Analisis Sistem *Security Information and Event Management* (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan

Mardhiyah Nas[1)], Farchia Ulfiah[2)], Ulya Putri[3)]
[1,2,3] Teknik Elektro, Politeknik Negeri Ujung Pandang
email: mardhiyahnas@poliupg.ac.id[1] , mkpoltek2020@gmail.com[2], ulyaputri071@gmail.com[3]

Abstract

The South Sulawesi Communication Informatics Statistics and Standardization Office is an implementer of government affairs that assists in carrying out government affairs in the fields of communication, informatics, statistics, and signage. Currently, agencies are utilizing technological developments to maximize their performance, such as the use of web servers to provide information and provide services. But of course this can cause problems such as data theft. Because of the many threats that can attack at any time. Therefore, an application is needed that can prevent this from happening. In order to overcome this, a monitoring system is implemented using the Wazuh application which is an application of SIEM. to find out how this application works in the event of an attack, testing will be carried out using 2 types of attacks, namely Distributed Denial of Service (DDoS) Slowloris and Brute Force. In this test, data will be taken in the form of application responses, namely the response time of the Wazuh application and the classification of the Wazuh application level against DDoS and Brute Force attacks which will be displayed on the Wazuh application Dashboard. Based on the test results, the wazuh application successfully detects DDoS Slowloris and Brute force attacks and can classify these two attacks at levels 3 to 10.

Keyword: *SIEM, Wazuh App, DDoS, Brute Force*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi sangatlah pesat sehingga masyarakat lebih mudah melakukan aktivitas dalam berbagai bidang khususnya pada bidang teknologi informasi. Dibalik kemajuan teknologi tersebut, tentu saja terdapat ancaman dan serangan yang dapat terjadi kapan saja. Ancaman ini dapat memberikan dampak negatif seperti kebocoran, kehilangan data penting, kerusakan pada *server* yang dapat merugikan instansi terkait. Ancaman dan serangan tersebut dapat terjadi pada *server* misalnya pada *server* di bidang pemerintah, pendidikan, serta perusahaan.

Pada saat ini instansi-instansi memanfaatkan perkembangan Teknologi guna untuk memaksimalkan kinerjanya. Contohnya penggunaan *web server* sebagai media internet untuk memberikan informasi, memberikan layanan, serta sebagai penyimpanan data. Namun tentu saja hal ini dapat menimbulkan masalah seperti pencurian data oleh orang yang tidak bertanggung jawab, maka dari itu pentingnya memperkuat keamanan pada jaringan demi mencegah hal ini terjadi khususnya keamanan pada *web server*. Demi mengatasi hal tersebut, Diskominfo-SP Sulawesi Selatan melakukan pemantauan menggunakan *Security Information and Event Management* (SIEM) yang berfungsi untuk mengumpulkan data keamanan dari *log* pada jaringan, aplikasi serta *hardware* [1].

Adapun aplikasi yang digunakan untuk pemantauan yaitu aplikasi Wazuh yang merupakan aplikasi *opensource* untuk pemantauan *web server*. Aplikasi Wazuh menyajikan informasi keamanan jaringan dan mengumpulkan *log* pada sistem maka dari itu, penelitian ini akan dilakukan suatu pengujian pada aplikasi Wazuh untuk memahami bagaimana aplikasi ini bekerja apabila terjadi serangan pada *website*. Adapun metode serangan yang akan digunakan adalah *Distributed Denial of Service* (DDoS) *Slowloris* dan *Bruto Force*.

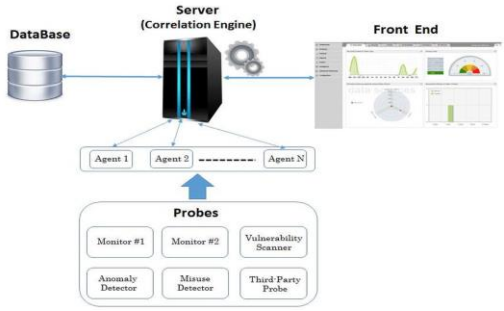
II. KAJIAN LITERATUR

A. Keamanan Jaringan (*Cyber Security*)

Cyber Security berasal dari dua kata *cyber* yang berarti dunia maya dan *security* yang berarti keamanan. Maka dari itu *cyber security* diartikan sebagai keamanan siber. *Cyber security* berperan dalam mendeteksi, memperbaiki atau menurunkan tingkatan resiko dari ancaman siber dan serangan siber serta seluruh kegiatan yang memberi ancaman terhadap keamanan seluruh komponen sistem siber [1].

B. *Security Information and Event Management* (SIEM)

SIEM adalah sebuah sistem yang dapat mendeteksi serangan serta respon pada sistem keamanan akan serangan yang melalui analisis *log* dari beragam *event-log* dari data secara *real time*. *Log* merupakan informasi dari perangkat yang berisi kegiatan dari *log* tersebut, mulai dari lalu lintas jaringan, status dari perangkat dan lainnya [1]. SIEM berbasis *Artificial Intelligence* (AI) mampu membuat keputusan atau mengubah perilaku yang sesuai, yang dapat meningkatkan kemampuan deteksi dengan menemukan lebih banyak titik buta, mengurangi ketergantungan intervensi manual karena beberapa reaksi dapat diotomatisasi [7]. Arsitektur SIEM dapat dilihat pada Gambar 1.

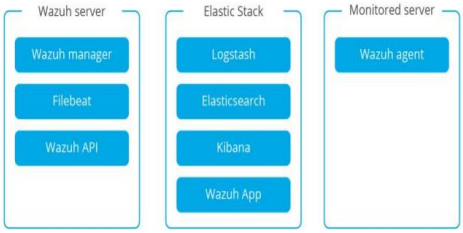


Gambar 1 Arsitektur SIEM

C. Aplikasi Wazuh

Aplikasi Wazuh adalah sebuah perangkat yang menyajikan fitur vasibilitas keamanan yang lebih dalam pada infrastruktur dengan memantau *host* pada sistem operasi dan pada aplikasi [3].

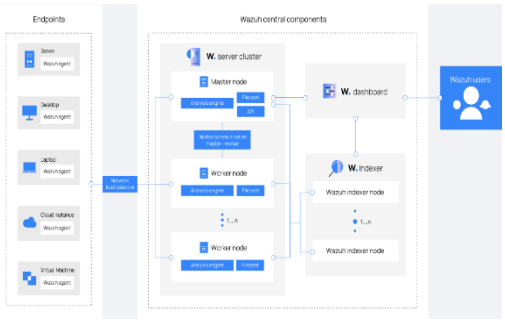
1. Komponen Aplikasi Wazuh
   - Wazuh *Server* merupakan perangkat yang digunakan sebagai manajemen agen dan *dashboard* sistem *monitoring* baik file *integrity*, *intrusion*, walaupun *log*.
   - Wazuh *Agent* merupakan perangkat yang diinstal pada perangkat *endpoint* untuk melakukan pembacaan sistem, pengumpulan log serta mengirimkan ke wazuh *server* [1].
   - *Elastic Stack* adalah rangkaian terbuka proyek sumber untuk *management log*, termasuk *elasticsearch*, kibana, *filebeat*, dan lainnya. Proyek yang sangat relevan dengan solusi wazuh adalah *filebeat*, *elasticsearch*, kibana. Komponen Wazuh dapat dilihat pada Gambar 2.



Gambar 2. Komponen Aplikasi Wazuh

2. Arsitektur Aplikasi Wazuh

Arsitektur aplikasi Wazuh didasarkan pada agen, yang berjalan pada titik akhir yang dipantau, yang meneruskan data keamanan ke manajer pusat. Selain itu, perangkat tanpa agen didukung dan dapat mengirimkan data *log* secara aktif melalui s*yslog*. Manajer menerjemahkan dan menganalisis informasi yang masuk, dan meneruskan hasilnya ke *elasticsearch* untuk pengindeksan dan penyimpanan [2]. Arsitektur aplikasi Wazuh ditunjukkan pada Gambar 3.



Gambar 3 Arsitektur Aplikasi Wazuh

D. *Distributed Denial of Service* (DDoS)

DDoS adalah jenis serangan yang dapat merusak atau menganggu sistem pada layanan. Cara kerja Serangan DDoS yaitu menghabiskan sumber daya yang dimiliki

oleh *server* sehingga tidak bisa diakses hingga tidak bisa menjalankan fungsinya. Umumnya penyerang sering waktu melakukan serangan dengan membanjiri trafik dalam jumlah paket yang besar yang dikirim ke *server* [5]. DDoS *Slowloris* merupakan serangan yang sangat bertarget yang memungkinkan satu *web server* untuk menjatuhkan *web server* lain tanpa mempengaruhi layanan atau port lain di jaringan target. Serangan ini menyelesaikan masalah dengan membuat koneksi ke *server* target, tetapi hanya mengirim sebagian permintaan. *Slowloris* terus-menerus mengirim lebih banyak header HTTP (*Hypertext Transfer-Transfer Protocol)*, tetapi tidak pernah menyelesaikan permintaan. *Server* yang ditargetkan membuat setiap koneksi palsu ini tetap terbuka. Ini akhirnya meluap karena kumpulan koneksi bersamaan maksimum, dan mengarah pada penolakan koneksi tambahan dari klien yang sah [6].

E. Brute Force

Serangan *Brute Force* merupakan jenis teknik serangan yang menyerang sebuah sistem keamanan komputer dengan melakukan percobaan terhadap semua *password* yang memungkinkan. [5].

F. *VirtualBox*

Oracle VM VirtualBox atau sering disebut dengan *VirtualBox* merupakan salah satu produk perangkat lunak yang sekarang dikembangkan oleh *Oracle.* Aplikasi ini pertama kali dikembangkan oleh perusahaan Jerman, Innotek GmbH. Februari 2008, Innotek GmbH diakusisi oleh *Sun Microsystems. Sun Microsystem* kemudian juga diakuisisi oleh *Oracle*. *VirtualBox* berfungsi untuk melakukan virtualisasi sistem operasi. *VirtualBox* juga dapat digunakan untuk membuat virtualisasi jaringan komputer sederhana. Penggunaan *VirtualBox* ditargetkan untuk *Server*, desktop dan penggunaan embedded. Berdasarkan jenis VMM yang ada, *VirtualBox* merupakan jenis *hypervisor type* 2. *Oracle VM VirtualBox* adalah perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama [8].

G. *Kali Linux*

Kali Linux adalah distribusi berlandasan distribusi Debian GNU/Linux untuk tujuan forensik digital dan digunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh *Offensive Security*. *Kali linux* dikembangkan oleh pengembang *Backtrack* sebelumnya yaitu Mati Aharoni bersama pengembang baru bernama Devon Kearns dari *Offensive Security* [9].

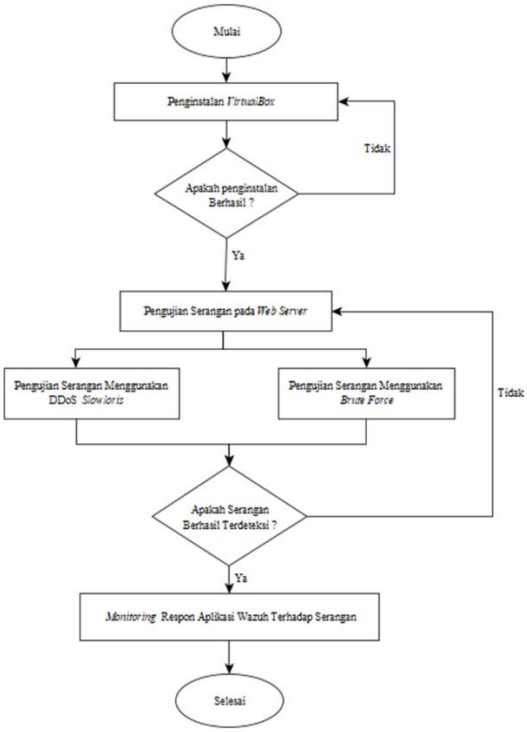
III. METODE PENELITIAN

Pada penelitian ini akan dialakukan pengujian menggunakan 2 jenis serangan yaitu DdoS *Slowloris* dengan jumlah serangan 10.000, 15.000 dan 20.000 paket data dan *Brute Force* dengan jumlah serangan 20.470 paket data. Data yang akan diambil yaitu waktu respon aplikasi Wazuh dan klasifikasi level aplikasi Wazuh terhadap serangan Ddos *Slowloris* dan *Brute Force.* Klasifikasi level aplikasi Wazuh ditunjukkan pada Tabel 1.

Tabel 1 Klasifikasi Level Serangan Aplikasi Wazuh

Level	Indikator	Keterangan
0	Diabaikan	Tidak ada tindakan yang diambil, digunakan untuk menghindari hasil positif palsu. Aturan ini dipindai sebelum yang lainnya. Serta, peristiwa yang tidak memiliki relevansi keamanan.
2	Pemberitahuan sistem prioritas rendah	Pemberitahuan sistem atau pesan status. Pemberitahuan ini tidak memiliki relevansi keamanan.
3	*Event* yang disahkan/berhasil	Ini termasuk upaya login yang berhasil, peristiwa *firewall* yang diizinkan, dll.
4	Kesalahan prioritas rendah pada sistem	Kesalahan yang terkait dengan konfigurasi yang buruk atau perangkat/aplikasi yang tidak digunakan. Hal ini tidak memiliki relevansi keamanan dan biasanya disebabkan oleh instalasi *default* atau pengujian perangkat lunak.
5	Kesalahan yang disebabkan oleh pengguna	Ini termasuk kata sandi yang terlewat, tindakan yang ditolak dengan sendirinya, hal ini tidak memiliki relevansi keamanan.
6	Serangan dengan relevansi rendah	Ini mengindikasikan adanya worm atau virus yang tidak berpengaruh pada sistem (seperti kode merah untuk *server apache*, dll). Ini juga termasuk peristiwa IDS yang sering terjadi dan kesalahan yang sering terjadi.
7	Pencocokan "kata yang tidak baik"	Ini termasuk kata-kata seperti "buruk", "kesalahan", dll. Peristiwa ini sering kali tidak diklasifikasikan dan mungkin memiliki relevansi keamanan.
8	Pertama kali dilihat	Ini termasuk peristiwa yang pertama kali dilihat. Pertama kali peristiwa IDS ditembakkan atau pertama kali pengguna masuk. Ini juga mencakup tindakan yang relevan dengan keamanan (seperti dimulainya *sniffer* atau semacamnya).
9	Kesalahan dari sumber yang tidak valid	Seperti upaya untuk masuk sebagai pengguna yang tidak dikenal atau dari sumber yang tidak valid. Mungkin memiliki relevansi keamanan (khususnya jika diulang). Ini juga termasuk kesalahan terkait akun "admin" (*root*).
10	kesalahan yang dibuat oleh pengguna	Ini termasuk beberapa kali kata sandi yang salah, beberapa kali gagal login, dll. Hal-hal ini

Adapun *Flowchart* tahap penelitian ditampilkan pada Gambar 4.



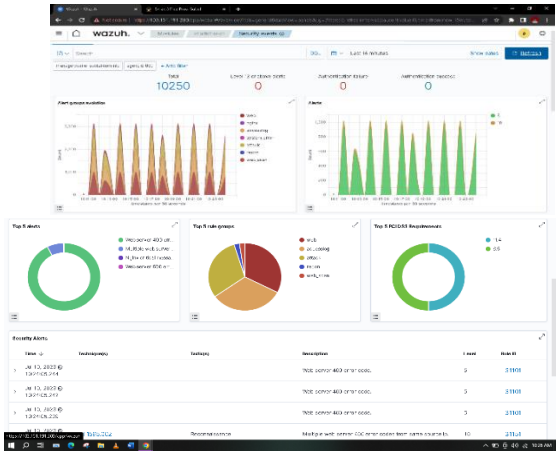
Gambar 4 *Flowchart* Tahap Penelitian

Pada Gambar 4 merupakan *flowchart* tahapan penelitian. Tahap pertamaa yang dilakukan adalah penginstalan *Virtualbox* yang nantinya digunakan untuk menjalankan *Kali Linux.* Setelah penginstalan berhasil, langkah selanjutnya akan dilakukan pengujian pada aplikasi Wazuh menggunakan 2 jenis serangan yaitu DDoS *Slowloris* dan *Brute Force.* Apabila pengujian berhasil terdeteksi, maka akan dilakukan pemantauan menggunakan aplikasi Wazuh dan apabila pengujian tidak terdeteksi, maka akan dilakukan pengujian ulang.

IV. HASIL DAN PEMBAHASAN

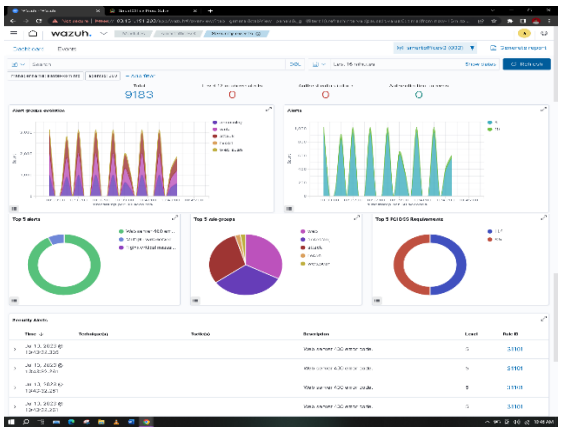
Pada pengujian ini menggunakan 2 jenis serangan yaitu DDoS *Slowloris* dengan jumlah serangan sebanyak 10.000, 15.000 dan 20.000 paket data dan *Brute Force* dengan jumlah serangan sebanyak 20.470 paket data.

A. Pengujian DDoS *Slowloris* dengan jumlah serangan 10.000 paket data



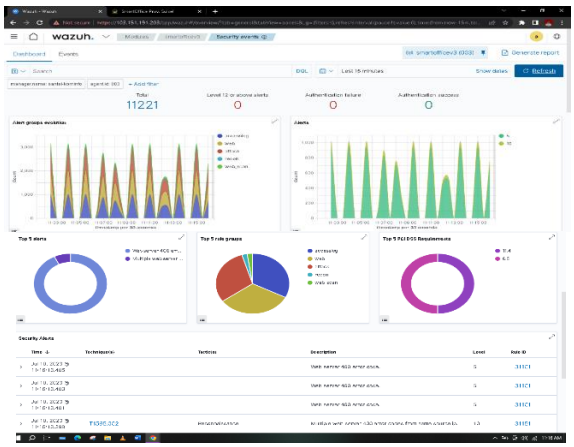
Gambar 5 Hasil pemantauan Serangan DDoS *Slowloris* dengan Jumah 10.000 Paket Data

B. Pengujian DDoS *Slowloris* dengan jumlah serangan 15.000 paket data



Gambar 6 Hasil pemantauan Serangan DDoS *Slowloris* dengan Jumah 15.000 Paket Data

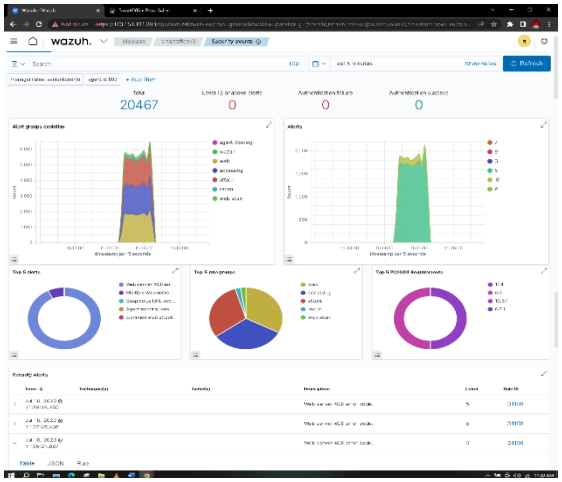
C. Pengujian DDoS *Slowloris* dengan jumlah serangan 20.000 paket data



Gambar 7 Hasil Pemantauan Serangan DDoS *Slowloris* dengan Jumah 20.000 Paket Data

Pada Gambar 5, Gambar 6, dan Gambar 7 merupakan hasil pemantauan pada aplikasi

Wazuh menggunakan serangan DDoS *Slowloris* dengan jumlah 10.000, 15.000. dan 20.000 paket data yang ditampilkan pada *dashboard*. Pada Pada *dashboard* tersebut ditampilkan grafik yang berisi informasi aktifitas agen yang dipantau. Informasi yang ditampilkan dalam *dashboard* ini berupa jumlah autentikasi gagal dan autentikasi yang berhasil, waktu serangan terjadi serta beberapa grafik yang menampilkan 5 data tertinggi dari beberapa kategori seperti top 5 serangan atau peringatan yang masuk, top 5 *rule grup*, dan top 5 *Payment Card Industry Data Security Standard* (PCI DSS) *requirements*. Pada *dashboard* tersebut juga dapat dilihat tingkatan level dari serangan yang masuk. Aplikasi wazuh mengklasifikasikan serangan menjadi beberapa level mulai dari level 0-15. Level 0-6 dikategorikan sebagai tingkat serangan yang rendah, 7-11 dikategorikan sebagai tingkat serangan menengah, dan level 11-15 dikategorikan sebagai tingkat serangan yang tinggi. Pada pengujian serangan DDoS *Slowloris* dengan jumlah 10.000, 15.000 dan 20.000 paket data aplikasi Wazuh berhasil mendeteksi serangan ini dengan deskripsi *web server 400 error* dan *Nginx critical massage* dan level 10 dengan deskripsi *multiple web server 400 error codes from same secure ip.*



Gambar 4 Hasil pemantauan Serangan Brute Force

Pada pengujian menggunakan serangan *Brute Force* aplikasi Wazuh berhasil mendeteksi serangan ini dengan level serangan yang berbeda yaitu level 9 dengan deskripsi *Agen Even Queue*, level 10 dengan deskripsi *Multiple Web Server 400 Error Codes from Same Secure Ip*, level 6 dengan deskripsi *Common Web Attack*, level 5 dengan deskripsi *Web Server 400 Error*, level 8 dengan deskripsi *Maximum Authentication Attempts Exceeded* dan level 3 dengan deskripsi *Nginx Error Massage.*

Tabel 2 Hasil Deteksi Serangan menggunakan Aplikasi Wazuh

No	Jenis Serangan	Jumlah Serangan (Paket Data)	Status Serangan	Waktu Penyerangan (Pukul)	Waktu terdeteksi (Pukul)
1	DDoS *Slowloris*	10.000	Terdeteksi	10:24:05	10:24:05
		15.000	Terdeteksi	10:45:32	10:45:32
		20.000	Terdeteksi	11:16:13	11:16:13
2	*Brute Force*	20.470	Terdeteksi	11.38.19	11.38.19
		11	Terdeteksi	16:44:46	16:44:46

Tabel 2 merupakan hasil dari deteksi serangan menggunakan aplikasi Wazuh. Pada tabel tersebut aplikasi Wazuh berhasil mendeteksi serangan secara cepat atau tidak ada waktu keterlambatan pada saat pengujian dilakukan ini berarti aplikasi Wazuh dapat mendeteksi serangan secara *real time*.

V. KESIMPULAN

1. Aplikasi Wazuh dapat mendeteksi adanya serangan DDoS *Slowloris* dengan jumlah yang berbeda yaitu 10.000, 15.000, 20.000 paket data dan *Brute Force* dengan jumlah serangan 20.470 paket data secara *real time*.
2. Aplikasi Wazuh dapat mengklasifikasikan level serangan DDoS Slowloris dengan jumlah serangan 10.000, 15.000, dan 20.000 paket data pada level 5 dengan deskripsi *Web Server 400 Error* dan *Nginx Critical Massage* serta level 10 dengan deskripsi *Multiple Web Server 400 Error Codes from Same Secure Ip*.
3. Pada pengujian menggunakan serangan *Brute force* aplikasi Wazuh dapat mengklasifikakan serangan ini mulai dari level 3 dengan deskripsi *Nginx Error Massage*, level 5, dengan deskripsi *Web Server 400 Error*, level 6 dengan deskripsi *Common Web Attack*, level 8 dengan deskripsi *Maximum Authentication Attempts Exceeded*, level 9 dengan deskripsi *Agen Even Queue* dan level 10 dengan deskripsi *Multiple Web Server 400 Error Codes from Same Secure Ip*.

UCAPAN TERIMA KASIH

Penulis mengucapkan banyak terima kasih kepada Dinas Komunikasi Informatika Statistik dan Persandian Selawesi Selatan yang telah memberi dukungan, kepercayaan dan

memberikan sumber daya yang dibutuhkan pada penelitian ini.

REFERENSI

[1] Khotimah, H., Bimantoro, F., & Kabanga, R. S. (2022). Implementasi Security Information and Event Management (SIEM) Pada Aplikasi SMS CEnter Pemenrintah Daerah Provinsi Tenggara Barat. *JBegaTI, 3*, 213-219.

[2] Stankovic, S., Gajin, S., Petrovic, R., member, & IEEE. (2022). A Review Of Wazuh Tool Capaabilities For Detecting Attacks Based on Log Analysis. *IceTRAN*, 1-5.

[3] Pratama, M. D., Nova, F., & Prayama, D. (2022). Wazuh Sebagai Log Event Menagement dan Deteksi Celah Keamanan pada *Server* dari Serangan DoS. *Jitsi, 3*, 1-7.

[4] Yasin, A., & Mohidin, I. (2018). DAMPAK SERANGAN DDOS PADA SOFEWARE BASED OPENFOW SWITCH DI PERANGKAT HG553. *Jtech, vol 6*, 72.

[5] Gunawan, I. (2016, September). PENGGUNAAN BRUTE FORCE ATTACK DALAM PENERAPANNYA PADA CRYPT8 DAN CSA-RAINBOW TOOL UNTUK MENCARI BISS. *InfoTekJar, vol 1*, 52-53.

[6] Artha Kusuma, G. H. (2022). Sistem Firewall untuk Pencegahan DDOS ATTACK di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing (JIAC), Vol.3*, 53.

[7] Granadillo, G. G., Zarzosa, S. G., & Diaz, R. (2021). security Information and Event Management (SIEM): Analysis,Trends, and Usage in Critical Infrastructures. *MDPI*, 1-28.

[8] Artha Kusuma, G. H. (2022). Sistem Firewall untuk Pencegahan DDOS ATTACK di Masa Pandemi Covid-19. *journal of Informatics and Advanced Computing (JIAC), vol.3*, 53-54.

[9] Sutarti, Pancaro, A. P., & Saputra, F. I. (2018). IMPLEMENTASI IDS (INTRUSION DETECTION SYSTEM) PADA SISTEM KEAMANAN JARINGAN SMAN 1 CIKEUSAL. *PROSISKO, Vol 5* , 3-4.