SAIN TEKOM
ISSN 2088-1770 (Print)
ISSN 2503-3247 (Online)
Vol. 15 No. 2 (2025) 153-164

JURNAL
SAINTEKOM
Sains, Teknologi, Komputer, dan Manajemen

Implementasi Wazuh-ELK-Suricata untuk Deteksi Privilege Escalation di Ubuntu Server

*Setio Ardy Noswantoro[1], M. Ziaurrahman[2], Miftahurrizqi[3], Muhammad Achiril Haq[4] , Reza Athallah Rashid[5]
[1,2,3)]Sistem Informasi, Universitas Muhammadiyah Palangkaraya
[4)]Manajemen, Universitas Muhammadiyah Palangkaraya
[5)]Ilmu Komputer, Universitas Muhammadiyah Palangkaraya
Jl. RTA Milono, Langkai, Kec. Pahandut, Kota Palangka Raya, Kalimantan Tengah
Email: [1]setioardy@gmail.com, [2]m.ziaurrahman1994@gmail.com, [3]miftahurrizqii@gmail.com,
[4]achirilhaq@gmail.com, [5]rezaathallah123@gmail.com,

ABSTRACT

Privilege escalation is one of the most critical cyberattacks because it enables adversaries with limited rights to gain full system control. Such attacks often act as gateways to larger data breaches, as seen in the 2016 Uber incident that exposed 57 million users' personal data. This study implements and evaluates an open-source integrated intrusion detection system by combining Wazuh (HIDS), Suricata (NIDS), and the ELK Stack (Elasticsearch, Logstash, Kibana) on Ubuntu Server.Experiments were conducted through privilege escalation attack simulations using Metasploit, covering kernel exploits, misconfigurations, and software vulnerabilities. Findings reveal that the integrated system delivers broader detection compared to the default Wazuh configuration, capturing both host-level activities and network traffic. Quantitatively, a major difference was observed in response time: the integrated system detected and blocked malicious actions within 1–2 seconds, whereas the standalone system required 2–5 minutes and lacked automated blocking capabilities.Additionally, integration with the Kibana dashboard provided real-time, interactive visualization of threats, enabling administrators to trace attack patterns and respond swiftly. Overall, this research demonstrates that an integrative approach enhances detection accuracy, shortens response time, and significantly improves the quality of cybersecurity monitoring.

Keywords : cybersecurity; wazuh; suricata; ELK stack; metasploit

ABSTRAK

Privilege escalation merupakan salah satu bentuk serangan siber yang berbahaya karena memungkinkan penyerang dengan hak akses terbatas memperoleh kendali penuh atas sistem. Serangan ini berpotensi menjadi pintu masuk bagi insiden kebocoran data yang lebih luas, sebagaimana pernah terjadi pada kasus Uber tahun 2016 yang mengakibatkan terekspos nya 57 juta data pengguna. Penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi sistem deteksi intrusi terintegrasi berbasis open-source dengan menggabungkan Wazuh (HIDS), Suricata (NIDS), dan ELK Stack (Elasticsearch, Logstash, Kibana) pada Ubuntu Server. Pengujian dilakukan melalui simulasi serangan privilege escalation menggunakan Metasploit, mencakup eksploitasi kernel, kesalahan konfigurasi, dan kerentanan perangkat lunak. Hasil eksperimen menunjukkan bahwa sistem terintegrasi mampu memberikan cakupan deteksi yang lebih luas dibandingkan konfigurasi Wazuh standar, mencakup aktivitas host maupun lalu lintas jaringan. Secara kuantitatif, perbedaan signifikan terlihat pada aspek waktu respons: sistem terintegrasi dapat mendeteksi dan memblokir serangan hanya dalam 1–2 detik, sedangkan sistem standar membutuhkan waktu 2–5 menit tanpa pemblokiran otomatis. Selain itu, integrasi dengan dashboard Kibana memungkinkan visualisasi ancaman secara real-time yang interaktif dan informatif, sehingga mempermudah administrator dalam menganalisis pola serangan dan mengambil keputusan cepat. Dengan demikian, penelitian ini menegaskan keunggulan pendekatan integratif dalam meningkatkan efektivitas deteksi, kecepatan respons, dan kualitas pemantauan keamanan siber secara menyeluruh.

Kata kunci : keamanan siber; wazuh; suricata; ELK stack; metasploit

Diterima Redaksi: 23-07-2025 | Selesai Revisi: 13-09-2025 | Diterbitkan Online: 30-09-2025

1. PENDAHULUAN

Ancaman keamanan siber seperti *privilege escalation* semakin marak terjadi dan berdampak serius terhadap integritas serta kerahasiaan sistem informasi (Moneva et al., 2024; Rajyashree et al., 2024). *Privilege escalation* merupakan bentuk serangan yang memungkinkan penyerang dengan hak akses rendah memperoleh kendali penuh atas system (Happe & Cito, 2024; Mehmood et al., 2023). Serangan ini kerap menjadi pintu masuk menuju pelanggaran data yang lebih luas (Moneva et al., 2024; Rajyashree et al., 2024). Salah satu kasus nyata terjadi pada Uber tahun 2016, ketika penyerang berhasil mencuri data pribadi 57 juta pengguna dan pengemudi melalui eskalasi hak akses, yang diawali dari akses ke repositori GitHub internal (Kalekar et al., 2024).

Untuk mengidentifikasi dan menganalisis potensi kerentanan seperti ini, pengujian dengan kerangka kerja *penetration testing* seperti Metasploit menjadi metode umum yang banyak digunakan (Al-Sabaawi & Alrowidhan, n.d.; Skandylas & Asplund, 2025; Zhang et al., 2025). Metasploit memungkinkan simulasi berbagai skenario serangan nyata, termasuk eksploitasi celah keamanan, *privilege escalation*, dan *post-exploitation* dalam lingkungan sistem operasi seperti Linux (McKinnel et al., 2018; Al-Sabaawi & Alrowidhan, 2022).

Sementara itu, platform Wazuh telah dikenal luas sebagai sistem deteksi intrusi berbasis host (*Host-based Intrusion Detection System* / HIDS) yang mampu melakukan pemantauan log dan integritas file untuk mendeteksi anomali secara *real-time(Glass-Vanderlan et al., 2018; Hajamydeen et al., 2024; Sworna et al., 2023)*. Beberapa studi telah memanfaatkan Wazuh dalam konteks pemantauan server, terutama dalam mendeteksi serangan *brute force*, aktivitas tidak sah, dan manipulasi sistem file (Aditya et al., 2024; Patoni et al., 2024). Namun, pendekatan tersebut masih terbatas pada pemantauan berbasis host dan belum mencakup lalu lintas jaringan secara menyeluruh.

Permasalahan ini menunjukkan adanya celah (gap) dalam cakupan deteksi Wazuh standar, khususnya terhadap serangan yang beroperasi melalui jaringan. Oleh karena itu, pendekatan yang menggabungkan pemantauan berbasis host dan jaringan diperlukan untuk memberikan perlindungan yang lebih komprehensif.

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

Integrasi dengan Suricata, sebagai Network-based Intrusion Detection System (NIDS), serta ELK Stack (Elasticsearch, Logstash, dan Kibana) sebagai platform agregasi dan visualisasi log, diyakini dapat meningkatkan efektivitas sistem deteksi intrusi secara menyeluruh(Rosa et al., 2021).

Permasalahan ini menunjukkan adanya celah dalam cakupan deteksi Wazuh standar, khususnya terhadap serangan yang beroperasi melalui jaringan. Oleh karena itu, pendekatan yang menggabungkan pemantauan berbasis host dan jaringan diperlukan untuk memberikan perlindungan yang lebih komprehensif. Integrasi dengan Suricata sebagai *Network-based Intrusion Detection System* (NIDS), serta ELK Stack (Elasticsearch, Logstash, dan Kibana) sebagai platform agregasi dan visualisasi log, diyakini dapat meningkatkan efektivitas sistem deteksi intrusi secara menyeluruh (Rosa et al., 2021; Zhang et al., 2025).

Penelitian ini bertujuan untuk mengimplementasikan sistem keamanan terintegrasi yang menggabungkan Wazuh, Suricata, dan ELK Stack pada Ubuntu Server guna mendeteksi serangan privilege escalation yang disimulasikan menggunakan Metasploit. Dengan pendekatan eksperimental, penelitian ini diharapkan dapat menunjukkan keunggulan sistem terintegrasi dibandingkan dengan konfigurasi Wazuh standar, baik dari segi kecepatan deteksi, cakupan ancaman, maupun kemudahan visualisasi.

2. METODE

Penelitian ini menggunakan pendekatan eksperimental dengan tujuan menguji efektivitas integrasi Wazuh, ELK Stack, dan Suricata dalam mendeteksi serangan privilege escalation pada sistem operasi Ubuntu Server. Eksperimen dilakukan di lingkungan virtual yang dikontrol menggunakan VMware untuk memastikan kestabilan dan keamanan saat proses pengujian.

2.1. Infrastruktur Sistem

Infrastruktur sistem terdiri dari tiga komponen utama, yaitu Wazuh sebagai Host-based Intrusion Detection System (HIDS), Suricata sebagai Network-based Intrusion Detection System (NIDS), serta ELK Stack (Elasticsearch dan Kibana) sebagai alat pengelola dan visualisasi data log keamanan. Fungsi masing-masing komponen utama tersebut disajikan dalam Tabel ***1***

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

Tabel 1. Fungsi Komponen Wazuh, ELK Stack, dan Suricata

Nama	Fungsi
Wazuh	Memantau aktivitas pada sistem host, seperti perubahan file dan upaya akses tidak sah.
Suricata	Mendeteksi lalu lintas jaringan yang mencurigakan melalui inspeksi paket.
ELK Stack	Mengumpulkan, mengelola, dan memvisualisasikan log dari Wazuh dan Suricata.

2.2. Simulasi Serangan

Setelah sistem dibangun, dilakukan simulasi serangan menggunakan Metasploit Framework untuk menguji kemampuan sistem dalam mendeteksi serangan privilege escalation. Simulasi ini mencakup eksploitasi terhadap kerentanan kernel, misconfiguration, dan software vulnerabilities pada Ubuntu Server. Tahapan simulasi serangan tersebut dirangkum dalam Tabel 2.

Tabel 2. Tahapan Simulasi Serangan

Tahapan	Deskripsi
Penggunaan *Metasploit*	Digunakan untuk mensimulasikan serangan *privilege escalation*.
Jenis Kerentanan yang Disimulasikan	Meliputi eksploitasi kernel, kesalahan konfigurasi, dan kerentanan perangkat lunak.
Evaluasi Deteksi Ancaman	Sistem memonitor aktivitas dan lalu lintas jaringan selama serangan berlangsung.
Tujuan Simulasi	Mengukur efektivitas deteksi dan kemampuan visualisasi sistem keamanan.

2.3. Pengumpulan Data

Data dikumpulkan dari aktivitas log yang dihasilkan oleh Wazuh dan Suricata selama proses simulasi serangan berlangsung. Seluruh log dianalisis menggunakan Elasticsearch dan divisualisasikan dengan Kibana. Proses deteksi ancaman melalui komponen sistem dijelaskan secara rinci dalam Tabel 3

Tabel 3. Proses Deteksi Ancaman melalui Komponen Sistem

Proses	Deskripsi
Pemantauan oleh *Wazuh*	Mendeteksi aktivitas mencurigakan di server dan menghasilkan log sistem.
Pemantauan oleh *Suricata*	Mendeteksi lalu lintas jaringan yang mencurigakan dan menghasilkan log jaringan.
Pengumpulan Log	Log dikumpulkan oleh Wazuh Agent dan dikirim ke Wazuh Manager melalui Filebeat.
Visualisasi melalui *Kibana*	Data log dianalisis dan divisualisasikan secara real-time di dashboard Kibana.

2.4. Analisis Hasil

Analisis dilakukan terhadap data log yang dikumpulkan untuk mengevaluasi efektivitas sistem dalam mendeteksi dan memvisualisasikan serangan. Tahapan analisis hasil deteksi tersebut dirangkum dalam Tabel ***4***

Tabel 4. Tahapan Analisis Hasil Deteksi

Tahapan Analisis	Deskripsi
Evaluasi Deteksi Ancaman	Menganalisis akurasi sistem dalam mendeteksi serangan *privilege escalation*.
Visualisasi Pola Serangan	Pola serangan divisualisasikan dalam *timeline*, jenis ancaman, dan intensitasnya.

2.5. Evaluasi Sistem

Evaluasi dilakukan untuk menilai kinerja sistem keamanan secara menyeluruh, meliputi deteksi dan analisis serangan siber.

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

Pertama, evaluasi deteksi ancaman menunjukkan sistem terintegrasi (Wazuh + Suricata + ELK Stack) mampu mengenali berbagai serangan, termasuk privilege escalation, baik di level host maupun jaringan. Ini memberi cakupan deteksi lebih luas dibanding sistem standar.

Waktu respons diuji dengan membandingkan Wazuh standar dan terintegrasi. Integrasi dengan Suricata (sebagai NIDS) dan visualisasi melalui Kibana mempercepat notifikasi dan analisis, sehingga respons lebih efisien.

Dari aspek visualisasi, dashboard Kibana dinilai informatif dan interaktif, memudahkan administrator memahami pola serangan, sumber ancaman, dan mengambil keputusan cepat.

Terakhir, efektivitas keseluruhan menunjukkan integrasi berjalan optimal. Sistem mampu menganalisis data real-time dan menyajikan informasi relevan secara cepat, meningkatkan visibilitas dan respons insiden.

Dengan demikian, evaluasi membuktikan bahwa sistem terintegrasi lebih unggul dalam deteksi, respons, dan penyajian data dibanding pendekatan tunggal.

3. HASIL DAN PEMBAHASAN

3.1. Skema Pengujian

Skema pengujian melibatkan dua konfigurasi sistem, yaitu Wazuh Standar (HIDS) tanpa integrasi dan Wazuh Terintegrasi yang menggabungkan ELK Stack serta Suricata (NIDS), semuanya diimplementasikan dalam lingkungan Ubuntu Server berbasis Virtual Machine untuk mensimulasikan kondisi nyata secara terisolasi.

Simulasi serangan privilege escalation dilakukan menggunakan framework Metasploit. Jenis-jenis serangan yang diuji mencakup:

a. Software Vulnerabilities: Kerentanan aplikasi pada server target, seperti FTP Vsftpd versi 2.3.4 yang memiliki exploit publik.
b. Misconfiguration: Kesalahan konfigurasi seperti membiarkan port FTP/21 terbuka, yang dapat dimanfaatkan untuk eksplorasi kerentanan.
c. Kernel Exploit: Eksploitasi pada kernel Ubuntu Server yang memungkinkan penyerang memperoleh hak akses root dan menghapus file penting pada server target.

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

Hasil pengujian menunjukkan bahwa Wazuh Terintegrasi memberikan deteksi lebih komprehensif dengan menggabungkan analisis host dan lalu lintas jaringan, serta secara otomatis memblokir alamat IP yang terdeteksi dengan rule seperti 100200 (Nmap Script) dan 5710 (SSH login tidak dikenal) selama 60 detik. Sebaliknya, Wazuh Standar hanya mendeteksi aktivitas mencurigakan di sisi host dan log yang dihasilkan sulit dianalisis karena kurangnya visualisasi mendalam.

3.2. Hasil Evaluasi Sistem

Berdasarkan pengujian, ditemukan bahwa Wazuh Terintegrasi unggul dalam deteksi ancaman, mampu mengenali ancaman lebih beragam, termasuk lalu lintas jaringan yang tidak terjangkau Wazuh Standar yang hanya memantau aktivitas file system dan login. Integrasi dengan Suricata (NIDS) memberikan cakupan pengawasan lebih luas.

Dari sisi waktu respons, integrasi dengan Suricata dan visualisasi real-time melalui Kibana mempercepat identifikasi dan analisis ancaman, memungkinkan respons yang lebih cepat. Dashboard Kibana yang interaktif memudahkan administrator dalam memahami konteks serangan dan tren keamanan untuk pengambilan keputusan yang lebih efisien.

Penggunaan custom rule pada Suricata memungkinkan penyesuaian deteksi untuk kebutuhan spesifik, seperti pengawasan terhadap protokol atau port sensitif, menambah fleksibilitas kebijakan keamanan.

Secara keseluruhan, integrasi Wazuh, Suricata, dan ELK Stack meningkatkan deteksi, analisis, dan respons terhadap serangan secara real-time, menghasilkan sistem pertahanan yang lebih adaptif dan responsif. Perbandingan antara Wazuh Standar dan Wazuh Terintegrasi dapat dilihat pada Tabel ***5***.

Tabel 5. Perbandingan Wazuh Standar dan Wazuh Terintegrasi

Aspek Evaluasi	Wazuh Standar	Wazuh Terintegrasi
Deteksi Ancaman	Terbatas pada host	Host dan jaringan
Visualisasi Data	Tidak tersedia	Dashboard interaktif (Kibana)
Waktu Respon	Lambat	Cepat dan real-time
Akurasi Deteksi	Terbatas pada file/login	Deteksi komprehensif dengan Suricata
Fitur Tambahan	Tidak ada	Custom rule, auto-block IP, prioritas ancaman

3.3. Evaluasi Sistem Keamanan

Evaluasi sistem dilakukan untuk mengukur kinerja dan efektivitas

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

keamanan yang dibangun, mencakup empat aspek utama: deteksi ancaman, waktu respon, kualitas visualisasi, dan efektivitas sistem secara keseluruhan. Evaluasi deteksi ancaman bertujuan menilai kemampuan sistem dalam mengidentifikasi berbagai jenis serangan, baik yang mengancam jaringan maupun sistem host, memastikan cakupan deteksi yang luas dan relevan dengan ancaman terkini. Aspek waktu respon mengukur kecepatan sistem dalam merespons ancaman, yang penting untuk meminimalkan dampak serangan. Evaluasi kualitas visualisasi berfokus pada sejauh mana informasi ancaman disajikan secara jelas melalui dashboard Kibana, yang membantu administrator dalam memahami insiden dan mempercepat pengambilan keputusan. Terakhir, evaluasi efektivitas sistem menilai kinerja integrasi Wazuh, Suricata, dan ELK Stack dalam mendukung deteksi dan analisis real-time, memastikan bahwa ketiga komponen bekerja sinergis dan optimal dalam menghadapi serangan.

3.4. Keunggulan dan Tantangan Implementasi

Hasil penelitian mengonfirmasi bahwa integrasi Wazuh, Suricata, dan ELK Stack mampu membentuk sistem keamanan yang lebih komprehensif dan adaptif terhadap ancaman, khususnya privilege escalation. Namun, sistem ini juga menghadapi sejumlah tantangan teknis yang perlu diperhatikan. Keunggulan dan kekurangan dari sistem Wazuh terintegrasi disajikan dalam Tabel 6.

Tabel 6. Keunggulan dan Kekurangan Wazuh Terintegrasi

Keunggulan	Kekurangan
Deteksi ancaman yang lebih luas dan akurat	Membutuhkan konfigurasi awal yang kompleks
Visualisasi yang mendalam untuk pengambilan keputusan	Memerlukan sumber daya perangkat yang lebih besar
Dukungan custom rule untuk fleksibilitas keamanan sistem	Membutuhkan pemahaman teknis yang memadai

3.5. Implikasi Hasil Penelitian

Pendekatan hybrid yang menggabungkan Host-based Intrusion Detection System (HIDS) dan Network-based Intrusion Detection System (NIDS) telah terbukti meningkatkan cakupan dan akurasi deteksi intrusi dibandingkan penggunaan sistem tunggal. Sebuah studi di Computer Networks memperlihatkan bahwa penggabungan fitur dari host dan jaringan dengan model klasifikasi dua-tahap menghasilkan peningkatan skor F1 hingga 8,1 % pada dataset CICIDS 2018 dibandingkan metode tradisional (Chen et al., 2024). Di sisi lain, sistem hybrid yang mengolah data host dan trafik

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

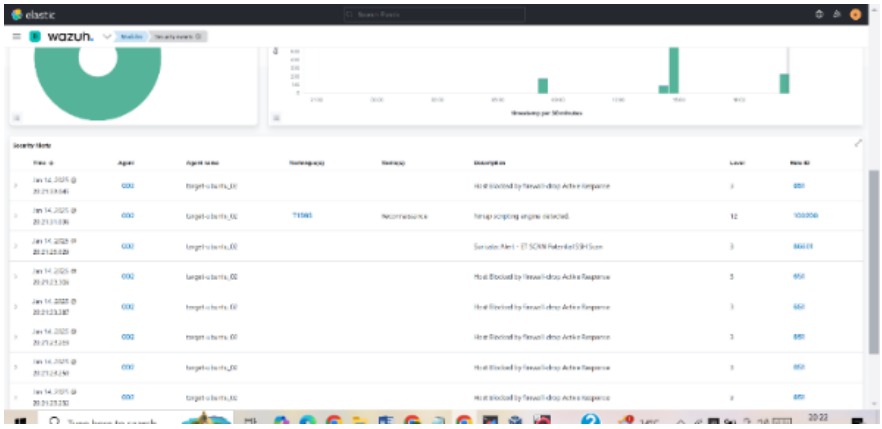
jaringan terbukti lebih efektif mengurangi false positives dan meningkatkan akurasi deteksi secara keseluruhan (Talukder et al., 2023).

3.6. Pembahasan

Hasil penelitian menunjukkan bahwa integrasi Wazuh, Suricata, dan ELK Stack secara signifikan meningkatkan kemampuan deteksi dan respons terhadap ancaman keamanan, khususnya privilege escalation pada sistem berbasis Linux. Temuan ini mendukung literatur sebelumnya yang menekankan pentingnya pendekatan deteksi berlapis (layered detection) untuk melindungi sistem dari serangan yang kompleks (Ardiyansyah et al., 2024; Mukhopadhyay et al., 2011)

Pada konfigurasi standar, Wazuh hanya memonitor file sistem, login user, dan anomali sistem. Namun, setelah diintegrasikan dengan Suricata (sebagai NIDS), sistem mampu menganalisis lalu lintas jaringan secara real-time, mendeteksi signature-based attack, serta mengaktifkan fitur seperti auto-blocking untuk IP mencurigakan. Hasil ini menunjukkan bahwa kolaborasi antara HIDS dan NIDS memberikan cakupan pengawasan yang lebih luas serta mitigasi ancaman yang lebih efektif.

Kualitas visualisasi juga menjadi aspek krusial dalam sistem keamanan. Dashboard Kibana memungkinkan administrator untuk mengidentifikasi pola serangan secara cepat melalui grafik interaktif. Tampilan visualisasi deteksi serangan melalui integrasi Wazuh dan Suricata ditunjukkan pada Gambar ***1***.

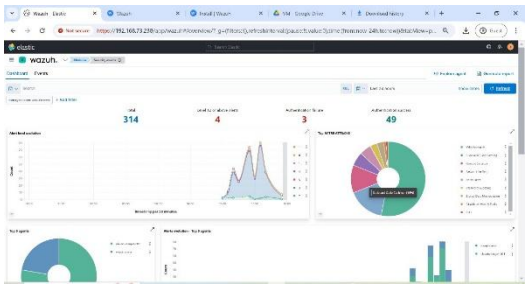


Gambar 1. Visualisasi deteksi serangan pada dashboard Wazuh–Kibana.

Contoh visualisasi pengujian yang ditampilkan berupa:

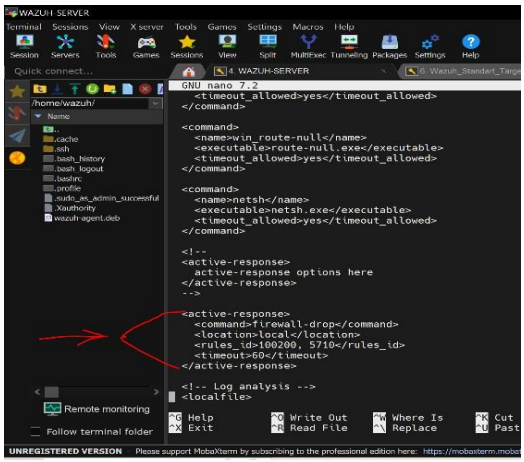
a. Gambar 2 Kibana Dashboard (menampilkan jumlah serangan dalam bentuk grafik batang/garis).

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis



Gambar 2. Jumlah serangan dalam grafik

b. Gambar 3 *Custom rule* Suricata (screenshot konfigurasi firewall-drop).



Gambar 3. *Rule* Suricata

c. Alert Wazuh ketika host diserang Nmap/Metasploit (Gambar 4 menampilkan pesan "Host Blocked by firewall").

Gambar 4. *Alert* Wazuh

Gambar 4 log terlihat timeline yang sangat rapat:

a. **20:21:30.6 → Nmap scripting engine detected** (deteksi awal).
b. **20:21:31–20:21:32 → Host langsung diblokir** oleh Suricata/Wazuh (active response "firewall-drop").

Artinya, **respon hanya memakan waktu sekitar 1–2 detik** sejak serangan terdeteksi sampai sistem melakukan aksi mitigasi (blocking).

Dalam pengujian ini ukuran **"cepat"** atau **"lambat"** diukur dari:

a. **Delay alert** (berapa lama log baru muncul setelah serangan berjalan).
b. **Respons sistem** (apakah hanya mendeteksi atau langsung memblokir).
c. **Visualisasi** (apakah admin bisa langsung melihat pola serangan atau harus membaca log manual).

Hasilnya:

a. **Wazuh standar → lambat**: respon 2–5 menit lebih lama, tidak ada pemblokiran otomatis.
b. **Wazuh terintegrasi → cepat**: respon real-time, deteksi lebih akurat, dan Suricata mampu langsung memblokir host penyerang berdasarkan custom rule

Ini konsisten dengan temuan oleh (Aditya et al., 2024) yang menyatakan bahwa visualisasi log berdampak signifikan terhadap efisiensi penanganan insiden keamanan.

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

Evaluasi waktu respons sistem juga memperlihatkan perbedaan signifikan. Konfigurasi terintegrasi merespons lebih cepat karena rule Suricata berjalan secara real-time dan langsung mengirim log ke Wazuh untuk diproses oleh sistem alerting. Ini menunjukkan bahwa efektivitas sistem keamanan tidak hanya bergantung pada jumlah log yang dikumpulkan, tetapi juga kecepatan sistem dalam melakukan korelasi dan notifikasi.

Namun demikian, implementasi sistem ini juga menghadapi tantangan, terutama dalam hal kompleksitas konfigurasi dan kebutuhan sumber daya. Proses integrasi antar komponen (Wazuh, Suricata, Filebeat, Elasticsearch, Kibana) memerlukan pemahaman teknis yang cukup serta tuning parameter yang sesuai dengan kebutuhan organisasi. Hal ini sejalan dengan tantangan yang diidentifikasi dalam studi oleh (Pfsense et al., n.d.), di mana sistem deteksi yang kompleks cenderung sulit diimplementasikan di lingkungan organisasi dengan keterbatasan teknis.

Meskipun demikian, dari perspektif biaya, solusi berbasis open-source ini tetap lebih ekonomis dibandingkan solusi komersial, dan dapat disesuaikan dengan kebutuhan organisasi secara modular.

Dengan demikian, dapat disimpulkan bahwa pendekatan integratif antara HIDS, NIDS, dan visualisasi log merupakan strategi efektif dalam membangun sistem pertahanan siber yang adaptif dan tangguh, terutama untuk lingkungan sistem terbuka seperti Ubuntu Server.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa integrasi Wazuh, Suricata, dan ELK Stack meningkatkan efektivitas deteksi dan respons terhadap serangan privilege escalation di Ubuntu Server. Sistem terintegrasi ini menggabungkan pemantauan host (HIDS) dari Wazuh, inspeksi lalu lintas jaringan (NIDS) dari Suricata, dan visualisasi data real-time melalui Kibana. Dibandingkan dengan Wazuh standar yang hanya memantau file dan login, integrasi ini memperluas deteksi ancaman, termasuk serangan berbasis jaringan. Hasil evaluasi menunjukkan peningkatan kecepatan respons, kualitas visualisasi yang lebih informatif, serta fleksibilitas dalam penerapan custom rule.

Meski begitu, penerapan sistem ini menghadapi tantangan terkait

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

konfigurasi teknis, konsumsi sumber daya, dan kebutuhan pemahaman mendalam terhadap setiap komponen. Namun, pendekatan open-source ini tetap ekonomis, adaptif, dan modular, menawarkan solusi keamanan yang tangguh bagi institusi. Dengan demikian, integrasi HIDS, NIDS, dan visualisasi log menjadi strategi efektif untuk membangun sistem pertahanan siber yang responsif dan berkelanjutan, terutama pada sistem terbuka seperti Ubuntu Server.

DAFTAR PUSTAKA

Aditya, R., Muhyidin, Y., & Singasatia, D. (2024). Implementasi Security Information And Event Management (SIEM) Untuk Monitoring Keamanan Server Menggunakan Wazuh. *Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(5). https://doi.org/10.61132/merkurius.v2i4.289

Al-Sabaawi, A., & Alrowidhan, T. A. (n.d.). *Detecting Network Security Vulnerabilities and Proactive Strategies to Mitigate Potential Threats*.

Ardiyansyah, F., Setiawan, K., & Sutisna, N. (2024). Implementasi IDS pada Jaringan Komputer Menggunakan Snort Berbasis Chatbot Telegram. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(4), 1614–1623. https://doi.org/10.57152/malcom.v4i4.1561

Chen, Z., Simsek, M., Kantarci, B., Bagheri, M., & Djukic, P. (2024). Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier. *Computer Networks*, *250*, 110576. https://doi.org/https://doi.org/10.1016/j.comnet.2024.110576

Glass-Vanderlan, T. R., Iannacone, M. D., Vincent, M. S., Qian, Chen, & Bridges, R. A. (2018). *A Survey of Intrusion Detection Systems Leveraging Host Data*. http://arxiv.org/abs/1805.06070

Hajamydeen, A. I., Hasni, M., & Abdullah, M. I. (2024). *Integrating Wazuh for Efficient Real-Time Threat Monitoring and Vulnerability Assessment in a SOC Environment* (pp. 292–320). https://doi.org/10.4018/979-8-3693-2814-9.ch013

Happe, A., & Cito, J. (2024). *Got Root? A Linux Priv-Esc Benchmark*. http://arxiv.org/abs/2405.02106

Kalekar, S. M., Sharma, U., & Mangesh Kalekar, S. (2024). Article ID: IJCET_15_04_062 Cite this Article: Ujjwal Sharma and Samruddhi Mangesh Kalekar, Dissecting the Uber Security Breach: Root Cause Analysis and Mitigation Strategies. *International Journal of Computer Engineering and Technology (IJCET)*, *15*(4), 715–720. https://doi.org/10.5281/zenodo.13368425

Mehmood, M., Amin, R., Muslam, M., Xie, J., & Aldabbas, H. (2023). Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning. *IEEE Access*, *PP*, 1. https://doi.org/10.1109/ACCESS.2023.3273895

Moneva, A., Ruiter, S., & Meinsma, D. (2024). Criminal expertise and hacking efficiency. *Computers in Human Behavior*, *155*.

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis

https://doi.org/10.1016/j.chb.2024.108180

Mukhopadhyay, I., Chakraborty, M., & Chakrabarti, S. (2011). A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems. *Journal of Information Security*, *02*(01), 28–38. https://doi.org/10.4236/jis.2011.21003

Pfsense, P., Sebagai, D. S., Pendeteksi, A., Pencegahan, D., Keamanan, S., Pada, J., Server, W., Sufardy, D. B., & Widiasari, I. R. (n.d.). *THE USE OF PFSENSE AND SURICATA AS A NETWORK SECURITY ATTACK DETECTION AND PREVENTION TOOL ON WEB SERVERS*. *9*(2), 2024.

Rajyashree, R., Mathi, S., Saravanan, G., & Sakthivel, M. (2024). An Empirical Investigation of Docker Sockets for Privilege Escalation and Defensive Strategies. *Procedia Computer Science*, *233*, 660–669. https://doi.org/10.1016/j.procs.2024.03.255

Rosa, L., Cruz, T., Freitas, M. B. de, Quitério, P., Henriques, J., Caldeira, F., Monteiro, E., & Simões, P. (2021). Intrusion and anomaly detection for the next-generation of industrial automation and control systems. *Future Generation Computer Systems*, *119*, 50–67. https://doi.org/10.1016/j.future.2021.01.033

Skandylas, C., & Asplund, M. (2025). Automated penetration testing: Formalization and realization. *Computers and Security*, *155*. https://doi.org/10.1016/j.cose.2025.104454

Sworna, Z. T., Mousavi, Z., & Babar, M. A. (2023). NLP methods in host-based intrusion detection systems: A systematic review and future directions. *Journal of Network and Computer Applications*, *220*, 103761. https://doi.org/https://doi.org/10.1016/j.jnca.2023.103761

Talukder, Md. A., Hasan, K. F., Islam, Md. M., Uddin, Md. A., Akhter, A., Yousuf, M. A., Alharbi, F., & Moni, M. A. (2023). A dependable hybrid machine learning model for network intrusion detection. *Journal of Information Security and Applications*, *72*, 103405. https://doi.org/https://doi.org/10.1016/j.jisa.2022.103405

Zhang, W., Xing, J., & Li, X. (2025). *Penetration Testing for System Security: Methods and Practical Approaches*. http://arxiv.org/abs/2505.19174

DOI: https://doi.org/10.33020/saintekom.v15i2.941
Lisensi: CC BY-SA 4.0 | Copyright © 2025, Penulis