Implementasi *Wazuh* untuk Deteksi *Brute Force* pada *Web Server* dengan Metodologi NIST

Mochamad Yudiansyah[1], Boy Yuliadi[2]
[1,2] Program Studi Teknik Informatika, Universitas Dian Nusantara
Jalan Tanjung Duren Barat II No. 1, Grogol, Jakarta Barat, Indonesia
e-mail: [1]411221035@mahasiswa.undira.ac.id, *[2]boy.yuliadi@undira.ac.id

Abstrak

Perkembangan teknologi informasi telah mendorong organisasi untuk memanfaatkan layanan digital berbasis web, namun juga meningkatkan risiko ancaman keamanan siber, termasuk juga serangan brute force. Pada penelitian ini bertujuan untuk mengimplementasikan Wazuh sebagai platform Security Information and Event Management (SIEM) dan Extended Detection and Response (XDR) untuk mendeteksi serangan brute force pada web server Apache berbasis Linux Debian. Dalam metode penelitian ini, mengacu pada NIST Special Publication 800-115, yang meliputi tahap perencanaan, penemuan, penyerangan, dan pelaporan. Simulasi serangan juga dilakukan menggunakan tools software seperti THC-Hydra v9.6 dipadukan dengan wordlist rockyou.txt yang berisi 14.344.399 kata sandi melalui 16 thread selama delapan jam pengujian. Hasil implementasi telah menunjukkan bahwa Wazuh mampu mencatat dan menampilkan 4.287.844 serangan secara real-time, dengan 1.071.483 di antaranya merupakan peringatan Level 12 yang telah mengonfirmasi aktivitas serangan dari brute force, serta berhasil mencatat alamat IP dari sumber serangan dengan akurasi 100%. Temuan ini menunjukkan bahwa Wazuh sangat efektif dalam mencatat serangan, mencatat IP dari sumber serangan, dan menampilkan grafik ancaman keamanan dalam bentuk visualisasi dibandingkan pemantauan yang hanya mengandalkan Apache access log mentah yang tidak memberikan grafik visualisasi.

Kata kunci *— Wazuh; brute force; SIEM; web server; NIST SP 800-115*

Abstract

The rapid advancement of information technology has encouraged organizations to adopt web-based digital services, while simultaneously increasing the risk of cybersecurity threats, including brute force attacks. This study aims to implement Wazuh as a Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) platform to detect brute force attacks targeting an Apache web server running on Debian Linux. The research methodology follows the NIST Special Publication 800-115 framework, which consists of the planning, discovery, attack, and reporting phases. The attack simulation was conducted using THC-Hydra v9.6 in combination with the rockyou.txt wordlist containing 14,344,399 password entries, executed through 16 parallel threads over an eight-hour testing period. The implementation results demonstrate that Wazuh successfully recorded and visualized 4,287,844 security events in real time, including 1,071,483 Level 12 alerts that confirmed brute force attack activities. In addition, Wazuh accurately identified the source IP addresses of the attacks with 100% accuracy. These findings indicate that Wazuh is highly effective in recording attack events, identifying the originating IP addresses, and presenting security threats through intuitive visualizations, outperforming conventional monitoring that relies solely on raw Apache access logs without graphical visualization.

Keywords *— Wazuh; brute force; SIEM; web server; NIST SP 800-115*

Submitted: 29 Juni 2026
Published: 30 September 2026

1. PENDAHULUAN

Perkembangan teknologi dan informasi telah banyak mendorong perubahan pada peradaban manusia dalam mengelola informasi pada di berbagai organisasi dan institusi. Dari aktivitas yang sebelumnya dilakukan secara manual, seperti penyampaian informasi, pertukaran data, dan pengelolaan administrasi, kini telah beralih ke *platform* digital yang telah terhubung melalui jaringan internet [1]. Meskipun memberikan kemudahan dalam berakses dan mengelola layanan, kondisi tersebut juga meningkatkan resiko terhadap berbagai ancaman keamanan siber. Pelaku serangan dapat memanfaatkan celah kerentanan pada sebuah website maupun server untuk memperoleh akses yang tidak sah, mengganggu pelayanan digital, atau mencuri informasi seperti data yang bersifat sensitif [2]. Tingginya tingkat ancaman siber di Indonesia tercermin dari kasus insiden keamanan yang menargetkan infrastruktur digital nasional. Salah satu kasus yang menonjol adalah serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS) pada tahun 2024 yang mengakibatkan gangguan terhadap berbagai layanan publik dan instansi pemerintah, sekaligus menunjukkan pentingnya alat keamanan siber [3], [4]. Kondisi tersebut menegaskan bahwa menerapkan alat deteksi dini untuk meningkatkan keamanan sangatlah penting untuk ancaman siber.

Dari banyaknya berbagai serangan yang pernah terjadi pada web server, ada satu serangan yang tak luput dari perhatian. Salah satunya adalah serangan *brute force,* yaitu teknik serangan yang dilakukan melalui percobaan kombinasi *username* dan *password* secara berulang hingga *username* dan *password* yang valid berhasil ditemukan oleh pelaku serangan [5]. Serangan ini sulit dikenali secara langsung oleh *administrator web server* karena aktivitasnya hanya tercatat dalam *log* sistem, seperti kegagalan *autentikasi* yang berulang dan pola akses mencurigakan yang berasal dari alamat IP tertentu [6]. Oleh karena itu, diperlukan suatu *platform* pemantauan keamanan yang mampu mengumpulkan data, menganalisis sumber serangan, dan mencatat data *log* secara terstruktur. Oleh karena itu ada satu alat perangkat lunak sebagai solusi yang dapat digunakan sebagai *administrator,* yaitu alat perangkat lunak *Wazuh.* Wazuh adalah perangkat lunak *open source* yang mempunyai kemampuan *Security Information and Event Management* (SIEM), *Extended Detection and Response* (XDR), serta *endpoint security* untuk mendukung proses deteksi dini dan pemantauan ancaman keamanan secara *real-time* [7], [12].

Ada beberapa penelitian terdahulu yang telah menggunakan *Wazuh* sebagai alat deteksi serangan *brute force* pada berbagai lingkungan. Salah satunya dilakukan oleh Park et al. [8] yang berfokus pada deteksi serangan *SSH* menggunakan data *log router,* sedangkan Agghey et al. [9] menerapkan pendekatan *machine learning* untuk mendeteksi aktivitas *brute force* pada layanan *SSH* dalam lingkungan yang terkontrol. Sementara itu, Aji et al. [5] menganalisis serangan *brute force* pada *web server Nginx,* Shafiyyah [10] melakukan penelitian pada *active response* dalam *Wazuh*, dan Farrel et al. [13] mengimplementasikan *Wazuh* SIEM dengan fitur *active response* serta notifikasi *Telegram* untuk melakukan forensik dari serangan b*rute force* dengan tingkat deteksi mencapai 100%. Meskipun demikian, masih terdapat keterbatasan penelitian yang secara khusus membahas implementasi pada *rule-based detection* pada *Wazuh* untuk mendeteksi serangan *brute force* berbasis *HTTP* terhadap *web server Apache* yang berjalan pada sistem operasi *Linux Debian*, terutama dapat dianalisis secara visual saat serangan secara terjadi.

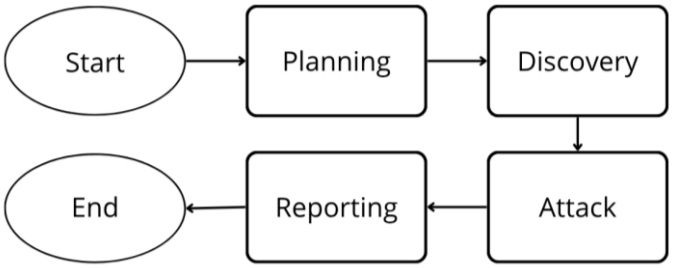
Berdasarkan dari penelitian sebelumnya, penelitian ini bertujuan untuk mengimplementasikan *Wazuh* sebagai *platform Security Information and Event Management* (SIEM) dan *Extended Detection and Response* (XDR) untuk mendeteksi serangan *brute force* pada *web server Apache* berbasis *Linux Debian.* Selain itu, penelitian ini melakukan efektivitas pada *rule-based detection* yang akan diterapkan dalam proses identifikasi aktivitas pada sebuah serangan. Untuk mencapai tujuan tersebut, penelitian akan menggunakan metodologi NIST *Special Publication* 800-115 yang menyediakan tahapan pengujian keamanan secara terstruktur, dengan meliputi fase perencanaan, penemuan, penyerangan, dan pelaporan [11]. Hasil dari

Submitted: 29 Juni 2026
Published: 30 September 2026

penelitian ini diharapkan dapat menjadi referensi bagi *administrator* agar bisa mengimplementasikan solusi pemantauan keamanan berbasis *open source* guna meningkatkan kemampuan deteksi ancaman pada infrastruktur *server*.

2. METODE PENELITIAN

Pada penelitian ini, metode yang digunakan adalah *National Institute of Standards and Technology* (NIST) *Special Publication* 800-115 sebagai kerangka kerja pengujian keamanan yang terdiri atas empat tahapan, yaitu perencanaan *(planning),* penemuan *(discovery)*, penyerangan *(attack),* dan pelaporan *(reporting)* [11]. Lingkungan pengujian juga dirancang menggunakan tiga perangkat komputer fisik yang masing-masing perangkat komputer menjalankan mesin virtual berbasis *VirtualBox* dalam jaringan lokal. Penelitian ini juga menerapkan pendekatan eksperimental dengan membangun lingkungan pengujian yang terkontrol *(controlled testbed)* untuk mensimulasikan kondisi serangan *brute force* secara nyata. Pendekatan tersebut juga memungkinkan proses pengujian yang dilakukan secara terstruktur dengan variabel yang dapat dikendalikan, dari meliputi konfigurasi jaringan, perangkat lunak yang digunakan, serta parameter serangan yang telah ditetapkan secara terstruktur. Seluruh komponen pengujian ini juga dikonfigurasikan dalam satu segmen jaringan lokal yang terisolasi, sehingga lalu lintas yang dihasilkan selama proses serangan dapat direkam secara optimal tanpa dipengaruhi oleh faktor eksternal yang tidak relevan.



Gambar 1. Flowchart Alur Penelitian 800-115

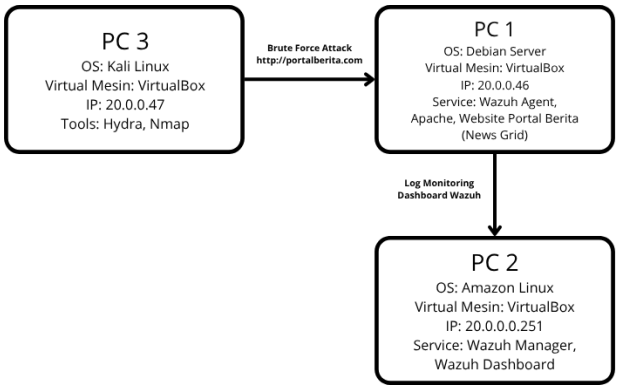
Berdasarkan pada Gambar nomor 1, penelitian ini menerapkan empat tahapan yang disusun secara berurutan sesuai dengan metodologi NIST. Tahap perencanaan meliputi penyusunan topologi jaringan dan dikonfigurasi diawal sistem. Tahap penemuan mencakup kegiatan *reconnaissance* serta identifikasi *endpoint pada* target. Tahap penyerangan akan dilakukan melalui simulasi *brute force* dengan menggunakan *Hydra*. Adapun tahap pelaporan yang meliputi proses pengumpulan data dan analisis terhadap peringatan yang dihasilkan oleh *Wazuh*. Seluruh tahapan dilaksanakan secara terstruktur dan berurutan untuk menjaga konsistensi dari hasil pengujian.

2.1 Planning

Pada tahap perencanaan, akan dilakukan perancangan topologi jaringan serta persiapan seluruh komponen yang akan digunakan pada lingkungan pengujian. Komputer pertama dengan alamat IP 20.0.0.46 dikonfigurasi sebagai *server* target yang menggunakan sistem operasi *Linux Debian Trixie* dan menjalankan layanan *web Apache2* untuk menghosting aplikasi portal berita *NewsGrid* pada *domain portalberita.com.* Server tersebut juga akan dipasang *Wazuh Agent* versi 4.14.5 yang berfungsi mengumpulkan data *log,* mencatat data yang masuk dan mengirimkannya ke *Wazuh Manager* untuk dianalisis lebih lanjut. Komputer kedua dengan alamat IP 20.0.0.251 akan berperan sebagai pusat pemantauan keamanan dengan menjalankan *Wazuh Manager* yang akan dideploy menggunakan *file Open Virtual Appliance* (OVA). Sementara itu, komputer ketiga dengan alamat IP 20.0.0.47 akan digunakan sebagai mesin penyerang yang menjalankan sistem

Submitted: 29 Juni 2026
Published: 30 September 2026

operasi *Kali Linux* yang dilengkapi perangkat lunak seperti *THC-Hydra* versi 9.6 untuk melakukan simulasi serangan pada *brute force.*



Gambar 2. Topologi Jaringan *Virtualbox* Pengujian

Pada gambar 2 ,menunjukkan adanya konfigurasi tiga mesin *virtual* yang saling terhubung dalam satu segmen jaringan lokal yang menggunakan alamat IP statis. *Server* target dan *Wazuh Manager* akan dikonfigurasikan untuk mendukung proses pengiriman data *log* dari *Wazuh Agen*t ke *Wazuh Manager*, sedangkan mesin *Kali Linux* itu sendir akan ditempatkan pada segmen jaringan yang sama sebagai mesin penyerang untuk melakukan simulasi serangan dari lingkungan internal. Konfigurasi tersebut juga dirancang agar seluruh lalu lintas jaringan yang dihasilkan selama proses serangan dapat direkam dan dianalisis secara optimal oleh *Wazuh* tanpa dipengaruhi oleh pembatasan yang berasal dari aturan *firewall* yang tidak relevan.

Tabel 1. Spesifikasi Komponen Pengujian

Perangkat Keras / Lunak	**Peran**	**Sistem Operasi**
PC 1, VirtualBox v7.2.8, Intel i7 Gen 10700, RAM 32GB, Storage 2TB	*Server Target, Wazuh Agent, Apache2, NewsGrid, Wazuh Agent* v.4.14.5, IP 20.0.0.46	*Linux Debian Trixie*
PC 2, VirtualBox v7.2.8, Intel i7 Gen 10700, RAM 32GB, Storage 2TB	Pusat Monitoring, *Wazuh Manager*, IP 20.0.0.251	*Amazon Linux*
PC 3, VirtualBox v7.2.8, Intel i7 Gen 10700, RAM 32GB, Storage 2TB	Mesin Penyerang, *THC-Hydra v9.6*	*Kali Linux*

Berdasarkan Tabel 1, lingkungan pengujian terdiri atas tiga komponen utama yang masing-masing menggunakan komputer dengan spesifikasi prosesor I*ntel Core i7-10700,* RAM 32 GB, dan media penyimpanan berkapasitas 2 TB. Komputer pertama akan berfungsi sebagai *server* target yang akan menjalankan layanan *web Apache* serta *Wazuh Agent.* Komputer kedua akan berperan sebagai pusat pemantauan keamanan dengan menjalankan *Wazuh Manager* untuk mengelola dan menganalisis pada *log* keamanan. Sementara itu, komputer ketiga akan berfungsi sebagai mesin penyerang yang menjalankan sistem operasi *Kali Linux* dan dilengkapi dengan perangkat lunak *THC-Hydra* untuk melakukan simulasi serangan *brute force.* Penggunaan sistem operasi yang berbeda pada setiap komponen merepresentasikan lingkungan pengujian yang terstruktur, namun pada seluruh komponen akan tetap terhubung melalui konfigurasi jaringan yang sama dengan satu segmen.

Submitted: 29 Juni 2026
Published: 30 September 2026

2. 2 Discovery

Pada tahap penemuan ini, dilakukan kegiatan *reconnaissance* terhadap infrastruktur *server* target dengan menggunakan alat perangkat lunak yaitu *Nmap. Nmap* akan digunakan untuk mengidentifikasi *attack surface* yang tersedia. Pemindaian jaringan juga akan dilakukan dari mesin penyerang dengan memiliki alamat IP 20.0.0.47 yang akan menuju *server* target dengan alamat IP 20.0.0.46 guna mengidentifikasi *port* yang terbuka serta layanan yang aktif pada *web server*.

Hasil dari pemindaian akan menunjukkan bahwa *server* target telah menjalankan layanan *HTTP* pada *port* 80. Selanjutnya, akan dilakukan identifikasi terhadap *endpoint autentikasi* pada website *NewsGrid* yang berjalan pada domain *portalberita.com. Endpoint* yang telah berhasil diidentifikasi adalah */login.php,* yang menggunakan metode *HTTP POST* untuk pengiriman kredensial. Selain itu, parameter pada formulir *autentikasi juga* turut dianalisis sebagai dasar penyusunan konfigurasi serangan pada tahap fase ini.

2.3 Attack

Simulasi serangan yang menggunakan *brute force* akan dilakukan dengan alat perangkat lunak bernama *THC-Hydra* versi 9.6, alat perangkat lunak tersebut akan dijalankan dari mesin *Kali Linux* yang memiliki alamat IP 20.0.0.47 dan akan ditujukan ke *endpoint /login.php* pada *server* target yang beralamat IP 20.0.0.46. Dan konfigurasi serangan ini menggunakan nama pengguna tetap *"admin"* serta *wordlist rockyou.txt* yang berisi 14.244.399 entri dari kata sandi. Untuk meningkatkan jumlah dari percobaan *autentikasi* dalam periode tertentu, alat perangkat lunak seperti *Hydra akan* dijalankan dengan 16 thread paralel. Proses serangan akan berlangsung secara berkelanjutan selama delapan jam guna menghasilkan *volume untuk* data *log* yang memadai untuk keperluan analisis lebih lanjut. Selama pengujian berlangsung, alat seperti *Hydra* akan mencatat sebanyak 4.287.844 percobaan *login* untuk *autentikasi* gagal tanpa satu pun percobaan yang berhasil masuk ke akses dalam sistem. Pengujian juga dilakukan dalam dua tahap skenario, pada tahap pertama yaitu tanpa aktivasi *Wazuh* untuk memperoleh data dasar *(baseline)* dari *Apache access log* mentah. Setelah itu pada tahap kedua dengan menggunakan pemantauan seperti *Wazuh* untuk mengukur seberapa mampu alat *monitoring* tersebut mencatat pada deteksi *log* keamanan secara *real-time.*



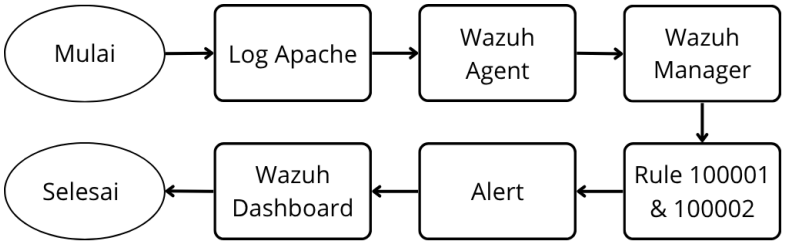
Gambar 4. Flowchart Simulasi Serangan THC-HYDRA

Berdasarkan pada gambar 4 diatas, tahap proses simulasi serangan akan diawali dengan persiapan *wordlist rockyou.txt* yang didalam filenya berisi lebih dari 14 juta entri kata sandi. Selanjutnya akan dilakukan konfigurasi target yang dapat meliputi penentuan dari alamat IP server (20.0.0.46), *endpoint /login.php*, serta metode *autentikasi HTTP POST.* Setelah konfigurasi selesai, *tools THC-Hydra* akan dijalankan menggunakan 16 *thread* paralel untuk menghasilkan jumlah percobaan *autentikasi* yang tinggi dalam waktu yang relatif singkat, yaitu 8 jam. Seluruh aktivitas yang akan dihasilkan selama proses tersebut, akan direkam ke dalam *Apache access log* sebagai sumber data yang akan digunakan pada tahap analisis berikutnya.

Submitted: 29 Juni 2026
Published: 30 September 2026

2.4 Reporting

Pada tahap *reporting*, seluruh data *log* dan peringatan keamanan yang telah dihasilkan selama proses pengujian, akan dikumpulkan melalui *dashboard Wazuh Manager.* Selanjutnya, dilakukanlah analisis mendalam terhadap *alert* yang terdeteksi, meliputi dari jumlah total peristiwa kejadian keamanan yang telah terekam oleh *wazuh*, lalu distribusi peringatan berdasarkan tingkat level *(alert level)*, dan serta rincian kejadian yang akan mencakup alamat IP dari sumber serangan dan informasi dalam waktu pelaksanaan *(timestamp).*



Gambar 5. Flowchart Mekanisme Deteksi Wazuh

Pada gambar 5 tersebut, akan menunjukkan alur deteksi *Wazuh* yang akan menggambarkan tahapan pemrosesan data dari sumber sampai dengan hasil. *Apache access log* yang akan dihasilkan oleh *server web,* terlebih dahulu dikumpulkan oleh *Wazuh Agent* yang telah terinstal pada *server* target. Dari data *log* tersebut, kemudian diteruskanlah ke *Wazuh Manager* untuk dianalisis lebih lanjut berdasarkan dari *Rule 100001* dan *Rule 100002.* Apabila ada teridentifikasi pola kegagalan *login* yang sesuai dengan *rule* yang telah dikonfigurasikan, sistem akan menghasilkan peringatan *(alert)* yang selanjutnya akan ditampilkan pada *dashboard Wazuh* dalam bentuk visualisasi atau grafik. Dari informasi tersebut juga dapat diakses oleh *administrator* sistem sebagai dasar untuk melakukan tindakan lanjut terhadap insiden keamanan yang telah terdeteksi.

3. HASIL DAN PEMBAHASAN

3.1 Kondisi Sebelum Implementasi Wazuh

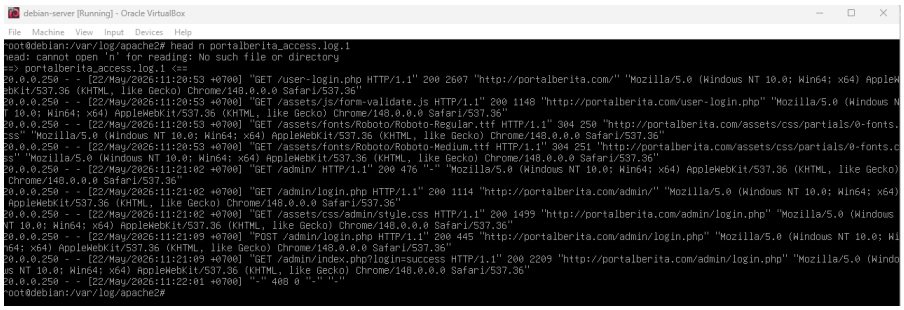
Pada tahap ini akan menjelaskan kondisi *web server* sebelum diimplementasi *software monitoring* seperti *Wazuh*, yang dibagi ke dalam dua tahap pengamatan. Tahap pertama akan menggambarkan kondisi normal pada *server* sebelum simulasi serangan *hydra* dilakukan, ketika seluruh aktivitas *web server* hanya akan dicatat melalui *Apache access log* sebagai satu-satunya alat pemantauan. Pada tahap kedua akan menggambarkan kondisi *Apache access log* setelah simulasi serangan *brute force* yang dilakukan untuk menunjukkan keterbatasan alat pada pencatatan tersebut dalam mendeteksi dan mengklasifikasikan aktivitas ancaman secara otomatis. Dari perbandingan kedua tersebut, pada tahap pengamatan ini akan menjadi dasar evaluasi terhadap pentingnya penerapan *platform Security Information and Event Management* (SIEM) seperti *Wazuh*, dalam mendukung proses deteksi ancaman yang lebih terstruktur.

3.1.1 Kondisi Log Apache Sebelum Brute Force

Sebelum pelaksanaan simulasi serangan dilakukan, *server web* target yang memiliki alamat IP 20.0.0.46 hanya bisa menggunakan *Apache access log* sebagai alat utama untuk pencatatan aktivitas pada *web server*. Dalam keadaan kondisi normal, *log* tersebut akan merekam berbagai aktivitas pengguna yang sah secara data mentah, seperti akses ke halaman portal berita, navigasi pada menu administrasi, serta satu *autentikasi* yang berhasil pada pukul 11.21 WIB dari alamat IP 20.0.0.250. Pada a*pache access log* akan disajikan dalam format teks yang memuat informasi seperti waktu akses, metode *HTTP, URL* yang diakses, kode *respons HTTP*, dan *user agent.* Meskipun mampu menyimpan informasi aktivitas secara rinci, mekanisme ini tidak dapat

Submitted: 29 Juni 2026
Published: 30 September 2026

menyediakan fitur peringatan otomatis maupun klasifikasi suatu kejadian serangan berdasarkan tingkat level *alert* ancaman.

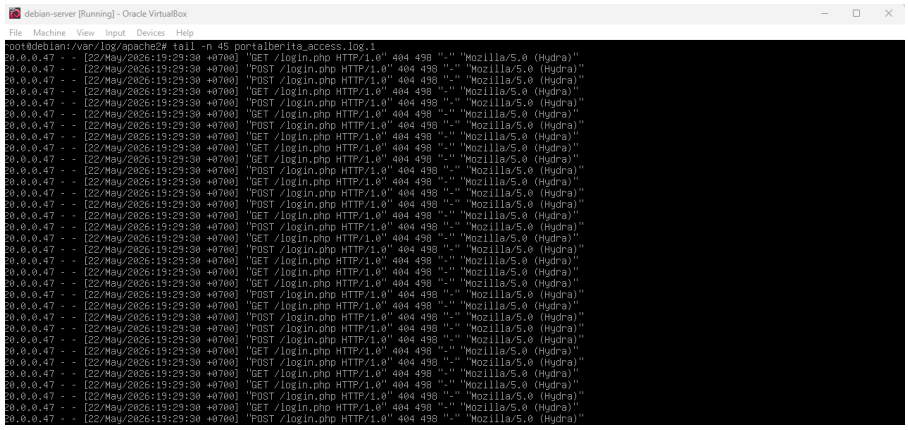


Gambar 6. Capture Apache Access Log Dalam Kondisi Normal Sebelum Serangan

Berdasarkan pada gambar 6, pada kondisi normal sebelum pelaksanaan serangan, *Apache access log* hanya merekam aktivitas rutin, seperti akses ke halaman portal berita, permintaan terhadap berkas statis, serta satu kali *autentikasi* berhasil yang dilakukan oleh *administrator* dari alamat IP 20.0.0.250. Pada tahap ini juga tidak ditemukan pola permintaan berulang yang mengindikasikan aktivitas mencurigakan maupun kegagalan *login* berulang yang berasal dari alamat IP yang sama, sehingga tidak terdapat peringatan keamanan yang dihasilkan. Kondisi tersebut menunjukkan bahwa *log* hanya dapat berfungsi sebagai media pencatatan aktivitas tanpa disertai mekanisme analisis keamanan secara aktif.

3.1.2 Kondisi Log Apache Setelah Brute Force

Setelah simulasi serangan *brute force* dijalankan menggunakan *tools THC-Hydra* dari mesin penyerang yang memiliki alamat IP 20.0.0.47, *Apache access log* mulai mencatat sejumlah besar data entri yang berulang berupa permintaan *GET* dan *POST* menuju *endpoint /login.php* dengan *user agent "Mozilla/5.0 (Hydra)"* yang menunjukkan adanya aktivitas otomatis dalam skala besar. Seluruh percobaan tersebut akan menghasilkan kode respons *HTTP 404* karena *endpoint /login.php* tidak ditemukan pada jalur *(path)* yang menjadi target serangan *Hydra.*



Gambar 7. Capture Apache Access log Selama Serangan Brute Force

Digambar 7 terlihat bahwa *Apache access log* telah mencatat ribuan data entri yang berulang dan berasal dari alamat IP 20.0.0.47 dengan *user agent "Mozilla/5.0 (Hydra)"* yang menargetkan *endpoint /login.php.* Meskipun aktivitas tersebut telah menunjukkan adanya indikasi yang kuat terhadap adanya serangan, seluruh informasi masih disajikan dalam bentuk teks mentah tanpa tanpilan dalam bentuk visualisasi, kategori, maupun peringatan otomatis. Untuk mengidentifikasi pola serangan tersebut, *administrator* perlu melakukan pemeriksaan dan

Submitted: 29 Juni 2026
Published: 30 September 2026

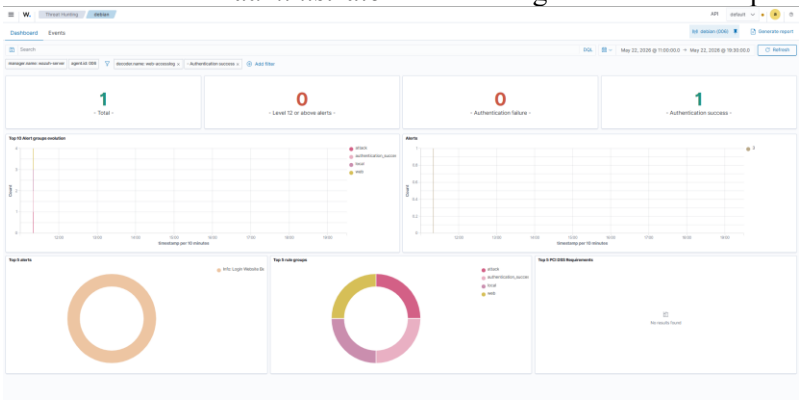
pencarian secara manual pada *file log*, yang akan menjadi kurang efisien serta berpotensi menyebabkan aktivitas yang mencurigakan tidak terdeteksi ketika data dari *volume log* yang dihasilkan sangatlah besar. Pada kondisi ini menunjukkan pentingnya penggunaan *platform SIEM* seperti *Wazuh* untuk mendukung proses deteksi dan analisis ancaman keamanan secara lebih efektif dan efisien.

3.2 Kondisi Setelah Implementasi Wazuh

Bagian ini menjelaskan hasil dari pemantauan *web server* setelah *Wazuh* berhasil diimplementasikan dan dikonfigurasi dengan *custom rule* yang telah ditetapkan. Pengamatan juga dilakukan dalam dua kondisi, yaitu kondisi normal pada *dashboard Wazuh* sebelum simulasi serangan dijalankan sebagai *baseline*, serta kondisi pada *dashboard Wazuh* selama simulasi serangan *brute force* berlangsung. Melalui perbandingan dari kedua kondisi tersebut, dapat dievaluasi sejauh mana efektivitas mekanisme pada *rule-based detection* yang diterapkan dalam mendeteksi, mengklasifikasikan, dan memvisualisasikan aktivitas serangan secara *real-time* dibandingkan dengan kondisi tanpa implementasi *Wazuh*.

3.2.1 Kondisi Normal Dashboard Wazuh Sebelum Brute Force

Perbandingan antara kondisi sebelum dan setelah pelaksanaan serangan, menunjukkan perbedaan yang sangat signifikan terhadap kemampuan deteksi yang dimiliki oleh *Wazuh*. Sebelum simulasi serangan dilakukan, pada *dashboard Wazuh* telah mencatat total 1 kejadian dengan 0 peringatan level 12, 0 *authentication failure,* dan 1 *authentication success,* yang menggambarkan aktivitas normal *administrator* dalam mengakses ke website portal berita.



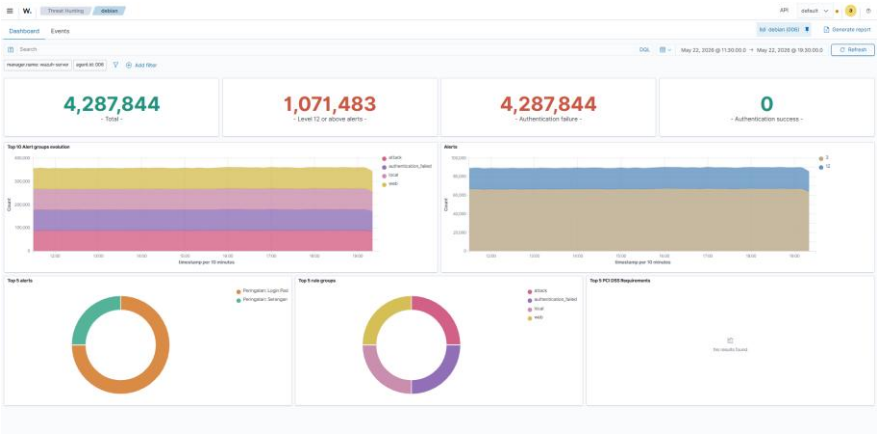
Gambar 8. Capture Dashboard Wazuh Sebelum Serangan

Pada Gambar 8 juga dijelaskan bahwa *dashboard Wazuh* telah menampilkan kondisi normal dengan jumlah total sebanyak 1 dan tanpa adanya indikasi serangan yang terdeteksi. Grafik yang menandakan per 10 menit menunjukkan tingkat aktivitas yang sangat rendah, sementara metrik *authentication failure* berada pada nilai 0. Kondisi tersebut digunakan sebagai *baseline* yang merepresentasikan aktivitas operasional *server* dalam keadaan normal tanpa ancaman keamanan. Pada situasi ini, *administrator* dapat melakukan pemantauan sistem dengan mudah untuk memastikan bahwa layanan berjalan dengan aman.

3.2.2 Kondisi Dashboard Wazuh Setelah Brute Force

Setelah simulasi serangan *brute force* dijalankan selama delapan jam pada rentang waktu 11.30 hingga 19.30 WIB, *dashboard Wazuh* akan menampilkan peningkatan jumlah yang terdeteksi secara *real-time.* Dari grafik pemantauan tersebut telah menunjukkan *volume* yang relatif konsisten, yaitu berkisar antara 80.000 hingga 100.000 pada setiap interval 10 menit selama periode pengujian berlangsung.

Submitted: 29 Juni 2026
Published: 30 September 2026



Gambar 9. Capture Dashboard Wazuh Selama Serangan

Berdasarkan Gambar 9, seluruh metrik yang ditampilkan pada *dashboard* akan menunjukkan peningkatan yang sangat signifikan. Dari jumlah keamanan yang tercatat mencapai 4.287.844, dengan 1.071.483 di antaranya termasuk dalam kategori *alert* level 12 yang menunjukkan terdeteksinya aktivitas *brute force.* Grafik dari jumlah pada interval 10 menit akan memperlihatkan pola yang relatif stabil pada kisaran 80.000 hingga 100.000, yang mengindikasikan bahwa serangan tersebut berlangsung secara berkelanjutan tanpa jeda yang berarti selama delapan jam pengujian. Melalui gambar visualisasi tersebut, *administrator* dapat segera mengidentifikasi adanya aktivitas serangan pada *web server* tanpa perlu melakukan pemeriksaan *log* secara manual seperti *apache access log*.

Tabel 2. Perbandingan Kondisi Sebelum dan Selama Serangan Brute Force

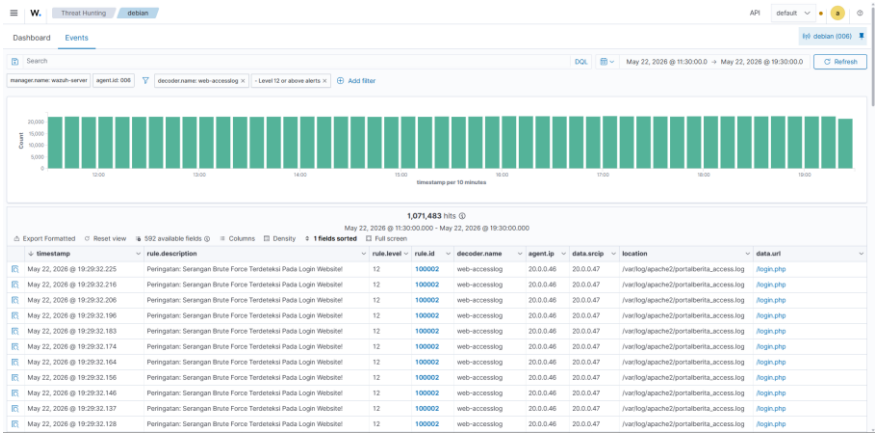
Metrik	**Sebelum Serangan**	**Selama Serangan**
Durasi periode (WIB)	11.00 - 11.30 (30 Menit)	11.30 - 19.30 (8 jam)
Authentication failure	0	4.287.844
Alert Level 12+ Rule 100002	0	1.071.483
Authentication success	*1 (administrator)*	0 (penyerang)
IP penyerang teridentifikasi	-	20.0.0.47

Dari Tabel 2, terlihat perbandingan yang sangat kontras antara kondisi sebelum dan selama serangan terjadi. Total *alert* yang melonjak dari hanya 1 akan menjadi lebih dari 4,2 juta dalam waktu delapan jam. Pada seluruh percobaan *autentikasi* dari penyerang (4.287.844) diklasifikasikan sebagai *authentication failure*. Sebanyak 1.071.483 di antaranya memicu peringatan Level 12 yang telah mengkonfirmasi terdeteksinya aktivitas *brute force (Rule 100002).* Nilai *authentication success* dari penyerang tetap 0, yang menegaskan bahwa *web server* berhasil menolak seluruh percobaan akses yang tidak sah. Selain itu, identifikasi IP penyerang (20.0.0.47) tercatat dengan akurasi 100% pada seluruh serangan selama pengujian berlangsung.

3.2.3 Analisis Detail Peringatan Level 3 dan Level 12 pada Wazuh Events

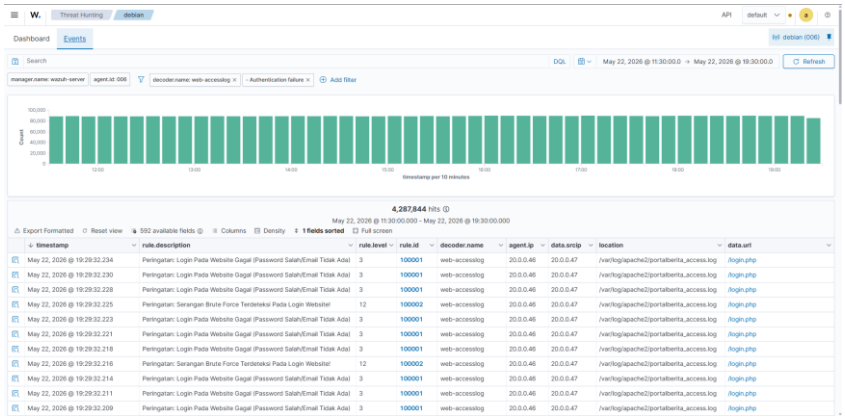
Pada tampilan detail *Level 12+ alerts*, setiap *alert* yang dihasilkan *Rule 100002* akan mencantumkan informasi, *rule.description* peringatan. Serangan *Brute Force* juga terdeteksi pada *Login Website!", rule.id 100002, rule.level 12, agent.ip* 20.0.0.46 sebagai *web server* yang dimonitor, *data.srcip* 20.0.0.47 sebagai IP penyerang, dan *location /var/log/apache2/portalberita_access.log,* serta *data.url /login.php. Timestamp* waktu setiap pengujian akan dicatat secara akurat hingga presisi per milidetik, dengan pengujian Level 12 yang terdeteksi pada pukul 11.30 WIB dan pengujian terakhir pada pukul 19.29 WIB.

Submitted: 29 Juni 2026
Published: 30 September 2026



Gambar 10. Capture Detail Peringatan Level 12+ (Rule 100002) Pada Wazuh Events

Pada gambar 10, akan terlihat detail peringatan yang dihasilkan oleh *Rule 100002* dengan sangat jelas. Setiap *alert akan* mencantumkan seluruh informasi yang diperlukan untuk investigasi, termasuk alamat IP sumber (20.0.0.47) yang teridentifikasi sebagai penyerang, *URL* target *(/login.php)*, serta lokasi *file log* yang memicu *alert* tersebut. *Timestamp* yang presisi hingga milidetik memungkinkan *administrator* untuk melakukan analisis kronologi serangan secara akurat. Informasi lengkap ini akan sangat berharga untuk keperluan audit dan bisa tindak lanjuti.



Gambar 11. Capture Detail Peringatan Level 3 (Rule 100001) Pada Wazuh Events

Pada gambar 11, akan terlihat detail yang dihasilkan oleh *Rule 100001* dengan tingkat Level 3, yang akan berfungsi sebagai peringatan awal terhadap setiap kegagalan *autentikasi* pada *web server*. Setiap data entri yang mencantumkan informasi *rule.description "Peringatan Login Pada Website Gagal"*, *rule.id 100001, rule.level 3, agent.ip* 20.0.0.46, serta *data.srcip* 20.0.0.47 yang mengidentifikasi alamat IP penyerang. Peringatan Level 3 ini akan menjadi fondasi utama yang selanjutnya memicu *Rule 100002* (Level 12) ketika pola serangan *brute force* berhasil terekam oleh *software monitoring Wazuh*.

4. KESIMPULAN

Penelitian ini berhasil mengimplementasikan *Wazuh* sebagai p*latform Security Information and Event Management* (SIEM) dan *Extended Detection and Response* (XDR) untuk mendeteksi serangan *brute force* pada *web server Apache* berbasis *Linux Debian* dengan mengacu pada metodologi NIST SP 800-115. Hasil dari pengujian ini akan menunjukkan bahwa *Wazuh* mampu mendeteksi dan memvisualisasikan sebanyak 4.287.844 *alerts* keamanan secara *real-time* selama delapan jam pengujian, dengan 1.071.483 di antaranya merupakan peringatan Level 12

Submitted: 29 Juni 2026
Published: 30 September 2026

yang terindentifikasi aktivitas *brute force* secara spesifik, disertai identifikasi alamat IP dari sumber serangan dengan tingkat akurasi mencapai 100%. Temuan ini juga menunjukkan bahwa implementasi *Wazuh* memberikan peningkatan yang sangat signifikan terhadap kemampuan deteksi pada ancaman keamanan, dibandingkan pemantauan yang hanya mengandalkan *Apache access log* secara mentah, sehingga layak dipertimbangkan sebagai solusi pemantauan keamanan berbasis *open source* bagi *administrator web server* dalam meningkatkan kemampuan deteksi ancaman pada infrastruktur *server*.

5. SARAN

Penelitian selanjutnya disarankan untuk mengimplementasikan *Wazuh* pada lingkungan yang lebih kompleks dan beragam agar bisa merepresentasikan kondisi yang nyata, sekaligus menerapkan *active response* secara otomatis dengan *firewall* untuk melakukan pemblokiran dari alamat IP penyerang secara otomatis dan tidak lagi diblok manual oleh *administrator web server*. Dan ruang lingkup pengujian ini juga dapat diperluas lagi dengan menambahkan beberapa skenario serangan lainnya, *seperti SQL injection, Cross-Site Scripting* (XSS), dan *Denial of Service* (DoS), dan bisa juga menggunakan metrik evaluasi yang lebih terukur secara ilmiah seperti *precision, recall,* dan *F1-score* agar efektivitas *web server* dapat dibandingkan secara lebih objektif dengan solusi SIEM lainnya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Boy Yuliadi, S.T., M.Kom. selaku dosen pembimbing yang telah memberikan arahan, bimbingan, dan masukan yang sangat berarti selama proses penelitian dan penulisan artikel ini berlangsung. Penulis juga mengucapkan terima kasih kepada Program Studi Teknik Informatika, Universitas Dian Nusantara yang telah menyediakan fasilitas dan dukungan akademik dalam pelaksanaan penelitian ini.

DAFTAR PUSTAKA

[1] T. Muhammad Fawaati and S. Frasetya, “Transformasi Digital Dan Peran SIM Dalam Organisasi Berbasis Data,” 2021.

[2] L. A. Putri and H. Ali, “Pengaruh Sistem Informasi Terhadap Inovasi Digital, Transformasi Digital, dan Customer Relationship Management (CRM)”, doi: 10.38035/dit.v1i3.

[3] F. Irfan Adristi and E. Ramadhani, “Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede,” 2024. [Online]. Available: https://journal.uii.ac.id/selma/index

[4] R. Rambe and F. F. Hermawan, “The Impact of Ransomware on Indonesia’s National Data Security: Case Study of Kominfo Data Leaks,” *Indonesian Journal on Computing (Indo-JC)*, vol. 10, no. 1, Aug. 2025, doi: 10.21108/indojc.v10i1.8976.

[5] R. P. Aji, Y. Prayudi, and A. Luthfi, “ANALYSIS OF BRUTE FORCE ATTACK LOGS TOWARD NGINX WEB SERVER ON DASHBOARD IMPROVED LOG LOGGING SYSTEM USING FORENSIC INVESTIGATION METHOD,” vol. 4, no. 1, pp. 39–48, 2023, doi: 10.20884/1.jutif.2023.4.1.644.

[6] Gede Parama Antara and Ika Dyah Agustia Rachmawati, “Implementasi dan Analisis Wazuh Sebagai Intrusion Detection System (IDS) dan Platform Monitoring,” *Jurnal Informasi, Sains dan Teknologi*, vol. 7, no. 2, pp. 290–303, Dec. 2024, doi: 10.55606/isaintek.v7i2.301.

[7] F. A. Saputra *et al.*, “Jurnal Informatika Terpadu IMPLEMENTASI WAZUH SIEM UNTUK MANAJEMEN LOG EVENT DI PESANTREN TEKNOLOGI INFORMASI

Submitted: 29 Juni 2026
Published: 30 September 2026

DAN KOMUNIKASI JOMBANG," *Jurnal Informatika Terpadu*, vol. 10, no. 2, pp. 146–155, 2024, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[8] J. Park, J. Kim, B. B. Gupta, and N. Park, "Network Log-Based SSH Brute-Force Attack DetectionModel," Computers, Materials and Continua, vol. 68, no. 1, pp. 887–901, Mar. 2021, doi: 10.32604/cmc.2021.015172.

[9] A. Z. Agghey, L. J. Mwinuka, S. M. Pandhare, M. A. Dida, and J. D. Ndibwile, "Detection of username enumeration attack on ssh protocol: Machine learning approach," Symmetry (Basel)., vol. 13, no. 11, Nov. 2021, doi: 10.3390/sym13112192.

[10] A. Shafiyyah, G. F. Nama, and R. A. Pradipta, "IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER," Jurnal Informatika dan Teknik Elektro Terapan, vol. 12, no. 2, Apr. 2024, doi: 10.23960/jitet.v12i2.4074.

[11] Syania Aulia Maherza, Bayu Hananto, and I Wayan Widi Pradnyana, "Penetration Testing Terhadap Website Sekolah Menengah Atas ABC dengan Metode NIST SP 800-115," vol. 19, no. 1, pp. 11–27, May 2023, doi: https://doi.org/10.52958/iftk.v19i1.4697.

[12] M. Dehan Pratama, F. Nova, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos." [Online]. Available: http://jurnal-itsi.org

[13] F. I. F. Farrel, Is Mardianto, S.Si, M.Kom, and Ir. Adrian Sjamsul Qamar, MTI, "Implementation of Security Information & Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System," Intelmatics, vol. 4, no. 1, pp. 1–7, Feb. 2024, doi: 10.25105/itm.v4i1.18529.

Submitted: 29 Juni 2026
Published: 30 September 2026