ANALISIS KINERJA SIEM WAZUH DENGAN FIM, YARA, DAN VIRUSTOTAL DALAM MENDETEKSI MALWARE PADA UBUNTU SERVER

SKRIPSI

ROBBY AKBAR ABDULLAH

2107421004

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2025

ANALISIS KINERJA SIEM WAZUH DENGAN FIM, YARA, DAN VIRUSTOTAL DALAM MENDETEKSI MALWARE PADA UBUNTU SERVER

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan

untuk Memperoleh Diploma Empat Politeknik

ROBBY AKBAR ABDULLAH

2107421004

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2025

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama	: Robby Akbar Abdullah
NIM	: 2107421004
Jurusan / Program Studi	: Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi	: Analisis Kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam Mendeteksi Malware pada Ubuntu Server

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 11 Juli 2025

Yang membuat pernyataan,

(Robby Akbar Abdullah)

NIM. 2107421004

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Robby Akbar Abdullah

NIM : 2107421004

Program Studi : Teknik Multimedia dan Jaringan

Judul Skripsi : Analisis Kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam Mendeteksi Malware pada Ubuntu Server

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Senin, tanggal 23, bulan Juni, tahun 2025 dan dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I : Iik Muhamad Malik Matin, S.Kom., M.T. ( )

Penguji I : Asep Kurniawan, S.Pd., M.Kom. ( )

Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom. ( )

Penguji III : Ariawan Andi Suhandana, S,Kom., M.Ti. ( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

(Dr. Anita Hidayati, S.Kom., M.Kom.)

NIP. 197908032003122003

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah *subhanahu wa ta'ala* atas pertolonganNya dan karuniaNya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam Mendeteksi Malware pada Ubuntu Server". Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk memperoleh gelar Diploma Empat Politeknik. Penulis menyadari bahwa tanpa bantuan dan dukungan dari berbagai pihak, penulis kesulitan dalam menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Iik Muhammad Malik Matin, S.Kom., M.T. selaku dosen pembimbing yang telah banyak membantu, mendukung, dan memberikan masukan serta saran kepada penulis selama pengerjaan skripsi ini hingga selesai.
2. Bunda, ayah, dan kakak yang telah memberikan bantuan dan dukungan material maupun moral yang nilainya tak terhingga.
3. Sahabat dan teman-teman seperjuangan yang telah memberikan bantuan dan dukungan dalam pengerjaan skripsi ini.
4. Seseorang bernama "Zae" yang selalu mendoakan, memberikan semangat, dan menjadi motivasi dalam menyelesaikan skripsi ini.

Penulis meminta maaf sebesar-besarnya apabila ada kesalahan atau kekurangan dalam proses pengerjaan skripsi ini. Penulis juga mengucapkan terima kasih sebanyak-banyaknya kepada seluruh pihak dan semoga Allah membalas kebaikan kalian semua. Penulis berharap skripsi ini bermanfaat bagi pembaca dan menjadi rujukan untuk melakukan penelitian selanjutnya.

Jakarta, 4 Juni 2025

Penulis

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini:

Nama	: Robby Akbar Abdullah
NIM	: 2107421004
Jurusan / Program Studi	: Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Analisis Kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam Mendeteksi Malware pada Ubuntu Server

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 11 Juli 2025

Yang menyatakan,

(Robby Akbar Abdullah)

NIM. 2107421004

ANALISIS KINERJA SIEM WAZUH DENGAN FIM, YARA, DAN VIRUSTOTAL DALAM MENDETEKSI MALWARE PADA UBUNTU SERVER

ABSTRAK

Seiring dengan pesatnya perkembangan teknologi, maka serangan siber juga semakin kompleks dan beragam. Serangan siber tersebut terjadi dalam berbagai sektor sehingga menyebabkan banyak permasalahan keamanan siber. Oleh karena itu, dibutuhkan suatu sistem yang dapat mendeteksi, mencegah, dan merespon serangan siber melalui Security Information and Event Management (SIEM). Solusi SIEM yang tepat adalah Wazuh karena bersifat zero-cost dan open-source. Namun, perlu dilakukan analisis kinerja SIEM Wazuh tersebut dalam mendeteksi serangan siber. Berdasarkan penelitian terdahulu, analisis kinerja SIEM hanya sebatas parameter tertentu dan menguji serangan web dan network attack saja sehingga perlu dianalisis dari sisi malware agar kinerjanya lebih baik. Analisis kinerja SIEM Wazuh menggunakan FIM, YARA, dan VirusTotal untuk mengetahui mana yang paling baik kinerjanya dalam mendeteksi malware dengan menggunakan parameter-parameter tertentu. Hasil dari penelitian ini adalah FIM tidak berhasil mendeteksi semua malware, YARA berhasil mendeteksi semua malware, dan VirusTotal hanya mendeteksi dua dari tiga malware karena bergantung kepada database threat intelligence VirusTotal.

***Kata Kunci**: FIM, Malware, VirusTotal, Wazuh, YARA*

DAFTAR ISI

DAFTAR GAMBAR

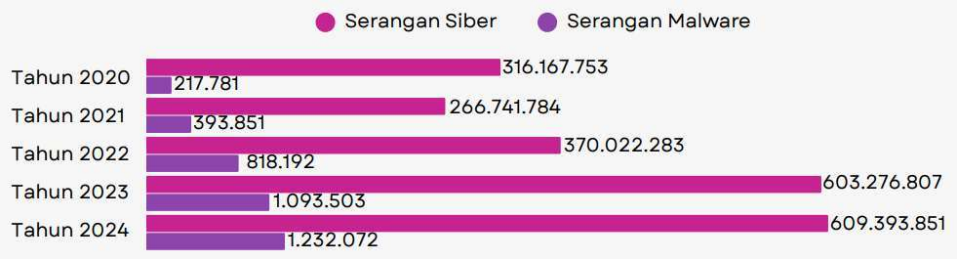
DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Era digital adalah era yang mengalami perkembangan teknologi dengan sangat pesat. Seiring dengan pesatnya perkembangan teknologi tersebut, maka serangan siber juga semakin kompleks dan beragam. Serangan siber tersebut ditujukan kepada infrastruktur teknologi dan informasi dalam berbagai sektor. Hal tersebut menyebabkan banyak sekali terjadinya permasalahan keamanan siber dikarenakan lemahnya sistem keamanan. (Husnul Khotimah, 2022)

Berdasarkan laporan tahunan *honeynet* yang diterbitkan oleh (Badan Siber dan Sandi Negara, 2024) jumlah serangan siber terutama *malware* setiap tahunnya mengalami peningkatan pada sistem *honeynet* secara keseluruhan. Data serangan *malware* yang tercatat pada sistem *honeynet* sebanyak 1.232.072 pada tahun 2024. Berikut adalah rekapitulasi serangan *malware* lima tahun terakhir pada sistem *honeynet* yang tercantum pada Gambar 1.1.



Gambar 1.1 Grafik Rekapitulasi Serangan Malware

Sumber: (Badan Siber dan Sandi Negara, 2024)

Berdasarkan permasalahan-permasalahan keamanan siber tersebut, maka dibutuhkan adanya suatu sistem yang dapat mendeteksi, mencegah, dan meresponnya. Oleh karena itu, dibutuhkan penerapan yang lebih efektif melalui *Security Information and Event Management* (SIEM). Teknologi SIEM ini dapat melakukan pengumpulan informasi keamanan yang berasal dari data *log* berbagai sumber secara *real-time*. (Husnul Khotimah, 2022)

Solusi SIEM yang tepat adalah menggunakan Wazuh karena bersifat *zero-cost* dan *open-source* sehingga mudah melakukan *custom* tanpa mengeluarkan biaya. Namun, perlu dilakukan analisis mengenai kinerja SIEM Wazuh tersebut dalam mendeteksi serangan siber. Penelitian yang dilakukan oleh (Oky Dwi Prasetyo, 2023) menganalisis kinerja SIEM Wazuh untuk menguji serangan *brute-force* dan *Denial of Service* (DoS) dengan parameter *signature-based detection* dan *anomaly-based detection*. Selain itu, terdapat penelitian yang serupa menganalisis kinerja SIEM IBM QRadar oleh (Adirosa, 2021) untuk menguji serangan *port scanning*, *password checking*, DoS, dan eksploit metasploitable 3 dengan parameter *flow source* dan *log source*. Selanjutnya, terdapat penelitian menganalisis kinerja SIEM Elastic Stack dan Splunk oleh (Alfandi, 2022) untuk menguji serangan *fingerprinting*, SQL *injection*, DoS, dan *port scanning* dengan parameter pengiriman notifikasi dan pengujian selama tiga hari.

Berdasarkan beberapa penelitian tersebut, pengujian hanya dilakukan dari serangan *web* dan *network attack* saja sehingga perlu dianalisis dari sisi *malware* agar kinerjanya lebih baik. *Malware* atau *malicious software* dapat berdampak berbahaya bagi sistem, rusaknya data, tersebarnya infeksi, dan banyak kerugian lainnya. Oleh karena itu, perlu dilakukan analisis kinerja SIEM Wazuh dalam mendeteksi *malware* pada *server* agar kinerjanya lebih baik. SIEM Wazuh secara *default* hanya terdapat *File Integrity Monitoring* (FIM) sehingga harus diinstalasi dengan YARA dan VirusTotal agar kinerjanya lebih baik. Selanjutnya, dapat dianalisis kinerja tersebut berdasarkan parameter-parameter yang telah ditentukan, yaitu jumlah *malware* yang terdeteksi, kecepatan deteksi *malware*, tingkat kesalahan, jenis *malware* yang terdeteksi, dan beban sistem yang digunakan sehingga dapat lebih cepat dan tanggap dalam menangani serangan siber terutama *malware*.

1.2 Perumusan Masalah

Berdasarkan hal-hal yang telah disampaikan di atas, maka rumusan permasalahannya:

1. Bagaimana rancang bangun SIEM Wazuh untuk mendeteksi serangan *port scanning*, *DoS*, *brute-force*, dan *malware*?
2. Bagaimana penerapan FIM, YARA, dan VirusTotal ke dalam SIEM Wazuh untuk mendeteksi *malware*?
3. Bagaimana hasil analisis kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware*?

1.3 Batasan Masalah

Penelitian ini berfokus pada:

1. SIEM yang digunakan terbatas pada Wazuh.
2. Penerapan *tools* dalam mendeteksi *malware* pada SIEM Wazuh terbatas pada FIM, YARA, dan VirusTotal.
3. *Server* yang dimonitoring terbatas pada sistem operasi Ubuntu *Server*.
4. Eksperimen yang dilakukan terbatas menggunakan *virtual machine* dalam ruang lingkup lokal dan berada pada jaringan yang sama.
5. Pengujian yang dilakukan terbatas pada serangan *port scanning*, *Denial of Service* (DoS), *brute-force*, dan *malware*.
6. Parameter-parameter yang diuji dalam mendeteksi *malware* terbatas pada jumlah *malware* yang terdeteksi, kecepatan deteksi *malware*, tingkat kesalahan, jenis *malware* yang dideteksi, dan beban sistem yang digunakan.
7. Analisis kinerja yang dilakukan pada SIEM Wazuh terbatas pada hasil pengujian serangan *port scanning*, *Denial of Service* (DoS), *brute-force*, dan *malware*.

1.4 Tujuan dan Manfaat

Penelitian ini memiliki tujuan yang akan dicapai, antara lain:

1. Merancang bangun SIEM Wazuh untuk mendeteksi serangan *port scanning*, *DoS*, *brute-force*, dan *malware*.
2. Menerapkan FIM, YARA, dan VirusTotal ke dalam SIEM Wazuh untuk mendeteksi *malware*.
3. Mengukur kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware*.

Penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak, antara lain:

1. Mahasiswa
   Penelitian ini dapat menjadi referensi dalam memahami dan mengembangkan penelitian di bidang keamanan siber.
2. Dosen
   Penelitian ini dapat menjadi bahan kajian tambahan dalam pengajaran topik-topik terkait keamanan siber.
3. Institusi
   Penelitian ini dapat menjadi bukti bahwa mahasiswa telah lulus kompetensi sesuai bidangnya.
4. Industri
   Penelitian ini dapat menjadi informasi teknis atau acuan dalam memilih metode deteksi yang sesuai untuk kebutuhan industri.
5. Masyarakat
   Penelitian ini dapat meningkatkan kesadaran akan bahayanya serangan siber dan pemahaman tentang pentingnya deteksi dini terhadap serangan siber.

1.5 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini:

A. BAB I PENDAHULUAN

Bab I berisi penjelasan mengenai jawaban apa dan mengapa penelitian ini perlu dilakukan. Bagian ini meliputi latar belakang masalah, perumusan masalah, batasan masalah, serta tujuan dan manfaat analisis kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware* pada Ubuntu *Server*.

B. BAB II TINJAUAN PUSTAKA

Bab II berisi penjelasan mengenai landasan teori atau studi literatur yang berhubungan antara karya peneliti sebelumnya dengan riset penelitian yang dilakukan saat ini.

C. BAB III METODOLOGI PENELITIAN

Bab III berisi penjelasan mengenai rancangan penelitian, tahapan penelitian, dan objek penelitian.

D. BAB IV HASIL DAN PEMBAHASAN

Bab IV berisi hasil dan pembahasan mengenai penelitian yang dilakukan meliputi analisis kebutuhan, perancangan, pengujian, dan hasil analisis pengujian.

E. BAB V PENUTUP

Bab V berisi penjelasan mengenai hasil akhir dari penelitian berupa kesimpulan dan saran secara singkat terhadap pembahasan yang telah diuraikan pada bagian isi.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat diambil kesimpulan sebagai berikut:

a. Rancang bangun SIEM Wazuh untuk mendeteksi serangan (*port scanning*, *DoS*, *brute-force*, dan *malware*) berjalan dengan baik, mulai dari instalasi Wazuh *server,* Wazuh *indexer*, Wazuh *dashboard*, Wazuh *agent,* Suricata, *web server* Apache, dan konfigurasi *firewall*.
b. Penerapan FIM, YARA, dan VirusTotal ke SIEM Wazuh berjalan dengan baik. Penerapan FIM dengan cara menambahkan direktori yang ingin dimonitor pada *file* konfigurasi OSSEC. Penerapan YARA dengan cara melakukan instalasi dan konfigurasi YARA, serta menambahkan *rules* dari YARA. Penerapan VirusTotal dengan cara menambahkan API *key* dari VirusTotal pada *file* konfigurasi OSSEC.
c. Hasil analisisnya adalah FIM tidak berhasil mendeteksi semua *malware* karena hanya mendeteksi berdasarkan integritas *file* saja, YARA berhasil mendeteksi semua *malware* karena mendeteksi berdasarkan *rules,* dan VirusTotal hanya berhasil mendeteksi dua dari tiga *malware* saja karena bergantung pada *database*. Oleh karena itu, *tools* yang paling baik dalam mendeteksi *malware* adalah YARA.

5.2 Saran

Saran yang dapat diterapkan untuk melakukan penelitian lebih lanjut sebagai berikut:

a. Melakukan analisis kinerja SIEM lain dalam mendeteksi serangan, seperti IBM QRadar, Elastic, Splunk, dan lain-lain untuk mengukur kinerja SIEM yang paling baik.

b. Menerapkan *tools* lain dalam mendeteksi *malware*, seperti MISP, Kaspersky, Hybrid Analysis, dan lain-lain. Selain itu, menerapkan *tools Endpoint Detection and Response* (EDR) untuk pemblokiran *malware*, seperti CrowdStrike, Microsoft Defender, SentinelOne, dan lain-lain.
c. Melakukan monitoring *server* dengan sistem operasi yang berbeda, seperti CentOS, Debian, Red Hat Enterprise Linux (RHEL), dan lain-lain.
d. Melakukan eksperimen menggunakan perangkat nyata dalam ruang lingkup global dan berada pada jaringan yang berbeda.
e. Menambahkan pengujian serangan-serangan lain, seperti berpacu pada MITRE ATT&CK dan OWASP Top 10.
f. Menambahkan pemblokiran *malware* dengan parameter seberapa cepat dan tepat *malware* tersebut diblokir.
g. Menambahkan analisis kinerja hasil pengujian serangan-serangan lain, seperti berpacu pada MITRE ATT&CK dan OWASP Top 10.

DAFTAR PUSTAKA

Adirosa, G., 2021. ANALISIS KINERJA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IBM QRADAR COMMUNITY EDITION DALAM MENDETEKSI ANCAMAN DAN SERANGAN SIBER PADA SERVER.

Alfandi, M., 2022. Analisa Security Information and Event Management (SIEM) Menggunakan Elastic Stack SIEM dan Splunk.

Azzah Shafiyyah, G. F. N. R. A. P., 2024. IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER. *JITET (Jurnal Informatika dan Teknik Elektro Terapan),* 12(2), pp. 1-13.

Badan Siber dan Sandi Negara, 2024. *Laporan Tahunan Layanan Honeynet BSSN,* s.l.: s.n.

Husnul Khotimah, F. B. R. S. K. I. B. K. W., 2022. Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *JBegaTI,* September, 3(2), p. 7.

Lintang, D., 2020. MONITORING AKTIVITAS USER PADA SYSTEM DENGAN MENGGUNAKAN EFK (ELASTICSEARCH, FLUENTD, KIBANA) STACK.

Muhammad Rijal Kamal, M. A. S., 2021. Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. *Automata,* 2(2), pp. 1-6.

Nur Rohman Rosyid, B. B. M. B. P. A. F. R. L. S., 2023. Deteksi Malware pada Jaringan Lokal Berbasis Honeypot dan Yara. *JURNAL SISTEMASI,* 12(1), pp. 186-193.

Nurul Qomariah, E. I. A. M. A. A., 2023. Analisis Malware Hummingbad Dan Copycat Pada Android Menggunakan Metode Hybrid. *Jurnal Cyber Security dan Forensic Digital,* 6(2), pp. 39-47.

Oky Dwi Prasetyo, P. H. T. A. B., 2023. Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* Juni, 7(6), pp. 2686-2692.

Prakoso, R. D., 2017. IMPLEMENTASI DAN PERBANDINGAN PERFORMA PROXMOX DALAM VIRTUALISASI DENGAN TIGA VIRTUAL SERVER. *JURNAL MANAJEMEN INFORMATIKA,* 8(1), pp. 1-8.

Stefan Stanković, S. G. R. P., 2022. A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis.

Thorarensen, C., 2021. A Performance Analysis of Intrusion Detection with Snort and Security Information Management. *DiVA.*

Yuriansyah Ilhamdi, Y. N. K., 2017. ANALISIS MALWARE PADA SISTEM OPERASI WINDOWS. *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia),* 2(1), pp. 1-12.

DAFTAR RIWAYAT HIDUP

Robby Akbar Abdullah

Lahir di salah satu kota Indonesia pada tahun 2003. Penulis merupakan anak kedua dari dua bersaudara. Saat ini penulis berdomisili di daerah Jakarta Selatan. Penulis menyelesaikan pendidikan Sekolah Dasar (SD) pada tahun 2015 dan pendidikan Sekolah Menengah Pertama (SMP) pada tahun 2018. Kemudian, penulis menyelesaikan pendidikan Sekolah Menengah Kejuruan (SMK) dengan jurusan Teknik Komputer dan Jaringan (TKJ) pada tahun 2021. Lalu, penulis menyelesaikan pendidikan Diploma Empat (D4) di Politeknik Negeri Jakarta dengan program studi Teknik Multimedia dan Jaringan (TMJ) pada tahun 2025.