IMPLEMENTASI DETEKSI ANOMALI DAN RESPON AKTIF MENGGUNAKAN WAZUH SIEM UNTUK PENCEGAHAN SERANGAN SIBER BERDASARKAN *ACCESS LOG* PADA *WEB SERVER APACHE*

TUGAS AKHIR

SETIAWAN

NIM 20106050060

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2024

HALAMAN PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1461/Un.02/DST/PP.00.9/08/2024

Tugas Akhir dengan judul : IMPLEMENTASI DETEKSI ANOMALI DAN RESPON AKTIF MENGGUNAKAN WAZUH SIEM UNTUK PENCEGAHAN SERANGAN SIBER BERDASARKAN LOG ACCESS PADA WEB SERVER APACHE

yang dipersiapkan dan disusun oleh:

Nama : SETIAWAN
Nomor Induk Mahasiswa : 20106050060
Telah diujikan pada : Rabu, 31 Juli 2024
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 66bf0b6fa6cf1

Penguji I

Ir. Muhammad Taufiq Nuruzzaman, S.T., M.Eng., Ph.D.
SIGNED

Valid ID: 66bf07b4b054e

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 66befd464d26a

Yogyakarta, 31 Juli 2024
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 66c2c027ce4db

SURAT PERNYATAAN KEASLIAN

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama : Setiawan
NIM : 20106050060
Program Studi : Informatika
Fakultas : Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 24 Juli 2024

Setiawan

NIM. 20106050060

SURAT PERSETUJUAN TUGAS AKHIR

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Setiawan
NIM : 20106050060
Judul Skripsi : Implementasi Deteksi Anomali Dan Respon Aktif Menggunakan Wazuh Siem Untuk Pencegahan Serangan Siber Berdasarkan *Access Log* Pada *Web Server Apache*

sudah dapat diajukan kembali kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Matematika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 24 Juli 2024

Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM.
NIP. 197510242009121002

LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.

ABSTRAK

Web server apache, sebagai salah satu *server* yang paling banyak digunakan, sering menjadi target serangan siber seperti *XSS, SQL injection*, dan *DoS*. Meskipun penting untuk melindungi *server* ini, Apache tidak memiliki kemampuan bawaan untuk mendeteksi dan merespons anomali lalu lintas data secara otomatis. Penelitian ini bertujuan untuk mengimplementasikan sistem deteksi anomali dan respon aktif pada *web server apache* dengan menggunakan *Wazuh* sebagai solusi SIEM *open-source*.

Metode yang digunakan dalam penelitian ini melibatkan pembuatan dan pengujian dummy *website* berbasis Apache yang dihosting dalam lingkungan virtual menggunakan Proxmox. Berbagai jenis serangan, termasuk *DoS*, *XSS*, dan *SQL injection* dilakukan untuk mengevaluasi efektivitas deteksi dan pemblokiran oleh sistem yang telah diimplementasikan. Proses ini mencakup analisis, desain, simulasi, implementasi, dan monitoring sistem.

Hasil penelitian menunjukkan bahwa *Wazuh* berhasil mendeteksi berbagai serangan, memberikan alert yang rinci, dan memblokir penyerang secara otomatis. Penelitian ini menyajikan model sistem yang tidak hanya melindungi dari serangan siber tetapi juga menyediakan alat analisis yang komprehensif untuk meningkatkan keamanan *web server*. Dengan demikian, pendekatan ini menawarkan solusi yang lebih kuat dalam menjaga keamanan dan meningkatkan ketahanan sistem terhadap ancaman siber.

Kata Kunci: Deteksi Anomali, Respon Aktif, *Wazuh* SIEM, *Web server apache*

ABSTRACT

Apache web server, one of the most widely used servers, is frequently targeted by cyberattacks such as XSS, SQL injection, and DoS. Despite its critical role, Apache lacks built-in capabilities to automatically detect and respond to traffic anomalies. This research aims to implement an anomaly detection and active response system on the Apache web server using Wazuh as an open-source SIEM solution.

The methodology used in this study involves creating and testing a dummy website based on Apache, hosted in a virtual environment using Proxmox. Various types of attacks, including DoS, XSS, and SQL injection, are performed to evaluate the effectiveness of the implemented detection and blocking system. This process includes analysis, design, simulation, implementation, and system monitoring.

The results indicate that Wazuh successfully detects various attacks, provides detailed alerts, and automatically blocks attackers. This research presents a model system that not only protects against cyberattacks but also offers a comprehensive analysis tool to enhance web server security. Thus, this approach provides a robust solution for safeguarding and improving system resilience against cyber threats.

Keywords: Anomaly Detection, Active Response, Wazuh SIEM, Apache Web server

PERSEMBAHAN

Karya ini dipersembahkan untuk:

Kedua orang tua penulis

Ayahanda Sulur

Ibunda Wagiyem

Keempat kakak ku

Sri Lestari

Yuliati

Hardi Wiyono

Jianto

KATA PENGANTAR

Penulis mengucapkan puji dan syukur kepada Allah Swt. karena telah melimpahkan berkah dan nikmat yang tidak terhingga, sehingga tugas akhir "Implementasi Deteksi Anomali Dan Respon Aktif Menggunakan Wazuh Siem Untuk Pencegahan Serangan Siber Berdasarkan Acess Log Pada Web Server Apache" dapat diselesaikan. Tugas akhir ini juga dapat diselesaikan atas bantuan berbagai pihak. Untuk itu penulis ingin menyampaikan terima kasih kepada semua pihak yang berjasa berikut ini.

1. Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., selaku dosen pembimbing skripsi yang selalu bersedia meluangkan waktu untuk memberikan arahan, bimbingan, dan motivasi untuk menyelesaikan dan menyempurnakan penulisan tugas akhir ini;

2. Mandahadi Kusuma, M.Eng., selaku dosen pembimbing akademik yang senantiasa membantu dan mengarahkan penulis selama berada di bangku perkuliahan;

3. Bapak dan Ibu dosen pada Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta, yang telah memberikan banyak ilmu;

4. Ibunda Wagiyem, yang selalu memberi dukungan dan do'a serta dorongan agar tugas akhir ini cepat terselesaikan;

5. Ayahanda Sulur, yang tidak pernah berhenti berdo'a untuk kebaikan anaknya walau tidak pernah ditunjukkan;

6. Kakak-kakak ku, Sri Lestari, Yuliati, Hardi Wiyono, dan Jianto yang senantiasa memberi dorongan agar tugas akhir ini cepat selesai;

8. Winy Devi Rahayu, kekasih yang tidak pernah berhenti menyemangati dan tidak lelah menemani;

9. Sahabat yang tergabung di dalam koalisi tronjal tronjol, Satria, Tegar, Fajar, Bintang, dan Ammar yang tidak lelah membersamai, menyangati, dan memotivasi;

Akhirnya, besar harapan penulis agar tugas akhir ini dapat memberikan kontribusi positif dalam kajian ilmu informatika. Penulis menyadari banyak kekurangan yang terdapat di dalam tugas akhir ini. Oleh sebab itu, penulis menerima kritik dan saran yang membangun sebagai upaya perbaikan dan pengembangan ke arah yang lebih baik.

Yogyakarta, 24 Juli 2024

Setiawan

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang cepat saat ini telah mengubah banyak aspek dalam masyarakat secara signifikan. Ketersediaan koneksi internet yang semakin meningkat memungkinkan berbagai tujuan dapat dengan mudah dikomunikasikan[1]. Salah satu contoh pemanfaatan internet adalah penggunaan *web server* pada aplikasi web untuk bertukar data, menawarkan layanan, dan menyimpan data[2]. Aplikasi web atau *website* adalah teknologi yang umum digunakan dalam bisnis, pemerintahan, pendidikan, dan berbagai bidang lainnya. *Website* adalah lokasi online yang menyediakan sumber data seperti teks, gambar, audio, dan animasi yang dikirim melalui protokol transfer hiperteks (HTTP) dari *web server*[3]. Aplikasi *website* merupakan teknologi yang masif digunakan saat ini. Apache adalah salah satu *web server* dengan market share terbesar di dunia, mencapai 31,4%[4].

Namun, penggunaan Apache sebagai *web server* yang luas menjadikannya target utama serangan siber, terutama untuk pencurian data dan gangguan sistem, sehingga meningkatkan risiko keamanan bagi website berbasis Apache[3]. Serangan siber yang umum, seperti *cross-site scripting* (XSS), paparan data sensitif, *SQL injection*, dan otentikasi yang buruk, menjadi ancaman serius bagi keamanan website[5]. Menurut OWASP, sepuluh kerentanan paling umum pada website termasuk XSS, serangan DDoS, dan *SQL injection*[6]. Laporan bulanan BSSN untuk periode Januari hingga Agustus 2023 mencatat ribuan serangan eksploitasi dan serangan web yang menargetkan website di seluruh Indonesia setiap bulannya[7]. Serangan ini berpotensi menyebabkan kerugian besar, termasuk pencurian dan kehilangan data, kerusakan sistem, dan penyalahgunaan informasi[8]. Pada skala perusahaan, dampaknya bisa lebih luas, mengakibatkan kerugian finansial, gangguan operasional, serta penurunan reputasi dan kepercayaan pengguna, yang dapat berdampak jangka panjang[9].

Risiko keamanan siber yang meningkat dalam beberapa tahun terakhir memunculkan tantangan baru untuk melakukan deteksi dan pencegahan dini. Untuk mencegah lebih banyak kerugian, organisasi harus membatasi ancaman serangan siber dengan mengambil langkah-langkah pencegahan dan reaksi. Deteksi anomali dan manajemen serangan siber perlu diupayakan sebagai solusi keamanan siber[10]. Deteksi anomali adalah proses analisis terhadap data yang signifikan pada sistem, bertujuan untuk mengidentifikasi data yang tidak berada dalam kondisi normal. Tujuannya adalah membantu mengatasi permasalahan keamanan sistem dengan menemukan pola atau perilaku yang tidak biasa[11]. Deteksi anomali bisa menjadi lebih efektif ketika terdapat respon aktif terhadap anomali tersebut. Respon aktif merupakan proses di mana sistem mampu mengaktifkan pertahanan untuk mencegah adanya serangan lebih lanjut[12].

Insiden berbahaya sering kali teridentifikasi melalui analisis log, tetapi untuk serangan yang lebih kompleks, hanya menganalisis log mungkin tidak cukup untuk mendeteksi insiden tersebut. Hal yang sama berlaku ketika seorang administrator sistem mengabaikan analisis log pada sistem[13]. Untuk menanggulangi masalah sejenis, diperlukan sebuah sistem deteksi serangan yang secara langsung mampu memberi informasi mengenai kondisi *server* ketika serangan terjadi. Hal ini bertujuan agar administrator dapat segera dan secara efisien mengambil tindakan pencegahan guna melindungi perangkat *server*[14]. Solusi keamanan dalam sistem kontrol *website* harus menggabungkan deteksi anomali perilaku secara *real-time*, memfasilitasi manajemen insiden yang cepat, dan menawarkan visualisasi cerdas dari jaringan bersama dengan simpul-simpul yang saling terhubung. SIEM (*Security Information* and *Event Management*) memandang kemampuan ini sebagai fitur integral[10]. Namun, *web server apache* pada dasarnya tidak memiliki kemampuan atau fitur khusus yang berfungsi untuk mendeteksi kejadian yang tidak biasa.

Berangkat dari kekurangan *web server apache* tersebut, *Security Information* and *Event Management* (SIEM) dapat menjadi solusi dari permasalahan keamanan siber yang telah disebutkan. SIEM adalah sistem pemantauan dan analisis keamanan yang beroperasi secara *real-time* melalui pembacaan terhadap riwayat log, dengan tujuan menghimpun berbagai aktivitas log dari sistem host untuk mendeteksi potensi serangan pada sistem host[10]. SIEM dapat melakukan visualisasi data log yang kemudian bisa difungsikan untuk monitoring secara langsung guna kebutuhan deteksi dan manajemen serangan siber[15]. *Wazuh Security Information* and *Event Management* (SIEM) adalah platform sentral yang memungkinkan deteksi dan kepatuhan melalui agregasi dan analisis telemetri secara *real-time*. Untuk cakupan keamanan yang lebih luas, *Wazuh* mengumpulkan data peristiwa dari berbagai sumber termasuk *acess log web server apache*[16]. *Wazuh* adalah platform SIEM *open-source* yang digunakan untuk deteksi ancaman dan manajemen informasi keamanan. *Wazuh* dipilih karena memiliki berbagai *rules* atau peraturan yang memungkinkan deteksi serangan siber seperti *DoS* (*Denial of service*s), *cross-site scripting* (*XSS*), dan *SQL injection*.

Penelitian ini berbasis eksperimen di lingkungan virtual. Dummy *website* berbasis *web server apache* akan dipasang pada sebuah *virtual machine* dengan bantuan Proxmox virtual environment. *Penetration testing* menjadi pilihan dalam proses pengujian karena relevan dalam menghasilkan log serangan yang bisa dianalisis. Dari hasil uji coba, diharapkan penelitian ini dapat memberikan gambaran pentingnya proses deteksi terhadap anomali yang muncul dalam aktivitas *server website*.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, ditemukan bahwa *web server apache* memiliki kekurangan signifikan, yakni tidak memiliki kemampuan untuk mendeteksi anomali yang terjadi selama lalu lintas data berjalan serta memberikan respon langsung terhadap anomali tersebut. Kekurangan ini mendasari rumusan masalah utama dalam penelitian ini, yaitu

mengimplementasikan proses deteksi terhadap anomali yang terjadi pada *web server apache* serta penerapan respon langsung terhadap insiden menggunakan alat *Wazuh* SIEM.

1.3. Batasan Masalah

Penelitian ini menambahkan beberapa batasan masalah agar fokus penelitian tidak bergeser dan tidak menyebar. Beberapa batasan masalah yang ditambahkan adalah sebagai berikut:

1.3.1. Aplikasi *web server* yang digunakan adalah Apache.
1.3.2. Menggunakan lingkungan *virtual machine* yang dibangun dalam *server* Proxmox.
1.3.3. Hasil yang difungsikan sebagai parameter adalah log serangan.
1.3.4. Serangan menggunakan konsep *penetration testing* berupa serangan *DoS*, *cross-site scripting* (*XSS*), dan *SQL injection*.
1.3.5. Penggunaan *Wazuh* SIEM untuk deteksi dan respon anomali.
1.3.6. Tidak mencakup pengujian serangan fisik atau non-siber.
1.3.7. Pengujian dilakukan dalam lingkungan tertutup dan terkontrol.
1.3.8. Integrasi dilakukan dengan teknologi *firewall* modsecurity.
1.3.9. Penggunaan alat iptables untuk DoS.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengimplementasikan sistem *web server apache* yang mampu mendeteksi anomali dan memberikan respon aktif dalam mencegah serangan siber. Diharapkan penelitian ini dapat menghasilkan model sistem yang tidak hanya memiliki kemampuan pertahanan terhadap serangan siber, tetapi juga dilengkapi dengan alat deteksi yang dapat menyediakan data untuk keperluan analisis di masa mendatang. Dengan demikian, sistem ini akan mampu memberikan perlindungan yang lebih komprehensif dan mendukung upaya peningkatan keamanan secara berkelanjutan.

1.5. Manfaat Penelitian

Hasil perancangan ini dapat dijadikan referensi untuk tindakan preventif terhadap serangan siber pada *web server*. Selain itu, penelitian ini memberikan gambaran mengenai pentingnya manajemen serangan melalui analisis log serangan pada *web server*, sehingga mendukung pengembangan strategi keamanan yang lebih efektif dan responsif.

BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan hasil perancangan dan pengujian yang telah dilakukan dalam penelitian dengan judul "IMPLEMENTASI DETEKSI ANOMALI MENGGUNAKAN *WAZUH* SEBAGAI SOLUSI SIEM BERDASARKAN *ACESS LOG* PADA *WEB SERVER APACHE*," dapat disimpulkan sebagai berikut:

1. Dengan implementasi *Wazuh*, log yang dihasilkan memiliki informasi yang lebih rinci dan disimpan dalam format JSON oleh *Wazuh* indexer. Hal ini memungkinkan log untuk diakses dan dianalisis dengan lebih mudah, meningkatkan efektivitas monitoring dan manajemen log secara keseluruhan.
2. *Wazuh* mampu mendeteksi berbagai jenis serangan, seperti *XSS*, *SQL injection*, dan *DoS*, dengan memanfaatkan *rules* yang telah dikonfigurasi pada *Wazuh manager*. Selain mendeteksi, sistem juga dapat melakukan pemblokiran otomatis terhadap sumber serangan melalui mekanisme respon aktif, meningkatkan keamanan sistem secara signifikan.
3. Dengan adanya fitur deteksi anomali, proses identifikasi serangan menjadi lebih mudah dan efisien. Sistem mampu memberikan deskripsi lengkap tentang setiap serangan yang terdeteksi, memungkinkan tim keamanan untuk memahami dan merespons ancaman dengan cepat. Ini mempermudah analisis dan pengambilan keputusan dalam menghadapi insiden keamanan.
4. Implementasi respon aktif membuat sistem lebih tahan terhadap percobaan serangan siber. Sistem dapat secara otomatis melakukan tindakan pertahanan tanpa harus menunggu respon manual dari manusia. Ini berarti bahwa ancaman dapat diatasi dengan segera, mengurangi risiko kerusakan lebih lanjut dan memastikan kontinuitas operasional yang lebih baik.

5. Sistem SIEM yang telah dibangun dengan menggunakan *Wazuh* memberikan kemudahan dalam proses analisis keamanan. Sistem ini mampu mengumpulkan, mengelola, dan menganalisis log dari berbagai sumber, memberikan wawasan yang mendalam tentang aktivitas jaringan dan potensi ancaman. Hal ini memfasilitasi analisis yang lebih komprehensif dan proaktif, memungkinkan organisasi untuk lebih siap menghadapi berbagai tantangan keamanan.
6. Implementasi modsecurity sebagai *firewall layer 7* menjadikan sistem mampu mencegah serangan *SQL injection* dan *XSS* yang berada di level aplikasi tanpa harus melakukan pemblokiran terhadap *ip address* penyerang dengan cara menolak parameter input yang mencurigakan. Log serangan juga masih bisa ditangkap oleh wazuh dan ditampilkan pada wazuh dashboard.
7. Alat iptables bisa digunakan untuk mencegah serangan *DoS* dengan cara membatasi koneksi TCP pada *port 80* dan menolak koneksi yang melebih batas yang telah ditentukan. Iptables sebagai alat bawaan linux tidak menjadikan wazuh kesulitan untuk menghasilkan alert dan menampilkan informasi serangan *DoS* dan wazuh dashboard.

5.2. Saran

Penelitian ini memiliki banyak sekali kekurangan yang masih bisa disempurnakan. Selain itu, potensi *wazuh* sebagai solusi SIEM masih sangat luas sehingga diperlukan pengembangan lebih lanjut untuk memanfaatkan semua potensi yang ada. Pengembangan lanjutan akan melahirkan solusi keamanan siber dengan level yang lebih tinggi. Berikut beberapa saran yang bisa penulis berikan.

1. *Wazuh* adalah platform *open-source* yang dapat diintegrasikan dengan berbagai teknologi keamanan lainnya. Penelitian selanjutnya diharapkan dapat mengeksplorasi kolaborasi *Wazuh* dengan solusi keamanan seperti intrusion *detection* systems (IDS), data loss prevention (DLP), atau

threat intelligence platforms. Integrasi ini akan membantu menciptakan sistem pertahanan yang lebih komprehensif dan kuat.

2. Selain untuk deteksi anomali, *Wazuh* memiliki banyak fitur lain yang bisa dimanfaatkan. Penelitian mendatang diharapkan dapat mengimplementasikan fitur-fitur seperti deteksi kerentanan, deteksi malware, dan deteksi virus. Pemanfaatan fitur-fitur ini akan memperluas kemampuan *Wazuh* dalam menghadapi berbagai jenis ancaman keamanan.
3. *Wazuh* tidak hanya terbatas pada monitoring Apache; platform ini juga dapat digunakan pada banyak objek teknologi lainnya. Penelitian berikutnya diharapkan dapat memanfaatkan *Wazuh* untuk objek teknologi lain seperti cloud, NAS, dan perangkat lainnya. Hal ini akan memperluas cakupan dan efektivitas *Wazuh* dalam berbagai lingkungan teknologi.

DAFTAR PUSTAKA

[1] D. T. Yuwono, "Analysis Performance Intrusion *Detection* System in Detecting Cyber-Attack on Apache *Web server*," *ITJRD*, pp. 169–178, Feb. 2022, doi: 10.25299/itjrd.2022.7853.

[2] 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*," *JINACS*, pp. 275–282, Jan. 2023, doi: 10.26740/jinacs.v4n03.p275-282.

[3] D. Priyawati, S. Rokhmah, and I. C. Utomo, "*Website* Vulnerability *Testing* and Analysis of Internet Management Information System Using OWASP," *International Journal*, vol. 03, no. 03, 2022.

[4] Yosia, "6 Rekomendasi *Web server* Paling Banyak Digunakan di 2021 | Blog Wowrack." Accessed: Jun. 22, 2024. [Online]. Available: https://www.wowrack.com/id-id/blog/cloud-id/6-rekomendasi-web-*server*-paling-banyak-digunakan-di-2021/

[5] G. Guntoro, L. Costaner, and M. Musfawati, "ANALISIS KEAMANAN *WEB SERVER* OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING)," *JIPI*, vol. 5, no. 1, p. 45, Jun. 2020, doi: 10.29100/jipi.v5i1.1565.

[6] O. OWASP Team, "OWASP Top 10:2021." Accessed: Nov. 27, 2023. [Online]. Available: https://owasp.org/Top10/

[7] T. BSSN, “Monitoring Keamanan Siber 2023 | www.bssn.go.id.” Accessed: Jun. 25, 2024. [Online]. Available: https://www.bssn.go.id/monitoring-keamanan-siber-2023/

[8] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, “MANAJEMEN KEAMANAN CYBER DI ERA DIGITAL,” *JoBE*, vol. 11, no. 1, p. 23, Jun. 2023, doi: 10.46273/jobe.v11i1.365.

[9] A. Nurain, R. A. G. Gultom, and R. E. Indrajit, “Manajemen Ketahanan Risiko Siber pada Internet of Things dan Cyber Physical System,” vol. 06, no. 02, 2024.

[10] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, “*Security Information* and *Event Management* (SIEM): Analysis, Trends, and Usage in Critical Infrastructures,” *Sensors*, vol. 21, no. 14, p. 4759, Jul. 2021, doi: 10.3390/s21144759.

[11] M. R. Kamal and M. A. Setiawan, “Deteksi Anomali dengan *Security Information* and *Event Management* (SIEM) Splunk pada Jaringan UII,” 2021.

[12] M. Danish, “Enhancing Cyber Security through Predictive Analytics: *Real-time* Threat *Detection* and *Response*,” 2024.

[13] Bojana Vilendečić, Ratko Dejanović, and Predrag Ćurić, “The Impact of Human Factors in the Implementation of SIEM Systems,” *JEE*, vol. 5, no. 4, Jul. 2017, doi: 10.17265/2328-2223/2017.04.004.

[14] H. D. Heluka and W. Sulistyo, “Perancangan Dan Implementasi *Security Information* and *Event Management* (SIEM) pada Layanan Virtual *Server*,” vol. 19, no. 2, 2023.

[15] A. R. Muhammad, P. Sukarno, and A. A. Wardana, “Integrated *Security Information* and *Event Management* (SIEM) with Intrusion *Detection* System (IDS) for Live Analysis based on Machine Learning,” *Procedia Computer Science*, vol. 217, pp. 1406–1415, 2023, doi: 10.1016/j.procs.2022.12.339.

[16] *Wazuh*, “SIEM,” *Wazuh*. Accessed: Jun. 28, 2024. [Online]. Available: https://*wazuh*.com/platform/siem/

[17] E. Stephani, Fitri Nova, and Ervan Asri, “Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion *Detection* System) Menggunakan Suricata Pada *Web server*,” *jitsi*, vol. 1, no. 2, pp. 67–74, Dec. 2020, doi: 10.30630/jitsi.1.2.10.

[18] A. Rahma, F. Indriyani, and T. A. A. Sandi, “Perancangan Dan Implementasi Monitoring Perangkat *Server* Menggunakan Zabbix Pada PT. Rizki Tujuh Belas Kelola,” *j-insan*, vol. 3, no. 2, pp. 85–95, Dec. 2023, doi: 10.31294/jinsan.v3i2.3009.

[19] F. C. Anam, G. M. A. Sasmita, and I. P. A. E. Pratama, “Implementation of *Security Information* and *Event Management* (SIEM) for Monitoring IT Assets Using Alienvault OSSIM (Case Study: Udayana University Information Resources Unit),” *jitter*, vol. 4, no. 3, p. 1956, Nov. 2023, doi: 10.24843/JTRTI.2023.v04.i03.p03.

[20] D. D. Lopez, M. B. Uribe, and C. S. Cely, “Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM - Díaz López - 2018 - Wireless Communications and Mobile Computing - Wiley Online Library.” Accessed: Jun. 30, 2024. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1155/2018/3029638

[21] “Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM),” *IJIES*, vol. 15, no. 6, pp. 667–681, Dec. 2022, doi: 10.22266/ijies2022.1231.59.

[22] W. Abidian and M. A. Setiawan, “Implementasi Splunk dalam Membangun *Security Information* and *Event Management* Berdasarkan Log *Firewall* (studi kasus: Jaringan UII),” 2021.

[23] M. F. Imran, “*CYBERSECURITY* STRATEGIES AND MEASURES HOAX IN THE DIGITALIZATION ERA,” *Dinamika Governance : Jurnal Ilmu Administrasi Negara*, vol. 14, no. 1/April, Art. no. 1/April, Jan. 2024, doi: 10.33005/jdg.v14i1/April.4352.

[24] D. Han *et al.*, “Anomaly *Detection* in the Open World: Normality Shift *Detection*, Explanation, and Adaptation,” in *Proceedings 2023 Network* and *Distributed System Security Symposium*, San Diego, CA, USA: Internet Society, 2023. doi: 10.14722/ndss.2023.24830.

[25] D. D. Santos, “*Cybersecurity* Incident *Response* in eHealth,” 2023.

[26] C. Arfanudin, B. Sugiantoro, and Y. Prayudi, “ANALYSIS OF ROUTER ATTACK WITH *SECURITY INFORMATION* AND *EVENT MANAGEMENT* AND IMPLICATIONS IN INFORMATION SECURITY

INDEX," *csecurity*, vol. 2, no. 1, pp. 1–7, Jul. 2019, doi: 10.14421/csecurity.2019.2.1.1388.

[27] H. Khotimah, F. Bimantoro, and R. S. Kabanga, "Implementasi *Security Information* and *Event Management* (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat," *JBegaTI*, vol. 3, no. 2, Sep. 2022, doi: 10.29303/jbegati.v3i2.752.

[28] N. J. Yeager and R. E. McGrath, *Web server Technology*. Morgan Kaufmann, 1996.

[29] N. Kew, *The Apache Modules Book: Application Development with Apache*. Prentice Hall Professional, 2007.

[30] S.-P. Oriyano, *Penetration testing Essentials*. John Wiley & Sons, 2016.