10.37817/ikraith-informatika.v8i3
P-ISSN :2580-4316
E-ISSN :2654-8054

Implementasi Sistem Manajemen Log untuk Penanggulangan Serangan Server dengan SIEM

[1]Willy Permana Putra, [2]Renol Burjulius, [3]Muhammad Anis Al Hilmi, [4]A. Sumarudin
[1]Rekayasa Perangkat Lunak, Politeknik Negeri Indramayu, Indramayu
[2]Sistem Informasi Kota Cerdas, Politeknik Negeri Indramayu, Indramayu
[3,4]Teknik Informatika, Politeknik Negeri Indramayu, Indramayu

E-mail: [1]willy_p@polindra.ac.id, [2]burjuliusrenol@gmail.com, [3]alhilmi1@gmail.com, [4]shumaru@polindra.ac.id

ABSTRAK

Dalam era digital saat ini, keamanan informasi menjadi fokus utama bagi organisasi di seluruh dunia. Teknologi yang berkembang pesat membawa manfaat besar, namun juga menimbulkan ancaman dan serangan siber yang semakin canggih. Salah satu pendekatan untuk mengatasi tantangan ini adalah melalui Security Information and Event Management (SIEM). SIEM mengintegrasikan Pengelolaan Informasi Keamanan (SIM) dan Pengelolaan Peristiwa Keamanan (SEM) untuk mengumpulkan, menganalisis, dan melaporkan data keamanan dari berbagai sumber dalam jaringan, sehingga memungkinkan deteksi, respons, dan pengelolaan insiden keamanan dengan lebih efektif. Penelitian ini berfokus pada penanganan serangan server dengan memanfaatkan Wazuh SIEM sebagai sistem peringatan dini. Metodologi yang digunakan mencakup pengaturan topologi jaringan untuk mendeteksi serangan Distributed Denial of Service (DDoS) menggunakan SIEM, pengumpulan dan analisis data log, korelasi data untuk mengidentifikasi ancaman, serta respons terhadap ancaman yang terdeteksi. Hasil penelitian menunjukkan bahwa SIEM sangat penting dalam keamanan siber modern, memberikan kemampuan deteksi dan respons ancaman secara real-time. Dalam uji coba, sistem berhasil mendeteksi dan memblokir 42 serangan secara efektif. Kesimpulannya, SIEM menyediakan visibilitas dan kontrol keamanan yang lebih besar, memungkinkan organisasi untuk mendeteksi dan merespons ancaman keamanan yang kompleks secara efisien dan efektif. SIEM modern, dengan analitik canggih dan pembelajaran mesin, mampu mengidentifikasi pola anomali dan ancaman baru, sehingga memperkuat pertahanan keamanan siber organisasi.

Kata kunci : ***SIEM, Wazuh, DDoS, Log, real-time***

ABSTRACT

In the current digital era, information security has become a primary focus for organizations worldwide. Rapid technological advancements have brought significant benefits but also introduced increasingly sophisticated cyber threats and attacks. One approach to addressing these challenges is through Security Information and Event Management (SIEM). SIEM integrates Security Information Management (SIM) and Security Event Management (SEM) to collect, analyze, and report security data from various network sources, enabling more effective detection, response, and management of security incidents. This study focuses on handling server attacks using Wazuh SIEM as an early warning system. The methodology involves setting up a network topology to detect Distributed Denial of Service (DDoS) attacks using SIEM, collecting and analyzing log data, correlating data to identify threats, and responding to detected threats. The results indicate that SIEM is crucial in modern cybersecurity, providing real-time threat detection and response capabilities. The system successfully detected and blocked 42 attacks during the trial. In conclusion, SIEM offers greater security visibility and control, enabling organizations to detect and respond to complex security threats efficiently and effectively. Modern SIEM systems, equipped with advanced analytics and machine learning, can identify anomaly patterns and new threats, thus strengthening an organization's cybersecurity defenses.

Keyword : ***SIEM, Wazuh, DDoS, Log, real-time***

P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v8i3

1. PENDAHULUAN

Dalam era digital saat ini, keamanan informasi telah menjadi salah satu fokus utama bagi organisasi di seluruh dunia. Kemajuan teknologi telah membawa berbagai manfaat, tetapi juga menghadirkan tantangan baru dalam bentuk ancaman dan serangan siber yang semakin canggih. Salah satu pendekatan yang digunakan untuk mengatasi tantangan ini adalah melalui penerapan *Security Information and Event Management* (SIEM).

SIEM adalah sebuah teknologi yang mengintegrasikan dua fungsi utama: pengelolaan informasi keamanan (Security Information Management, SIM) dan pengelolaan peristiwa keamanan (Security Event Management, SEM). Sistem SIEM berfungsi untuk mengumpulkan, menganalisis, dan melaporkan data keamanan dari berbagai sumber dalam jaringan. Dengan demikian, SIEM memungkinkan organisasi untuk mendeteksi, merespons, dan mengelola insiden keamanan dengan lebih efektif.

Seiring dengan perkembangan teknologi, SIEM juga mengalami evolusi yang signifikan. Pada awalnya, SIEM difokuskan pada pengumpulan log dan korelasi data sederhana. Namun, dengan meningkatnya kompleksitas ancaman siber, SIEM modern telah dilengkapi dengan kemampuan analitik yang lebih canggih, termasuk analitik prediktif dan pembelajaran mesin (machine learning). Hal ini memungkinkan SIEM untuk tidak hanya mendeteksi ancaman yang sudah dikenal, tetapi juga mengidentifikasi pola-pola anomali yang dapat mengindikasikan ancaman baru.

Dilansir dari Badan Siber dan Sandi Negara meng Ingatkan Ada 203 Juta Anomali Trafik Berstatus Compromised Mengancam Ekonomi Digital Indonesia(*BSSN Ingatkan Ada 203 Juta Anomali Trafik Berstatus Compromised Mengancam Ekonomi Digital Indonesia*, 2023). Ditahun 2021 sendiri dapat dilihat trafik Anomali yang sangat tinggi hingga mencapai jutaan trafik dalam waktu satu bulan ditunjukan oleh aktivitas beberapa alamat IP. Banyaknya anomali ini dalam waktu singkat ini dapat disebabkan oleh aktivitas ZBot, trojan, dan malware lainnya.

Dalam penelitian ini, bagaimana menangani serangan yang terjadi pada server dengan memanfaatkan Wazuh SIEM sebagai sistem peringatan dini atau *early warning system*. Dalam konsep yang dilakukan berupa mendeteksi serangan kemudian melakukan Tindakan seperti pemblokiran.

2. LANDASAN TEORI

Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) adalah sistem keamanan yang menggabungkan fungsi pengelolaan informasi keamanan (Security Information Management, SIM) dan pengelolaan peristiwa keamanan (Security Event Management, SEM). SIEM dirancang untuk menyediakan visibilitas waktu nyata dan analisis historis terhadap insiden keamanan melalui pengumpulan dan analisis data dari berbagai sumber dalam jaringan. Menurut CSO Online, "SIEM menggabungkan manajemen *log* dan analisis keamanan dalam satu *platform* terpadu untuk memberikan stabilitas dan kontrol yang lebih besar atas peristiwa keamanan di seluruh jaringan perusahaan"(Securonix SIEM as a Service Has Behavior Analytics Baked In, 2020).

Komponen Utama Siem

SIEM terdiri dari beberapa komponen kunci yang bekerja bersama untuk menyediakan visibilitas dan kontrol keamanan yang komprehensif:

1. Pengumpulan Log: SIEM mengumpulkan data *log* dari berbagai sumber seperti *firewall*, sistem deteksi intrusi (IDS), server aplikasi, dan perangkat jaringan lainnya.
2. Normalisasi Data: Data yang dikumpulkan dinormalisasi untuk memastikan format yang konsisten, sehingga memungkinkan analisis lebih lanjut.
3. Korelasi Peristiwa: SIEM menganalisis dan mengkorelasikan peristiwa keamanan

P-ISSN :2580-4316
E-ISSN :2654-8054

untuk mengidentifikasi pola dan indikasi serangan yang mungkin terjadi.
4. Pelaporan dan Alarm: SIEM menghasilkan laporan dan alarm untuk memberitahu tim keamanan tentang insiden keamanan yang perlu ditindaklanjuti.

SANS Institute menjelaskan bahwa "SIEM modern tidak hanya bergantung pada pengumpulan log sederhana tetapi juga mengintegrasikan analitik canggih dan pembelajaran mesin untuk mendeteksi anomali dan ancaman yang sebelumnya tidak diketahui".

Implementasi SIEM melibatkan beberapa tahap kritis, termasuk perencanaan, pengaturan, dan pemantauan berkelanjutan. Menurut Gartner, "Implementasi SIEM yang berhasil membutuhkan pemahaman mendalam tentang arsitektur jaringan organisasi dan kebutuhan spesifik keamanan mereka. Proses ini biasanya dimulai dengan evaluasi dan seleksi solusi SIEM yang sesuai, diikuti dengan pengaturan dan konfigurasi sistem, serta pelatihan staf untuk mengelola dan memanfaatkan sistem secara efektif".

Suricata

Suricata adalah mesin deteksi ancaman sumber terbuka yang dapat mendeteksi serangan jaringan, mengidentifikasi lalu lintas mencurigakan, dan menghasilkan data *log* peristiwa keamanan. Suricata dapat diintegrasikan dengan SIEM untuk memberikan lapisan tambahan analisis keamanan jaringan. *The Open Information Security Foundation* (OISF) menyatakan bahwa "Suricata dirancang untuk memberikan deteksi ancaman yang cepat dan akurat dengan menggunakan analisis multi-threading dan mendukung berbagai format *log*".

Penelitian oleh SANS Institute menemukan bahwa "Menggunakan alat seperti Elasticsearch, Kibana, dan Filebeat bersama dengan SIEM dapat meningkatkan kemampuan organisasi dalam mendeteksi dan merespons ancaman keamanan dengan menyediakan analisis peristiwa yang komprehensif dan mendalam".

Wazuh

Wazuh adalah platform keamanan open-source yang menyediakan solusi komprehensif untuk pemantauan keamanan, deteksi ancaman, dan respons insiden. Wazuh adalah alat yang sangat efektif dalam mendeteksi dan menangani serangan serta ancaman keamanan. Dengan fitur-fitur canggih seperti pemantauan berkelanjutan, integrasi threat intelligence, dan respons otomatis, Wazuh memberikan perlindungan yang kuat dan respons cepat terhadap insiden keamanan.(Documentation Wazuh, n.d.).

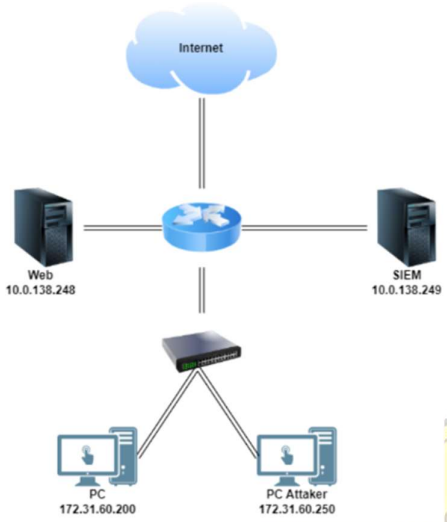
Beberapa penelitian telah menyoroti manfaat dan tantangan dalam penerapan SIEM. Misalnya, penelitian oleh SANS Institute menemukan bahwa "SIEM dapat secara signifikan meningkatkan kemampuan organisasi dalam mendeteksi dan merespons ancaman keamanan dengan menyediakan analisis peristiwa yang komprehensif dan mendalam". Namun, penelitian juga menunjukkan bahwa SIEM dapat menghadapi tantangan dalam hal skalabilitas dan kompleksitas pengelolaan data, terutama dalam lingkungan jaringan yang besar dan heterogen.

Penelitian oleh Security Boulevard menunjukkan bahwa kerentanan dalam sistem SIEM, seperti ketergantungan pada data log yang dapat dimanipulasi, masih menjadi tantangan utama. Penelitian ini menekankan pentingnya kombinasi antara SIEM dengan solusi keamanan lainnya, seperti sistem deteksi intrusi (IDS) dan intelijen ancaman, untuk meningkatkan efektivitas deteksi dan respons.

3. METODOLOGI

Dalam percobaan penelitian ini, eksperimen dilakukan sebagai berikut:

P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v8i3



Gambar 1. Topologi Perancangan

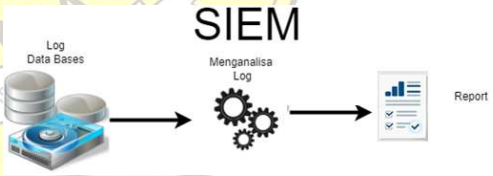
Gambar di atas menunjukkan topologi jaringan yang digunakan untuk mendeteksi serangan *Distributed Denial of Service* (DDoS) menggunakan sistem SIEM (Security Information and Event Management). Berikut adalah penjelasan mengenai elemen-elemen yang ada dalam gambar:

- **Internet**: Sumber lalu lintas jaringan yang dapat berisi pengguna yang sah dan potensi penyerang.
- **Router**: Perangkat yang menghubungkan jaringan internal dengan internet. Router ini mengatur lalu lintas data masuk dan keluar dari jaringan.
- **Web Server (10.0.138.248)**: Server ini merupakan target dari potensi serangan DDoS. Web server ini dapat melayani permintaan dari pengguna internet.
- **SIEM (10.0.138.249)**: Sistem SIEM ini digunakan untuk mengumpulkan, menganalisis, dan mengkorelasikan data log dari berbagai perangkat jaringan untuk mendeteksi aktivitas mencurigakan, termasuk serangan DDoS. SIEM ini juga berfungsi untuk memberikan notifikasi dan laporan tentang insiden keamanan yang terdeteksi.
- **Switch**: Perangkat ini menghubungkan beberapa perangkat dalam jaringan lokal (LAN) dan mengatur lalu lintas data antar perangkat yang terhubung.
- **PC (172.31.60.200)**: Komputer ini merupakan pengguna sah yang berada dalam jaringan internal. PC ini dapat mengakses web server dan juga terhubung dengan SIEM untuk pengawasan.
- **PC Attacker (172.31.60.250)**: Komputer ini disimulasikan sebagai penyerang yang mencoba meluncurkan serangan DDoS ke web server. Aktivitas penyerang ini diawasi oleh SIEM untuk mendeteksi dan mengatasi ancaman.

Tahapan

- **Pengumpulan Data**: SIEM mengumpulkan log dari web server, router, dan perangkat lain.
- **Analisis Data**: SIEM menganalisis data log untuk mengidentifikasi pola lalu lintas yang mencurigakan atau anomali yang mengindikasikan serangan DDoS.
- **Korelasi**: SIEM mengkorelasikan data dari berbagai sumber untuk mendapatkan gambaran yang komprehensif tentang potensi ancaman.
- **Respon**: Jika SIEM mendeteksi serangan DDoS, sistem ini dapat memberikan notifikasi kepada tim keamanan dan memulai langkah-langkah mitigasi seperti memblokir IP penyerang atau mengalihkan lalu lintas ke server cadangan.

Setelah data diterima, maka bisa digambarkan proses selanjutnya



Gambar 2. Proses Data Log

- **Log Data Base:** Pengumpulan data log dari berbagai sumber.
- **Menganalisis Log:** Memproses dan menganalisis data log yang telah dikumpulkan untuk mendeteksi ancaman dan anomali.
- **Report:** Menghasilkan laporan berdasarkan analisis yang dilakukan untuk memberikan wawasan dan tindakan keamanan yang diperlukan.

P-ISSN :2580-4316
E-ISSN :2654-8054

4. HASIL DAN PEMBAHASAN

Dalam proses penerapan penelitian ini, langkah pertama yang dilakukan adalah menyusun topologi jaringan sesuai dengan topologi yang telah ditentukan. Selanjutnya, dilakukan konfigurasi IP pada masing-masing PC dan server serta sistem SIEM. Dalam penelitian ini, PC Web yang memiliki alamat IP 10.0.138.248 berfungsi sebagai target serangan. Sementara itu, alamat IP 10.0.138.249 digunakan untuk SIEM yang bertugas mengolah data log. Adapun PC dengan alamat IP 172.31.60.250 berperan sebagai penyerang atau attacker.

Tabel 1 Topologi sekema

PC	Sistem Operasi	IP	Ket
Web	Centos 7	10.0.138.248	Targer sasaran
SIEM	Ubuntu 24.04 LTS	10.0.138.249	Analisis data
Attacker	Kali 2024.2	172.31.60.250	Penyerang
PC	Ubuntu 24.04 LTS	172.31.60.200	Uji ping ke server web

Konfigurasi PC Web

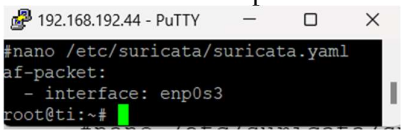
Konfigurasi agent

```
#curl -o wazuh-agent-4.8.1-1.x86_64.rpm
https://packages.wazuh.com/4.x/yum/wazuh-
agent-4.8.1-1.x86_64.rpm && sudo
WAZUH_MANAGER='10.0.138.249' rpm -ihv
wazuh-agent-4.8.1-1.x86_64.rpm
```

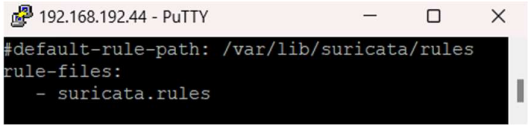
Konfigurasi Suricata

```
sudo yum -y install suricata
wget https://rules.emergingthreats.net/open/...
suricata-6.0.3/emerging.rules.tar.gz
sudo tar zxvf emerging.rules.tar.gz
sudo rm /etc/suricata/rules/* -f
sudo mv rules/*.rules /etc/suricata/rules/
sudo rm -f /etc/suricata/suricata.yaml
sudo wget -O /etc/suricata/suricata.yaml..
https://packages.wazuh.com/4.3/suricata.yml
```

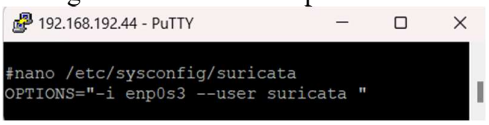
Menentukan interface pada Centos



Menentukan aturan



Konfigurasi servis suricata pada Centos

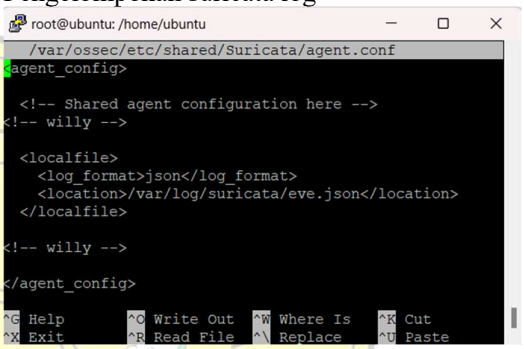


Start Suricata

```
#sudo systemctl daemon-reload
#sudo systemctl enable suricata
#sudo systemctl start suricata
```

Konfigurasi PC SIEM

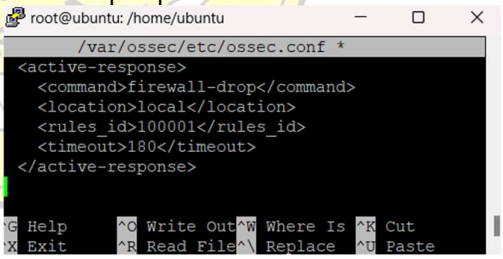
Pengelompokan suricata log



rule Suricata alerts

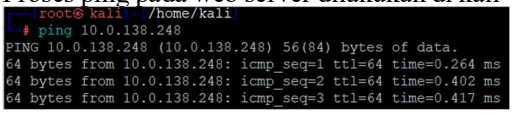
```
<rule id="100001" level="12">
    <if_sid>86600</if_sid>
    <field name="event_type">^alert$</field>
    <match>ET SCAN Nmap Scripting Engine User-Agent
    Detected (Nmap Scripting Engine)</match>
    <description>Nmap Telah terdeteksi. </description>
    <mitre>
      <id>T1595</id>
    </mitre>
  </rule>
```

active respon pemblokiran



Percobaan

Proses ping pada web server dilakukan di kali



Cek proses ping

```
# sudo tcpdump -i eth0 icmp
```

P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v8i3

```
┌──(root㉿kali)-[/home/kali]
└─# sudo tcpdump -i eth0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol dec
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144
IP kali > 10.0.138.248: ICMP echo request, id 26168, seq 1, length 64
IP 10.0.138.248 > kali: ICMP echo reply, id 26168, seq 1, length 64
IP kali > 10.0.138.248: ICMP echo request, id 26168, seq 2, length 64
IP 10.0.138.248 > kali: ICMP echo reply, id 26168, seq 2, length 64
IP kali > 10.0.138.248: ICMP echo request, id 26168, seq 3, length 64
IP 10.0.138.248 > kali: ICMP echo reply, id 26168, seq 3, length 64
```

Menjalankan Nmap scan

```
# sudo nmap -sS --script=vuln 10.0.138.248
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS --script=vuln 10.0.138.248
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 23:36 EDT
Nmap scan report for 10.0.138.248
Host is up (0.00033s latency).
All 1000 scanned ports on 10.0.138.248 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: BC:24:11:68:2A:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 32.35 seconds
```

Pengecekan koneksi

```
┌──(root㉿kali)-[/home/kali]
└─# sudo tcpdump -i eth0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:35:55.'kali: ICMP host 10.0.138.248 unreachable - admin prohibited, length 52
23:35:55.'kali: ICMP host 10.0.138.248 unreachable - admin prohibited, length 52
23:35:55.'kali: ICMP host 10.0.138.248 unreachable - admin prohibited, length 52
23:35:55.'kali: ICMP host 10.0.138.248 unreachable - admin prohibited, length 52
```

Proses ping ke-2

```
┌──(root㉿kali)-[/home/kali]
└─# sudo tcpdump -i eth0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:36:15.kali > 10.0.138.248: ICMP echo request, id 26217, seq 8, length 64
23:36:16.kali > 10.0.138.248: ICMP echo request, id 26217, seq 9, length 64
23:36:17.kali > 10.0.138.248: ICMP echo request, id 26217, seq 10, length 64
23:36:18.kali > 10.0.138.248: ICMP echo request, id 26217, seq 11, length 64
```

Dari uji coba diatas menunjukan Unreachable dan Admin Prohibited yang menunjukan bahwa lalu lintas ICMP ke atau dari host 10.0.138.248 diblokir oleh aturan firewall atau kebijakan jaringan yang diberlakukan oleh administrator. Ini bisa berarti bahwa ada aturan firewall. Host 10.0.138.248 mengirimkan pesan "unreachable - admin prohibited" untuk memberitahu bahwa akses diblokir oleh aturan yang diterapkan oleh administrator jaringan.

Tampilan respon pada dashboard

Security Alerts

	Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
›	Jul 28, 2024 @ 10:55:03.273			Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed	3	86601
›	Jul 28, 2024 @ 10:55:03.273	T1595	Reconnaissance	Nmap Telah terdeteksi	12	100001
›	Jul 28, 2024 @ 10:54:55.345			Host Blocked by firewall-drop Active Response	3	651

Dari tampilan dashboard terlihat bahwa telah terdeteksi dengan ID rule 100001 sebagi Nmap detection, dan untuk pembelokiran dengan ID rule 651 serta untuk tampilan agent dengan ID rule 86601.

Tampilan grafik pada dashboard

ncmap View: Data

Download CSV

rule.id: Descending	Count
86601	173
100001	42
651	42

Rows per page: 20 1

Terilihat jelas dari gambar diatas menunjukan berapa banyak serangan yang dilakukan ke server yang ditunjukan oleh Count sebanyak 42 kali dan melakukan pemblokiran sebanyak 42 kali.

5. KESIMPULAN

SIEM adalah alat yang sangat krusial dalam keamanan siber modern, memberikan organisasi kemampuan untuk mengumpulkan, menganalisis, dan merespons data keamanan dari berbagai sumber. Dengan SIEM, deteksi dan respons terhadap ancaman keamanan yang kompleks dapat dilakukan secara real-time. Hasil uji coba menunjukkan bahwa proses serangan dapat terdeteksi langsung, termasuk jumlah serangan dan waktu terjadinya. Misalnya, dalam uji coba tersebut, terdeteksi sebanyak 42 kali serangan.

6. Ucapan terima kasih

Kami mengucapkan terima kasih yang sebesar-besarnya kepada Politeknik Negeri Indramayu atas dukungan dan kepercayaan yang diberikan dalam bentuk dana penelitian untuk proyek kami yang berjudul "Implementasi Sistem Manajemen Log untuk Penanggulangan Serangan Server dengan SIEM".

Dukungan ini sangat berarti bagi kami dan akan sangat membantu dalam mengembangkan dan menerapkan sistem manajemen log yang efektif untuk mengidentifikasi dan menangani serangan terhadap server. Kami berharap hasil dari penelitian ini dapat memberikan kontribusi yang positif dan bermanfaat bagi kemajuan teknologi keamanan informasi.

DAFTAR PUSTAKA

8 Ancaman Cyber Security di Tahun 2023. (2023, July 28). Https://Itgid.Org/. https://itgid.org/insight/artikel-cobit/8-ancaman-cyber-security-di-tahun-2023/

Arifin, M. N., Sugiartowo, S., & Susilowati, E. (2018). DESAIN DAN IMPLEMENTASI LOG EVENT MANAGEMENT SERVER MENGGUNAKAN ELASTICSEARCH LOGSTASH KIBANA (ELK STACK). *Prosiding Seminar Nasional Sains Dan Teknologi (SEMNASTEK)*. https://jurnal.umj.ac.id/index.php/semnastek/article/view/3451

BSSN Ingatkan Ada 203 Juta Anomali Trafik Berstatus Compromised Mengancam Ekonomi Digital Indonesia. (2023, August 30). Https://Www.Bssn.Go.Id/. https://www.bssn.go.id/bssn-ingatkan-ada-203-950-480-anomali-trafik-berstatus-compromised-mengancam-ekonomi-digital-indonesia/

Cobb, M. (2023, July 12). *The history, evolution and current state of SIEM*. Https://Www.Techtarget.Com/. https://www.techtarget.com/searchsecurity/tip/The-history-evolution-and-current-state-of-SIEM

Documentation Wazuh. (n.d.). Documentation Wazuh.

Farrel, F. I. F., Is Mardianto, S. S. M. K., & Ir. Adrian Sjamsul Qamar, M. (2024). Implementation of Security Information & Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System. *Intelmatics*, *4*(1), 1–7. https://doi.org/10.25105/itm.v4i1.18529

Harikanth, M., & Rajarajeswari, P. (2019). Malicious Event Detection Using ELK Stack Through Cyber Threat Intelligence. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(7), 882–886. https://www.ijitee.org/portfolio-item/g6018058719/

Kamal, M. R., & Setiawan, M. A. (2021). DeteksiAnomalidenganSecurity Information and Event Management(SIEM) Splunk padaJaringanUII. *Automata Publishes Academic Articles for Students and Lecturers of the Department of Informatics, Islamic University of Indonesia*, *2*(2). https://journal.uii.ac.id/AUTOMATA/article/view/19522

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

Lopez-Araiza, C., & Cankaya, E. C. (2017). A Comprehensive Analysis of Security Tools for Network Forensics. *Journal of Medical - Clinical Research & Reviews*, *1*(3), 1–9. https://doi.org/10.33425/2639-944X.1021

Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., & Zunino, R. (2019). The Applicability of a SIEM Solution: Requirements and Evaluation. *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, 132–137. https://doi.org/10.1109/WETICE.2019.00036

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

Pratama, N. F. (2023). Design of Information Security Early Detection System DISKOMINFO Bandung Regency. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *10*(Vol 10 No 1 (2023): JATISI (Jurnal Teknik Informatika dan Sistem Informasi)).

Securonix SIEM as a service has behavior analytics baked in. (2020, June 2). Https://Www.Csoonline.Com/.

Sekharan, S. S., & Kandasamy, K. (2017). Profiling SIEM tools and correlation engines for security analytics. *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 717–721. https://doi.org/10.1109/WiSPNET.2017.8299855

Serangan Siber 6 Juta Kali di Indonesia Sepanjang September 2023, Perbankan Jadi Sasaran Utama. (2023, November 1). Https://Www.Liputan6.Com/. https://www.liputan6.com/tekno/read/5438165/serangan-siber-6-juta-kali-di-indonesia-sepanjang-september-2023-perbankan-jadi-sasaran-utama

Sholihah, W., Pripambudi, S., & Mardiyono, A. (2020). Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack). *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, *2*(1), 12–20. https://doi.org/10.35746/jtim.v2i1.79

Tarigan, C., Engel, V. J. L., & Angela, D. (2018). Sistem Pengawasan Kinerja Jaringan Server Web Apache dengan Log Management System ELK (Elasticsearch, Logstash, Kibana). *Jurnal Telematika*, *2018: Industrial Engineering Seminar and Call for Paper (IESC) 2018*. https://journal.ithb.ac.id/index.php/telematika/article/view/218

Vazão, A., Santos, L., Piedade, M. B., & Rabadão, C. (2019). SIEM Open Source Solutions: A Comparative Study. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–5. https://doi.org/10.23919/CISTI.2019.8760980