lingkungan linux, serta memperbaiki kelemahan keamanan yang ada.

### **1.5 Manfaat Penelitian**

Beberapa manfaat dari penelitian ini sebagai berikut:

1. Meningkatkan keamanan linux yang bisa memberikan kontribusi signifikan dalam memperkuat keamanan sistem operasi linux.
2. Mengurangi risiko kerentanan terhadap malware dengan menggunakan SIEM berbasis Wazuh, organisasi dapat lebih cepat mendeteksi dan merespons ancaman malware.
3. Memperbaiki kebutuhan analisis *log* yang dapat meningkatkan kapabilitas deteksi.
4. Membantu dalam mengumpulkan informasi berupa log terkait yang masuk ke dalam server.
5. Praktisi keamanan dan peneliti lainnya yang tertarik dengan bidang SIEM dan deteksi malware pada platform linux dapat menggunakan penelitian ini sebagai sumber referensi.

### **1.6 Metodologi Penelitian**

Beberapa metode yang dipakai pada skripsi penelitian ini adalah sebagai berikut:

#### **1. Studi Pustaka**

Pada tahap pertama, studi skripsi akan dimulai dengan mengumpulkan referensi yang diperoleh dari sumber tertulis terpercaya, seperti jurnal, buku, artikel, ilmiah, makalah, skripsi maupun situs internet yang membahas tentang jaringan, keamanan siber, dan SIEM.

#### **2. Analisis dan Perancangan Sistem**

Pada tahapan ini, peneliti akan menganalisa Wazuh sebagai salah satu komponen kunci yang dirancang untuk mendeteksi, menganalisis, dan mengatasi ancaman keamanan pada infrastruktur perangkat komputer serta melakukan analisis apa yang akan dibutuhkan dalam penelitian untuk memulai perancangan sistem segera.

### 3. Implementasi Sistem

Pada tahap ini, peneliti melaksanakan proses pembuatan sistem *virtual machine* berdasarkan diagram alir (*flowchart*) yang telah dirancang sebelumnya. Pembuatan sistem ini akan menggunakan Wazuh yang terintegrasi dengan layanan lain terkait.

### 4. Pengujian Sistem

Pada tahap ini, peneliti akan menunjukkan kinerja SIEM dengan menggunakan *tools* yaitu Wazuh untuk mendapatkan hasil dari pengujian yang sedang berjalan dan membuktikan bahwa Wazuh dapat menangkap kerentanan serangan yakni mendeteksi dan membersihkan *malicious software*.

### 5. Dokumentasi Sistem

Pada tahap ini, peneliti melakukan proses penyusunan laporan yang dimulai dari metode pertama yakni analisis hingga pengujian dalam skripsi.

## 1.7 Penelitian Relevan

Beberapa penelitian sebelumnya yang terkait dengan penelitian ini, antara lain:

1. Berdasarkan buku (Chuvakin, 2010) dengan judul SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IMPLEMENTATION, penelitian mengenai SIEM adalah penelitian teknologi yang memungkinkan organisasi untuk mengubah data keamanan yang tersebar dalam sistem dan jaringan mereka menjadi informasi yang relevan, terukur, dan berarti. Dengan menggabungkan kemampuan pengumpulan data, analisis, dan pelaporan, SIEM membantu organisasi mengidentifikasi ancaman keamanan yang mungkin terjadi, memungkinkan respons yang cepat terhadap insiden, dan meningkatkan kemampuan deteksi dan pemantauan keamanan secara keseluruhan.
2. Berdasarkan penelitian (Adenasi & Novarina, 2017) yang membahas tentang malware dapat menyebabkan kerusakan pada data, mencuri informasi pribadi, merusak sistem operasi, atau bahkan mengunci akses ke file penting. Keberadaan malware adalah ancaman serius bagi keamanan dan integritas sistem komputer dan jaringan. Seiring dengan perkembangan

teknologi, jenis dan varian malware terus berkembang, memerlukan upaya konstan untuk mendeteksi, mencegah, dan menghapusnya.

3. Berdasarkan penelitian (Harjono, 2013) menyatakan bahwa penting untuk selalu berhati-hati saat membuka tautan atau lampiran dari sumber yang tidak dikenal atau mencurigakan. Selain itu, memastikan perangkat dan perangkat lunak selalu diperbarui dengan versi keamanan terbaru dapat membantu mencegah infeksi malware.
4. Berdasarkan penelitian (Sakinah, 2022) penelitian SIEM diharapkan dapat menyampaikan hasil pengujian dan analisis serta menawarkan solusi untuk mengatasi ancaman perangkat SIEM.
5. Berdasarkan penelitian (Kamal & Setiawan, 2021) menjelaskan bahwa teknologi SIEM dapat mengumpulkan banyak data dan dapat mengkorelasikan dan menganalisis kejadian dari berbagai sumber untuk menentukan apakah itu serangan atau tidak.
6. Berdasarkan penelitian (Pratama, Nova, & Prayama, 2022) yang membahas tentang wazuh, merupakan perangkat berbasis perangkat lunak sumber terbuka khusus SIEM berguna sebagai sistem pencegahan gangguan berbasis host. Analisis log, pemeriksaan integritas, deteksi rootkit, peringatan basis waktu, dan tindakan aktif semua dilakukan oleh Wazuh. Wazuh adalah perangkat yang memantau host pada tingkat sistem operasi dan aplikasi untuk meningkatkan visibilitas keamanan infrastruktur.

## **1.8 Sistematika Penulisan**

Sistematika penulisan skripsi yang digunakan dalam penelitian ini adalah sebagai berikut:

### **BAB 1 PENDAHULUAN**

Latar belakang pemilihan judul, rumusan masalah, batasan masalah, tujuan dan keuntungan penelitian, serta metodologi dan sistematika penulisan penelitian dibahas dalam bab ini.

### **BAB 2 LANDASAN TEORI**

Pada bab ini dijelaskan beberapa teori yang berkaitan dengan penelitian dan menguraikan perihal tinjauan pustaka yang

berhubungan dengan judul penelitian.

### **BAB 3 ANALISIS DAN PERANCANGAN**

Bab ini menjelaskan mengenai rancangan penelitian, seperti spesifikasi sistem, topologi, prosedur penelitian dan alur eksekusi penelitian.

### **BAB 4 IMPLEMENTASI DAN PENGUJIAN**

Bab ini berisi tentang batasan pengaplikasian perangkat lunak berbahaya ke *agent* berdasarkan dokumentasi pada bab sebelumnya serta pembahasan hasil dari pengujian telah dilakukan untuk memastikan bahwa tujuan dan keuntungan penelitian telah dicapai.

### **BAB 5 KESIMPULAN DAN SARAN**

Bab ini memuat ringkasan temuan yang didapati oleh penulis pada studi penelitian serta saran dari peneliti sebagai anjuran untuk penelitian yang terkait kedepannya.

## **BAB 2**

### **LANDASAN TEORI**

#### **2.1 Keamanan Siber**

##### *2.1.1 Definisi keamanan siber*

Keamanan Siber adalah praktik dan proses yang dirancang untuk melindungi sistem komputer, jaringan, data sensitif dari penggunaan, akses, atau perubahan yang tidak sesuai, serta dari serangan atau gangguan yang berasal dari dunia digital. Tujuannya adalah berfokus pada menjaga keamanan, integritas, dan ketersediaan informasi dan sistem digital, sehingga memastikan operasi yang lancar dan melindungi dari potensi ancaman keamanan. Keamanan Siber mencakup berbagai strategi, kebijakan, teknologi, dan tindakan yang diterapkan untuk mengatasi dan mencegah ancaman keamanan seperti serangan siber, peretasan, pencurian data, dan kegiatan berbahaya lainnya. Keamanan siber sering digunakan sepanjang waktu karena dunia kita semakin terhubung secara digital baik penggunaan individu sehari-hari maupun dalam lingkup luas seperti organisasi bahkan negara dalam rangka menjaga keamanan data rahasia. Keamanan siber sangat penting dalam hampir semua aspek kehidupan modern, terutama dengan meningkatnya ketergantungan pada teknologi digital. Kehilangan keamanan siber dapat memiliki dampak serius terhadap individu, organisasi, dan masyarakat secara keseluruhan (Broto, 2013).

Keamanan siber dilakukan melalui serangkaian praktik dan metodologi untuk melindungi sistem, jaringan, dan data dari ancaman keamanan digital. Ini melibatkan identifikasi risiko, implementasi kebijakan keamanan, penggunaan teknologi keamanan, pengujian penetrasi, pemantauan, dan respon terhadap insiden. Dengan demikian, ilmu keamanan siber adalah suatu pendekatan komprehensif untuk memastikan keamanan informasi dan infrastruktur digital.

Selain itu, keamanan siber juga melibatkan pemantauan tren dan ancaman keamanan terbaru, serta penelitian terus-menerus untuk mengidentifikasi dan mengatasi risiko keamanan baru yang muncul. Seluruh proses ini memerlukan keterlibatan dan kerjasama antara profesional keamanan siber, administrator sistem, dan personil terkait keamanan di organisasi.

### 2.1.2 Fungsi keamanan siber

Keamanan siber berfungsi untuk melindungi informasi, sebagai berikut (Stallings, 1999):

1. *Data Protection* (Perlindungan Data), mengenai teknik enkripsi untuk melindungi informasi dari akses yang tidak sesuai.
2. *Prevention of Malware Attacks* (Pencegahan Serangan Malware), memberikan wawasan tentang metode untuk mencegah dan mendeteksi malware.
3. *Access Management* (Pengelolaan Akses), memaparkan konsep pengelolaan akses, termasuk kontrol keamanan dan penerapan kebijakan akses yang memastikan sumber daya tertentu hanya dapat diakses oleh pihak yang berwenang.
4. *Intrusion Detection* (Deteksi Intrusi), mengulas konsep deteksi intrusi dan penggunaan sistem deteksi intrusi untuk melacak dan mendeteksi aktivitas mencurigakan.
5. *Security Monitoring* (Pemantauan Keamanan), menyajikan informasi tentang pentingnya pemantauan keamanan dan alat-alat untuk mendeteksi serta mencegah ancaman keamanan.
6. *Disaster Recovery* (Pemulihan Bencana), mendiskusikan strategi pemulihan bencana, termasuk perencanaan cadangan dan prosedur pemulihan setelah insiden keamanan.
7. *Training and Security Awareness* (Pelatihan dan Kesadaran Keamanan), memberikan panduan tentang bagaimana mengembangkan budaya keamanan dan memberikan pelatihan untuk meningkatkan kesadaran keamanan di antara pengguna.
8. *Security Research* (Penelitian Keamanan), menyajikan informasi tentang tren terkini dalam penelitian keamanan siber dan kemajuan dalam teknologi

keamanan.

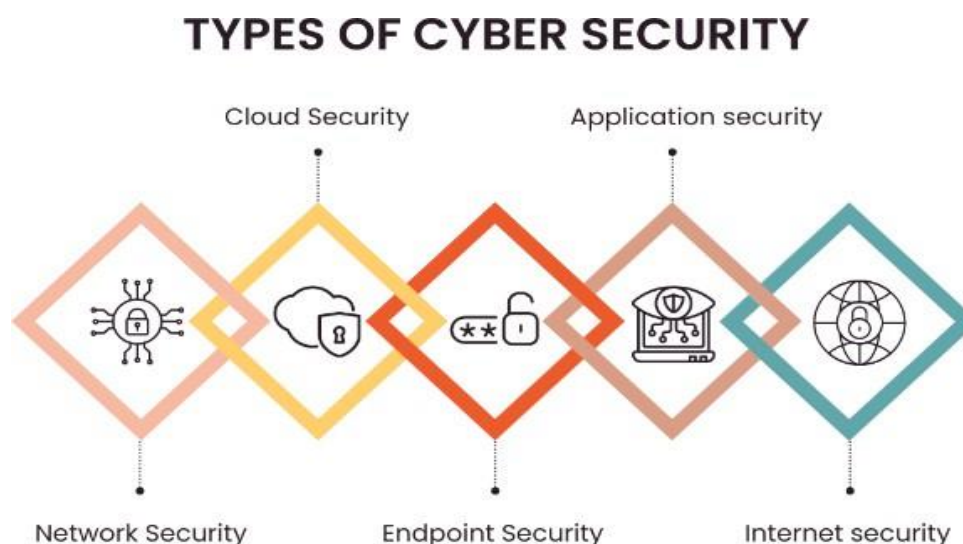
### 2.1.3 *Komponen keamanan siber*

Keamanan Siber memiliki 2 komponen utama yang berguna untuk membuat aman pada data yakni, komponen teknis dan komponen non-teknis yang digabung menjadi sebagai berikut (Stinson, 1955):

1. *Access control*, merupakan proses untuk mengatur siapa yang memiliki akses ke sistem komputer dan data, serta apa yang mereka dapat lakukan dengan data tersebut. *Access control* dapat dilakukan dengan berbagai metode, seperti password, token, dan biometrics.
2. *Vulnerability management*, merupakan proses untuk mengidentifikasi dan memperbaiki kerentanan keamanan pada sistem komputer dan perangkat lunak. Kerentanan keamanan dapat ditemukan secara terus-menerus, sehingga proses vulnerability management harus dilakukan secara terus-menerus.
3. *Incident response*, merupakan proses untuk menanggapi insiden keamanan, seperti serangan siber. Proses ini harus mencakup langkah-langkah untuk membatasi kerusakan, menyelidiki insiden, dan memulihkan diri dari serangan.
4. *Cryptography*, merupakan ilmu untuk melindungi informasi dengan membuatnya tidak bisa dibaca oleh sembarang tanpa kunci yang benar. *Cryptography* digunakan untuk mengamankan data saat disimpan dan ditransmisikan, serta untuk mengautentikasi pengguna dan perangkat.
5. *Security awareness and training*, merupakan proses untuk mendidik karyawan dan pengguna lainnya tentang risiko keamanan siber dan bagaimana melindungi diri masing-masing. Ini merupakan komponen penting dari setiap program keamanan siber, karena bahkan langkah-langkah keamanan yang paling canggih pun dapat diabaikan jika pengguna tidak berhati-hati.
6. *Risk management*, merupakan proses untuk mengidentifikasi, menilai, dan mengurangi risiko keamanan siber. *Risk management* merupakan proses yang berkelanjutan yang harus diintegrasikan ke dalam semua aspek operasi organisasi.

7. *Business continuity and disaster recovery*, merupakan proses untuk memiliki rencana bagaimana menjaga organisasi tetap beroperasi dalam peristiwa serangan siber atau bencana lainnya. Rencana ini harus mencakup langkah-langkah untuk mencadangkan data, memulihkan sistem, dan berkomunikasi dengan pelanggan dan karyawan.
8. *Threat intelligence*, merupakan proses mengumpulkan dan menganalisis informasi tentang ancaman siber. Informasi ini dapat digunakan untuk mengidentifikasi dan mengurangi risiko, serta untuk mengembangkan langkah-langkah keamanan baru.

#### 2.1.4 Jenis keamanan siber



**Gambar 2.1** *Jenis-Jenis Keamanan Siber*

Sumber: [www.theknowledgeacademy.com](http://www.theknowledgeacademy.com)

Berikut adalah beberapa jenis keamanan siber yang mencakup berbagai aspek perlindungan dalam dunia teknologi informasi:

1. *Network Security* (Keamanan Jaringan) berfokus pada perlindungan jaringan komputer dari ancaman. Ini termasuk melindungi jaringan dari serangan, akses tidak sah, dan penyadapan.
2. *Cloud Security* berfokus pada perlindungan data dan aplikasi yang disimpan



atau dijalankan di *cloud* yang termasuk melindungi *cloud* dari serangan.

3. *Endpoint Security* berfokus pada perlindungan perangkat individu seperti komputer, laptop, smartphone, dan perangkat lainnya dari ancaman siber.
4. *Application Security* (Keamanan Aplikasi) melibatkan langkah-langkah untuk melindungi aplikasi perangkat lunak dari serangan siber, termasuk pengujian keamanan dan penerapan praktik pengembangan aman.
5. *Internet Security* (Keamanan Internet) merujuk pada kumpulan tindakan yang dilakukan untuk melindungi sistem, data, dan jaringan dari ancaman dan bahaya yang muncul di dunia internet.

## **2.2 Security Information and Event Management (SIEM)**

Penelitian tentang Manajemen Peristiwa Informasi Keamanan (SIEM) diharapkan dapat menjelaskan hasil pengujian dan analisis SIEM serta menawarkan solusi untuk mengatasi data ancaman perangkat SIEM (Sakinah, 2022). Sistem pengelolaan informasi dan peristiwa keamanan (SIEM) adalah teknologi monitoring yang memiliki kemampuan untuk mendeteksi serangan dan respons sistem keamanan melalui analisis *log* dari berbagai peristiwa yang berasal dari berbagai sumber data secara *realtime*. Teknologi SIEM ini memiliki kemampuan untuk mengkorelasikan dan menganalisis data dari berbagai sumber untuk menentukan apakah peristiwa tersebut merupakan serangan atau tidak (Kamal & Setiawan, 2021).

## **2.3 Wazuh**

Wazuh adalah sebuah tools keamanan terbuka yang dimaksudkan untuk membantu organisasi menemukan, menganalisis, dan menanggapi risiko keamanan data. Wazuh adalah solusi keamanan host sumber terbuka yang menyediakan deteksi intrusi, analisis *log*, manajemen keamanan *endpoint*, dan integrasi SIEM untuk membantu melindungi sistem dan jaringan dari ancaman keamanan (Atken, 2017).

## **2.4 Virtual Machine (VM)**

*Virtual Machine* atau Mesin Virtual adalah emulasi dan virtualisasi

sistem komputer, yang menyediakan fungsionalitas komputer fisik dan didasarkan pada arsitektur komputer. Implementasi dapat mencakup perangkat lunak, perangkat keras khusus, atau kombinasi keduanya. VM menjalankan sistemnya sendiri dan berpisah secara fungsi dengan mesin lain di perangkat yang sama bahkan dengan perangkat itu sendiri. Mesin virtual dapat melaksanakan skrip, program, bahkan aplikasi secara virtual seperti menggunakan perangkat yang berbeda.

## 2.5 Linux

Linux adalah sistem operasi komputer opensource lalu bisa dapat disesuaikan. Sistem operasi ini dibuat oleh Linus Torvalds, seorang mahasiswa Finlandia tahun 1991. Awalnya, Torvalds mengembangkan linux sebagai proyek hobinya. Ia ingin membuat sistem operasi yang kuat dan dapat disesuaikan, tetapi tidak mahal seperti sistem operasi komersial. Linux diawali dengan kernel Linux, bagian inti sistem yang mengelola memori dan perangkat keras. Kernel Linux ditulis dalam bahasa C dan C++.

Linux biasanya dikemas sebagai distribusi (distro) linux yang mencakup kernel, perangkat lunak, dan pustaka sistem pendukung, banyak di antaranya disediakan oleh Proyek GNU. Banyak distribusi Linux menggunakan nama "Linux", tetapi Free Software Foundation menggunakan dan merekomendasikan nama "GNU/Linux" untuk menekankan penggunaan dan pentingnya program GNU di banyak distribusi linux. Linux bebas untuk dipublikasikan, dimodifikasi, dan disebarluaskan. (Badar, 2017).

## 2.6 Amazon Linux

Amazon Web Services (AWS) mengembangkan distro Linux bernama Amazon Linux yang dirilis pada tahun 2010, dirancang untuk memaksimalkan kinerja dalam lingkungan cloud AWS. Amazon Linux menyediakan gambar mesin Amazon (AMI) untuk memulai *instance* Amazon Elastic Compute Cloud (EC2) dengan konfigurasi yang telah diatur.

Amazon Linux 2 rilis tahun 2017, sistem operasi yang aman dan berfungsi untuk berbagai tujuan, seperti pengembangan, pengujian, dan produksi.. Versi terbaru membawa banyak pembaruan, seperti kernel terbaru,

dukungan untuk Docker, systemd, dan disertifikasi oleh berbagai lembaga keamanan, termasuk NIST(National Institute of Standards and Technology). Pada ekosistem, Amazon Linux banyak digunakan, terutama untuk mengelola *instance* EC2 dan implementasi aplikasi di AWS.

## 2.7 Ubuntu

Ubuntu, distro linux pertama yang dirilis oleh Canonical Ltd. pada tahun 2004 yang berfokus pada menjadi sistem operasi *open source* yang dapat diakses dan mudah digunakan semua orang. Dukungan komunitas besar, pembaruan perangkat lunak rutin, antarmuka pengguna yang ramah, dan pengelola paket yang kuat adalah beberapa keuntungan Ubuntu. Ubuntu sangat stabil dan dapat digunakan di banyak server, desktop, dan perangkat IoT (Negus, 2008).

## 2.8 Malicious Software

*Malicious software* merupakan *software* yang dimaksudkan untuk menyebabkan kerusakan atau mengganggu komputer atau sistem informasi tanpa persetujuan atau pengetahuan pengguna. Malware dapat menyebabkan kerusakan pada data, mencuri informasi pribadi, merusak sistem operasi, atau bahkan mengunci akses ke file penting. Keberadaan malware adalah ancaman serius bagi keamanan dan integritas sistem komputer dan jaringan. Seiring dengan perkembangan teknologi, jenis dan varian malware terus berkembang, memerlukan upaya konstan untuk mendeteksi, mencegah, dan menghapusnya (Adenasi & Novarina, 2017).

Malware dapat dikelompokkan berdasarkan tujuan penyerang menjadi dua kategori, yaitu malware umum dan malware terpilih. Malware umum, seperti contohnya berupa launcher, diciptakan untuk menyerang sebanyak mungkin komputer korban. Jenis malware ini umumnya lebih mudah terdeteksi karena banyak perangkat lunak keamanan yang telah mempersiapkan diri untuk menghadapi jenis serangan semacam ini. Sementara itu, malware terpilih, seperti contohnya *information-stealing malware*, dirancang khusus untuk menargetkan suatu instansi. Karena tidak tersebar secara luas, malware jenis ini lebih berbahaya daripada malware biasa karena produk keamanan yang digunakan korban mungkin tidak dapat melindungi mereka dari serangan malware terpilih.

## 2.9 VirusTotal

VirusTotal adalah layanan daring yang menawarkan analisis malware dan keamanan siber. VirusTotal mengumpulkan banyak produk antivirus dan mesin pemindai online yang disebut *contributors*. Data gabungan dari *contributors* ini memungkinkan pengguna untuk memeriksa virus yang mungkin terlewatkan oleh perangkat lunak anti-virus milik pengguna atau memverifikasi virus berada. Pihak software anti-virus dapat mengirimkan duplikat file yang ditandai oleh pemindaian lain tetapi diteruskan ke mesin mereka sendiri, yang membantu meningkatkan perangkat lunak dan kemampuan VirusTotal sendiri. Selain itu, pengguna dapat memindai URL yang dicurigai dan mencari melalui kumpulan data VirusTotal (Lardionis, 2012).

## 2.10 Application Programming Interface (API)

Aplikasi Programming Interface (API) merupakan set protokol dan aturan yang dapat membuat berbagai perangkat lunak atau aplikasi berkomunikasi dan berinteraksi satu sama lain. API bertindak sebagai perantara yang memungkinkan suatu program menggunakan fungsionalitas atau layanan dari program atau platform lain tanpa harus mengetahui bagaimana implementasinya secara rinci.

API memungkinkan pengembang untuk mengintegrasikan atau menggunakan fitur tertentu dari suatu sistem tanpa perlu mengakses seluruh kode sumber. Selain itu, API juga melibatkan konsep autentikasi, di mana pengguna atau aplikasi harus memberikan kredensial untuk mengakses sumber daya yang dilindungi.

API sangat penting dalam pengembangan perangkat lunak modern karena memungkinkan integrasi yang lebih mudah antara aplikasi, memfasilitasi pengembangan kolaboratif, dan memungkinkan inovasi yang lebih cepat. Dokumentasi API yang baik menjadi kunci untuk memahami cara menggunakan API, dan keberadaan API telah memainkan peran sentral dalam ekosistem perangkat lunak yang saling terkait dan terintegrasi (Lane, 2019).

## 2.11 File Integrity Monitoring (FIM)

Pemantauan integritas dokumen (FIM) adalah pengendalian atau proses internal

yang melakukan proses memverifikasi integritas *file* sistem operasi dan perangkat lunak aplikasi melalui penggunaan teknik verifikasi antara status *file* terkini dan garis dasar. Metode perbandingan ini sering kali melibatkan penghitungan checksum kriptografi yang diketahui dari garis dasar asli *file* dan membandingkannya dengan *checksum* terhitung dari status *file* saat ini. Atribut *file* lainnya juga dapat digunakan untuk memantau integritas. Umumnya, tindakan melakukan FIM diotomatisasi menggunakan kontrol internal seperti aplikasi atau proses. Pemantauan tersebut dapat dilakukan secara acak, pada interval pemungutan suara yang ditentukan, atau secara *real-time* (Ionx, 2012).

## **2.12 European Institute for Computer Antivirus Research (EICAR) test file**

EICAR *file* tes adalah sebuah *file* yang dikembangkan oleh European Institute for Computer Antivirus Research (EICAR) dan Computer Antivirus Research Organization (CARO) untuk mengevaluasi tanggapan program antivirus komputer. File pengujian ini memungkinkan untuk menguji perangkat lunak anti-virus tanpa harus menggunakan virus komputer asli, alih-alih menggunakan malware asli, yang dapat menyebabkan kerusakan nyata. Dan pada penelitian ini, alih-alih merancang atau membuat sebuah virus yang dapat berdampak langsung ke perangkat, penulis menggunakan file test ini dan mengimplementasikannya ke dalam mesin virtual klien dengan alasan uji coba Wazuh SIEM dalam mendeteksi dan mengeksekusi malware.

## **BAB 3**

### **ANALISIS DAN PERANCANGAN**

#### **3.1 Analisis**

Untuk mendapatkan pemahaman yang tepat tentang suatu topik dan memahami maknanya secara keseluruhan, analisis berarti menguraikan bagian-bagiannya secara menyeluruh dan meninjau hubungan antar bagian (Darminto, 2002). Sebelum memulai perancangan dan pengembangan sistem, proses analisis adalah proses yang pertama kali dimulai, yang dibagi menjadi analisis masalah, dan analisis kebutuhan.

##### *3.1.1. Analisis masalah*

Analisis masalah bertujuan untuk mencari sumber dari sebuah masalah. Penelitian ini akan melakukan identifikasi masalah dalam hal keamanan siber sebagai acuan kebutuhan mencari solusi dalam mendeteksi dan membasmi *malicious software*. Seiring dengan perkembangan teknologi, sistem informasi dan jaringan menjadi semakin kompleks dan terhubung secara luas. Meskipun hal ini membawa manfaat dalam hal fungsionalitas dan keterhubungan, namun juga meningkatkan potensi kerentanan dan serangan siber.

Penelitian ini menggunakan metode 5-Whys untuk mempermudah proses analisis pada tahap mengidentifikasi masalah. Metode ini adalah metode tanya-jawab sederhana yang cukup efektif ketika fokus utamanya adalah mengidentifikasi sebab dan akibat dari suatu masalah. Metode ini dilakukan dengan bertanya "mengapa" sebanyak lima kali atau lebih, di antaranya:

1. Mengapa untuk mendeteksi Malicious Software pada linux dibutuhkan Security Information and Event Management (SIEM) basis Wazuh?

Mendeteksi malware pada Linux memerlukan SIEM Wazuh karena SIEM menyediakan solusi terpadu untuk memantau, menganalisis, dan merespons aktivitas keamanan di lingkungan linux. Wazuh dapat mengumpulkan dan menganalisis data log dari berbagai sumber dalam sistem operasi linux, membantu mengidentifikasi potensi ancaman dan pola perilaku mencurigakan. Wazuh menjadi alat yang berguna untuk menjaga keamanan sistem linux dan mendeteksi aktivitas *software* berbahaya dengan lebih efisien karena dilengkapi dengan aturan deteksi intrusi, kecerdasan ancaman, dan kemampuan respons cepat.

2. Mengapa malware pada sistem operasi Linux dapat membahayakan operasi dan keamanan baik individu maupun organisasi?

Malware sejatinya sangatlah berbahaya jika terjangkit pada perangkat pada Linux yang biasanya dipakai sebagai server dapat membahayakan operasi dan keamanan individu dan organisasi karena dapat merusak data, menyebabkan gangguan operasional, dan berpotensi menyebar ke sistem lain, menyebabkan kerugian data dan penurunan produktivitas.

3. Mengapa Wazuh lebih baik daripada pilihan lain untuk melindungi SIEM?

Wazuh melindungi SIEM lebih baik daripada opsi lain berdasarkan kebutuhan dan situasi penggunaan. Wazuh menerima penghargaan SC Awards sebagai *Best SIEM Solution* pada tahun 2023. Penghargaan ini diberikan karena platformnya mudah digunakan dan terintegrasi dengan alat pihak ketiga dengan baik. Wazuh dapat dianggap lebih baik oleh beberapa pengguna karena kemampuannya dalam menyediakan integrasi yang kokoh dengan SIEM, aturan deteksi intrusi yang kuat, serta dukungan untuk pemantauan dan respons keamanan secara holistik. Tetapi evaluasi ini bergantung pada banyak hal, seperti kebutuhan khusus untuk keamanan, biaya, dan kompleksitas lingkungan.

4. Mengapa menggunakan Wazuh untuk melakukan analisis malware dapat

memberikan informasi dan tanggapan yang lebih cepat dan akurat?

Wazuh dapat mendeteksi malware yang telah dimodifikasi untuk menghindari deteksi. Wazuh mendeteksi malware dengan teknik deteksi perilaku untuk menghindari deteksi, dan Wazuh dapat segera mengirimkan peringatan kepada tim keamanan. Wazuh juga dapat digunakan untuk menggabungkan data dari berbagai sistem keamanan. Ini termasuk integrasi Wazuh dengan sistem manajemen respons insiden, yang memungkinkan Wazuh untuk memberi tim keamanan informasi yang lebih lengkap dan akurat.

5. Mengapa dalam penelitian mendeteksi dan mengeksekusi malware membutuhkan analisis mendalam?

Analisis mendalam diperlukan karena memberikan pemahaman yang lebih komprehensif tentang sifat dan perilaku malware tersebut. Analisis mendalam juga memungkinkan peneliti untuk mengidentifikasi taktik, teknik, dan prosedur yang digunakan oleh malware untuk mengembangkan tindakan perlindungan yang lebih efektif. Selain itu, analisis mendalam memungkinkan peneliti untuk mengidentifikasi bagaimana malware berinteraksi dengan sistem dan jaringan, sehingga memungkinkan peneliti untuk mengidentifikasi potongan-potongan malware yang tidak dikenal.

### 3.1.2. Analisis kebutuhan

Analisis kebutuhan merupakan proses yang berkonsentrasi diidentifikasi dan pemahaman persyaratan yang diperlukan untuk merancang sistem agar dapat mencapai kesimpulan. Analisis kebutuhan terdiri dari dua bagian yakni :

#### 1. Kebutuhan fungsional

Kebutuhan fungsional adalah penjelasan perihal penggambaran fungsi yang disiapkan oleh sistem. Penelitian ini memiliki kebutuhan fungsional, yaitu:

- a. Menjamin bahwa log pada klien tercatat pada server.
- b. Melakukan penentuan frekuensi dalam pengumpulan data *log*.
- c. Melakukan konfigurasi perihal integrasi *agent* dengan *server* dan juga Wazuh SIEM.



- d. Menetapkan standar perihal kondisi yang diperlukan, seperti kode untuk mendeteksi dan mengeksekusi malware.
  - e. Menentukan karakter malware yang dianalisa, yakni EICAR test *file*, sebuah *file* berisi virus dengan tujuan pengembangan.
  - f. Melakukan konfigurasi tambahan perihal notifikasi pelaporan malware.
  - g. Pencatatan dokumentasi dengan mempertimbangkan prosedur.
2. Kebutuhan non-fungsional
- Kebutuhan non-fungsional adalah deskripsi pendukung perihal sistem yang dapat berupa batasan, fitur, dan proses tambahan dari sistem. Penelitian ini memiliki kebutuhan non-fungsional, yakni:
- a. Terlaksana pada saat *server* dan klien berada dalam jaringan yang sama.
  - b. Klien di-*define* di *server* berdasarkan IP Address, yang dapat berubah kapan saja, yang dimana jika alamat IP klien berubah maka harus di-*define* ulang pada *server*.
  - c. Menggunakan *single node* pada *server*, yang membuat Wazuh Indexer, Wazuh Dashboard, dan Wazuh Manager berada pada satu mesin virtual.
  - d. Terjadinya eksekusi pada saat terjangkitnya virus di klien merupakan respon dari Wazuh yang telah diintegrasikan dengan VirusTotal yang di-*define* dengan API *key*.
  - e. Hanya mereka yang memiliki pengetahuan dasar tentang jaringan dan keamanan siber, seperti administrator, yang dapat memahami dan menganalisis hasil log dan simulasi dari penelitian ini.

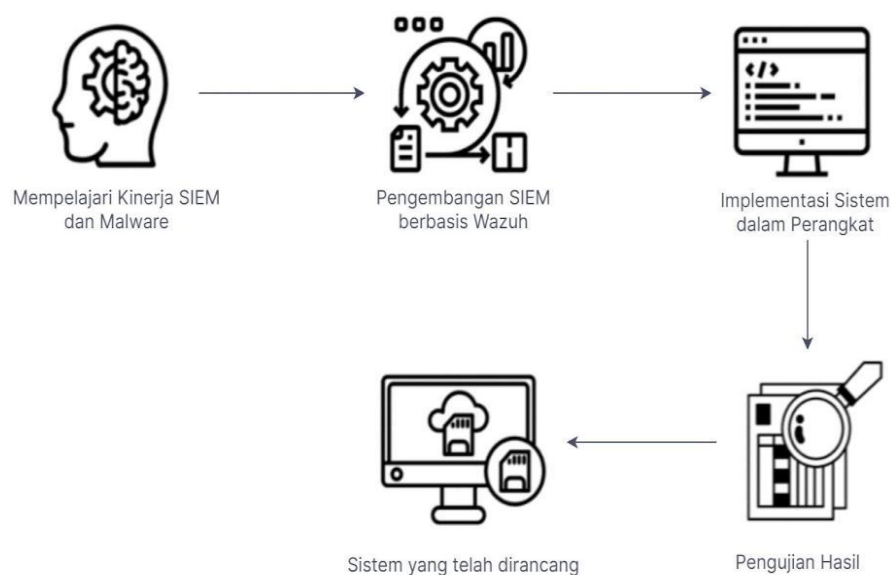
### 3.2 Perancangan Sistem

Perancangan sistem adalah tahap perencanaan menjelaskan sistem diterapkan. Fokus tahapan ini adalah meningkatkan efisiensi dan efektivitas sistem, dan perancangan ini mencakup detail sistem yang dirancang dengan menggunakan bentuk diagram, termasuk bagaimana proses alur sistem program penelitian ini dirancang.

#### 3.2.1. Diagram umum penelitian

Diagram umum penelitian menunjukkan proses yang dilakukan saat penelitian, seperti perumusan masalah, pengumpulan dan analisis data, dan penyusunan

laporan. Ini membantu memahami proses penelitian karena disediakan secara visual.



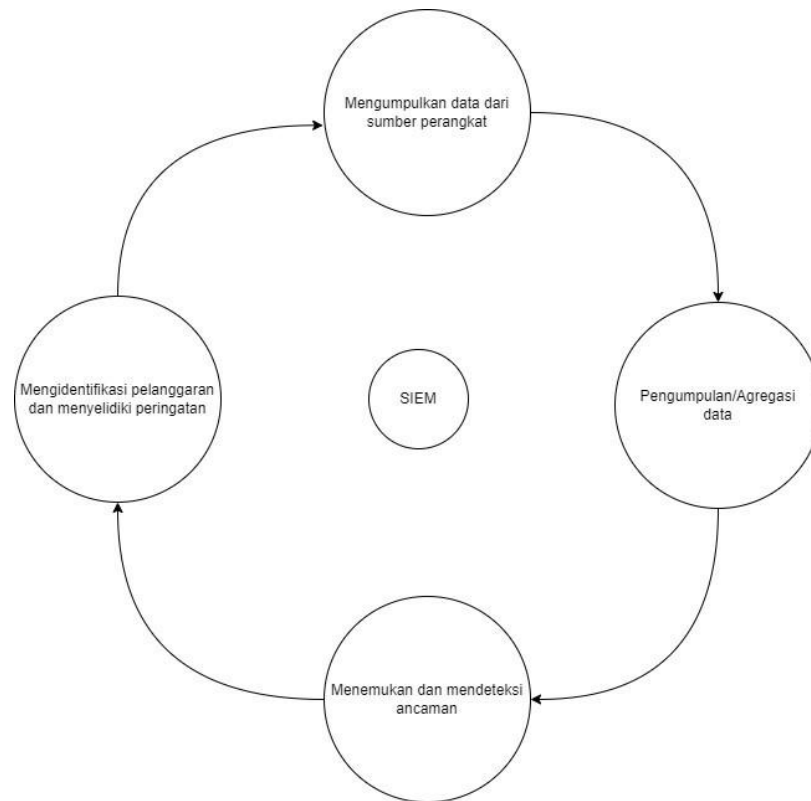
**Gambar 3.1** Alur Penelitian

Berdasarkan Gambar 3.1 dapat dilihat bahwa alur penelitian ini digambarkan dalam bentuk diagram visual, mempelajari cara *Security Information and Event Management* (SIEM) dan juga *malicious software* mengumpulkan data dari berbagai sumber publik, seperti jurnal, buku, dan artikel. Setelah dilakukan pencarian dari berbagai sumber, informasi yang didapat dieksekusi dengan menggunakan Wazuh sebagai *tools* SIEM yang akan digunakan. Mengimplementasikan fitur sistem Wazuh SIEM yang diunduh pada sistem operasi linux melalui Ubuntu. Fitur tersebut akan mendeteksi dan membersihkan Malware. Setelah sistem selesai yang dirancang selesai, dilakukan tahap pengujian untuk mendapatkan kesimpulan apakah sesuai dengan analisis yang diharapkan, menganalisa *Security Information and Event Management* (SIEM) berbasis Wazuh dalam mendeteksi *malicious software* pada sistem operasi linux.

### 3.2.2. Diagram umum SIEM

Pada penelitian kali ini SIEM dirancang untuk dapat melakukan fungsinya, yaitu

mengumpulkan, menganalisis, mengelola, dan melaporkan data keamanan dari berbagai sumber di dalam organisasi. SIEM juga membantu mendeteksi dan menangani ancaman keamanan serta memantau dengan baik aktivitas jaringan.



**Gambar 3.2** Alur Proses SIEM

Berdasarkan gambar 3.2, dapat dilihat pula alur proses SIEM bekerja yakni dimulai pada

1. Tahap pengumpulan data, SIEM pertama-tama mengumpulkan data keamanan dari berbagai sumber, termasuk log sistem, perangkat jaringan, aplikasi, dan perangkat lainnya.
2. Tahap agregasi data, setelah data dikumpulkan, maka SIEM memetakan dan mengkorelasikan data dari berbagai sumber untuk mencari pola atau serangkaian peristiwa yang dapat menunjukkan serangan atau pelanggaran keamanan.
3. Tahap menemukan dan mendeteksi ancaman, SIEM mendeteksi kejadian yang mencurigakan atau aneh, sistem dapat menghasilkan notifikasi atau peringatan segera kepada tim keamanan untuk mengambil tindakan.
4. Tahap mengidentifikasi pelanggaran dan menyelidiki peringatan, setelah menemukan dan mendeteksi adanya ancaman, maka fitur pada SIEM dapat

merespons dengan tindakan yang sesuai, seperti mengisolasi sistem, mematikan akses, atau mengambil tindakan lain yang diperlukan.

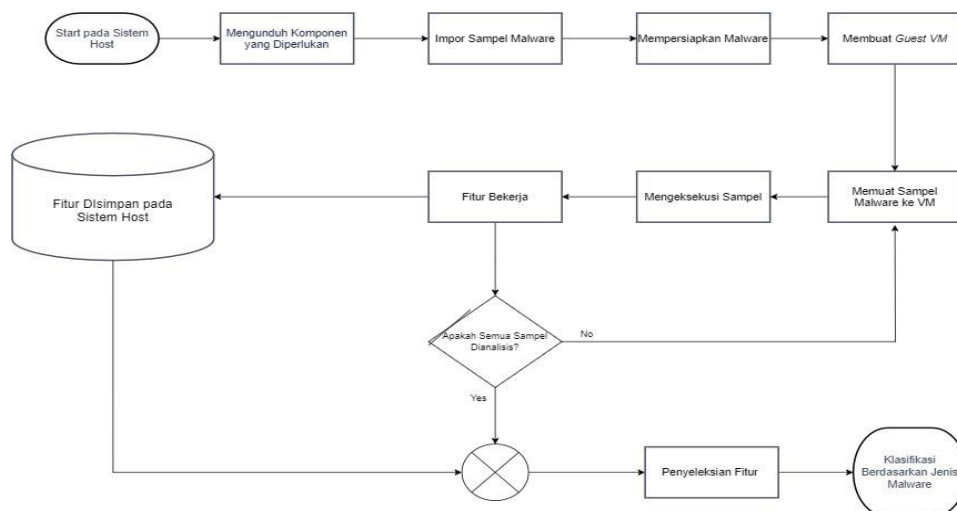
Dengan mengintegrasikan *Security Information Event Management* (SIEM), individu atau bahkan organisasi terkait dapat meningkatkan kemampuan untuk mendeteksi, mencegah, dan merespons terhadap ancaman keamanan yang lebih efektif dengan membutuhkan konfigurasi, pemeliharaan, dan pemantauan yang tepat untuk memberikan manfaat yang maksimal.

### **3.3 *Flowchart* (Diagram Alir)**

Diagram alir (*flowchart*) merupakan wujud gambar visual yang mewakili dari urutan proses atau langkah-langkah dalam suatu sistem, algoritma, atau prosedur yang diwakilkan dengan bantuan simbol grafis yang memiliki arti di setiap simbolnya yang membuat runtutan proses lebih jelas.

#### **3.3.1. *Flowchart analisis malware***

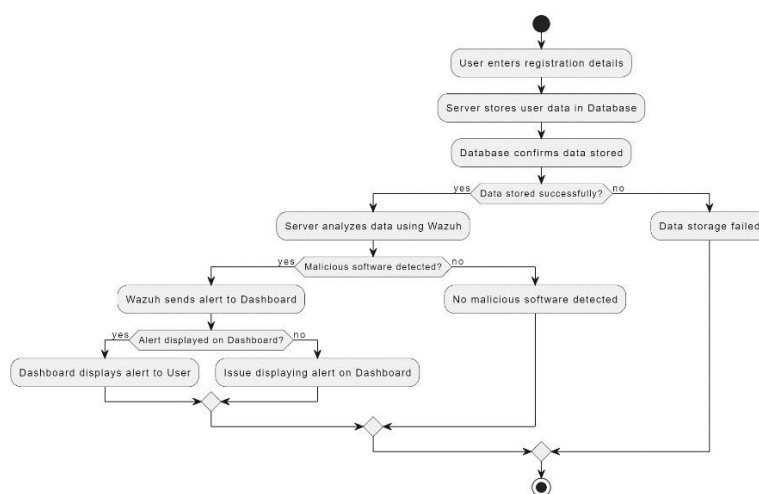
Pada Gambar 3.4, *flowchart* analisis malware terlihat bagaimana proses buatan malware terjangkit ke perangkat dan cara menanggulangnya apabila memiliki fitur seperti SIEM. Malware dapat menjangkit perangkat dengan berbagai cara. Salah satu seperti melalui tautan atau lampiran malware yang dimana pengguna dapat menerima email atau pesan teks dengan tautan atau lampiran yang terinfeksi dan jika pengguna mengklik tautan atau membuka lampiran tersebut, maka malware dapat diunduh di perangkat. Penting untuk selalu berhati-hati saat membuka tautan atau lampiran dari sumber yang tidak dikenal atau mencurigakan. Selain itu, memastikan perangkat dan perangkat lunak selalu diperbarui dengan versi keamanan terbaru dapat membantu mencegah infeksi malware.



**Gambar 3.3** Flowchart Analisis Malware

### 3.3.2. Flowchart penelitian

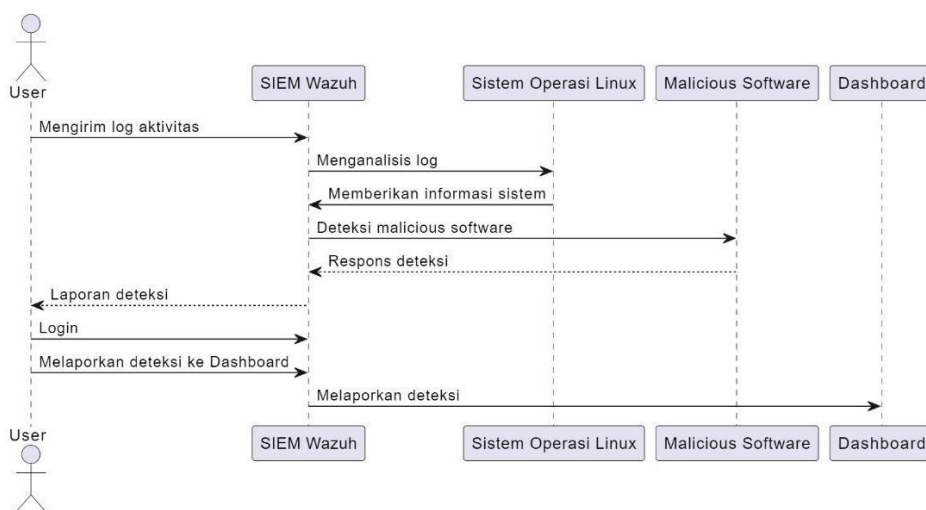
Pada Gambar 3.4, *flowchart* penelitian dengan SIEM yang merupakan sebuah representasi grafis dari metodologi penelitian yang melibatkan penggunaan sistem pengelolaan informasi keamanan dan peristiwa dalam mengumpulkan, menganalisis, dan menafsirkan data keamanan untuk keperluan penelitian. *Flowchart* ini merinci langkah-langkah yang diperlukan untuk merencanakan, mengimplementasikan, dan mengevaluasi penelitian yang menggunakan SIEM sebagai alat utama dalam mengumpulkan dan menganalisis data keamanan. Dengan menggunakan simbol visual yang terstruktur, *flowchart* ini membantu memvisualisasikan alur kerja penelitian, memudahkan pemahaman tentang proses yang dilakukan, serta membantu mengidentifikasi titik penting dalam analisis.



**Gambar 3.4** Flowchart Penelitian

### 3.4 Sequence Diagram (Diagram Urutan)

*Diagram sequence* atau diagram urutan adalah representasi grafis dari urutan interaksi antara objek atau entitas dalam sebuah sistem atau proses. Diagram ini menggambarkan bagaimana pesan atau peristiwa dikirimkan dari satu objek ke objek lain dalam waktu tertentu, memperlihatkan urutan langkah-langkah yang terjadi dalam sebuah proses atau interaksi sistem. Pada Gambar 3.x, *diagram sequence* penelitian ini urutan interaksi antara komponen-komponen utama dalam analisis SIEM berbasis Wazuh untuk mendeteksi perangkat lunak berbahaya pada sistem operasi linux. Diagram ini memvisualisasikan langkah-langkah yang diperlukan dalam proses deteksi, analisis, dan respons terhadap ancaman keamanan yang berasal dari perangkat lunak berbahaya. Dengan menggunakan simbol-simbol grafis yang terstruktur, *diagram sequence* ini membantu pemahaman tentang alur kerja serta hubungan antar komponen dalam sistem SIEM berbasis Wazuh untuk tujuan deteksi keamanan pada lingkungan linux.



**Gambar 3.5** Diagram urutan penelitian

## BAB 4

### IMPLEMENTASI DAN PENGUJIAN

#### 4.1 Implementasi

Setelah tahap analisis dan perancangan, implementasi dan pengujian adalah tahap berikutnya. Implementasi atau penerapan yang dilakukan pada penelitian ini untuk meningkatkan kemampuan deteksi dan manajemen keamanan sistem operasi Linux. Ini mencakup penggunaan Wazuh sebagai SIEM, pengaturan *manager* Wazuh untuk mengumpulkan log, penggabungan alat anti malware, analisis *log* dan tindakan terhadap ancaman.

**Tabel 4.1** *Spesifikasi Perangkat Lunak*

No	Perangkat Lunak	Versi	Kegunaan
1	VMWare	VMWare 17	VMWare adalah <i>software</i> virtualisasi mesin, pada penelitian kali ini baik Wazuh Server yang menggunakan Amazon Linux dan Wazuh Agent yang menggunakan Ubuntu diinstal pada VMWare.
2	Amazon Linux	Amazon Linux 2	Amazon Linux diinstal sebagai sistem operasi server di dalam mesin virtual diinstal Wazuh Dashboard, Wazuh Manager, Wazuh Indexer, Filebeat-OSS dan komponen lain yang digunakan pusat kontrol keamanan.

3	Ubuntu	Ubuntu 22.04.3 LTS	Ubuntu pada penelitian ini diinstall untuk sebagai wadah Wazuh <i>agent</i> yang akan sumber yang akan di-monitoring.
4	Wazuh	Wazuh 4.4.5	Wazuh digunakan sebagai <i>tools</i> SIEM pada penelitian ini yang berfungsi melakukan pemantauan dan analisis data atau <i>log</i> dengan acuan serangan
5	Filebeat-OSS	Filebeat-OSS 7.10.2	Filebeat-OSS diinstal dan merupakan perangkat yang bermanfaat sebagai mengumpulkan, memusatkan, mengirimkan log ke Wazuh <i>Manager</i> dari berbagai sumber.
6	jq	jq 1.6	jq diinstal untuk melakukan pemrosesan dan manipulasi data dalam format JSON. Pada penelitian ini jq berguna untuk sebuah utilitas yang memproses input JSON dari <i>script</i> respons aktif

#### 4.1.1 Spesifikasi laptop dan virtual machine yang digunakan

Pada tahap implementasi digunakan beberapa perangkat yang mendukung proses pengerjaan penelitian ini, diantaranya adalah perangkat laptop dan perangkat *virtual machine* baik *server* maupun *agent*.

Laptop yang digunakan untuk merancang penelitian dan menjalankan *virtual machine* adalah ASUS dengan spesifikasi sebagai berikut:

**Tabel 4.2** Spesifikasi Laptop yang Digunakan

Seri	Prosesor (CPU)	Inti Prosesor	RAM	Memori	Grafis (GPU)
ASUS (M409DA)	2.10 GHz (4 CPUs)	2 core	20480 MB (20 GB)	256 GB	2 GB



Berdasarkan Tabel 4.1 laptop ASUS dengan seri M409DA memiliki:

- 4 inti pemrosesan yang independen dan memiliki kecepatan dari setiap intiprosesor dalam menjalankan instruksi sebesar 2.10 GHz.
- 2 inti pemrosesan yang independen yang memungkinkan prosesor menangani tugas secara bersamaan (*multitasking*).
- Penyimpanan utama dengan sifat penyimpanan sementara sebesar 20480 MB yang setara dengan 20 GB.
- Penyimpanan dengan jangka panjang yang bersifat permanen sebesar 256GB.
- *Graphics Processing Unit* atau kartu grafis AMD sebesar 2 GB yang bertujuan untuk meningkatkan kinerja grafis pada perangkat.

*Tools virtual machine* yang digunakan adalah VMWare. Baik *server* maupun *agent* diunduh pada VMWare. Server pada penelitian memiliki system operasi linux dengan distro Amazon Linux 2. Berikut merupakan spesifikasi teknis dari server wazuh:

**Tabel 4.3 Spesifikasi Server**

OS	Prosesor (CPU)	RAM	Harddisk	Network Adapter
Amazon Linux 2	2	4 GB	50 GB	NAT

Berdasarkan Tabel 4.3 berikut merupakan penjelasan mengenai spesifikasi dari server wazuh yang memiliki atau menggunakan:

- Sistem operasi Linux dengan distro Amazon Linux 2.
- 2 prosesor yang bertujuan untuk memproses tugas secara bersamaan, yang dapat meningkatkan kinerja secara keseluruhan, terutama dalam aplikasi yang mendukung pemrosesan paralel.
- Memori komputer mesin sementara sebesar 4 GB.
- Penyimpanan pada *server* VM sebanyak 50 GB.
- NAT (Network Address Translation) merujuk pada salah satu cara

jaringan yang memungkinkan mesin virtual berinteraksi dengan jaringan luar.

**Tabel 4.4** *Spesifikasi Agent*

OS	Prosesor (CPU)	RAM	Harddisk	Network Adapter
Ubuntu 22.04.3 LTS	2	2 GB	49 GB	NAT

Berdasarkan Tabel 4.4 berikut merupakan penjelasan mengenai spesifikasi dari agen wazuh yang memiliki atau menggunakan:

- Sistem operasi Linux dengan distro Ubuntu 22.04.3 LTS
- 2 prosesor yang bertujuan untuk memproses tugas secara bersamaan, yang dapat meningkatkan kinerja secara keseluruhan, terutama dalam aplikasi yang mendukung pemrosesan paralel.
- Penyimpanan VM sementara atau RAM sebesar 2 GB
- Penyimpanan Harddisk sebesar 49 GB.
- NAT (Network Address Translation) merujuk pada salah satu cara jaringan yang memungkinkan mesin virtual berinteraksi dengan jaringan luar.

#### 4.1.2 Instalasi dan Konfigurasi Wazuh Server

Instalasi server wazuh dan konfigurasinya dilakukan oleh administrator yang paham dengan jaringan yang dilakukan berdasarkan dengan tahapan yang telah beredar sebagai landasan untuk melakukan hal tersebut. Proses instalasi juga dilakukan secara root karena memiliki tingkat akses dan kontrol tertinggi yang membantu dalam proses dalam menjalankan perintah pada tahap ini. Pada penelitian kali ini, server wazuh diinstal menggunakan *single node*, yang mengacu pada konfigurasi dimana semua komponen wazuh dijalankan pada satu server. Ini mencakup wazuh *manager*, *dashboard*, *indexer*, dan *filebeat*. Konfigurasi ini membuat seluruh infrastruktur wazuh berjalan pada satu mesin,

yang bermanfaat untuk pengujian dan implementasi yang lebih sederhana. Salah satu keuntungan penggunaan *single node* pada penginstalan server Wazuh adalah bahwa itu lebih mudah untuk dikonfigurasi dan dikelola, cocok untuk kepentingan penelitian ini yang dilakukan untuk keperluan lingkungan kecil, dan meminimalkan kompleksitas infrastruktur. Meskipun lebih sederhana, konfigurasi *single node* dapat membuat pengalaman pengguna lebih cepat dan lebih mudah, terutama untuk pengujian dan implementasi skala kecil.

#### a. Wazuh *Indexer*

Tahap pertama proses instalasi adalah menambah repositori Wazuh dengan perintah sesuai dengan Gambar 4.1 dan Gambar 4.2 dibawah ini.

```
[root@wazuh-server ~]# rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

**Gambar 4.1** Penambahan Repositori Wazuh

```
[root@wazuh-server ~]# echo -e '[wazuh]\ngpgcheck=1\nfpfkey=https://packages.wazuh.com/key/GPG-KEY-Wazuh\nenabled=1\nname=EL-$releasever - Wazuh\nbaseurl=https://packages.wazuh.com/4.x/yum/\nprotect=1 ; tee /etc/yum.repos.d/wazuh.repo'
```

**Gambar 4.2** Penambahan Repositori Wazuh

Tahap selanjutnya adalah melakukan pengunduhan program dan *file* konfigurasi yang berguna untuk melakukan enkripsi komunikasi antar komponen wazuh, dapat dilihat pada Gambar 4.3 dibawah ini.

```
[root@wazuh-server ~]# curl -s0 https://packages.wazuh.com/4.4/wazuh-certs-tool.sh && curl -s0 https://packages.wazuh.com/4.4/config.yml
```

**Gambar 4.3** Mengunduh Skrip dan Konfigurasi Wazuh

Selanjutnya melakukan edit *file* konfigurasi *./config.yml* yang telah di download sebelumnya dengan mengganti nama node dan alamat IP yang sesuai, pada penelitian kali ini, alamat IP ditetapkan sama karena server dibuat dengan *single node*. Proses edit dapat dilihat pada Gambar 4.4 dibawah ini.



```

GNU nano 2.9.8                               ./config.yml                               Modified
nodes:
  indexer:
    -name: node-1
    ip:192.168.224.133

  server:
    -name: wazuh-1
    ip:192.168.224.133

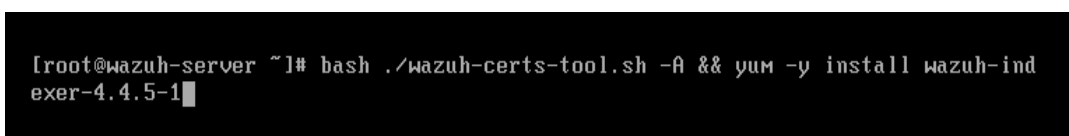
  dashboard:
    -name: dashboard
    ip:192.168.224.133

^G Get Help  ^O Write Out ^W Where Is  ^R Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line

```

**Gambar 4.4** Konfigurasi Wazuh

Tahap berikutnya yakni menjalankan program yang telah diunduh sebelumnya dan tahap terakhir adalah mengunduh package Wazuh *indexer* yang dapat dilihat pada Gambar 4.5 dibawah.



```

[root@wazuh-server ~]# bash ./wazuh-certs-tool.sh -A && yum -y install wazuh-indexer-4.4.5-1

```

**Gambar 4.5** Skrip *Running* dan Unduh *Package* Wazuh Indexer

Setelah tahap diatas telah dilakukan, perlu dilakukan menyunting *file* konfigurasi `/etc/wazuh-indexer/opensearch.yml` seperti terlihat pada Gambar 4.6 sesuai dengan yang telah dilakukan pada file `./config.yml`.

```

GNU nano 2.9.8 /etc/wazuh-indexer/opensearch.yml Modified

network.host: "192.168.224.133"
node.name: "node-1"
cluster.initial_master_nodes:
- "node-1"
cluster.name: "wazuh-cluster"

node.max_local_storage_nodes: "3"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/wazuh-indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/wazuh-indexer.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/wazuh-indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/wazuh-indexer.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false
plugins.security.ssl.http.enabled_ciphers:

^G Get Help ^O Write Out ^W Where Is ^R Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^_ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

**Gambar 4.6** Konfigurasi pada Wazuh Indexer

Lalu untuk memastikan Wazuh indexer sudah berjalan atau tidak dapat dilihat melalui command yang dapat dilihat pada Gambar 4.7 dibawah ini.

```

[root@wazuh-server ~]# systemctl status wazuh-indexer
■ wazuh-indexer.service - Wazuh-indexer
   Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2024-02-09 04:17:32 UTC; 32min ago
     Docs: https://documentation.wazuh.com
   Main PID: 5310 (java)
    CGroup: /system.slice/wazuh-indexer.service
            └─5310 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopense...

Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.boot...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.boot...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.boot...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.boot...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.boot...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.cli...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.cli...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.cli...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.boot...
Feb 09 04:15:54 wazuh-server systemd-entrypoint[5310]: at org.opensearch.boot...
Hint: Some lines were ellipsized, use -l to show in full.
[root@wazuh-server ~]#

```

**Gambar 4.7** Status Wazuh Indexer

#### b. Wazuh Manager (Wazuh Server)

Dikarenakan sistem pada penelitian ini menggunakan *single node*, jadi tahap pertama yang seharusnya menambahkan repositori Wazuh tidak perlu dilakukan karena, pada IP Address yang sama sudah terdapat repositori tersebut. Setelah repositori Wazuh sudah ditambahkan, tahap berikutnya yang dilakukan adalah melakukan penginstalan package Wazuh Manager kedalam server, seperti yang dapat dilihat pada Gambar 4.8 dibawah.

```
[root@wazuh-server ~]# yum -y install wazuh-manager-4.4.5-1
```

**Gambar 4.8** Instalasi Wazuh Manager

Tahap selanjutnya adalah memberikan perintah *enable* dan *start* Wazuh manager, untuk mengaktifkan dan menjalankan Wazuh manager sesuai Gambar 4.9 dan Gambar 4.10 dibawah ini.

```
[root@wazuh-server ~]# systemctl daemon reload && systemctl enable wazuh-manager
```

**Gambar 4.9** Pengaktifan Wazuh Manager

```
[root@wazuh-server ~]# systemctl start wazuh-manager
```

**Gambar 4.10** Memulai Wazuh Manager

Untuk memastikan Wazuh Manager sudah berjalan atau tidak dapat dilihat melalui *command* yang dapat dilihat pada Gambar 4.11 dibawah ini.

```

-9047 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts
/wazuh-apid.py
-9123 /var/ossec/bin/wazuh-integratord
-9144 /var/ossec/bin/wazuh-authd
-9250 /var/ossec/bin/wazuh-db
-9293 /var/ossec/bin/wazuh-execd
-9347 /var/ossec/bin/wazuh-analysisd
-9370 /var/ossec/bin/wazuh-syscheckd
-9451 /var/ossec/bin/wazuh-remoted
-9565 /var/ossec/bin/wazuh-logcollector
-9675 /var/ossec/bin/wazuh-monitord
-9753 /var/ossec/bin/wazuh-modulesd

Feb 09 04:15:35 wazuh-server env[5311]: Started wazuh-db...
Feb 09 04:15:36 wazuh-server env[5311]: Started wazuh-execd...
Feb 09 04:15:38 wazuh-server env[5311]: Started wazuh-analysisd...
Feb 09 04:15:39 wazuh-server env[5311]: Started wazuh-syscheckd...
Feb 09 04:15:41 wazuh-server env[5311]: Started wazuh-remoted...
Feb 09 04:15:42 wazuh-server env[5311]: Started wazuh-logcollector...
Feb 09 04:15:43 wazuh-server env[5311]: Started wazuh-monitord...
Feb 09 04:15:43 wazuh-server env[5311]: 2024/02/09 04:15:43 wazuh-modulesd: WARN
ING: 'update_from_year' option cannot be used for 'nvd' provider.
Feb 09 04:15:45 wazuh-server env[5311]: Started wazuh-modulesd...
Feb 09 04:15:47 wazuh-server env[5311]: Completed.
[root@wazuh-server ~]# systemctl status wazuh-manager -l

```

**Gambar 4.11** Status Wazuh Manager

#### c. Wazuh Dashboard

Dikarenakan sistem pada penelitian ini menggunakan *single node*, jadi tahap pertama yang seharusnya menambahkan repositori Wazuh tidak perlu dilakukan karena, pada IP Address yang sama sudah terdapat repositori tersebut. Setelah repositori Wazuh sudah ditambahkan, tahap berikutnya yang dilakukan adalah melakukan penginstalan package Wazuh Dashboard kedalam server, seperti yang dapat dilihat pada Gambar 4.12 dibawah.

```
[root@wazuh-server ~]# yum -y install wazuh-dashboard-4.4.5-1
```

**Gambar 4.12** Instalasi Wazuh Dashboard

Tahap selanjutnya adalah memberikan perintah *enable* dan *start* Wazuh Indexer, untuk mengaktifkan dan menjalankan Wazuh manager sesuai Gambar 4.13 dan Gambar 4.14 dibawah ini.

```
[root@wazuh-server ~]# systemctl daemon reload && systemctl enable wazuh-dashboa
rd
```

**Gambar 4.13** Pengaktifan Wazuh Dashboard

```
[root@wazuh-server ~]# systemctl start wazuh-dashboard
```

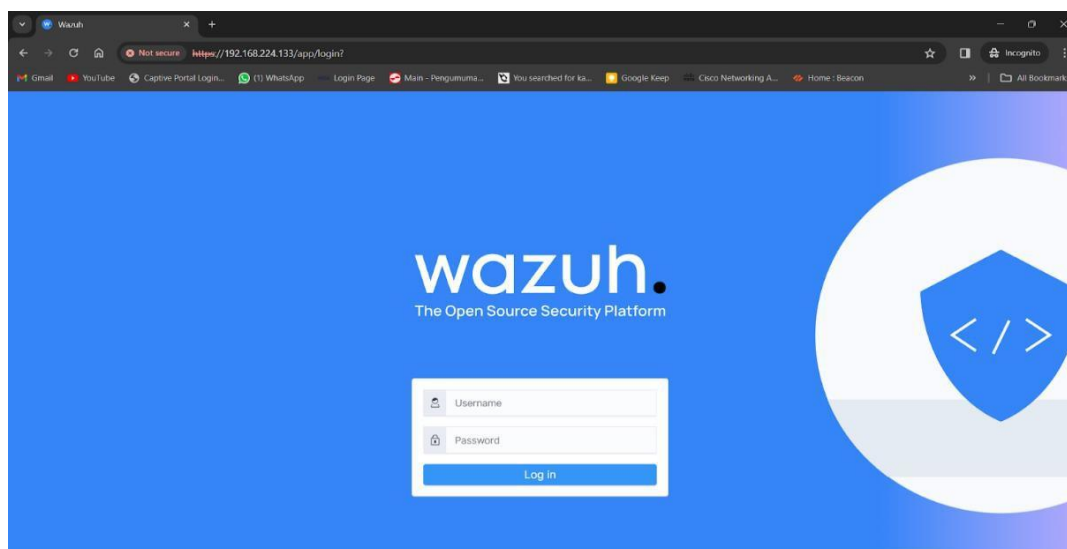
**Gambar 4.14** Wazuh Dashboard Dimulai

Setelah tahap diatas telah dilakukan, perlu dilakukan penyuntingan pada file konfigurasi `/etc/wazuh-dashboard/opensearch_dashboards.yml` seperti dapat dilihat pada Gambar 4.15 untuk memusatkan host Wazuh Dashboard dan URL Wazuh Indexer yang digunakan untuk penampungan kueri yang akan dilakukan.

```
GNU nano 2.9.8 /etc/wazuh-dashboard/opensearch_dashboards.yml Modified
server.host: 0.0.0.0
opensearch.hosts: https://192.168.224.133:9200
server.port: 443
opensearch.ssl.verificationMode: certificate
# opensearch.username: kibanaserver
# opensearch.password: kibanaserver
opensearch.requestHeadersAllowlist: ["securitytenant", "Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/wazuh-dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wazuh
opensearch_security.cookie.secure: true
```

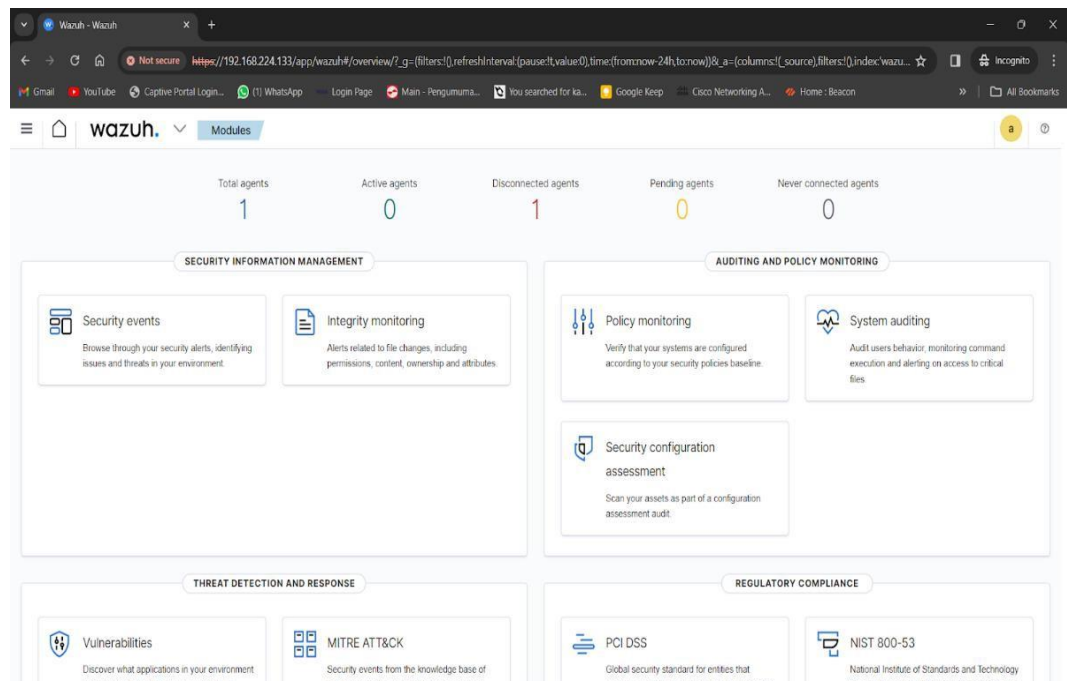
**Gambar 4.15** Konfigurasi Wazuh Dashboard

Berikut tampilan Wazuh Dashboard untuk membuktikan bahwa dapat digunakan yang dapat dilihat pada Gambar 4.16 dan Gambar 4.17 dibawah ini.



**Gambar 4.16** Halaman Login Wazuh Dashboard





**Gambar 4.17** Tampilan Depan Wazuh Dashboard

#### d. Filebeat

Tahap pertama yang akan dilakukan adalah mengunduh package Filebeat dan file konfigurasi Filebeat yang dapat dilihat pada Gambar 4.18 dibawah.

```
[root@wazuh-server ~]# yum -y install filebeat && curl -so /etc/filebeat/filebeat.yml https://package.wazuh.com/4.4/tpl/wazuh/filebeat/filebeat.yml
```

**Gambar 4.18** Instalasi Filebeat

Setelah tahap diatas telah dilakukan, perlu dilakukan penyuntingan pada file konfigurasi `/etc/filebeat/filebeat.yml` seperti dapat dilihat pada Gambar 4.19 untuk mendata alamat IP Wazuh Indexer yang akan terhubung.

```
GNU nano 2.9.8 /etc/filebeat/filebeat.yml Modified

Wazuh - Filebeat configuration file
output.elasticsearch.hosts:
  - 192.168.224.133:9200
  - <elasticsearch_ip_node_2>:9200
  - <elasticsearch_ip_node_3>:9200

output.elasticsearch:
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/wazuh-server.pem"
  ssl.key: "/etc/filebeat/certs/wazuh-server-key.pem"
etup.template.json.enabled: true
etup.template.json.path: '/etc/filebeat/wazuh-template.json'
etup.template.json.name: 'wazuh'
etup.ilm.overwrite: true
etup.ilm.enabled: false
```

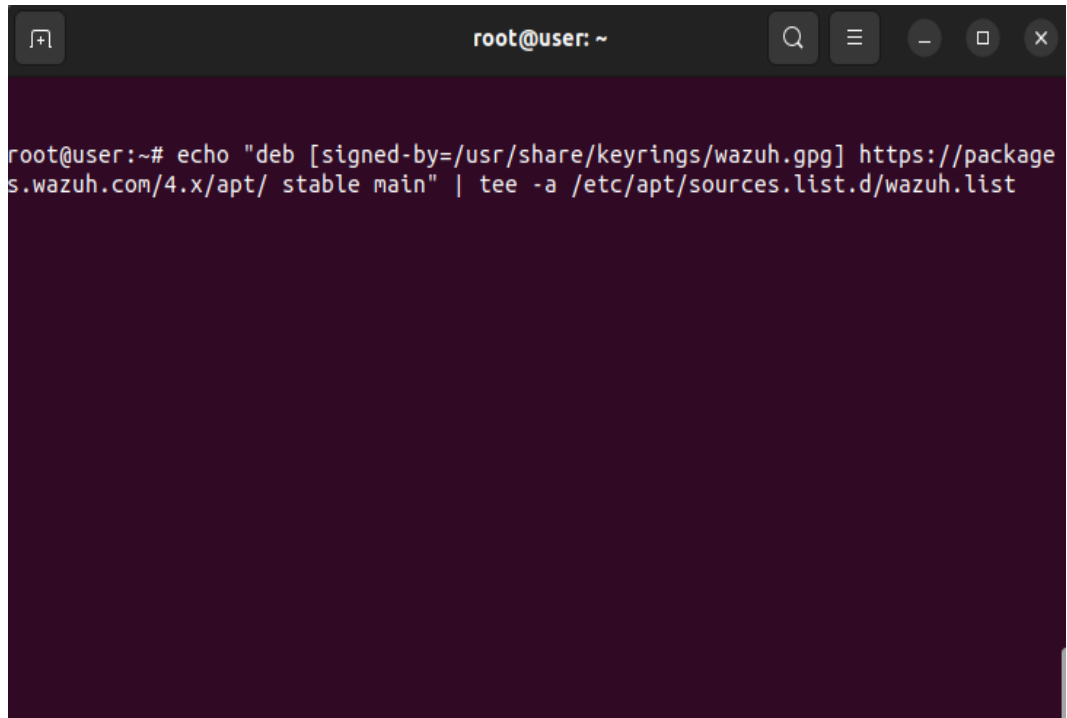
**Gambar 4.19** Konfigurasi Filebeat

#### 4.1.3 Menghubungkan Wazuh Agent dengan Wazuh Server

Wazuh agent pada penelitian ini adalah sumber yang akan diawasi atau dimonitor. Proses ini dilakukan secara *root* karena memiliki tingkat akses dan kontrol tertinggi yang membantu dalam proses dalam menjalankan perintah pada tahap ini. Hal pertama yang akan dilakukan adalah menambahkan repositori Wazuh ke dalam sistem yang dapat dilihat pada Gambar 4.20 dan Gambar 4.21 dibawah ini.

```
root@user: ~
root@user:~# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

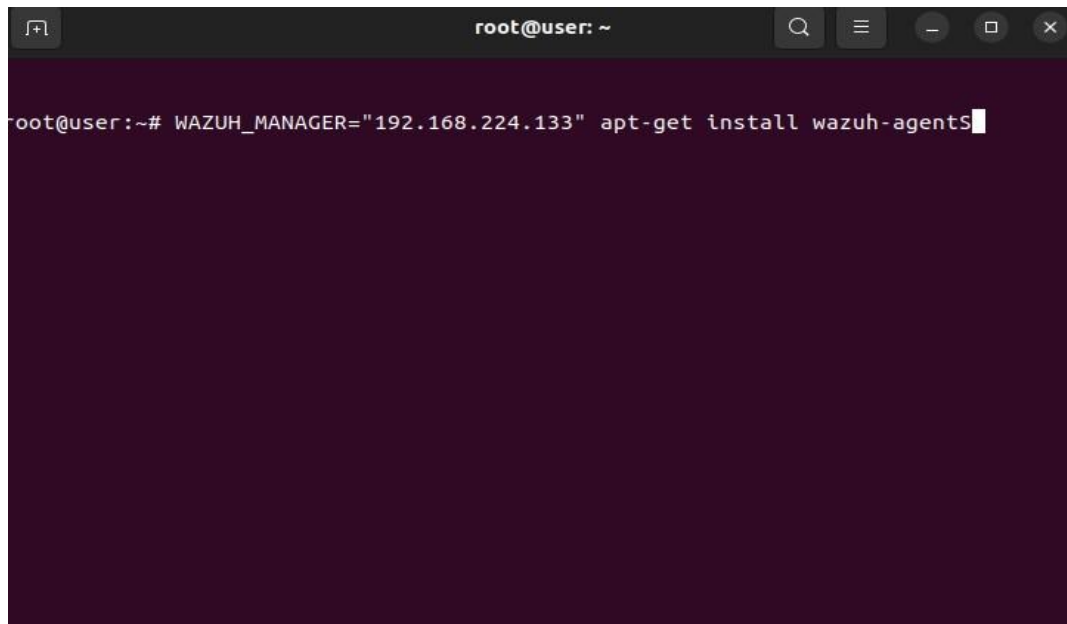
**Gambar 4.20** Menambahkan Repositori Wazuh

A terminal window with a dark purple background. The title bar shows 'root@user: ~' and standard window controls. The command entered is: `root@user:~# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list`

```
root@user:~# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

**Gambar 4.21** Menambahkan Repositori Wazuh

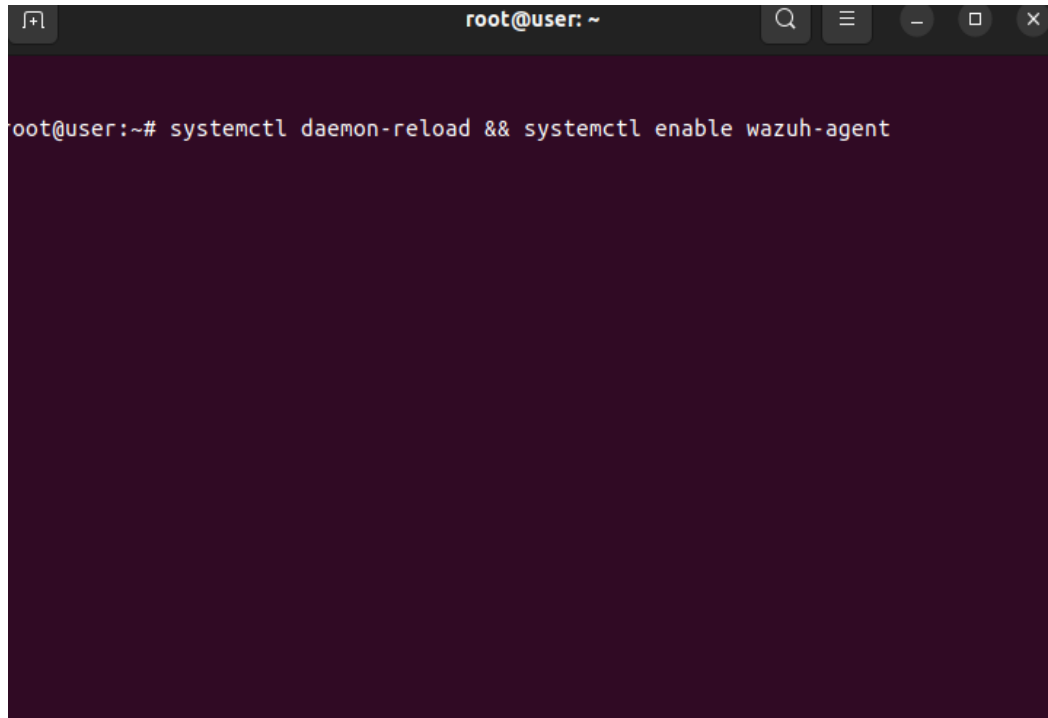
Lalu setelah itu untuk deploy Wazuh Agent, hal yang perlu dilakukan adalah menentukan Wazuh Server yang dilakukan dengan *define* alamat IP pada perintah yang dapat dilihat pada Gambar 4.22.

A terminal window with a dark purple background. The title bar shows 'root@user: ~' and standard window controls. The command entered is: `root@user:~# WAZUH_MANAGER="192.168.224.133" apt-get install wazuh-agentS`

```
root@user:~# WAZUH_MANAGER="192.168.224.133" apt-get install wazuh-agentS
```

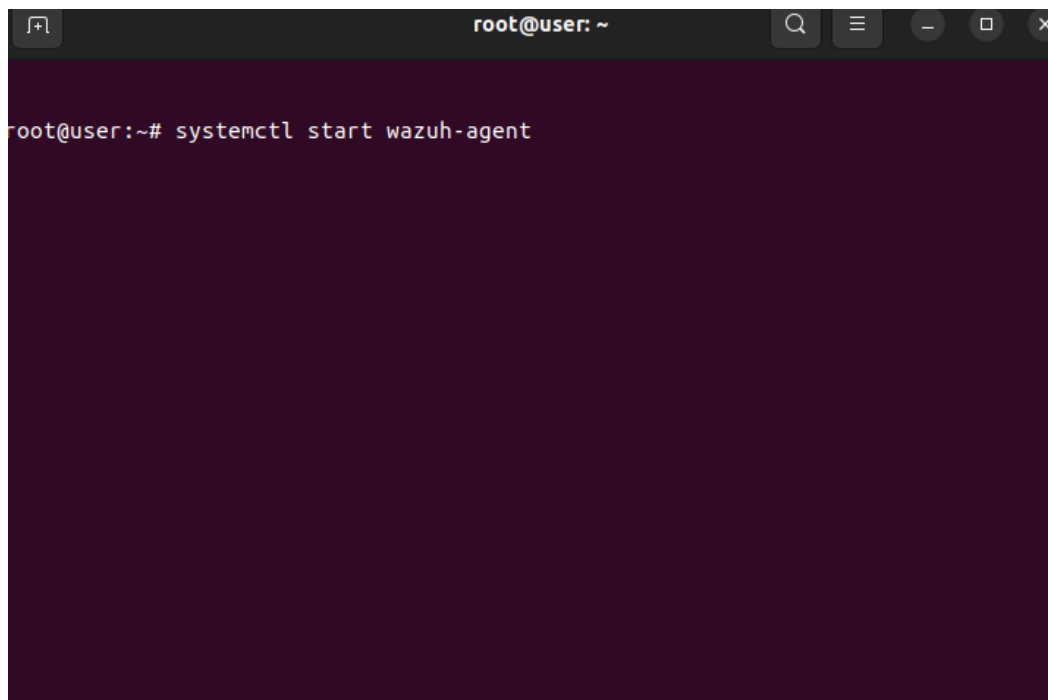
**Gambar 4.22** Menghubungkan Wazuh Manager dengan Wazuh Agent

Tahap selanjutnya adalah memberikan perintah *enable* dan *start* Wazuh Indexer, untuk mengaktifkan dan menjalankan Wazuh manager sesuai Gambar 4.23 dan Gambar 4.24 dibawah ini.

A terminal window with a dark purple background. The title bar shows 'root@user: ~' and standard window controls. The command 'systemctl daemon-reload && systemctl enable wazuh-agent' is entered at the prompt.

```
root@user:~# systemctl daemon-reload && systemctl enable wazuh-agent
```

**Gambar 4.23** Mengaktifkan Wazuh Agent

A terminal window with a dark purple background. The title bar shows 'root@user: ~' and standard window controls. The command 'systemctl start wazuh-agent' is entered at the prompt.

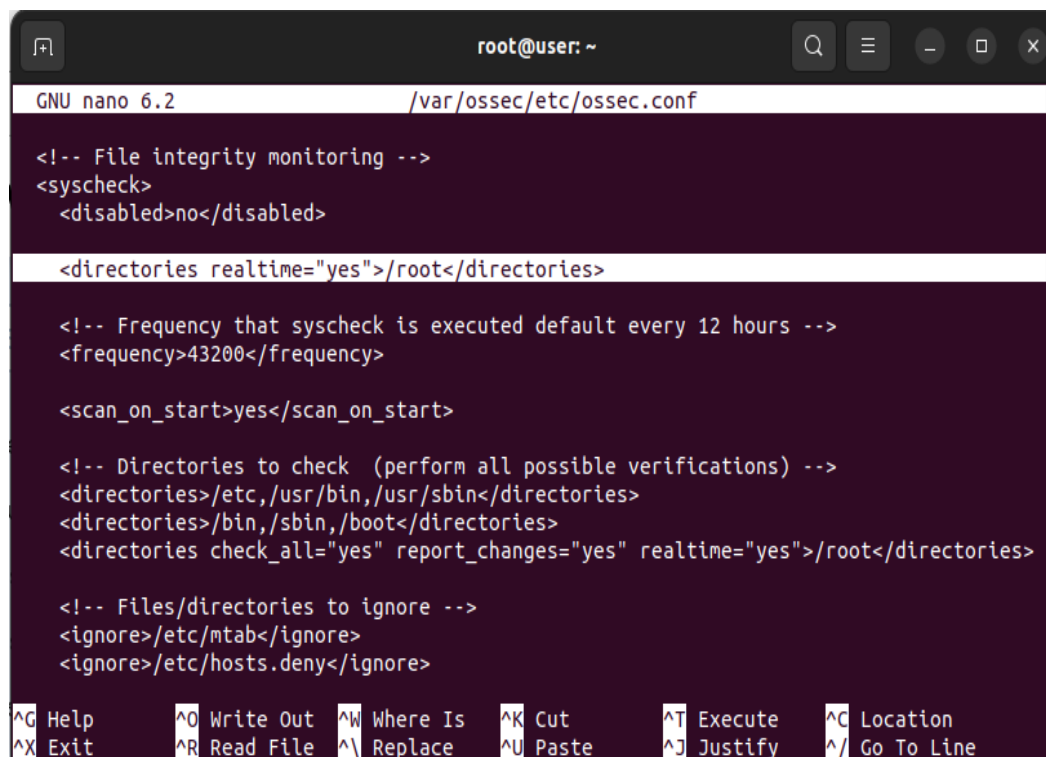
```
root@user:~# systemctl start wazuh-agent
```

**Gambar 4.24** Starting Wazuh Agent

#### 4.1.4 Konfigurasi File Integrity Monitoring

Pemantauan integritas *file* adalah pengendalian atau proses internal yang melakukan proses memverifikasi integritas *file* sistem operasi dan perangkat lunak aplikasi dengan menggunakan teknik verifikasi antara status *file* saat ini dan garis dasar yang diketahui dan baik. Proses ini dilakukan secara *root* karena memiliki tingkat akses dan kontrol tertinggi yang membantu dalam proses dalam menjalankan perintah.

Langkah awal perlu dilakukan yakni menyunting file konfigurasi */var/ossec/etc/ossec.conf* pada Wazuh Server. Hal yang perlu dilakukan adalah menambahkan direktori untuk memantau dalam blok `<syscheck>` yang dapat dilihat pada Gambar 4.25.



```

root@user: ~
GNU nano 6.2 /var/ossec/etc/ossec.conf

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <directories realtime="yes">/root</directories>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
  <directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>

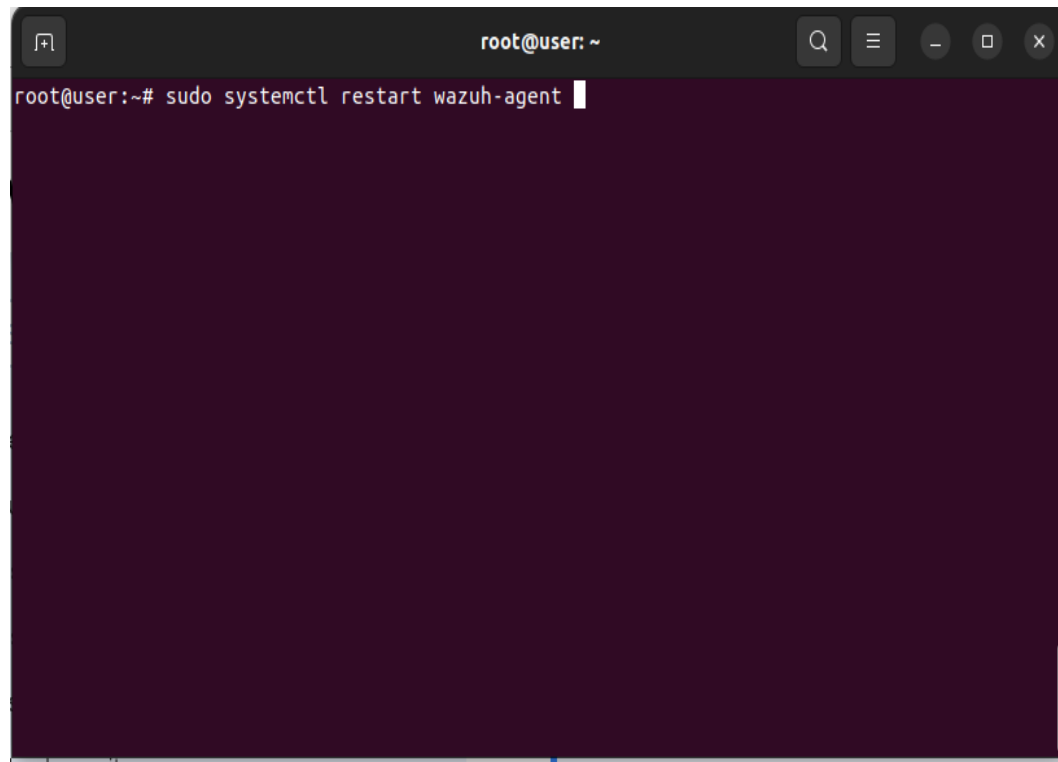
  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line

```

**Gambar 4.25** Edit konfigurasi pada server

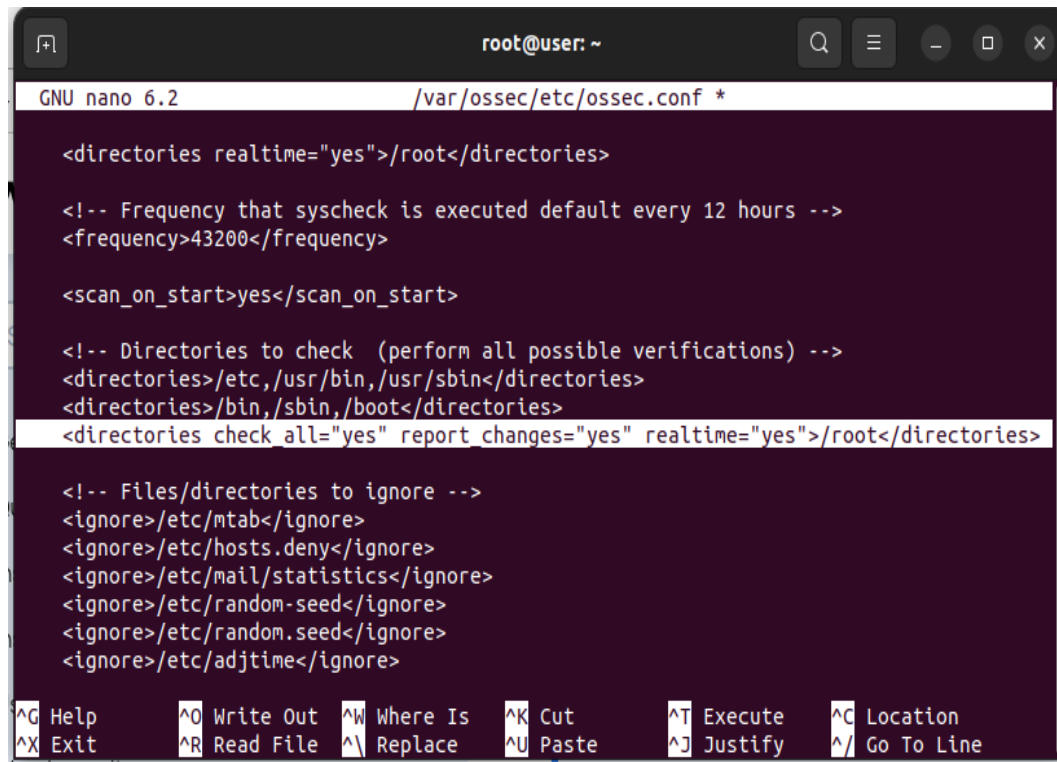
Langkah selanjutnya, untuk menerapkan perubahan konfigurasi, Wazuh Agent harus dimulai ulang yang dapat dilihat pada Gambar 4.26.



**Gambar 4.26** Restart Wazuh Agent

#### *4.1.4 Konfigurasi Untuk Deteksi dan Penghapusan Malicious Software*

Pada tahap menjelaskan bagaimana konfigurasi agar tahap yang sudah dilakukan sebelumnya dapat berguna untuk mencapai tujuan mendeteksi dan membasmi malware. Proses ini dilakukan secara *root* karena memiliki tingkat akses dan kontrol tertinggi yang membantu dalam proses dalam menjalankan perintah pada tahap ini. Pada agent, hal pertama yang dilakukan adalah menambah direktori dalam blok `<syscheck>` pada file konfigurasi `/var/ossec/etc/ossec.conf` untuk memastikan bahwa proses pemantauan dilakukan secara *realtime* yang dapat dilihat pada Gambar 4.27.



```

root@user: ~
GNU nano 6.2 /var/ossec/etc/ossec.conf *

<directories realtime="yes">/root</directories>

<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>

<scan_on_start>yes</scan_on_start>

<!-- Directories to check (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories>/bin,/sbin,/boot</directories>
<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>

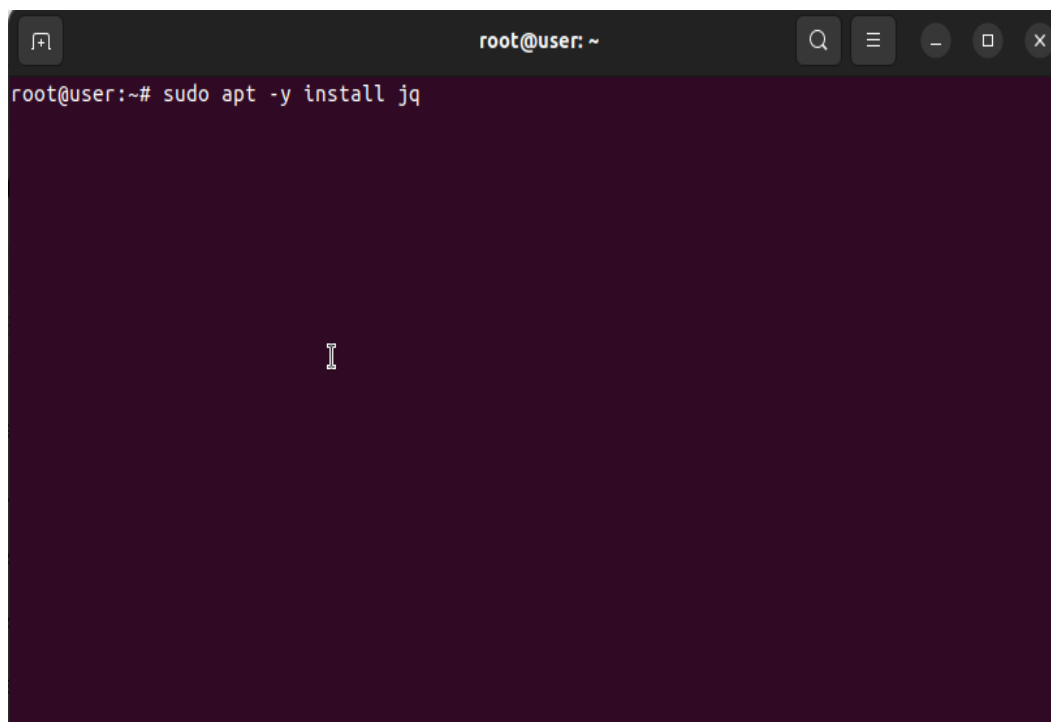
<!-- Files/directories to ignore -->
<ignore>/etc/mtab</ignore>
<ignore>/etc/hosts.deny</ignore>
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/random.seed</ignore>
<ignore>/etc/adjtime</ignore>

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line

```

**Gambar 4.27** Wazuh Running Realtime

Lalu setelah itu, melakukan instalasi jq yang berguna sebagai utilitas yang memproses input JSON dari skrip respons aktif yang dapat dilihat pada Gambar 4.28 dibawah ini.



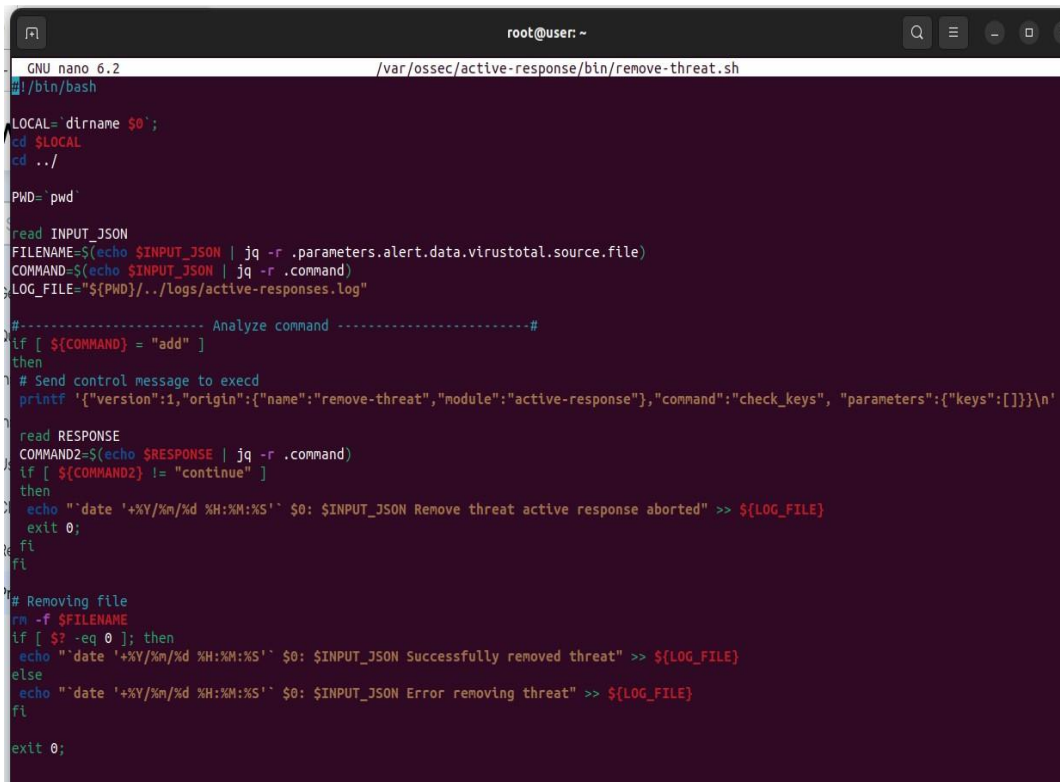
```

root@user: ~
root@user:~# sudo apt -y install jq

```

**Gambar 4.28** Instalasi jq

Selanjutnya, membuat program yang ditulis dalam bahasa Shell Script yang berfungsi untuk mengeksekusi *file* berbahaya dari perangkat yang dapat dilihat pada Gambar 4.29 dibawah ini.



```

GNU nano 6.2 /var/ossec/active-response/bin/remove-threat.sh
#!/bin/bash

LOCAL='dirname $0';
cd $LOCAL
cd ../

PWD='pwd'

read INPUT_JSON
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.data.virustotal.source.file)
COMMAND=$(echo $INPUT_JSON | jq -r .command)
LOG_FILE="${PWD}/../logs/active-responses.log"

#----- Analyze command -----#
if [ ${COMMAND} = "add" ]
then
# Send control message to execd
printf '{"version":1,"origin":{"name":"remove-threat","module":"active-response"},"command":"check_keys", "parameters":{"keys":[]}}\n'

read RESPONSE
COMMAND2=$(echo $RESPONSE | jq -r .command)
if [ ${COMMAND2} != "continue" ]
then
echo "date '+%Y/%m/%d %H:%M:%S'" $0: $INPUT_JSON Remove threat active response aborted" >> ${LOG_FILE}
exit 0;
fi
fi

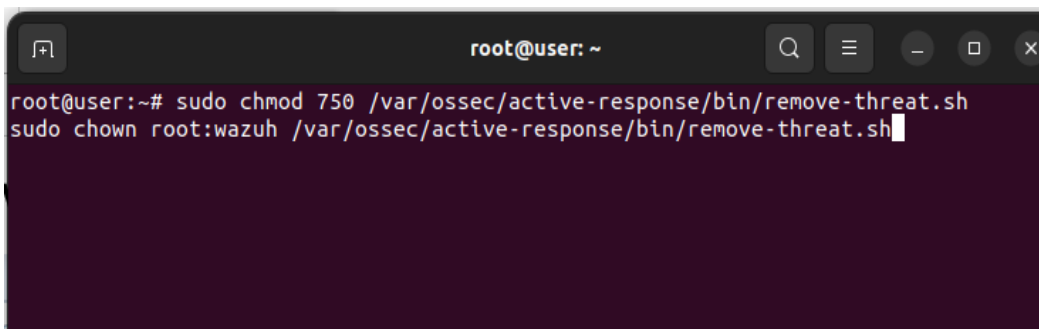
# Removing file
rm -f $FILENAME
if [ $? -eq 0 ]; then
echo "date '+%Y/%m/%d %H:%M:%S'" $0: $INPUT_JSON Successfully removed threat" >> ${LOG_FILE}
else
echo "date '+%Y/%m/%d %H:%M:%S'" $0: $INPUT_JSON Error removing threat" >> ${LOG_FILE}
fi

exit 0;

```

**Gambar 4.29** Skrip Eksekusi

Setelah itu program file yang sudah dibuat diubah izin file tersebut agar pemilik memiliki izin baca (4), izin tulis (2), dan izin eksekusi (1), wazuh memiliki izin baca (4) dan izin eksekusi (1), pengguna lain tidak memiliki izin apapun (0) dan mengubah kepemilikan file. Dalam hal ini, file tersebut akan dimiliki oleh pengguna (*root*) dan wazuh seperti yang dapat dilihat pada Gambar 4.30 dibawah ini.



```

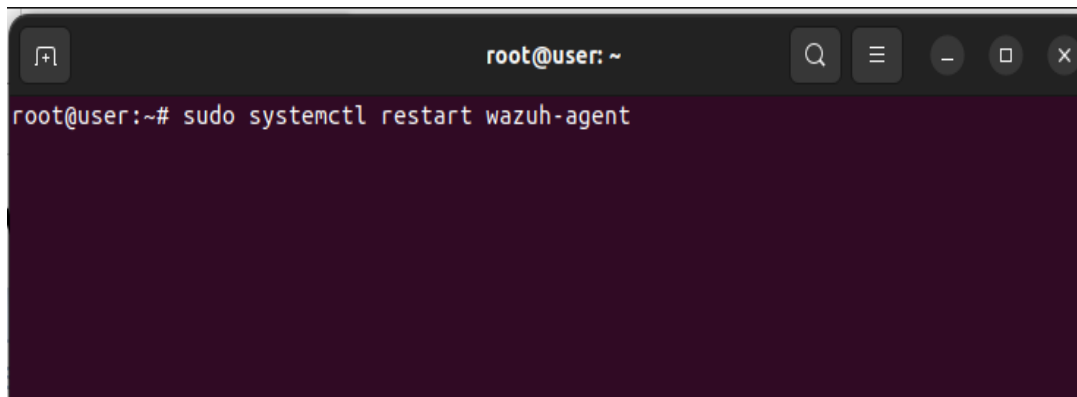
root@user: ~
root@user:~# sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh
sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh

```



**Gambar 4.30** Perintah Izin dan Kepemilikan Skrip

Langkah terakhir yang dilakukan pada Wazuh Agent adalah memulai ulang perangkat agar menerapkan perubahan seperti yang dapat dilihat pada Gambar 4.31 dibawah ini.



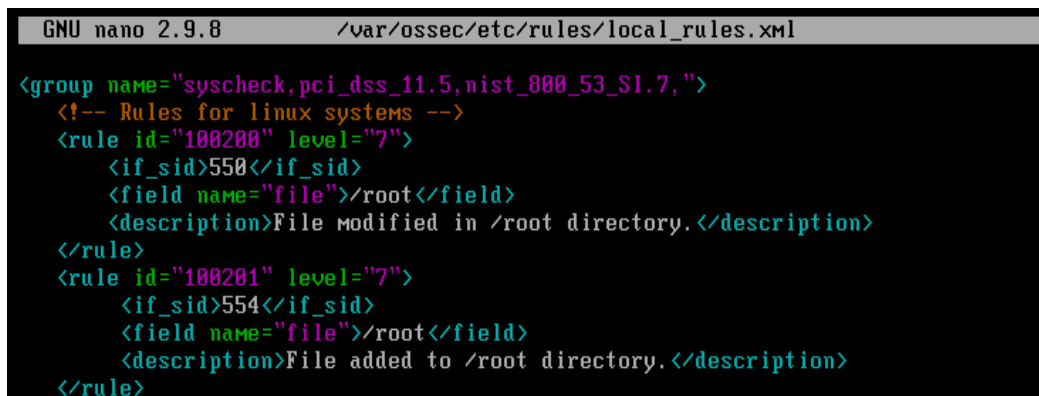
```

root@user: ~
root@user:~# sudo systemctl restart wazuh-agent

```

**Gambar 4.31** Restart Wazuh Agent

Pada sisi Wazuh Server, hal yang pertama kali dilakukan adalah menambahkan rules pada file `/var/ossec/etc/rules/local_rules.xml` untuk memperingatkan perihal perubahan pada direktori pada pemantauan integritas file seperti yang dapat dilihat pada Gambar 4.32 dibawah ini.



```

GNU nano 2.9.8 /var/ossec/etc/rules/local_rules.xml

<group name="syscheck,pci_dss_11.5,nist_800_53_S1.7">
  <!-- Rules for linux systems -->
  <rule id="100200" level="7">
    <if_sid>550</if_sid>
    <field name="file">/root</field>
    <description>File modified in /root directory.</description>
  </rule>
  <rule id="100201" level="7">
    <if_sid>554</if_sid>
    <field name="file">/root</field>
    <description>File added to /root directory.</description>
  </rule>

```

**Gambar 4.32** Penambahan Rule di Server

Lalu setelah itu, seperti yang dapat dilihat pada Gambar 4.33 menambahkan blok baru pada file konfigurasi `/var/ossec/etc/ossec.conf` yang berfungsi mengaktifkan respon aktif dan memicu skrip yang telah dibuat ketika VirusTotal menandai file sebagai berbahaya.

```

GNU nano 2.9.8 /var/ossec/etc/ossec.conf

  <location>/var/log/secure</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/maillog</location>
</localfile>

</ossec_config>

<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key>4851b36bc6a4ee64f0d88eed524d2ed1ed1539733c31bc09b1a62fbcd4333e5$
    <rule_id>100200,100201</rule_id>
    <alert_format>json</alert_format>
  </integration>

  <command>
    <name>remove-threat</name>

```

**Gambar 4.33** File Konfigurasi pada Server

```

GNU nano 2.9.8 /var/ossec/etc/ossec.conf

  <alert_format>json</alert_format>
</integration>

<command>
  <name>remove-threat</name>
  <executable>remove-threat.sh</executable>
  <timeout_allowed>no</timeout_allowed>
</command>

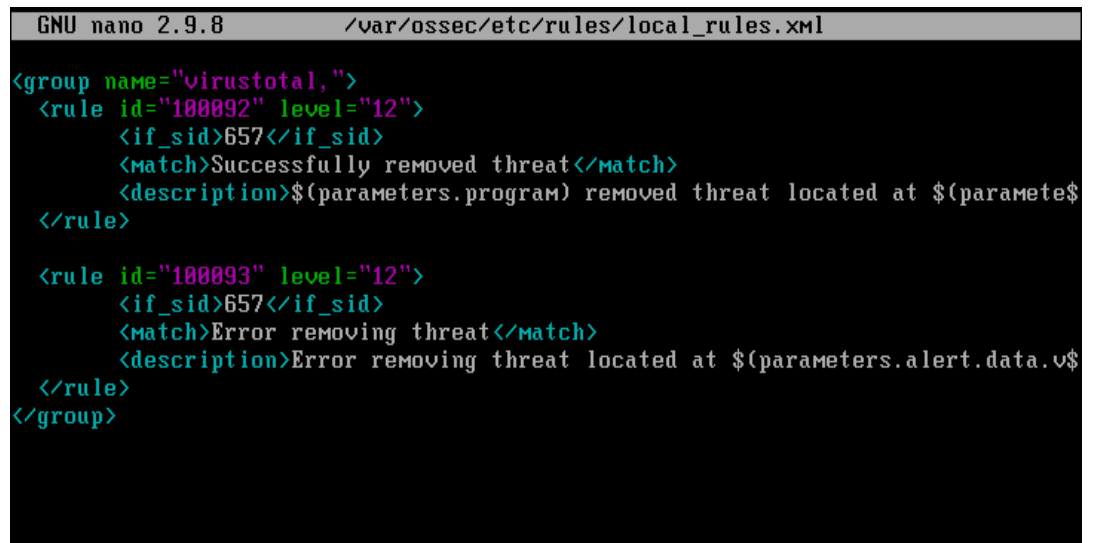
<active-response>
  <disabled>no</disabled>
  <command>remove-threat</command>
  <location>local</location>
  <rules_id>87105</rules_id>
</active-response>

</ossec_config>

```

**Gambar 4.34** File Konfigurasi pada Server

Langkah berikutnya menambahkan rules pada *file* */var/ossec/etc/rules/local\_rules.xml* untuk melakukan deskripsi atas respon skrip aktif yang dapat dilihat pada Gambar 4.35 dibawah ini.



```

GNU nano 2.9.8 /var/ossec/etc/rules/local_rules.xml

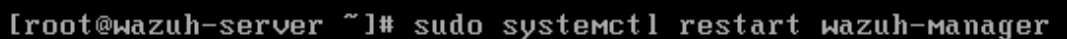
<group name="virustotal,">
  <rule id="100092" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>$(parameters.program) removed threat located at $(paramete$
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.v$
  </rule>
</group>

```

**Gambar 4.35** Penambahan *Rule* pada Server

Langkah terakhir yang dilakukan pada sisi Wazuh server adalah melakukan *restart* pada server untuk mengaktifkan perubahan konfigurasi yang sebelumnya sudah diatur seperti yang dapat dilihat pada Gambar 4.36 dibawah ini.



```

[root@wazuh-server ~]# sudo systemctl restart wazuh-manager

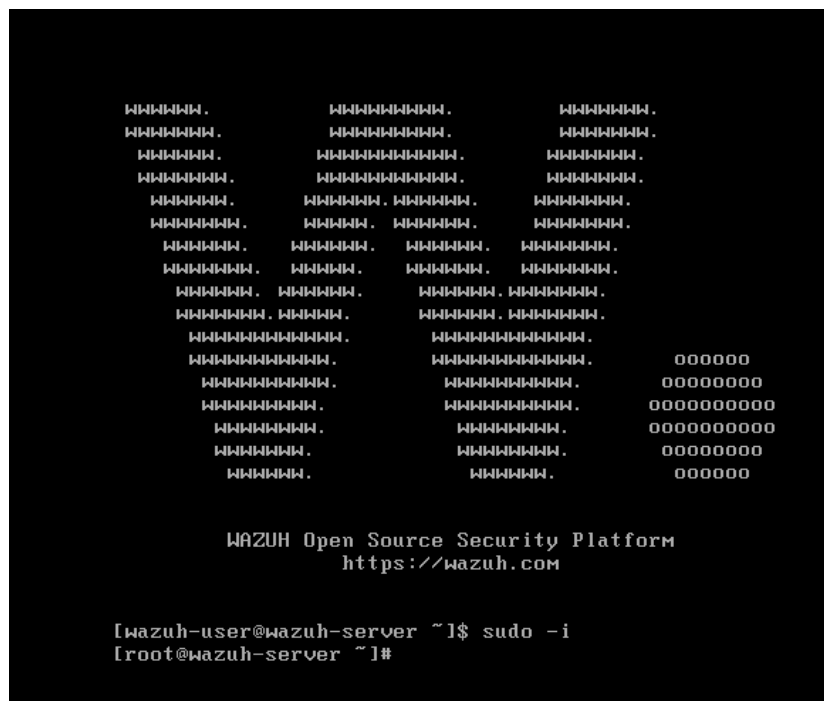
```

**Gambar 4.36** Restart Wazuh Manager

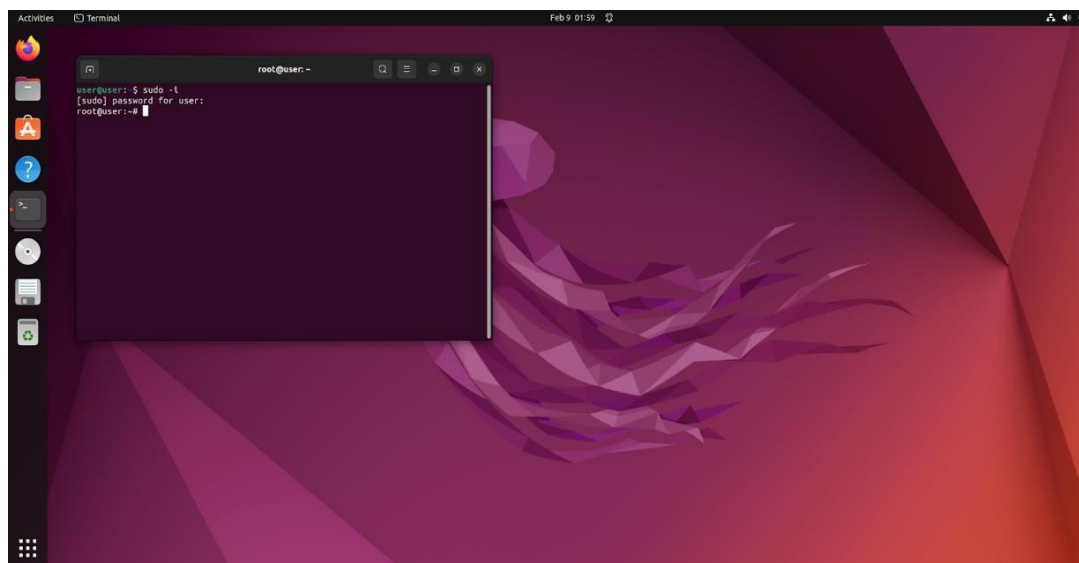
## 4.2 Pengujian

Sistem yang telah dirancang dan dikembangkan diuji coba dalam penelitian ini. Pengujian dilakukan dengan menganalisis proses pendeteksian dan penghapusan malicious software basis Wazuh secara *realtime*.

Pada pengujian kali ini, baik server dan agen harus dihidupkan secara bersamaan. Tampilan server dan agent dapat dilihat pada Gambar 4.37 dan Gambar 4.38 dibawah ini.

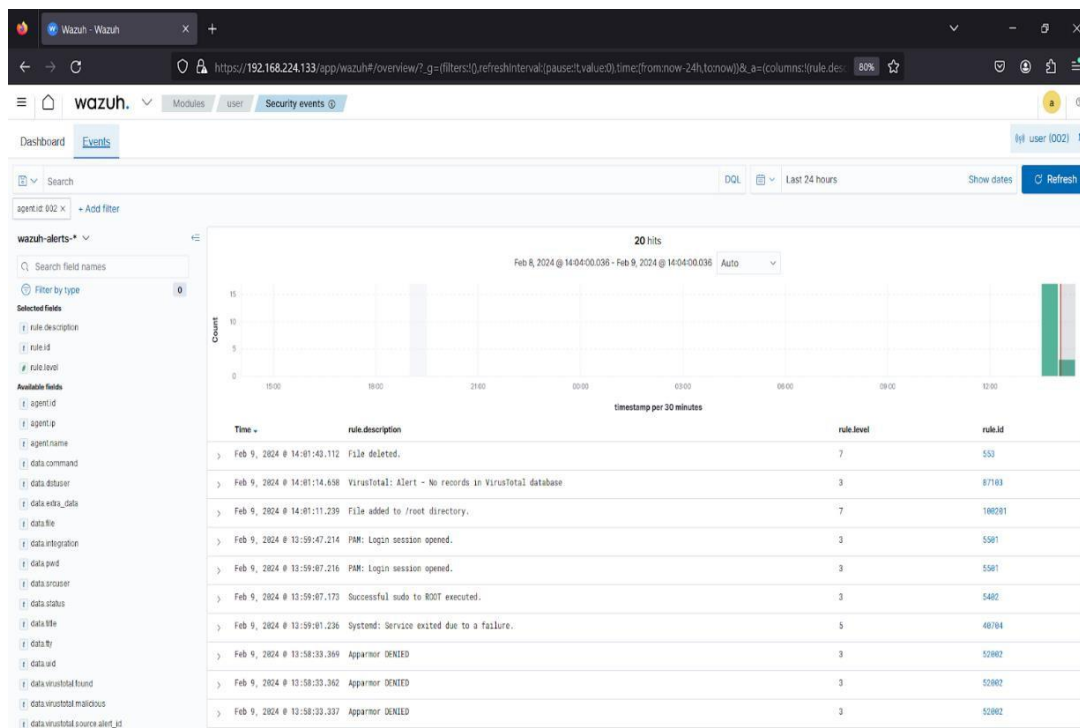


**Gambar 4.37** Tampilan Depan Wazuh Server



**Gambar 4.38** Tampilan Depan Agent

Wazuh dapat mendeteksi data *log* akses *agent* secara *realtime* baik saat aktivitas login maupun perubahan *file* yang sebelumnya diatur pada fungsi *file integrity monitoring* (FIM) yang dapat dilihat pada Gambar 4.39 dibawah ini.



**Gambar 4.39** File Integrity Monitoring

Pengujian serangan pada penelitian ini menggunakan EICAR *file test* yang berfungsi sebagai mengevaluasi tanggapan program antivirus komputer. *File* pengujian ini memungkinkan untuk menguji perangkat lunak anti-virus tanpa harus menggunakan virus komputer asli, alih-alih menggunakan malware asli, yang dapat menyebabkan kerusakan nyata. Alih-alih merancang atau membuat sebuah virus yang dapat berdampak langsung ke perangkat *file test* digunakan dan mengimplementasikannya ke dalam mesin virtual klien dengan alasan uji coba Wazuh SIEM dalam mendeteksi dan mengeksekusi malware.

Pada sisi agent, hal yang dilakukan adalah mengunduh tes *file* EICAR kedalam direktori */root* dengan perintah seperti dilihat pada Gambar 4.40 dibawah ini untuk melakukan pengujian deteksi dan pembasmian malware pada penelitian.

A terminal window with a dark background. The title bar shows 'root@user: ~' and standard window controls. The command 'sudo curl -LO https://secure.eicar.org/eicar.com && ls -lah eicar.com' is entered and executed. The output is not visible in the image.

```
root@user:~# sudo curl -LO https://secure.eicar.org/eicar.com && ls -lah eicar.com
```

**Gambar 4.40** Pengunduhan File Terdeteksi Malware

Pengujian malware dengan bantuan test *file* EICAR berhasil di deteksi oleh Wazuh dengan bantuan dari VirusTotal sebagai virus dan Wazuh langsung menghapus dokumen tersebut dengan skrip yang telah dirancang sebelumnya karena dianggap sebagai malware. Hasil dari deteksi dan menghapus malware dapat dilihat pada Gambar 4.41 dibawah ini. Dan dapat dilihat pada Gambar 4.42 bahwa *file* terindikasi *malicious software* telah berhasil dieksekusi oleh Wazuh berkat skrip dan integrasi yang telah dilakukan.

```

root@user:~# sudo curl -LO https://secure.eicar.org/eicar.com && ls -lah
eicar.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  C
urrent                        Dload  Upload  Total   Spent    Left   S
peed
  0     0     0     0     0     0     0     0  --:--:--  --:--:--  --:--:--
  0     0     0     0     0     0     0     0  --:--:--  --:--:--  --:--:--
100   68  100   68     0     0    56     0  0:00:01  0:00:01  --:--:--
    56
-rw-r--r-- 1 root root 68 Feb  9 02:08 eicar.com
root@user:~#

```

**Gambar 4.41** Respon Terhadap Perintah pada Terminal Agent

Time	rule.description	rule.level	rule.id
> Feb 9, 2024 @ 14:09:08.483	active-response/bin/remove-threat.sh removed threat located at /root/eicar.com	12	100092
> Feb 9, 2024 @ 14:09:08.311	File deleted.	7	553
> Feb 9, 2024 @ 14:09:08.183	VirusTotal: Alert - /root/eicar.com - 64 engines detected this file	12	87185
> Feb 9, 2024 @ 14:08:57.962	PAM: Login session closed.	3	5582
> Feb 9, 2024 @ 14:08:56.922	File added to /root directory.	7	100201

**Gambar 4.42** Hasil Monitoring pada Wazuh Dashboard atas File Terindikasi Malware

## **BAB 5**

### **PENUTUP**

#### **5.1 Kesimpulan**

Berdasarkan tahap implementasi yang telah diipaparkan pada penelitian analisis security information and event management basis wazuh dalam mendeteksi malicious software pada sistem operasi linux, disimpulkan bahwa:

1. Wazuh SIEM terbukti dapat melakukan proses yang dapat mendeteksi dan membasmi dokumen terinfeksi malware pada sistem operasi linux yang dibantu dengan integrasi VirusTotal melalui API *key*.
2. *Log* serangan yang dilakukan dapat direkam oleh Wazuh SIEM yang dapat diakses pada halaman Wazuh Dashboard pada bagian *Events* secara *realtime*. Wazuh SIEM menyimpan serangan yang terdeteksi. Ini memungkinkan administrator untuk menganalisis dan melihat serangan yang terjadi.
3. Skrip yang telah dirancang terbukti dapat melakukan fungsinya sesuai dengan yang diharapkan dengan dibantu juga tools pendukung seperti Filebeat untuk pencatatan *log* ke Wazuh Indexer, VirusTotal yang dapat memberikan informasi tambahan tentang entitas yang relevan, meningkatkan pemahaman tentang keamanan sistem, dan jq yang melakukan pemrosesan dan manipulasi data dalam format JSON.

#### **5.1 Saran**

Saran yang diberikan untuk penelitian selanjutnya adalah sebagai berikut:

1. Disarankan untuk melakukan penelitian lebih lanjut melakukan penelitian SIEM dengan tools lain dan jenis serangan berbeda pula.
2. Penelitian selanjutnya dapat dilakukan menggunakan metode multinode karena metode ini meningkatkan distribusi beban kerja, skalabilitas, lapisan keamanan tambahan, isolasi fungsi, meningkatkan ketahanan terhadap kegagalan, dan mempermudah manajemen dan pemeliharaan sistem.



3. Disarankan untuk melakukan penelitian dengan menerapkan integrasi *tools* selain VirusTotal dalam menganalisa *file* terindikasi *malicious software*, seperti Yara, Google Safe Browsing, dan lainnya.

## DAFTAR PUSTAKA

- Adenasi, R., & Novarina, L. A. (2017). MALWARE DYNAMIC, *Journal of Education and Information Communication Technology*, 1, 37–43.
- Ariyus, D. (2018). *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi*. Yogyakarta: CV Andi Offset.
- Broto, G., S., D. (2013). "Ancaman Cyber Attack Dan Urgensi Keamanan Informasi Nasional", <https://sdppi.kominfo.go.id/berita-ancaman-cyber-attack-dan-urgensi-keamanan-informasi-nasional-26-2079>. Diakses pada 18 Agustus 2023.
- Campbell, Tony. (2016). *Practical Information Security Management: A Complete Guide to Planning and Implementation (1st edition)*. Apress.
- Chuvakin, A. (2010). SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IMPLEMENTATION (Vol. 1). *Syngress Publishing*.
- Clarke, J. (2009). SQL Injection Attacks and Defense. In SQL Injection Attacks and Defense. *ELSEVIER*.
- Kamal, M. R., & Setiawan, M. A. (2021). Deteksi Anomali dengan Security Information and Event Management ( SIEM ) Splunk pada Jaringan UII. *AUTOMATA*, 4.
- Harjono (2013). “Deteksi Malware Dalam Jaringan Menggunakan Dionaea”, <https://jurnalnasional.ump.ac.id/index.php/Techno/article/view/96>. Diakses pada 3 Oktober 2023.
- Lane, Kin, (2019). "Intro to APIs: History of APIs" <https://blog.postman.com/intro-to-apis-history-of-apis/>. Diakses pada 17 Januari 2024.
- Lardinois, Frederic (2012). "Google Acquires Online Virus, Malware and URL Scanner VirusTotal". *TechCrunch*. Diakses pada 17 Januari 2024.
- Maiwald E. (2013). *Network Security A Beginner's Guide, Third Edition (A. Brandt (ed.)). The McGraw-Hill Companies*.
- Negus, Christopher. (2007). *Ubuntu Linux Toolbox (1st edition)*. Wiley.
- Pratama, M. D., Nova, F., Pratama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *Jurnal Ilmiah Teknologi Sistem Informasi*.
- Rihal M., (2010). “Implementasi Analisa Security Information Management Menggunakan OSSIM pada Sebuah Perusahaan”, <http://lib.ui.ac.id/file?file=digital/20249100-R031079.pdf>. Diakses 1 Juli 2023.
- Sakinah, T. (2022). “Analisis Log Sistem Pada Security Information And Event Management Untuk Mendeteksi Data Exfiltration”.

<http://repository.upnvj.ac.id/id/eprint/19760>. Diakses pada 2 Oktober 2023.

Stallings, William. (2016). *Network Security Essentials: Applications and Standards* (6th edition). *Pearson*.

Stinson, Douglas. (2005). *Cryptography: Theory and Practice* (3rd edition). *Chapman and Hall/CRC*.

Tipton, H.F., & Krause, M. (2007). *Information Security Management Hand Book*. (6th ed.). *New York: Auerbach Publication Taylor & Francis Groups*.

Verisys - How it Works. (2021). Ionx Solutions. Diakses pada 17 Januari 2024, dari <https://www.ionxsolutions.com/products/verisys-fim#:~:text=How%20it%20Works,check%20manually%20at%20any%20time>.