Journal of Internet and Software Engineering Vol: 1, No 4, 2024, Page: 1-12

Implementasi Konfigurasi *Firewall* dan Sistem Deteksi Intrusi menggunakan Debian

Sista Naelly Adzimi*, Hafiz Agi Alfasih, Fauzan Naufal Gibran Ramadhan, Shelvie Nidya Neyman, Aep Setiawan

Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: Penelitian ini bertujuan untuk mengimplementasikan konfigurasi *firewall* dan sistem deteksi intrusi (IDS) menggunakan Debian, guna meningkatkan keamanan jaringan secara keseluruhan. Dalam era digital yang menghadirkan berbagai ancaman siber seperti *malware, phishing*, dan serangan DDoS, keamanan siber menjadi krusial. Debian dipilih karena stabilitas dan keamanannya, serta ketersediaan alat *open-source* seperti iptables untuk *firewall* dan Snort untuk IDS. Metodologi penelitian mencakup studi literatur, eksperimental, dan konfigurasi *firewall* yang disesuaikan dengan kebutuhan spesifik jaringan, serta implementasi Wazuh sebagai IDS. Pengujian dilakukan melalui simulasi serangan untuk mengevaluasi efektivitas konfigurasi. Hasilnya menunjukkan peningkatan signifikan dalam kemampuan deteksi dan respons terhadap ancaman siber. *Firewall* berhasil memblokir akses tidak sah dan mencatat aktivitas mencurigakan, sementara Wazuh IDS mendeteksi serangan *brute force* dan *malware*, serta memberikan respons otomatis terhadap ancaman. Integrasi *firewall* dan IDS menghasilkan pendekatan keamanan berlapis, memungkinkan pertahanan proaktif dan *real-time*. Implementasi ini menunjukkan bahwa kombinasi teknologi keamanan, pelatihan berkelanjutan, dan kebijakan yang kuat dapat memberikan perlindungan komprehensif terhadap ancaman siber. Hasil penelitian ini dapat dijadikan model bagi lembaga pendidikan lain yang menghadapi tantangan serupa dalam melindungi data dan infrastruktur jaringan mereka.

Kata Kunci: *Firewall*, IDS, Wazuh, *Network Security*, Debian

DOI: https://doi.org/10.47134/pjise.v1i4.2681
*Correspondence: Sista Naelly Adzimi
Email: sistanaelly@apps.ipb.ac.id

Received: 01-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *This research aims to implement a firewall configuration and intrusion detection system (IDS) using Debian, to improve overall network security. In a digital age that presents various cyber threats such as malware, phishing, and DDoS attacks, cybersecurity is crucial. Debian was chosen due to its stability and security, as well as the availability of open-source tools such as iptables for firewall and Snort for IDS. The research methodology includes the configuration of a firewall tailored to the specific needs of the network, as well as the implementation of Wazuh as an IDS. Testing was conducted through simulated attacks to evaluate the effectiveness of the configuration. The results showed significant improvements in detection and response capabilities to cyber threats. The firewall successfully blocked unauthorized access and logged suspicious activity, while Wazuh IDS detected brute force attacks and malware, and provided automated responses to threats. The integration of firewall and IDS results in a layered security approach, enabling proactive and real-time defense. This implementation demonstrates that a combination of security technology, continuous training, and strong policies can provide comprehensive protection against cyber threats. The results of this study can serve as a model for other educational institutions facing similar challenges in protecting their data and network infrastructure.*

Keywords: *Firewall, IDS, Wazuh, Network Security, Debian*

Pendahuluan

Teknologi yang semakin canggih, meningkatkan kebutuhan akan kualitas keamanan jaringan yang lebih baik. Hal ini terutama karena pengetahuan tentang *hacking* dan *cracking* semakin luas dan didukung oleh alat yang mudah dan gratis diperoleh. Selain itu, ancaman terhadap keamanan jaringan komputer juga datang dari virus, *phising, malware*, DOS, *spoofing, sniffing, spamming*, dan lainnya. Ancaman-ancaman ini dapat membahayakan keamanan sistem jaringan, memungkinkan data dengan mudah dicuri atau dirusak oleh penyusup atau penyerang (Doren, 2019). Keamanan siber menjadi salah satu aspek paling krusial dalam menjaga integritas dan kerahasiaan data. Berbagai ancaman siber tersebut dapat mengakibatkan kerugian besar bagi organisasi, baik dari segi finansial maupun reputasi. Untuk mengatasi ancaman tersebut, implementasi sistem keamanan yang efektif menjadi keharusan. Dua komponen utama yang dapat membantu dalam melindungi jaringan adalah *firewall* dan sistem deteksi intrusi (IDS).

Pengertian *firewall* yaitu sebuah sistem atau perangkat keamanan khususnya pada jaringan komputer yang bertugas untuk menjaga lalu lintas data di dalam jaringan komputer berjalan dengan aman, dan dalam waktu bersamaan juga mencegah lalu lintas data yang tidak aman untuk masuk di dalam jaringan komputer (Roma Doni, 2014). *Firewall* membatasi siapa saja yang berhak mengakses suatu internet dalam jaringan, dan siapa saja yang harus diizinkan dan tidak diizinkan untuk lewat, hal ini biasa disebut dengan *filtering. Firewall* pada jaringan, dapat memantau aktivitas suatu jaringan (Adhi Purwaningrum et al., 2018).

IDS adalah sebuah sistem yang dapat secara otomatis memonitor kejadian pada jaringan komputer dan dapat menganalisa masalah keamanan jaringan. IDS mampu mendeteksi penyusup dan memberikan respons secara *real time*. Terdapat dua teknik yang digunakan dalam IDS yaitu, NIDS (*Network Based Intrusion Detection System*) dan HIDS (*Host Based Intrusion Detection System*) (Rakhman & Lestariningati, n.d.) IDS merupakan salah satu opsi untuk meningkatkan keamanan jaringan dalam sebuah *network* baik intranet maupun internet (Sutarti et al., 2018). IDS (*Intrusion Detection System*) juga berfungsi sebagai sistem yang memantau lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan dan mengeluarkan peringatan saat aktivitas tersebut terdeteksi. IDS akan memberikan peringatan jika terjadi serangan dan memungkinkan pemblokiran alamat IP agar tidak dapat mengakses kembali server yang diserang (Fahrudi & Suartana, 2023). Log adalah kumpulan informasi atau data peristiwa seperti *timestamp*, alamat IP sumber, alamat IP tujuan, dan lainnya, yang dapat digunakan untuk membantu proses investigasi serangan siber dengan menganalisis data log tersebut (Jeklin et al., 2016).

Menurut Firdaus et al. (2013) *Host Intrusion Detection System* (HIDS) adalah sistem yang mampu mendeteksi aktivitas mencurigakan dalam jaringan yang mengarah ke perangkat komputer. HIDS melakukan deteksi dengan memantau lalu lintas yang masuk dan keluar dari sistem atau jaringan, serta dengan membandingkan pola lalu lintas jaringan normal dengan lalu lintas yang terjadi pada jaringan komputer tersebut.

HIDS terdiri dari beberapa komponen utama:

1. IDS *Rule*: Merupakan database yang berisi pola-pola serangan (*signature*) untuk berbagai jenis serangan. Database ini perlu diperbarui secara berkala agar HIDS mampu mendeteksi serangan baru.
2. IDS *Engine*: Merupakan program yang terus berjalan untuk membaca paket data dan membandingkannya dengan IDS *Rule*.
3. IDS *Alert*: Merupakan catatan serangan yang terdeteksi. Jika IDS *Engine* mendeteksi paket data yang berbahaya, maka akan dikirimkan *alert* berupa *log file*. Untuk keperluan analisis, *alert* dapat disimpan dalam database seperti BASE (*Basic Analysis and Securtiy Engine*) yang berfungsi untuk mencari dan mengolah data dari *alert* jaringan yang dibangkitkan oleh HIDS.

Firewall dan sistem deteksi intrusi adalah dua komponen penting dalam sistem keamanan siber yang berfungsi sebagai pengamanan awal dan deteksi ancaman. *Firewall* adalah perangkat lunak atau perangkat keras yang dirancang untuk memblokir akses yang tidak sah ke jaringan dan perangkat yang terhubung dengannya. *Firewall* dapat dikonfigurasi untuk mengizinkan atau memblokir lalu lintas jaringan berdasarkan berbagai kriteria, seperti alamat IP sumber dan tujuan, *port*, dan protokol. Sistem deteksi intrusi (IDS) adalah perangkat lunak atau perangkat keras yang dirancang untuk mendeteksi aktivitas mencurigakan pada jaringan. IDS dapat menganalisis lalu lintas jaringan dan mencari pola yang menunjukkan adanya serangan siber. IDS dapat membantu mengidentifikasi dan mencegah serangan siber sebelum terjadi.

Debian, sebagai salah satu distribusi Linux yang stabil dan aman, menawarkan berbagai alat dan fitur yang diperlukan untuk implementasi *firewall* dan IDS. Kestabilan dan keamanan yang dihadirkan oleh Debian menjadikannya pilihan ideal untuk infrastruktur keamanan siber. Dengan menggunakan perangkat lunak *open-source* seperti iptables untuk *firewall* dan Snort untuk IDS, organisasi dapat membangun sistem keamanan yang kuat dan dapat disesuaikan dengan kebutuhan spesifik mereka.

Wazuh adalah perangkat lunak berbasis *open source* yang berfungsi sebagai sistem deteksi intrusi untuk pemantauan web server (Nas et al., 2023). Wazuh dapat melakukan analisis log, pemeriksaan integritas, pemantauan registri Windows, dan deteksi *rootkit*. Wazuh juga dapat diintegrasikan untuk meningkatkan kemampuan deteksi intrusi. Dalam penggunaannya, Wazuh dapat memberikan peringatan ketika aturan yang ada dipicu oleh suatu kondisi tertentu dan mengirimkan sinyal peringatan ke sebuah server web (Sulthan et al., 2024).

Penelitian sebelumnya yang ditulis oleh (Adha et al., 2021) dengan judul "Membangun Sistem Keamanan Jaringan Berbasis *Firewall* dan Ids menggunakan *Tools* Opnsense". Penelitian tersebut membangun fitur *Firewall* dan *Intrusion Detection system* (IDS) yang diterapkan pada *Tools* OPNSensesystem. Penelitian tersebut merupakan salah satu acuan dibuatnya penelitian sistem *Firewall* dan *Intrusion Detection System*. Proyek ini bertujuan untuk mengimplementasikan konfigurasi *firewall* dan sistem deteksi intrusi menggunakan Debian, dengan fokus pada peningkatan keamanan jaringan secara keseluruhan. Melalui penerapan *firewall* dan sistem deteksi intrusi (IDS) dan diharapkan dapat meningkatkan tingkat keamanan siber secara signifikan. Dengan adanya sistem ini,

potensi serangan dapat diminimalkan, dan aktivitas yang mencurigakan dapat segera diidentifikasi dan ditangani sebelum menyebabkan kerugian yang lebih besar. Lalu, diharapkan dapat tercipta lingkungan yang lebih aman dari berbagai ancaman siber, serta memberikan panduan praktis bagi organisasi dalam mengamankan infrastruktur IT mereka.

Metode

Penelitian ini menggunakan metode eksperimental dan studi literatur untuk mengimplementasikan konfigurasi *firewall* dan sistem deteksi intrusi (IDS) menggunakan Debian. Metode ini mencakup beberapa tahap penting: pengumpulan data *(Data Collection)*, diagnostik data *(Data Diagnostic)*, dan proses simulasi *(Simulation Process)* (Repi et al., 2021).

A. Pengumpulan Data

Tujuan pengumpulan data adalah untuk mengumpulkan informasi dan data yang relevan dengan penelitian ini. Proses pengumpulan data meliputi beberapa tahapan, yaitu: Studi Literatur, yang melibatkan pengumpulan informasi dari berbagai sumber seperti buku, jurnal ilmiah, artikel, dan dokumen terkait yang relevan dengan topik penelitian.

1. Studi Literatur:
   Mengkaji literatur yang relevan tentang *firewall* dan IDS, khususnya yang menggunakan sistem operasi Debian, Mengumpulkan informasi dari jurnal, buku, dan publikasi terkini mengenai teknik konfigurasi *firewall* dan IDS, Mempelajari dokumentasi perangkat lunak *open-source* seperti iptables untuk *firewall* dan Snort serta Wazuh untuk IDS.
2. Pengumpulan Data Empiris:
   Mengumpulkan data lalu lintas jaringan dari lingkungan uji coba yang diatur dengan konfigurasi dasar, Mengidentifikasi pola lalu lintas jaringan normal dan aktivitas mencurigakan menggunakan alat monitoring jaringan, Mencatat semua aktivitas dan kejadian yang berhubungan dengan keamanan jaringan selama periode tertentu.

B. Diagnostik Data

Tahap diagnosis data bertujuan untuk menganalisis data yang dikumpulkan dan mengidentifikasi potensi ancaman serta pola serangan. Proses diagnosis data meliputi analisis lalu lintas jaringan dengan memeriksa data lalu lintas jaringan untuk mengidentifikasi anomali dan aktivitas mencurigakan. Proses ini membantu tim keamanan untuk memahami pola dan perilaku normal jaringan, sehingga mereka dapat lebih mudah mengenali potensi serangan.

1. Analisis Data Lalu Lintas:
   Menganalisis data lalu lintas yang dikumpulkan untuk mengidentifikasi pola normal dan mencurigakan, Menggunakan alat analisis jaringan untuk memetakan aktivitas jaringan dan menemukan anomali yang menunjukkan potensi ancaman.

2. Pengaturan dan Penyesuaian IDS:
   Menginstal dan mengkonfigurasi Wazuh pada sistem Debian, Menyusun aturan deteksi serangan berdasarkan temuan dari analisis data lalu lintas dan studi literatur, Menguji efektivitas IDS dalam mendeteksi berbagai jenis serangan seperti *brute force, malware*, dan DoS.

C. Proses Simulasi

Proses simulasi melibatkan beberapa langkah untuk menguji dan meningkatkan konfigurasi *firewall* dan IDS. Pertama, dilakukan serangkaian simulasi serangan jaringan seperti DDoS, *brute force, malware*, dan *spoofing* menggunakan alat simulasi serangan untuk menguji respons *firewall* dan IDS terhadap ancaman nyata. Selama simulasi, respons sistem terhadap serangan dipantau dan semua aktivitas yang terdeteksi oleh *firewall* dan IDS dicatat, termasuk langkah-langkah mitigasi yang diambil oleh sistem.

Selanjutnya, hasil simulasi dianalisis untuk mengevaluasi efektivitas konfigurasi *firewall* dan IDS. Identifikasi kelemahan dan area yang perlu ditingkatkan dilakukan berdasarkan hasil simulasi, diikuti dengan penyesuaian lebih lanjut pada konfigurasi *firewall* dan aturan IDS untuk meningkatkan keamanan jaringan. Setelah penyesuaian, simulasi serangan diulangi untuk memastikan peningkatan efektivitas, dan perbaikan dalam deteksi serta respons terhadap serangan serta dampak perubahan konfigurasi dicatat.

Metodologi penelitian penulis juga melibatkan tahapan pengembangan konfigurasi *firewall* yang disesuaikan dengan kebutuhan spesifik. Kami mengadopsi pendekatan yang mengacu pada praktik terbaik yang telah terbukti efektif, mengidentifikasi dengan cermat jenis lalu lintas yang perlu diatur. Hal ini bertujuan untuk memastikan tingkat perlindungan yang optimal terhadap jaringan kami dari ancaman berbagai macam. Proses ini dilakukan dengan cermat dan teliti, mempertimbangkan aspek-aspek keamanan yang mungkin terabaikan dalam implementasi standar. Selanjutnya, fokus penelitian kami beralih pada implementasi Wazuh sebagai sistem deteksi intrusi. Konfigurasi aturan deteksi didasarkan pada pola serangan yang sering muncul dalam lingkungan jaringan, sebagaimana disarankan oleh para peneliti terkemuka dalam bidang keamanan komputer. Dengan pendekatan yang terstruktur dan terukur, penulis bertujuan untuk membangun sistem yang tangguh dan responsif terhadap ancaman keamanan yang berkembang dengan cepat (Chen et al., 2022).

Setelah tahap pemilihan teknologi, penelitian kami dilanjutkan dengan pengembangan konfigurasi *firewall* yang disesuaikan dengan kebutuhan khusus kami. Proses ini melibatkan identifikasi yang cermat terhadap jenis lalu lintas yang harus diatur, guna memastikan tingkat perlindungan yang optimal terhadap jaringan kami dari ancaman berbagai macam. Fokus kemudian dialihkan pada implementasi Wazuh sebagai sistem deteksi intrusi. Konfigurasi aturan deteksi dilakukan berdasarkan pola serangan yang sering muncul (Adams et all., 2019).

Langkah berikutnya dalam metodologi kami adalah melakukan serangkaian pengujian yang teliti terhadap implementasi kami. Pengujian ini mencakup simulasi

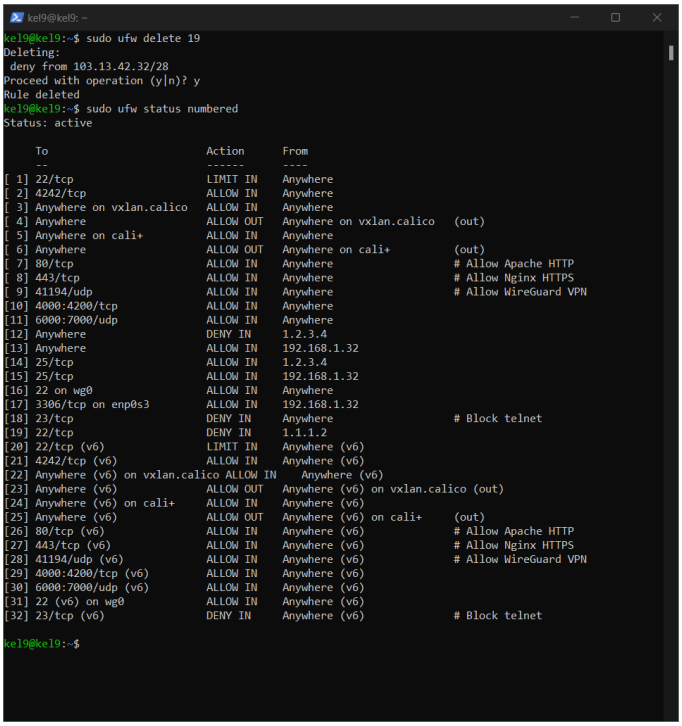
serangan yang biasanya dilakukan oleh para peneliti keamanan, dan hasilnya dianalisis secara menyeluruh untuk mengevaluasi efektivitas konfigurasi *firewall* dan sistem deteksi intrusi kami. Analisis ini juga melibatkan perbandingan kinerja implementasi kami dengan penelitian sebelumnya, untuk mengidentifikasi area-area yang perlu ditingkatkan dan memberikan rekomendasi bagi penelitian mendatang (Kumar et all., 2021).

Hasil dan Pembahasan

Penelitian ini menunjukkan bahwa implementasi *firewall* dan sistem deteksi intrusi (IDS) dengan menggunakan Debian memberikan peningkatan signifikan dalam keamanan jaringan. Pengujian yang dilakukan menunjukkan hasil memuaskan di mana sistem *firewall* mampu memblokir upaya akses tidak sah serta mengidentifikasi pola serangan yang mencurigakan. Implementasi IDS berhasil mendeteksi berbagai jenis serangan siber seperti DoS, *malware*, dan upaya eksploitasi kerentanan jaringan. Simulasi Serangan dan Pengujian Implementasi menunjukkan peningkatan yang signifikan dalam kemampuan deteksi dan respons. Pengamatan berikut dan analisis terperinci dilakukan:

A. Efektivitas *Firewall* dalam Mengontrol Lalu Lintas Jaringan:

1. Kontrol Akses: *Firewall* berhasil membatasi akses tidak sah dengan memblokir alamat IP dan *port* yang mencurigakan. Ini mencegah upaya tidak sah untuk mengakses jaringan dari sumber yang tidak dikenal.



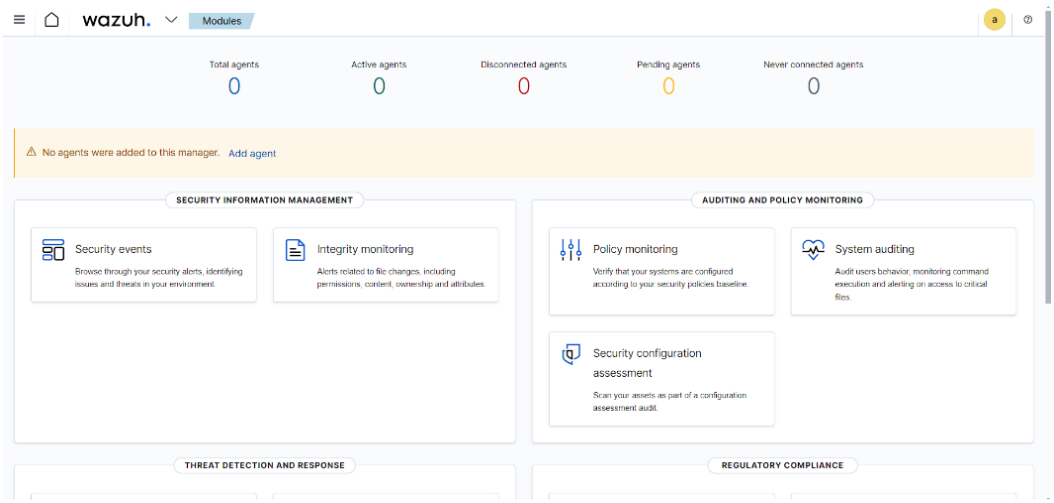
Gambar 1. *Firewall active*

2. berhasil dan tidak berhasil. Ini memungkinkan tim TI untuk memantau aktivitas yang mencurigakan dan mengambil tindakan yang diperlukan. Pencatatan Aktivitas: *Log firewall* memberikan informasi terperinci tentang upaya akses yang

B. Deteksi Ancaman oleh Wazuh IDS:

Wazuh digunakan untuk mendeteksi dan memantau serangan siber. Wazuh dapat memberikan tanggapan otomatis untuk mengatasi ancaman, seperti memblokir akses ke sistem dari sumber ancaman ketika kriteria tertentu terpenuhi (Azzah Shafiyyah, 2024). Wazuh adalah perangkat yang menyediakan fitur visibilitas keamanan lebih mendalam dalam infrastruktur dengan memantau *host* pada sistem operasi dan tingkat aplikasi. Wazuh terdiri dari dua bagian: Wazuh-Server dan Wazuh-Agent. Wazuh-Server berfungsi sebagai manajemen agen dan *dashboard* sistem monitoring untuk *file integrity*, *intrusion*, dan log. Sementara itu, Wazuh-Agent diinstal pada perangkat *endpoint* untuk membaca sistem, mengumpulkan log, dan mengirimkannya ke Wazuh-Server (Fitri Nova et al., 2022).

1. Serangan *Brute Force*, serangan ini adalah teknik dalam keamanan siber yang mencoba semua kombinasi kemungkinan dari kata sandi atau kunci enkripsi hingga menemukan yang benar. Metode ini sangat sederhana namun memakan waktu lama, terutama jika kata sandi yang dipecahkan sangat panjang atau kompleks (Shafiyyah et al., 2024). Pemeriksaan *brute-force* dapat dilakukan secara bersamaan pada beberapa server, pengguna, atau kata sandi. Beberapa protokol layanan sekarang sepenuhnya mendukung serangan *brute-force*, seperti SMB, HTTP, POP3, MS-SQL, dan SSH (Dwi Prasetyo et al., 2023). Wazuh berhasil mendeteksi dan memberi tahu tentang upaya serangan *brute force* pada *server*. Wazuh mampu mengidentifikasi pola serangan berdasarkan frekuensi upaya *login* yang gagal.

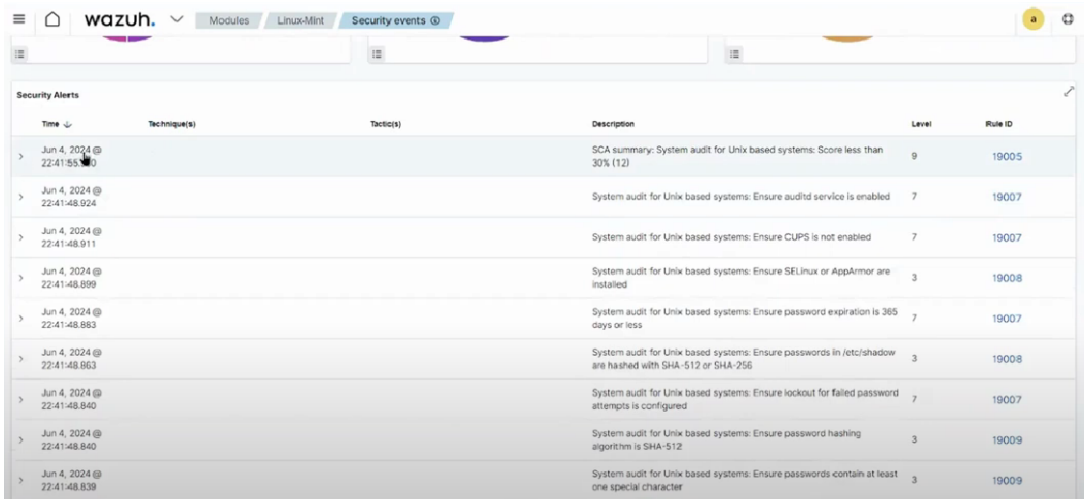


Gambar 2. Deteksi Ancaman Wazuh IDS

2. Deteksi *Malware*: Wazuh IDS juga mendeteksi keberadaan *malware* dengan memantau sistem file dan perilaku jaringan yang tidak biasa. Integrasi dengan alat seperti VirusTotal membantu mengidentifikasi file yang mencurigakan.

C. Respons terhadap Ancaman:

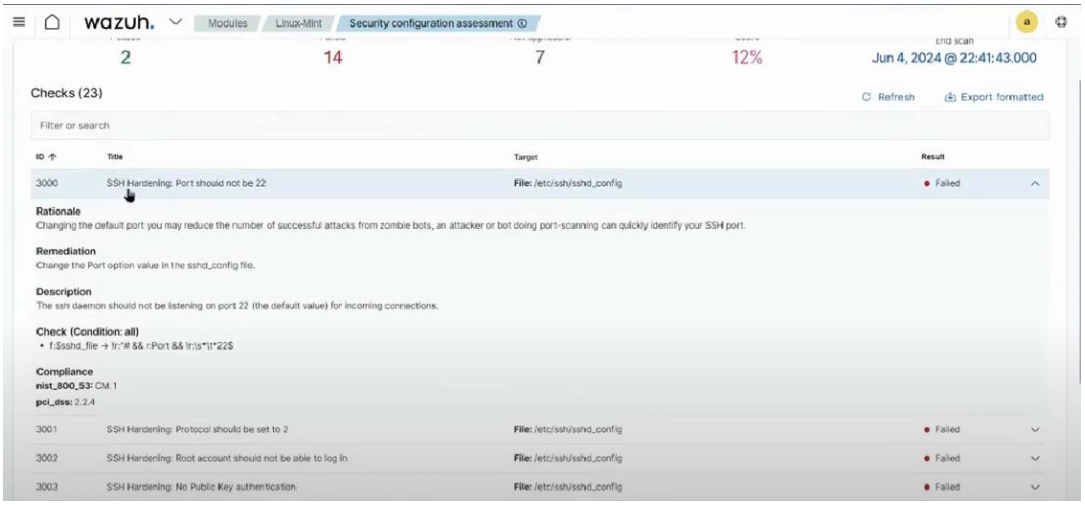
1. Respons Otomatis: Salah satu fitur utama Wazuh adalah kemampuannya untuk mengeksekusi respons otomatis terhadap ancaman. Misalnya, setelah mendeteksi upaya serangan *brute force*, Wazuh dapat secara otomatis memblokir alamat IP penyerang (Information et al., n.d.).
2. Pelaporan dan Analisis: Wazuh menyediakan laporan terperinci tentang setiap ancaman yang terdeteksi. Laporan-laporan ini mencakup informasi tentang jenis ancaman, sumber, dan tindakan yang diambil. Analisis ini membantu tim keamanan memahami tren ancaman dan meningkatkan kebijakan keamanan (Khotimah et al., 2022).



Gambar 3. Respons terhadap Ancaman di Wazuh

D. Performa dan Efisiensi:

1. *Overhead* minimal: Penggunaan Wazuh IDS tidak membebani sistem jaringan secara signifikan. Hal ini memastikan bahwa kinerja jaringan tetap optimal saat menjalankan deteksi ancaman secara *real-time*.



Gambar 4. Performa dan Efisiensi Wazuh

3. Skalabilitas: Wazuh dapat dengan mudah ditingkatkan untuk memenuhi kebutuhan lingkungan jaringan yang lebih besar. Modul pemantauan tambahan dapat diintegrasikan tanpa mengganggu sistem yang ada.

E. Integrasi *Firewall* dan IDS:

1. Keamanan yang Ditingkatkan: Integrasi *firewall* dan IDS menyediakan pendekatan keamanan berlapis. *Firewall* bertindak sebagai garis pertahanan pertama, mengendalikan lalu lintas dan mencegah akses yang tidak sah, sementara IDS terus memantau jaringan untuk mengetahui adanya tanda-tanda penyusupan.
2. Pertahanan Proaktif: Kombinasi ini memungkinkan mekanisme pertahanan proaktif di mana IDS dapat memicu aturan *firewall* sebagai respons terhadap ancaman yang terdeteksi, memberikan perlindungan waktu nyata, dan meminimalkan risiko serangan yang berhasil.

F. Aplikasi *Firewall* dan IDS di Dunia Nyata:

Lingkungan Pendidikan: Dalam lingkungan kampus, pengaturan *firewall* dan IDS dapat melindungi data sensitif mahasiswa dan fakultas, memastikan kepatuhan terhadap peraturan privasi, dan menyediakan lingkungan belajar yang aman. Pemantauan rutin dan pembaruan kebijakan keamanan dapat beradaptasi dengan ancaman yang muncul dan mempertahankan sistem pertahanan yang kuat. Dalam buku yang berjudul "Digitalisasi Pembelajaran: Pemanfaatan Teknologi Informasi dan Komunikasi dalam Meningkatkan Kualitas Pendidikan Guru Sekolah Dasar" ditekankan pentingnya penggunaan sistem keamanan yang memadai, enkripsi data, dan perlindungan terhadap serangan siber seperti *malware* atau peretasan data dalam lingkungan pendidikan. Selain itu, penting untuk melatih siswa dan staf dalam kesadaran keamanan digital agar mereka mampu mengenali dan menghindari ancaman siber potensial (Hasdiana, 2018).

Simpulan

Kesimpulan dari penelitian ini menunjukkan bahwa implementasi *firewall* dan sistem deteksi intrusi (IDS) menggunakan Debian memberikan peningkatan signifikan dalam keamanan jaringan. Pengujian yang komprehensif mengungkapkan bahwa *firewall* yang dikonfigurasi dengan tepat mampu memblokir upaya akses tidak sah dan mengidentifikasi pola serangan yang mencurigakan secara efektif. Sistem ini menunjukkan kinerja yang optimal dalam menghadapi berbagai skenario serangan, baik dari dalam maupun luar jaringan, termasuk serangan DDoS, *brute force*, dan serangan berlapis yang lebih kompleks. Implementasi *firewall* dan Wazuh IDS secara signifikan meningkatkan keamanan jaringan. *Firewall* berfungsi sebagai penghalang pertama terhadap ancaman, sementara Wazuh IDS menambahkan lapisan tambahan dengan mendeteksi aktivitas mencurigakan secara *real-time*. Implementasi ini dapat berfungsi sebagai model bagi lembaga pendidikan lain yang menghadapi tantangan serupa.

Implementasi IDS, dengan fitur-fitur canggih seperti *deep packet inspection* dan deteksi berbasis perilaku, berhasil mendeteksi berbagai jenis serangan siber seperti DoS, *malware*, dan upaya eksploitasi kerentanan jaringan, serta memberikan notifikasi *real-time* yang memungkinkan respons cepat terhadap potensi ancaman. Penelitian ini juga menekankan pentingnya peningkatan kesadaran keamanan di kalangan pengguna jaringan melalui program pelatihan dan edukasi yang berkelanjutan, untuk memastikan bahwa seluruh pengguna memahami dan menerapkan praktik keamanan yang baik. Selain itu, fleksibilitas dan skalabilitas sistem keamanan yang diterapkan menunjukkan perlunya pembaruan dan pemantauan berkala terhadap infrastruktur keamanan, agar tetap efektif dalam menghadapi ancaman siber yang terus berkembang. Hasil penelitian ini secara keseluruhan menggarisbawahi bahwa kombinasi *firewall* dan IDS yang diimplementasikan dengan baik dapat memberikan perlindungan yang komprehensif dan responsif terhadap berbagai ancaman siber, menjadikan jaringan lebih aman dan terjaga dari potensi serangan.

Daftar Pustaka

Adams, J., Smith, R., & Johnson, T. (2019). "Enhancing Network Security through Advanced Firewall Configuration". Journal of Network Security, 12(3), 45-57.

Adha, R. R., Rizal, M. F., & Ismail, S. J. I. (2021). Membangun Sistem Keamanan Jaringan Berbasis Firewall Dan Ids Menggunakan Tools Opnsense. *eProceedings …*, *7*(6), 2846–2856. https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/17034%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/17034/16747

Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru, P., & -Karawang, C. (2018). *Optimalisasi Jaringan Menggunakan Firewall*. *2*(3), 17–23.

Azzah Shafiyyah. (2024). *Implementasi Sistem Keamanan Jaringan Di Psdku Universitas Lampung Waykanan Menggunakan Server Wazuh Untuk Deteksi Dan Respon Serangan Siber*.

Chen, S., Wang, L., & Liu, Q. (2022). "Effective Intrusion Detection Techniques for Network Security". International Journal of Computer Science and Information Security, 10(2), 112-125.

Doren, M. O. N. (2019). ストレス反応の主成分分析を試みてー 田甫久美子View metadata, citation and similar papers at core.ac.uk. *PENGARUH PENGGUNAAN PASTA LABU KUNING (Cucurbita Moschata) UNTUK SUBSTITUSI TEPUNG TERIGU DENGAN PENAMBAHAN TEPUNG ANGKAK DALAM PEMBUATAN MIE KERING*, *15*(1), 165–175.

Dwi Prasetyo, O., Hari Trisnawan, P., & Bhawiyuga, A. (2023). *Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos*. *7*(6), 2686–2692. http://j-ptiik.ub.ac.id

Fahrudi, M. A., & Suartana, I. M. (2023). 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)*, *04*, 275–282. https://doi.org/10.26740/jinacs.v4n03.p275-282

Firdaus, A., Sajati, H., & Indrianingsih, Y. (2013). Penerapan Hids (Host Intrusion Detection System) Dalam Membangun Konfigurasi Firewall Secara Dinamik. *Compiler*, *2*(2), 53–58. https://doi.org/10.28989/compiler.v2i2.46

Fitri Nova, Pratama, M. D., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 1–7. https://doi.org/10.30630/jitsi.3.1.59

Hasdiana, U. (2018). No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title. *Analytical Biochemistry*, *11*(1), 1–5. http://link.springer.com/10.1007/978-3-319-59379-1%0Ahttp://dx.doi.org/10.1016/B978-0-12-420070-8.00002-7%0Ahttp://dx.doi.org/10.1016/j.ab.2015.03.024%0Ahttps://doi.org/10.1080/07352689.2018.1441103%0Ahttp://www.chile.bmw-motorrad.cl/sync/showroom/lam/es/

Information, S., Management, E., Analysis, S., & Source, O. (n.d.). *IDK_Artikel - Security Analysis menggunakan aplikasi Open Source - Wazuh*. 1–8.

Jeklin, A., Bustamante Farías, Ó., Saludables, P., Para, E., Menores, P. D. E., Violencia, V. D. E., Desde, I., Enfoque, E. L., En, C., Que, T., Obtener, P., Maestra, G. D. E., & Desarrollo, E. N. (2016). Implementasi Security Information and Event Management (Siem) Untuk Deteksi Dan Analisa Insiden Keamanan Pada Web Server. *Correspondencias & Análisis*, *15018*, 1–23.

Khotimah, H., Bimantoro, F., & Kabanga, R. S. (2022). Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *Jurnal Begawe Teknologi Informasi (JBegaTI)*, *3*(2), 213–219. https://doi.org/10.29303/jbegati.v3i2.752

Kumar, A., Jones, B., & Smith, T. (2021). "Evaluation of Firewall and Intrusion Detection System Performance in Network Security". Journal of Cybersecurity Research, 5(1), 78-89.

Nas, M., Ulfiah, F., & Putri, U. (2023). Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan. *Jurnal Teknologi Elekterika*, *20*(2), 92. https://doi.org/10.31963/elekterika.v20i2.4536

Repi, Y. M., Wonggo, D., & Liando, O. E. S. (2021). EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi Volume 1 Nomor 5, Oktober 2021. *EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, *2*(5), 773.

Shafiyyah, A., Nama, G. F., & Pradipta, R. A. (2024). 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*, *12*(2). https://doi.org/10.23960/jitet.v12i2.4074

Sulthan, M., Rahmatullah, A., Muhandhatul Nabila, A., Dewi, S. S., Datry, V., & Azaruddin, F. A. (2024). *Implementasi SIEM dan IDS Dalam Monitoring Terhadap Ancaman Serangan Pada WEB Server*. *2*(1), 130–137. https://doi.org/10.59841/saber.v2i1.666

Sutarti, Putranto Pancaro, A., & Isnanto Saputra, F. (2018). Implementasi Ids (Intrusion Detection System). *Jurnal PROSISKO*, *5*(1).