SISTEM KEAMANAN BERBASIS HOST-BASED INTRUSION DETECTION SYSTEM (HIDS) MENGGUNAKAN WAZUH

Alvin Kamil, Muhlis Tahir, Siti Juliah, Misfarah, Aini Laviva Rahmat, Yudha Dwi Mahendra
Pendidikan Informatika, Universitas Trunojoyo Madura
Jalan Raya Telang PO Box 2 Kamal-Bangkalan, Indonesia
220631100006@student.trunojoyo.ac.id

ABSTRAK

Perkembangan teknologi yang pesat meningkatkan kebutuhan akan sistem keamanan jaringan yang lebih andal, terutama akibat semakin meluasnya pengetahuan mengenai hacking dan cracking, serta kemudahan akses terhadap alat bantu serangan. Salah satu ancaman yang krusial adalah serangan *brute force* terhadap protokol SSH pada server. Untuk mengatasi hal tersebut, penelitian ini mengembangkan sistem keamanan berbasis *Host-based Intrusion Detection System* (HIDS) menggunakan Wazuh, dengan pendekatan metode *Waterfall* yang terdiri dari lima tahap: *requirement, design, implementation, verification, dan maintenance*. Hasil penelitian menunjukkan bahwa sistem yang dibangun mampu mendeteksi serangan *brute force* secara efektif dan memberikan peringatan secara real-time kepada administrator melalui Bot Telegram. Dengan demikian, sistem HIDS berbasis Wazuh ini terbukti efektif dan efisien dalam mendeteksi serangan terhadap server.

Kata kunci : *Cyber Security, HIDS, Jaringan Komputer, wazuh, server, Bruteforce*

1. PENDAHULUAN

Perkembangan teknologi yang semakin pesat meningkatkan kebutuhan akan kualitas keamanan jaringan yang lebih baik. Hal ini terjadi terutama karena pengetahuan tentang hacking dan cracking semakin meluas, ditunjang oleh ketersediaan alat-alat yang mudah diakses dan gratis. Di samping itu, ancaman terhadap keamanan jaringan komputer juga datang dari serangan siber seperti serangan brute force**,** virus, malware, dan serangan Denial of Service (DOS) serta berbagai bentuk serangan lainnya [1].

Ancaman serangan jaringan ke server meliputi berbagai jenis serangan yang dapat mengakibatkan akses tidak sah, pencurian data, atau kerusakan sistem. Salah satu ancaman utama adalah serangan Brute Force, yang bekerja dengan mencoba semua kombinasi username dan password secara berulang-ulang hingga menemukan yang benar, sehingga dapat mengakibatkan akses tidak sah ke server dan risiko kebocoran informasi. Selain itu, serangan ini dapat merusak integritas dan kerahasiaan data yang disimpan di server, serta mengganggu operasional sistem secara keseluruhan. Oleh karena itu, penerapan langkah-langkah keamanan yang tepat sangat penting untuk melindungi server dari ancaman tersebut[2].

Serangan Brute Force adalah metode serangan yang dilakukan dengan mencoba semua kemungkinan kombinasi username dan password secara berulang-ulang hingga menemukan kombinasi yang benar dan mendapatkan akses ke sistem atau jaringan yang dilindungi. Serangan ini bekerja tanpa memerlukan pengetahuan sebelumnya tentang password yang digunakan, melainkan mengandalkan kekuatan brute force untuk menebak password secara sistematis [2]. Serangan ini sering menargetkan perangkat seperti router, server, atau layanan online yang memiliki sistem autentikasi lemah atau tidak dilindungi dengan baik. Jika tidak diatasi, serangan Brute Force dapat menyebabkan akses tidak sah, pencurian data, dan gangguan operasional sistem. Untuk mencegah serangan ini, langkah-langkah seperti penggunaan password yang kuat, penerapan batasan percobaan login, dan deteksi serangan secara real-time sangat dianjurkan [2].

Intrusion Detection System (IDS) adalah solusi penting dalam pengamanan jaringan komputer yang berfungsi untuk mendeteksi aktivitas mencurigakan atau serangan dengan memantau lalu lintas jaringan dan menganalisis paket data yang masuk. Jika terdapat aktivitas mencurigakan, IDS akan memberikan peringatan kepada administrator jaringan agar dapat mengambil tindakan yang diperlukan [3]. Dengan demikian, IDS berperan sebagai sistem deteksi dini yang membantu melindungi jaringan dari potensi ancaman dan serangan yang tidak diinginkan [4]. Fungsi utamanya meliputi pemantauan lalu lintas jaringan dan aktivitas sistem untuk mengidentifikasi tanda-tanda serangan atau kegiatan ilegal serta memberikan peringatan kepada administrator jika ditemukan aktivitas yang mencurigakan [5]. Selain itu, IDS merupakan bagian penting dari sistem keamanan jaringan karena mampu memantau aktivitas secara real-time dan mencatat semua upaya gangguan, sehingga data dan sumber daya dapat terlindungi dari akses tidak sah serta digunakan untuk analisis peningkatan keamanan di masa mendatang [6] [7].

Wazuh adalah platform keamanan open-source yang terfokus pada deteksi ancaman dan pemantauan keamanan yang dapat membantu mendeteksi serangan atau ancaman terhadap sistem serta memberikan peringatan jika ada perubahan atau aktivitas mencurigakan pada file [8]. Selain itu, wazuh berfungsi sebagai solusi Host-based Intrusion Detection System (HIDS) dengan memindai sistem untuk mencari malware, rootkit, dan anomali mencurigakan, serta mendeteksi file tersembunyi,

proses tidak biasa, dan inkonsistensi dalam respons panggilan sistem [9]. Kemampuan monitoring log dari setiap agen yang terhubung memungkinkan wazuh mengidentifikasi aktivitas mencurigakan dan memberikan analisis mendalam tentang perilaku sistem [10], sekaligus memantau file konfigurasi untuk memastikan kepatuhan terhadap kebijakan keamanan dan standar yang ditetapkan [9].

Gambar 1. Wazuh *the open source security platform*

Dalam implementasinya, Wazuh juga telah terbukti efektif dalam mendeteksi serangan DDoS, misalnya serangan Slowloris, dengan mencatat aktivitas serangan dan memberikan peringatan melalui dashboard yang memungkinkan respon cepat dari tim keamanan [8]. Integrasinya dengan sistem lain seperti OSSEC, OpenSCAP, dan Elastic Stack meningkatkan kemampuan Wazuh dalam mendeteksi dan merespons ancaman melalui analisis data yang lebih komprehensif [9]. Pengujian kinerja juga menunjukkan efektivitas Wazuh sebagai HIDS dalam mendeteksi serangan yang disusun berdasarkan skema tertentu [11], sehingga implementasi Wazuh dapat meningkatkan keamanan data dengan menutup celah yang ada dan mencegah akses tidak sah [12].

Integrasi wazuh dengan Telegram dilakukan untuk mengirim alert hasil analisis data Wazuh secara real-time. Proses ini menggunakan API yang disediakan oleh bot Telegram untuk menghubungkan wazuh dengan Telegram, sehingga alert dapat dikirim langsung kepada pengguna, dan sistem ini dirancang untuk mengurangi jumlah pesan yang terkirim ketika aktivitas yang sama terjadi secara berulang, sehingga lebih efisien dalam penyampaian informasi [13]. Implementasi sistem ini melibatkan pemrograman menggunakan Python, di mana alert dari wazuh dikirim ke bot messenger melalui Telegram API yang telah disetting dalam script Python [13]. Dengan integrasi ini, administrator dapat dengan cepat mengetahui masalah yang terjadi pada server, bahkan ketika tidak berada di ruang monitoring [14].

Penelitian ini bertujuan untuk mengembangkan sistem keamanan jaringan yang efektif dengan menggunakan platform Wazuh sebagai solusi IDS dan HIDS, sehingga serangan siber seperti DDoS, brute force, malware, phishing, dan DoS dapat dideteksi secara dini melalui pemantauan real-time dan analisis paket data. Sistem ini diharapkan dapat memberikan peringatan kepada administrator untuk segera mengambil tindakan preventif. Selain itu, penelitian ini juga bertujuan mengintegrasikan Wazuh dengan Telegram guna mengirimkan alert secara real-time. Dengan menggunakan API Telegram dan pemrograman Python, alert dapat dikirim langsung ke pengguna, memudahkan respons cepat terhadap ancaman dan meningkatkan keseluruhan keamanan jaringan.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian di PSDKU Universitas Way Kanan Lampung, telah dikembangkan sebuah sistem keamanan jaringan untuk laboratorium komputer yang dirancang untuk melindungi dari serangan brute-force dan DoS. Sistem ini memanfaatkan platform wazuh sebagai server pemantauan dan menggunakan Fail2Ban untuk memblokir alamat IP para penyerang. Metodologi pengembangan yang diterapkan mengikuti model PPDIOO dari Cisco. Hasil penelitian menunjukkan bahwa sistem ini mampu bertahan dengan baik terhadap serangan brute-force, meskipun respons terhadap serangan DoS dengan koneksi HTTP kurang dari 4. 000 masih kurang memadai. Daya tahan maksimum server tercatat pada 3. 522. 013 koneksi, yang mengindikasikan perlunya perbaikan sistem agar dapat memberikan respons yang lebih cepat dan lebih efektif [14].

Penelitian kedua yang dilakukan oleh Oky Dwi Prasetyo dan timnya di Universitas Brawijaya mengeksplorasi kinerja sistem deteksi intrusi berbasis host (HIDS) dengan menggunakan platform Wazuh untuk menangani serangan brute-force dan DoS. Penelitian ini melibatkan dua skenario serangan brute-force yang dilakukan dengan alat Medusa dan Hydra, serta dua skenario serangan DoS menggunakan Hping3 dan Metasploit. Hasil pengujian menunjukkan bahwa Wazuh mampu mendeteksi serangan brute-force secara real-time, hal ini terlihat dari munculnya peringatan serta identifikasi yang sesuai dengan skema MITRE ATT&CK. [11].

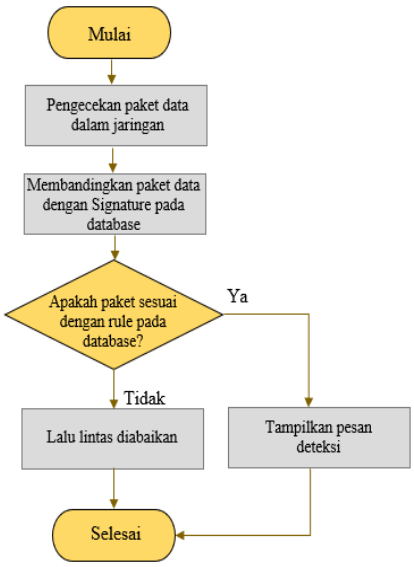
2.2. *Instruction Detection System* (IDS)

IDS adalah sistem keamanan yang dirancang untuk mendeteksi aktivitas mencurigakan atau serangan dalam jaringan. *Instruction Detection System* (IDS) dapat dibagi menjadi dua kategori utama: *Signature-Based Detection* dan *Anomaly-Based Detection*. Sistem berbasis tanda tangan mengidentifikasi ancaman berdasarkan pola yang telah diketahui, sementara sistem berbasis anomali mendeteksi perilaku yang tidak biasa dibandingkan dengan profil normal [15]. Berikut ini merupakan cara kerja *Signature-Based Detection* dan *Anomaly-Based Detection* [16]

2.3. *Signature-Based Detection*

Cara teknik deteksi berbasis tanda tangan yang dapat mendeteksi setiap serangan diilustrasikan pada Gambar 2. Menggunakan pola yang telah disimpan

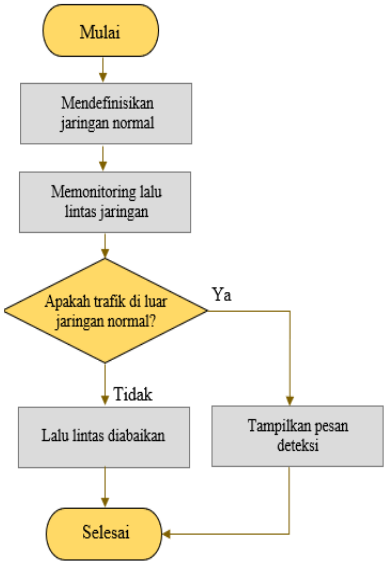
dalam basis data aplikasi IDS yang terpasang, pendekatan ini mendeteksi semua serangan. Dalam sistem IDS, pola ini digunakan untuk membandingkan lalu lintas atau paket data yang cocok dengan salah satu aturan yang ditetapkan.



Gambar 2. Cara kerja *signature-based detection*

Setelah aturan atau pola diidentifikasi, sistem deteksi intrusi berbasis tanda tangan akan memeriksa setiap paket yang melintasi jaringan dengan cara membandingkannya berdasarkan aturan basis data. Pesan deteksi yang disajikan sebagai serangan akan muncul jika paket yang diperiksa cocok dengan pola atau kriteria yang ditetapkan. Dengan demikian, administrator akan menerima peringatan deteksi serangan dari IDS Signature.

2.4. *Anomaly-Based Detection*



Gambar 3. Cara kerja anomaly-based detection

Kemampuan metode deteksi berbasis anomali untuk mengidentifikasi setiap serangan terlihat pada Gambar 3. Pendekatan ini pertama-tama menetapkan jaringan tipikal untuk mengidentifikasi setiap serangan. Penggunaan bandwidth, port, dan peralatan yang terkait dengan setiap jaringan merupakan bagian dari jaringan tipikal yang dimaksud. Jaringan tipikal ini berfungsi sebagai titik perbandingan.

Jika terdeteksi adanya lalu lintas yang tidak biasa, anomali IDS secara otomatis mengenalinya sebagai serangan dan memberi tahu administrator tentang serangan tersebut. Setiap lalu lintas yang dipantau akan diabaikan dan dianggap sebagai lalu lintas biasa, bukan serangan, jika jaringan beroperasi secara normal untuk sementara waktu.

Instruction Detection System (IDS) menerapkan berbagai pendekatan untuk menemukan lalu lintas atau paket data yang mencurigakan dalam jaringan, yang terbagi menjadi dua jenis, yakni pendekatan berbasis jaringan (NIDS) dan pendekatan berbasis host (HIDS) [17]. NIDS memantau lalu lintas jaringan untuk mendeteksi serangan di seluruh jaringan, sedangkan HIDS memantau aktivitas pada perangkat atau host individu untuk mendeteksi ancaman yang spesifik pada perangkat tersebut.

2.5. Wazuh

Fitur XDR (*External Data Representation*) dan SIEM (*Security Information and Event Management*), seperti analisis log, deteksi malware dan intrusi, pemantauan integritas file, evaluasi konfigurasi standar industri, deteksi kerentanan, dan dukungan kepatuhan regulasi, semuanya digabungkan dalam wazuh. wazuh merupakan program sumber terbuka yang berfungsi sebagai sistem deteksi berbasis host (titik akhir). Kirimkan pemberitahuan tepat waktu dan ambil tindakan proaktif. wazuh memantau host di lapisan sistem operasi dan aplikasi untuk menyediakan fitur visibilitas keamanan yang lebih baik pada infrastruktur. [14].

Wazuh berperan penting dalam mengatasi serangan siber. Fungsi utama wazuh yaitu sebagai pemantau keamanan, deteksi ancaman dan respons insiden. Namun karena wazuh ini bersifat open source yang berati kita bisa memodifikasi wazuh agar dapat menjalakan fungsi lainya di luar fungsi utama wazuh itu sendiri [5].

2.6. Telegram

Telegram adalah sebuah aplikasi yang menggunakan teknologi cloud, sehingga memungkinkan penggunanya untuk mengakses satu akun Telegram dari beberapa perangkat sekaligus. Selain itu, pengguna juga bisa denganmudah berbagi berkas sampai1,5 GB.Aplikasi Telegram dibuat oleh dua saudara asal Rusia, yaitu Nikolai Durov dan Pavel Durov. Mereka bekerja sama dalam peran yang berbeda. Nikolai bertanggung jawab atas pengembangan aplikasi, termasuk menciptakan protokol MTProto yang menjadi inti dari Telegram. Di sisi lain, Pavel fokus pada aspek pendanaan dan infrastruktur melalui Digital Fortress [17].

2.7. Hydra

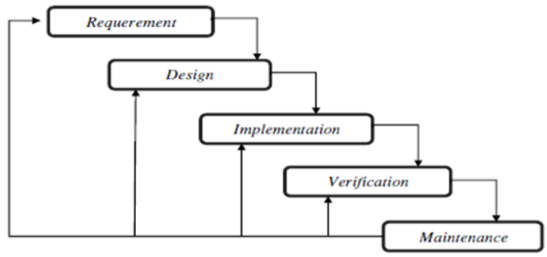
Hydra merupakan sebuah alat keamanan yang dapat digunakan untuk melakukan serangan berupa brute force terhadap berbagai jenis layanan otentikasi. Hydra memiliki kemampuan untuk melakukan percobaan terhadap berbagai kombinasi username dan password untuk mendapatkan akses sistem target. Penulis mengunakan hydra untuk melakukan serangan brute force ssh terhadap agen wazuh dan memastikan wazuh dapat mendekteksi dan memblokir serangan tersebut [5]**.**

2.8. *Brute Force*

Serangan brute-force terjadi saat peretas mencari kelemahan keamanan dan memanfaatkan kelemahan keamanan kata sandi untuk mendapatkan akses. Karena ketidakseimbangan ini, serangan akan secara otomatis menyesuaikan panjang dan campuran karakter yang digunakan dalam nama pengguna. Sampai Anda menemukan kata sandi yang bagus. Jadi, serangan brute-force merupakan serangan yang sangat berbahaya, untuk dapat mencegahnya para korban harus membuat kata sandi yang rumit dengan meningkatkan jumlah kata sandi [18].

3. METODE PENELITIAN

Waterfall merupakan metode pengembangan sistem yang setiap fasenya diselesaikan secara bergiliran. Sebelum beralih ke langkah berikutnya dalam proses implementasi metode Waterfall, setiap langkah akan diselesaikan terlebih dahulu, dimulai dari tahap pertama [19]. Metode waterfall terdiri dari lima tahapan, yaitu *requerement, design, implementation,verification, dan maintenance* [20].



Gambar 4. Alur metode waterfall

Berikut adalah tahapan-tahapan dari metode waterfall yang dapat dilihat pada gambar 4 berikut penjelasannya [20].

3.1. *Requerement*

Pada tahap ini, peneliti mengumpulkan dan memeriksa persyaratan untuk sistem keamanan yang akan dibuat. Tinjauan Pustaka dan analisis sistem. Elemen perangkat keras, perangkat lunak, dan keamanan yang akan dimasukkan ke dalam sistem HIDS melalui platform wazuh adalah produk akhir dari tahap ini.

3.2. *Design*

Tahap desain bertujuan untuk membangun struktur sistem keamanan jaringan menggunakan platform wazuh, yang mencakup komponen utama seperti wazuh Server, wazuh Agent, Dashboard, serta integrasi dengan Bot Telegram, agar sistem mampu mendeteksi serangan secara langsung dan mengirimkan notifikasi secara otomatis kepada administrator.

3.3. *Implementation*

Proses implementasi melibatkan pemasangan dan pengaturan wazuh pada server , penambahan wazuh Agent pada perangkat endpoint.

3.4. *Verification/ Testing*

Tahap pengujian dilakukan dengan mensimulasikan serangan siber berupa brute force pada SSH menggunakan alat seperti Hydra untuk menyerang login root server, kemudian memantau respons sistem melalui wazuh Dashboard untuk memastikan bahwa sistem dapat mendeteksi serangan tersebut secara real-time, memberikan pemberitahuan sesuai dengan jenis serangan.

3.5. *Maintenance*

Pada tahap maintenance dilakukan integrasi wazuh dengan Bot Telegram menggunakan API Telegram dan pemrograman Python, sehingga setiap anomali atau serangan yang terdeteksi oleh Wazuh dapat secara otomatis memicu pemberitahuan yang dikirim langsung ke administrator melalui Telegram.

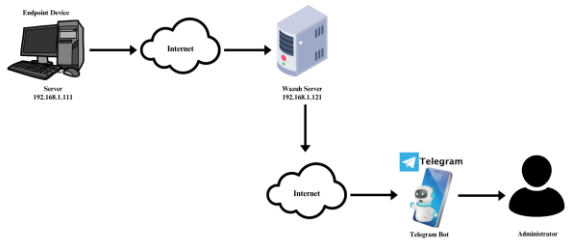
4. HASIL DAN PEMBAHASAN

4.1. *Requerement* (Kebutuhan)

Pada tahap ini peneliti menganalisa dan melakukan studi literatur untuk menentukan alat dan bahan apa saja yang dibutuhkan serta langkah-langkah konfigurasi yang dilakukan untuk membangun sistem keamanan berbasis host-based intrusion detection system (HIDS) menggunakan wazuh. Peneliti menggunakan laptop sebagai perangkat untuk melakukan percobaan menggunakan aplikasi virtual yakni virtualbox untuk membangun sistem keamanan.

4.2. *Design* (Desain)

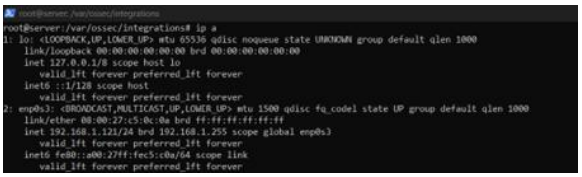
Pada tahap ini, akan dijelaskan skema sistem keamanan. Wazuh berfungsi sebagai HIDS yang berfungsi untuk mendeteksi anomali/serangan yang terjadi pada *endevice/agent*. Dalam sistem ini terdapat empat komponen utama, yaitu perangkat akhir, sumber jaringan (internet), BotTelegram dan server wazuh. wazuh melakukan pemindaian untuk mendeteksi anomali/serangan yang terjadi pada server, jika wazuh mendetaksi anomali/serangan yang terjadi maka wazuh akan mengirimkan peringatan kepada administrator melalui Bot Telegram yang telah di integrasikan.



Gambar 5. Skema sistem

4.3. Konfigurasi IP Wazuh-server

Peneliti mengonfigurasi alamat IP Wazuh-server menggunakan IP statis 192. 168. 1. 121/24, seperti yang terlihat pada Gambar 6, untuk memastikan Wazuh-server memiliki alamat IP yang tetap.



Gambar 6. Ip wazuh server

4.4. Konfigurasi Wazuh

Peneliti melaksanakan instalasi wazuh pada perangkat yang digunakan sebagai server wazuh, sebagaimana diperlihatkan pada gambar 7. wazuh terdiri dari beberapa komponen, yaitu wazuh indexer, wazuh server, dan wazuh dashboard, yang semuanya perlu dipasang agar sistem wazuh dapat beroperasi dengan baik. Untuk melakukan pemasangan wazuh, langkah yang diambil adalah dengan menginputkan perintah seperti yang ditunjukkan oleh gambar 7.

curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

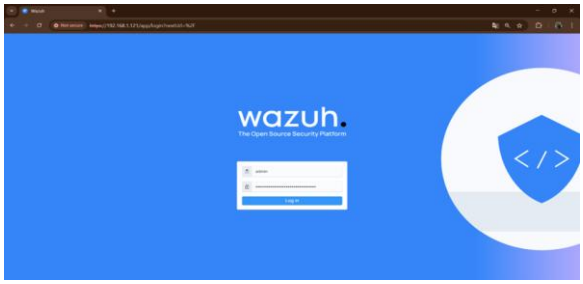
Gambar 7. Instalasi wazuh

Setelah proses instalasi komponen wazuh selesai, akan ditampilkan ringkasan yang menampilkan cara mengakses wazuh dashboard, serta username dan password default yang dapat digunakan untuk masuk ke dalamnya.

Gambar 8. Summary username dan password

4.5. Login Wazuh *Dashboard*

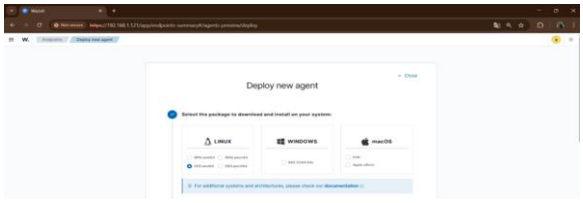
Peneliti mengakses dasbor wazuh menggunakan alamat IP tersebut melalui peramban web perangkat mereka. Peneliti memilih memakai Google Chrome untuk membuka dasbor wazuh dengan mengetikkan https://(IP server wazuh). Peneliti memasukkan https://192.168.1.121 pada peramban web, maka menu login dasbor wazuh akan muncul. Kemudian peneliti memasukkan nama pengguna dan kata sandi *default* yang telah disediakan oleh wazuh.



Gambar 9. Wazuh dashboard

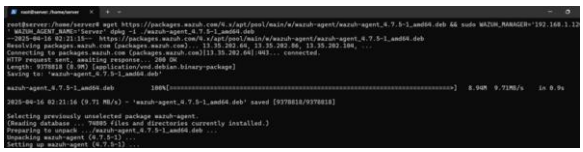
4.6. Penambahan Wazuh Agent

Setelah peneliti berhasil masuk ke dalam wazuh dashboard, langkah selanjutnya adalah mendeploy wazuh *agent* baru dengan memanfaatkan fitur *Deploy New Agent*. Hal ini bertujuan agar wazuh server bisa terhubung dengan wazuh agent. Seperti gambar 10, peneliti memilih DEB amd64, karena server *agent* menggunakan system operasi linux debian.



Gambar 9. Penambahan wazuh agent

Pada Gambar 11 dan 12 peneliti menggunakan Powershell dengan hak akses Administrator pada perangkat *endpoint* untuk menjalankan kedua perintah yang didapat dari wazuh. Langkah ini dilakukan untuk menginstal wazuh *agent* dan mengaktifkannya agar dapat berfungsi pada perangkat endpoint. pada gambar 11 ditunjukkan pemasangan wazuh *agent* pada server *agent* dan pada gambar 12 di tunjukkan perintah enable dan start wazuh agent serta pembuatan file wazuh-agent.service.



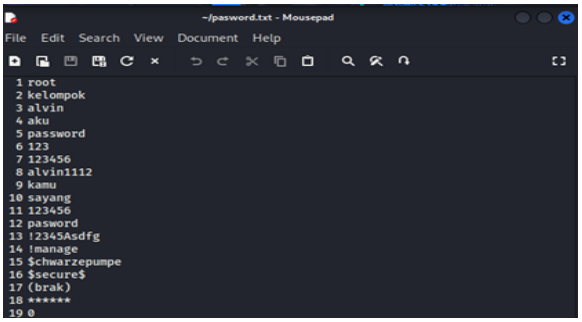
Gambar 10. Menginstal wazuh agent

Gambar 11. Enable dan start wazuh agent

4.7. *Testing* (Pengujian)

Pada tahap pengujian sistem keamanan ini, peneliti menggunakan serangan siber berupa serangan bruteforce yang menargetkan credential login root server. Penyerangan Bruteforce Attack menggunakan hydra, bertujuan untuk mengevaluasi kekuatan sistem keamanan melalui mekanisme penargetan serangan SSH Server. Hydra dapat menyerang *login* dengan berbagai protokol, tetapi dalam pengujian ini, SSH ditanam di server *agent* dengan penargetan utama yang mendapatkan password root dari SSH.

Selanjutnya membuat file paswort.txt yang berisikan sejumlah kemungkinan password yang mungkin digunakan oleh server yang menjadi target serangan.



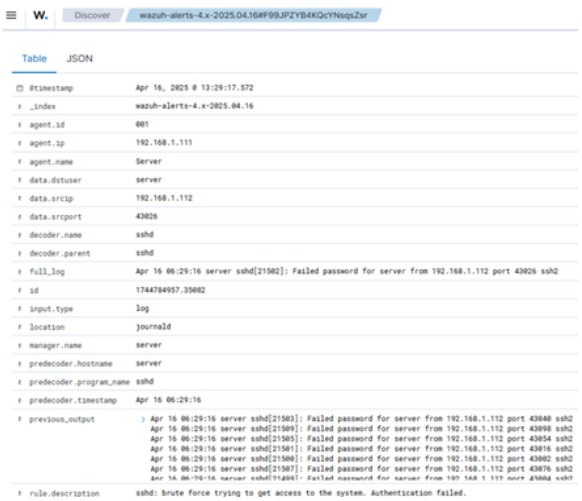
Gambar 12. File password

Perintah untuk menyerang menggunakan tool hydra, yang dijalankan pada terminal kali linux.

hydra -l server -P pasword.txt 192.168.1.111 ssh

Gambar 13. Penyerangan bruteforce

Setelah dilakukan pengujian serangan, maka akan muncul log peringatan pada wazuh dasbor terkait serangan yang terjadi, peringatan yang muncul pada wazuh dasbor seperti yang ditunjukkan oleh gambar 15.



Gambar 14. Log event pada wazuh dashboard

4.8. *Maintenance* (Pemeliharaan)

Pada tahap ini, peneliti mengintegrasikan wazuh dengan Bot Telegram. integrasi wazuh dengan telegram, peneliti melakukan langkah-langkah konfigurasi pada server yang dijadikan wazuh server untuk mengintegrasikan wazuh dengan Bot Telegram. Setelah diintegrasikan dengan Bot Telegram jika ada anomali/serangan yang terdeteksi oleh wazuh maka wazuh akan mengirimkan peringatan atau *alert* ke administrator menggunakan Bot Telegram. Seperti pada gambar 16 yang menunjukkan alert yang dikirimkan oleh wazuh, karena wazuh mendeteksi adanya anomali/serangan ssh bruteforce yang menyerang *agent* yang Bernama "server" dengan *alert*_level 10.

Gambar 15. Alert pada telegram

5. KESIMPULAN DAN SARAN

Dari hasil pengujian sistem keamanan berbasis host intrusion detection system (HIDS) menggunakan wazuh ini sangat efektif dan efisien dalam mendeteksi serangan yang terjadi pada server. Seperti yang telah di uji cobakan, sistem keamanan ini mampu mendeteksi serangan bruteforce ssh yang terjadi pada server. Dari 3 percobaan penyerangan yang dilakukan oleh peneliti menggunakan serangan BruteForce, sistem keamanan ini mampu mendeteksi seluruh serangan yang terjadi pada server dan maleporkannya kepada administrator menggunakan BotTelegram, dengan peringatan serangan sshd:brutfoce memiliki level peringatan "10" serta log serangan bisa dilihat pada wazuh dasbor. Saran untuk penelitian dimasa mendatang : 1. Pada penelitian ini hanya menggunakan satu jenis serangan siber yakni serangan bruteforce, untuk penelitian di masa mendatang bisa menggunakan serangan jenis lainnya untuk menguji sistem. 2. Penelitian ini sistem keamanan masih fokus

untuk mendeteksi serangan dan melaporkannya kepada administrator, untuk penelitian di masa mendatang bisa mengoptimalkan sistem keamanan dengan menambahkan fitur aktive respon untuk mencegah serangan yang terjadi.

DAFTAR PUSTAKA

[1] S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, and A. Setiawan, "Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian," Journal of Internet and Software Engineering, vol. 1, no. 4, pp. 1–12, Jun. 2024.

[2] S. Bahri, "Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router," INDOTECH Indonesian Journal of Education And Computer Science, vol. 1, no. 3, pp. 136–147, Dec. 2023.

[3] A. Khaliq and N. Sari, "Pemanfaatan Kerangka Kerja Investigasi Forensik Jaringan Untuk Identifikasi Serangan Jaringan Menggunakan Sistem Deteksi Intrusi (Ids)," Jurnal Nasional Teknologi Komputer, vol. 2, no. 3, pp. 150–158, Jul. 2022.

[4] I. M. Amir and Y. Mardiana, "Simulasi Intrusion Detection System (Ids) Dalam Keamanan Web Server Pada Jaringan," *Seminar Nasional Ilmu Komputer*, vol. 3, no. 1, pp. 69–82, Oct. 2023.

[5] S. A. Hidayat and D. Darlis, "Implementasi Intrusion Detection System Dalam Upaya Pencegahan Cyber Attack," *e-Proceeding of Applied Science*, vol. 10, no. 4, pp. 924–930, Aug. 2024.

[6] S. Khadafi, D. Y. Pratiwi, and E. Alfianto, "Keamanan Ftp Server Berbasiskan Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu," Jurnal Ilmiah NERO, vol. 6, no. 1, pp. 11–24, Apr. 2021.

[7] R. Fauzi, Y. Muhyidin, and D. Singasatia, "Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS)," Jurnal Sains Komputer & Informatika (J-SAKTI, vol. 7, no. 1, pp. 72–86, Mar. 2023.

[8] M. Mikyal, M. Lamada, and A. Wahid, "Implementasi Keamanan Server Aplikasi E-Raport SMK Negeri 1 Sinjai Menggunakan Wazuh," Jurnal Ilmiah Multi Disiplin, vol. 3, no. 1, pp. 3031–9498, Oct. 2024.

[9] M. D. Pratama, F. Nova, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos," Jurnal Ilmiah Teknologi Sistem Informasi, vol. 3, no. 1, pp. 1–7, Mar. 2022.

[10] R. M. Muhammad, I. D. Irawati, and M. Iqbal, "Implementasi Sistem Keamanan Jaringan Lokal Menggunakan Honeypot Dionaea, Dan Ids, Serta Analisis Malware Menggunakan Malware Analysis System," eProceedings of Applied Science, vol. 7, no. 3, pp. 1–7, Jun. 2021.

[11] O. D. Prasetyo, P. H. Trisnawan, and B. Adhitya, "Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 7, no. 6, pp. 2686–2692, Nov. 2023.

[12] G. P. Antara and I. D. A. 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.

[13] M. A. Fahrudi and I. M. Suartana, "Integrasi End-point Security Berbasis Agent dan Bot Messenger untuk Deteksi dan Monitoring Serangan pada Web Server secara Real-time," Journal of Informatics and Computer Science (JINACS), vol. 04, no. 03, pp. 275–282, Jan. 2023.

[14] 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 (JITET), vol. 12, no. 2, pp. 970–982, Apr. 2024.

[15] A. R. Syujak, K. Diantoro, V. Yuni T, A. Soderi, and P. A. Sucipto, "Integrasi Deep Packet Inspection dengan Intrusion Detection System (IDS) untuk Identifikasi Serangan DDoS dalam Jaringan Skala Besar," Jurnal Minfo Polgan, vol. 13, no. 2, pp. 1971–1975, Dec. 2024.

[16] P. Panagiotou, N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Host-based intrusion detection using signature-based and AI-driven anomaly detection methods," Information & Security, vol. 50, p. pp-zz, Sep. 2021.

[17] T. Purnama, Y. Muhyidin, and D. Singasatia, "Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi," JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK), vol. 14, no. 2, pp. 358–369, Sep. 2023.

[18] D. M. J. Putra, I. N. N. Y. Anantra, P. A. kusuma, P. D. J. Pratama, G. A. J. Saskara, and I. M. E. Listartha, "Analisis Perbandingan Serangan Hydra, Medusa Dan Ncrack Pada Password Attack," Jurnal Informatika Teknologi dan Sains (JINTEKS), vol. 4, no. 4, pp. 461–466, Nov. 2022.

[19] B. Fachri and R. Wahyu Surbakti, "Perancangan Sistem Dan Desain Undangan Digital Menggunakan Metode Waterfall Berbasis Website (Studi Kasus: Asco Jaya)," Journal of Science and Social Research, no. 3, pp. 263–267, Oct. 2021.

[20] K. J. T. Seran and V. N. Naiheli, "Pengembangan Media Promosi Potensi Desa Oepuah Dengan Menggunakan Metode Waterfall Development Of Promotional Media For Oepuah Village Potentiality Using Waterfall Method," Journal Of Information And Technology Unimor (JITU), vol. 1, no. 1, pp. 31–36, Mar. 2021.