

**ANALISIS KINERJA WAZUH DAN SURICATA SEBAGAI  
SISTEM DETEKSI SERANGAN PADA JARINGAN  
ENDPOINT**

**TUGAS AKHIR**



diajukan oleh:

**Nama : Muhammad Abdul Halim**

**NIM : 22.01.4875**

**PROGRAM DIPLOMA  
PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2025**

**ANALISIS KINERJA WAZUH DAN SURICATA SEBAGAI  
SISTEM DETEKSI SERANGAN PADA JARINGAN  
ENDPOINT**

**TUGAS AKHIR**

Diajukan untuk memenuhi salah satu syarat mencapai gelar Ahli Madya  
Komputer Program Diploma – Program Studi Teknik Informatika



diajukan oleh

**Nama : Muhammad Abdul Halim**

**NIM : 22.01.4875**

**PROGRAM DIPLOMA  
PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2025**

## HALAMAN PERSETUJUAN

### TUGAS AKHIR

#### ANALISIS KINERJA WAZUH DAN SURICATA SEBAGAI SISTEM DETEKSI SERANGAN PADA JARINGAN ENDPOINT

yang dipersiapkan dan disusun oleh

**Muhammad Abdul Halim**

**22.01.4875**

Telah disetujui oleh Dosen Pembimbing Tugas Akhir  
pada tanggal 7 Juli 2025

Dosen Pembimbing,

  
Pramodhita Ferdiansyah, M.Kom

**NIK. 190302409**

HALAMAN PENGESAHAN

TUGAS AKHIR

ANALISIS KINERJA WAZUH DAN SURICATA SEBAGAI  
SISTEM DETEKSI SERANGAN PADA JARINGAN  
ENDPOINT

yang disusun dan diajukan oleh

**Muhammad Abdul Halim**

**22.01.4875**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 21 Juli 2025

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Nila Feby Puspitasari, S.Kom., M.Cs.  
NIK. 190302161

Ali Mustopa, S.Kom., M.Kom.  
NIK. 190302192



Tugas Akhir ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Ahli Madya komputer  
Tanggal 21 Juli 2025

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusriani, M.Kom.  
NIK. 190302106

## HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : **Muhammad Abdul Halim**  
NIM : **22.01.4875**

Menyatakan bahwa Tugas Akhir dengan judul berikut:

**Analisis Kinerja Wazuh dan Suricata Sebagai Sistem Deteksi Serangan Pada Jaringan Endpoint**

Dosen Pembimbing : **Pramudhita Ferdiansyah, M.Kom.**

1. Karya tulis ini adalah benar-benar **ASLI** dan **BELUM PERNAH** diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan **gagasan, rumusan dan penelitian SAYA** sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima **SANKSI AKADEMIK** dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 21 Juli 2025

Yang Menyatakan,



Muhammad Abdul Halim

## HALAMAN PERSEMBAHAN

Puji syukur kehadiran Allah SWT atas limpahan Rahmat serta Karunia-Nya sehingga saya dapat menyelesaikan tugas akhir ini.

Dengan segala rasa hormat dan rasa sayang, saya persembahkan Tugas Akhir ini untuk kedua orang tua saya, bapak Hamidi Prasetya dan Ibu Partini yang sangat saya sayangi. Terima kasih atas segala limpahan doa, dukungan moral dan materi, serta pengorbanan yang sangat luar biasa untuk mendukung langkah dalam mengejar mimpi-mimpi.

Kakak tercinta Rohmah Susana Eka Putri dan Azis Arifin, serta Keponakan Tercinta Arsyila Zakiya Arifin, terimakasih telah memberikan semangat, mendukung, mendoakan dan memberikan keceriaan dalam setiap hari saya.

Terima kasih juga saya ucapkan untuk sahabat-sahabat saya yang telah menjadi sahabat terbaik saya selama di lingkungan perkuliahan, yang selalu memberikan dukungan, dorongan, dan selalu membantu dalam setiap kesulitan yang saya hadapi.

Terima kasih untuk semua yang telah membantu saya selama ini dalam meraih cita-cita.

## KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa, yang telah melimpahkan rahmat, hidayah, serta karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir ini dengan lancar. Tugas akhir ini disusun untuk memenuhi salah satu syarat kelulusan Program Diploma 3 pada Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Selain itu penulis dengan segala kerendahan hati ingin menyampaikan rasa terima kasih kepada semua pihak yang telah berjasa memberikan dukungan dan bantuan untuk menyelesaikan laporan tugas akhir ini. Untuk itu penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM, selaku Rektor Universitas Amikom Yogyakarta
2. Ibu Prof. Dr. Kusrini, M.Kom. selaku Dekan Program Fakultas Ilmu Komputer
3. Bapak Barka Satya, M.Kom, selaku Ketua Program Studi D3 Teknik Informatika Universitas Amikom Yogyakarta.
4. Bapak Pramudhita Ferdiansyah, M.Kom, selaku dosen pembimbing yang memberikan arahan, saran, dan motivasi terhadap penulis
5. Kedua orang tua, keluarga besar, dan teman-teman tercinta yang memberikan semangat dan doa kepada penulis.

Yogyakarta, 7 Juli 2025

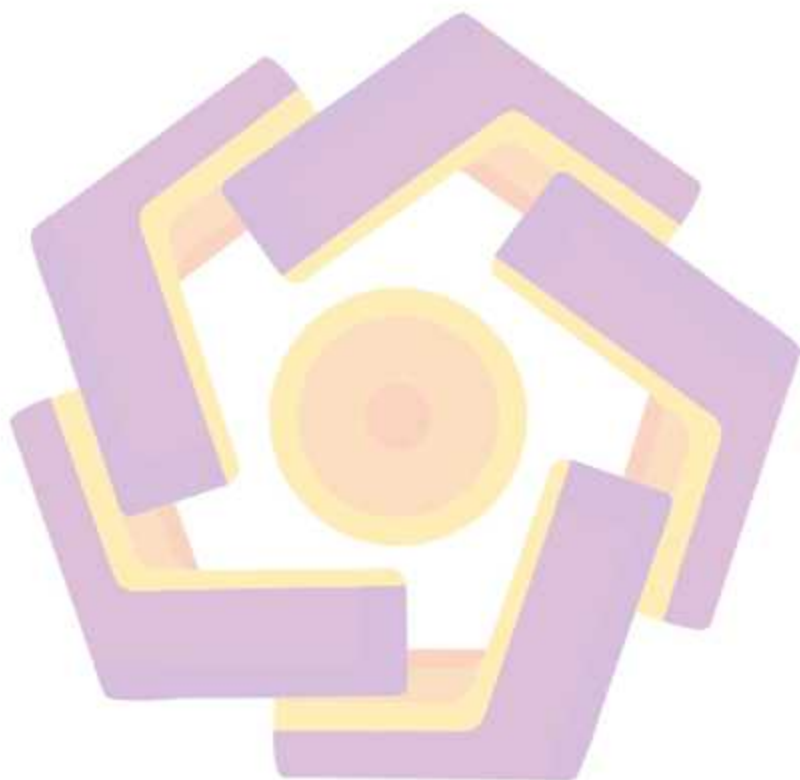
Penulis

## DAFTAR ISI

HALAMAN JUDUL .....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN .....	iv
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR.....	v
HALAMAN PERSEMBAHAN .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xiii
DAFTAR SINGKATAN .....	xiv
DAFTAR ISTILAH.....	xv
INTISARI .....	xvi
ABSTRACT.....	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Perumusan masalah .....	3
1.3 Tujuan Penelitian.....	3
1.4 Batasan Masalah .....	3
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA .....	6
2.1 Literature Review.....	6
2.2 Landasan Teori.....	14
2.2.1 Security Information and Event Management (SIEM).....	14
2.2.2 Wazuh.....	14
2.2.3 CIA ( <i>Confidentiality, Integrity, Availability</i> ) .....	18
2.2.4 Endpoint.....	18
2.2.5 Suricata .....	18
2.2.6 SQL Injection.....	19
2.2.7 DDoS .....	19
2.2.8 Brute Force .....	19

2.2.9 Port Scanning.....	20
2.2.10 SPDLIC (Security Policy Development Life Cycle) .....	20
<b>BAB III METODOLOGI PENELITIAN .....</b>	<b>21</b>
3.1 Objek Penelitian .....	21
3.2 Metode Penelitian.....	21
3.3 Alur Penelitian.....	21
3.4 Analisis.....	24
3.4.1 Analisis Kondisi Awal Endpoint.....	24
3.4.2 Pengumpulan Kebutuhan/Alat dan Bahan.....	26
3.5 Desain.....	27
3.5.1 Desain Komponen .....	27
3.5.2 Desain Arsitektur Sistem .....	28
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>30</b>
4.1 Implementasi .....	30
4.1.1 Instalasi Wazuh.....	30
4.1.2 Integrasi dengan <i>API Telegram(Bot)</i> .....	31
4.1.3 Instalasi Wazuh Agent.....	36
4.1.4 Instalasi dan Konfigurasi Suricata.....	38
4.1.5 Penambahan Custom Rule Suricata.....	40
4.2 Pengujian.....	42
4.2.1 Port Scanning.....	42
4.2.2 DDoS .....	43
4.2.3 Brute Force .....	44
4.2.4 SQL Injection.....	46
4.2.5 Validasi Hasil Pengujian.....	47
4.2 Evaluasi .....	59
4.4 Analisis dan Pengurnian Hasil.....	60
4.4.1 Analisis Hasil Deteksi Port Scanning.....	61
4.4.2 Analisis Hasil Deteksi DDoS SYN Flood .....	62
4.4.3 Analisis Hasil Deteksi Brute Force .....	63
4.4.4 Analisis Hasil Deteksi SQL Injection.....	64
4.4.5 Ringkasan Analisis .....	65
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>66</b>
5.1 Kesimpulan.....	66

5.2 Saran.....	66
DAFTAR PUSTAKA .....	67



## DAFTAR GAMBAR

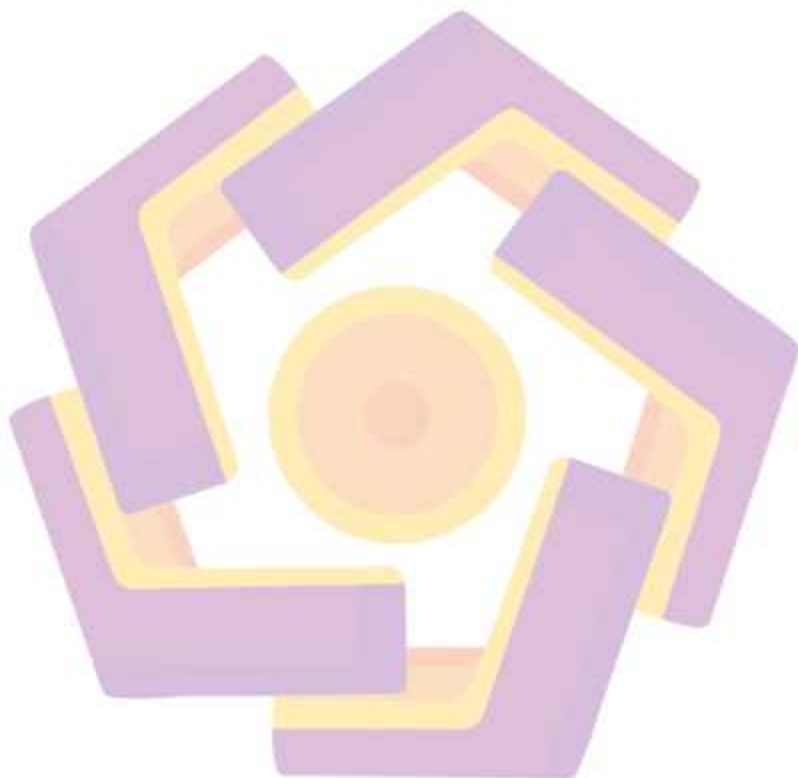
Gambar 1. 1 Grafik Trafik Anomali di Indonesia 2024[4] .....	1
Gambar 2. 1 Komponen Wazuh[15] .....	15
Gambar 2. 2 Wazuh Indexer[15] .....	15
Gambar 2. 3 Wazuh Server[15] .....	17
Gambar 2. 4 Wazuh Agent[15] .....	18
Gambar 2. 5 Metode Pengembangan Sistem SPDLC .....	20
Gambar 3. 1 Alur Penelitian .....	22
Gambar 3. 2 Pengujian Awal Serangan DDoS SYN Flood dengan Hping3 .....	25
Gambar 3. 3 Kecepatan Respon Server Sebelum dan Saat Terjadi Serangan .....	25
Gambar 3. 4 desain perancangan komponen Wazuh dan Suricata .....	28
Gambar 3. 5 Alur Sistem .....	29
Gambar 4. 1 Opsi Instalasi Wazuh pada Bash Script .....	30
Gambar 4. 2 Proses Instalasi Komponen Wazuh .....	31
Gambar 4. 3 Request Token API Telegram dengan BotFather .....	32
Gambar 4. 4 Melihat ID akun Telegram .....	32
Gambar 4. 5 Bash Script Integrasi Wazuh dengan Telegram .....	33
Gambar 4. 6 Python Script Notifikasi Telegram 1 .....	34
Gambar 4. 7 Python Script Notifikasi Telegram 2 .....	35
Gambar 4. 8 Baris Inisiasi Integrasi Telegram didalam Wazuh .....	36
Gambar 4. 9 Install Wazuh Agent .....	36
Gambar 4. 10 Daftar Agent Dari Wazuh Dashboard .....	37
Gambar 4. 11 Integrasi Suricata dengan Wazuh .....	37
Gambar 4. 12 Penambahan Log Apache Server Target .....	38
Gambar 4. 13 Repository resmi Suricata .....	38
Gambar 4. 14 Install Suricata .....	38
Gambar 4. 15 Konfigurasi Network Address Suricata.yml .....	39
Gambar 4. 16 Konfigurasi Global Stats Suricata .....	39
Gambar 4. 17 Konfigurasi af-packet Interface Suricata .....	39
Gambar 4. 18 Konfigurasi Lokasi Rules Suricata .....	40
Gambar 4. 19 Rule Port Scanning Suricata .....	40
Gambar 4. 20 Rule DDoS Suricata .....	41
Gambar 4. 21 Rule Brute Force Suricata .....	41
Gambar 4. 22 Rule SQL Injection Suricata .....	42
Gambar 4. 23 Pengujian Port Scanning NMAP .....	43
Gambar 4. 24 Pengujian DDoS SYN Flood Hping3 22.000 paket .....	43
Gambar 4. 25 Pengujian DDoS SYN Flood Hping3 110.000 paket .....	44
Gambar 4. 26 Pengujian Brute Force dengan NMAP .....	45
Gambar 4. 27 Pengujian Brute Force dengan Hydra .....	46
Gambar 4. 28 Pengujian SQL Injection SQLMAP .....	47
Gambar 4. 29 Log Deteksi Port Scanning Suricata fast.Log .....	48
Gambar 4. 30 Event Port Scanning pada Wazuh .....	48
Gambar 4. 31 Notifikasi Telegram Port Scanning .....	49
Gambar 4. 32 Log Deteksi DDoS SYN Flood 1 Suricata fast.log .....	50

Gambar 4. 33 Event DDoS SYN Flood 1 pada Wazuh .....	50
Gambar 4. 34 Notifikasi Telegram DDoS SYN Flood 1 .....	51
Gambar 4. 35 Log Deteksi DDoS SYN Flood 2 Suricata fast.log .....	51
Gambar 4. 36 Event DDoS SYN Flood 2 Wazuh .....	52
Gambar 4. 37 Notifikasi Telegram DDoS SYN Flood 2 .....	52
Gambar 4. 38 Log Deteksi Brute Force Nmap Suricata .....	53
Gambar 4. 39 Event Brute Force Nmap Wazuh .....	54
Gambar 4. 40 Notifikasi Telegram Brute Force Nmap .....	54
Gambar 4. 41 Log Deteksi Brute Force Hydra Suricata fast.log .....	55
Gambar 4. 42 Event Brute Force Hydra Wazuh .....	55
Gambar 4. 43 Notifikasi Telegram Brute Force Hydra .....	56
Gambar 4. 44 Log Deteksi SQL Injection Suricata fast.log .....	56
Gambar 4. 45 Event SQL Injection Wazuh .....	57
Gambar 4. 46 Notifikasi Telegram SQL Injection .....	57
Gambar 4. 47 Alert SQL Injection Wazuh .....	58
Gambar 4. 48 Alert Web Attack Wazuh .....	58
Gambar 4. 49 Pengujian DDoS SYN Flood Setelah Tuning .....	59
Gambar 4. 50 Alert DDoS setelah Tuning Threshold .....	60
Gambar 4. 51 Koneksi SSH Asli Terdeteksi Sebagai Brute Force Suricata .....	64



## DAFTAR TABEL

Tabel 2. 1 Perbandingan Penelitian .....	9
Tabel 3. 1 Spesifikasi VPS dan VM .....	26
Tabel 4. 1 Waktu Deteksi Suricata dan Wazuh .....	65
Tabel 4. 2 Waktu Wazuh mencatat dan mengirimkan menuju telegram .....	65




## DAFTAR SINGKATAN



SIEM	<i>Security Information and Event Management</i>
IDS	<i>Intrusion Detection System</i>
HIDS	<i>Host Based Intrusion Detection System</i>
VM	<i>Virtual Machine</i>
VPS	<i>Virtual Private Server</i>
API	<i>Application Programing Interface</i>
DDoS	<i>Distributed Denial of Service</i>
SQL	<i>Structured Query Language</i>
SSD	<i>Solid State Drive</i>
RAM	<i>Random Access Memory</i>
vCPU	<i>Virtual Central Unit Processing</i>
JSON	<i>JavaScript Object Notation</i>
SPDLC	<i>Security Policy Development Life Cycle</i>

## DAFTAR ISTILAH



Rule	Aturan atau intruksi aksi ketika sistem mengidentifikasi pola potensi ancaman dan serangan dalam jaringan.
Signature	Pola yang dianalisis dalam paket atau lalu lintas jaringan.
False Positif	Bukan serangan, terdeteksi.
True Positif	Benar Serangan, Terdeteksi.
Event	Catatan berisi informasi peristiwa atau insiden pada sistem.
Log	Kumpulan Event.
Alert	Laporan Insiden pada Sistem.
Threshold	Nilai minimum atau batas yang ditetapkan untuk suatu kondisi atau kriteria, yang jika dilampaui atau dicapai akan memicu tindakan tertentu.
Tools	Alat untuk membantu suatu kegiatan.

## INTISARI

*Endpoint* merupakan komponen yang rentan dan sering menjadi sasaran berbagai jenis serangan siber, mulai dari perusakan sistem hingga pencurian data penting. Untuk menjaga keamanan *endpoint*, dibutuhkan pemantauan. Namun, pemantauan secara konvensional seperti membaca log host memakan waktu dan sumber daya, sehingga serangan berpotensi tidak terdeteksi secara langsung. Untuk memastikan keamanan *endpoint*, tujuan penelitian adalah dengan mengembangkan sistem informasi keamanan, manajemen *event* dan sistem deteksi sehingga terdapat respon cepat ketika terjadi insiden.

Penelitian ini menggunakan pendekatan SPDLC (*Security Policy Development Life Cycle*) untuk membangun sistem keamanan jaringan. Wazuh sebagai SIEM (*Security Information and Event Management*) diimplementasikan untuk mengelola log dari *endpoint* dan mengirimkan alert ke API Telegram secara real-time. Wazuh mendeteksi anomali dengan menganalisis log host berdasarkan rule bawaan. Sistem juga dilengkapi Suricata sebagai IDS (*Intrusion Detection System*) yang memantau lalu lintas jaringan dan mencocokkannya dengan signature yang ada, untuk mendeteksi serangan seperti Port Scanning, DDoS, Brute Force, dan SQL Injection.

Pengujian dilakukan dengan menyerang server target yang menjalankan aplikasi web menggunakan 4 jenis serangan tersebut. Hasil pada pengujian menunjukkan, serangan dapat terdeteksi dengan waktu dari mulai serangan dilakukan hingga alert keluar pada notifikasi telegram, adalah antara 1 detik hingga paling lama 7 detik. Hasil ini menunjukkan bahwa kinerja Wazuh dan Suricata dapat mendeteksi berbagai jenis serangan secara real-time dengan delay yang relatif singkat, sehingga membantu meningkatkan keamanan *endpoint*.

**Kata kunci:** Wazuh, Suricata, Endpoint, Keamanan, Jaringan

## ABSTRACT

Endpoints are vulnerable components and are often targeted by various types of cyberattacks, ranging from system damage to the theft of critical data. Monitoring is required to maintain endpoint security. However, conventional monitoring methods such as reading host logs consume time and resources, potentially allowing attacks to go undetected immediately. To ensure endpoint security, the purpose of this research is to develop a security information system, event management, and detection system so that there is a quick response when an incident occurs.

This research uses the SPDLC (Security Policy Development Life Cycle) approach to build a network security system. Wazuh as a SIEM (Security Information and Event Management) is implemented to manage logs from endpoints and send alerts to the Telegram API in real time. Wazuh detects anomalies by analyzing host logs based on built-in rules. The system is also equipped with Suricata as an IDS (Intrusion Detection System) that monitors network traffic and matches it with existing signatures to detect attacks such as Port Scanning, DDoS, Brute Force, and SQL Injection.

Testing was carried out by attacking a target server running a web application using these four types of attacks. The results of the tests show that the attacks can be detected, with the time from when the attack starts until the alert appears on the Telegram notification being between 1 second and at most 7 seconds. These results indicate that the performance of Wazuh and Suricata can detect various types of attacks in real time with relatively short delays, thus helping to enhance endpoint security.

**Keyword:** Wazuh, Suricata, Endpoint, Security, Network