Volume XI Issue 2 Year 2026 | Page 616-627 | ISSN: 2527-9866
Received: ***07-05-2026*** | *Revised:* ***19-05-2026*** | *Accepted:* ***27-05-2026***

Implementation and Analysis of Security Information and Event Management at Bina Darma University

Suryayusra [1], Derri Anjuju[2], Aan Restu Mukti[3], Akhmad Khudri[4]
[1234]Bina Darma University, Palembang City, South Sumatra, Indonesia, 30111
e-mail: suryayusra@binadarma.ac.id[1], deriajuju@gmail.com[2], aanrestu@ymail.com[3], khudri@binadarma.ac.id[4]
*Correspondence: *211420117@studentbinadarmaacid*

Abstract: *This research aims to implement Security Information and Event Management (SIEM) using Wazuh on the Bina Darma University server for real-time network security monitoring. The research uses the Action Research method with planning, action, observation and reflection stages. Testing was carried out using three attack scenarios, namely Brute Force, SYN Flood, and SQL Injection on Windows and Ubuntu based virtual machine environments. The research results show that Wazuh succeeded in detecting four attempted Brute Force attacks, a real-time SQL Injection attack, and a SYN Flood attack with the help of Suricata. Telegram Bot integration successfully sends automatic notifications on Brute Force attacks. Performance testing showed CPU usage increased from 15% to 60% during the attack, while memory usage remained stable. This research is still limited to a simulation environment with a limited number of endpoints*

Keywords: *SIEM, Wazuh, Cyber Security, Intrusion Detection, Log Monitoring*

1. Introduction

Easy access to data and information without adequate awareness of information security can create threats that may arise at any time on servers managed by individuals or organizations, including government institutions, educational institutions, and businesses. Data and information are closely related because information cannot be generated without data, while data becomes meaningless without proper information processing. Therefore, protecting data and information within an organization is essential to maintain confidentiality, integrity, and availability of information assets [1].

Cyberattacks such as *brute force*, *Distributed Denial of Service* (DDoS), *SQL Injection*, malware, and unauthorized access can disrupt services and cause significant losses to organizations. One of the major cybersecurity incidents in 2024 involved UnitedHealth Group, which experienced a ransomware attack that disrupted healthcare payment systems nationwide for several weeks. The attackers gained access through stolen credentials and exploited vulnerabilities within the organization's infrastructure. This incident demonstrates that inadequate security monitoring systems can increase risks to information technology infrastructure. Similar risks may also occur in university server environments that store important academic and administrative data and require continuous security monitoring.

To improve server infrastructure security, a monitoring system capable of detecting threats in real time is required. One of the technologies that can be implemented is *Security Information and Event Management* (SIEM). SIEM is designed to collect, analyze, and monitor security logs from various network devices, servers, and applications in a centralized manner. This technology enables administrators to identify suspicious activities, detect cyberattacks, and

respond to incidents more effectively. One of the widely used open-source SIEM platforms is Wazuh because it provides features such as log monitoring, intrusion detection, file integrity monitoring, vulnerability detection, and real-time security analysis.

Several previous studies have discussed the implementation of SIEM using Wazuh for network security monitoring. However, most previous studies mainly focused on log monitoring and basic attack detection without integrating real-time notification systems for administrators. In addition, previous research was generally conducted in small-scale laboratory or enterprise environments and has not been widely implemented in university server ecosystems with different network traffic characteristics. Previous studies also tended to focus only on attack detection analysis without evaluating system performance during monitoring activities.

Research conducted by Citra Arfanudin (2019) showed that SIEM implementation could provide information regarding attacks occurring on routers to security administrators. However, not all attacks were successfully detected by the SIEM system [3]. Only DHCP Starvation, DHCP Rogue, SSH Bruteforce, and FTP Bruteforce attacks were recognized, while MAC Flooding, ARP Poisoning, CDP Flooding, and SYN Flooding attacks could not be detected because the router failed to send logs to the SIEM server. These limitations indicate that SIEM effectiveness is highly dependent on log collection mechanisms and system integration.

Based on these problems, this research focuses on implementing SIEM using Wazuh integrated with Telegram Bot to provide real-time attack notifications to administrators. The study was conducted within the server environment of Bina Darma University by testing several attack scenarios, including *brute force*, SYN Flood, and *SQL Injection* attacks. The contribution of this research lies in the implementation of SIEM within a university server environment, the integration of centralized real-time alert notifications, and the evaluation of system performance during attack detection processes. Through the implementation of Wazuh SIEM, server administrators are expected to perform security monitoring more effectively [16], quickly, and centrally so that potential cyber threats can be detected earlier before causing disruptions to university server services.

2. Literature Review

A. Cybersecurity and Information Security

Cybersecurity refers to technologies, policies, and security mechanisms used to protect systems, networks, servers, and digital assets from cyber threats and unauthorized access [4]. Information security focuses on protecting information assets to maintain confidentiality, integrity, and availability of data. According to ISO/IEC 17799:2005, information security aims to minimize risks and ensure business continuity [5]. Organizations rely on computer networks to support operational activities, making network security an important aspect of protecting valuable information assets from cyberattacks [6].

B. Types of Attacks

This research focuses on three attack scenarios used during the testing process, namely *Brute Force*, SYN Flood, and *SQL Injection* attacks.

1. **Brute Force Attack**
   A *Brute Force* attack is performed by repeatedly trying combinations of usernames and passwords to gain unauthorized access to a system.
2. **SYN Flood Attack**
   SYN Flood is a type of DDoS attack that overloads server resources by continuously sending SYN packets without completing the TCP connection process.

3. **SQL Injection Attack**
   SQL Injection exploits vulnerabilities in database queries by inserting malicious SQL commands to access or manipulate database information illegally.

C. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a system used to collect, monitor, and analyze security logs from multiple devices in a centralized manner [8]. SIEM helps administrators detect suspicious activities and respond to security incidents more effectively. One of the widely used open-source SIEM platforms is Wazuh. Wazuh provides features such as log monitoring, intrusion detection, file integrity monitoring, and real-time alert management [9].

D. Previous Research Comparison

Several previous studies have implemented SIEM for security monitoring; however, most focused only on basic log monitoring and attack detection without real-time notification integration or performance evaluation.

Researcher	Tools	Attack Types	Results
Citra Arfanudin (2019)	SIEM	DHCP, SSH Bruteforce	Some attacks detected
Previous Research	Wazuh	Intrusion Detection	Centralized monitoring
This Research	Wazuh + Telegram	Brute Force, SYN Flood, SQL Injection	Real-time monitoring and alert notification

Based on previous studies, this research contributes by implementing Wazuh integrated with Telegram Bot within a university server environment and evaluating its capability to detect cyberattacks in real time.

3. Methods

This study uses the *Action Research* method, which consists of four stages: *planning*, *action*, *observation*, and *reflection*. The research aims to implement and analyze Wazuh within the DSTI server environment of Bina Darma University for real-time security monitoring and attack detection. The experimental environment consisted of one Wazuh Server, 20 endpoint devices (10 Windows and 10 Ubuntu), and one attacker machine using Kali Linux. The SIEM system was implemented by installing Wazuh Server, Wazuh Dashboard, and Wazuh Agents, followed by Telegram Bot integration for real-time alert notifications. Several attack simulations were conducted, including *Brute Force*, SYN Flood, and *SQL Injection* attacks using penetration testing tools such as Hydra, hping3, and SQLMap. During the observation stage, system logs, alerts, CPU usage, memory usage, and detection performance were monitored through the Wazuh Dashboard.The reflection stage evaluated the effectiveness of Wazuh in detecting cyberattacks and supporting centralized security monitoring within the university server environment.

4. Results and Discussion

Research Design

In this research simulation, a server was designed using a virtual machine with Windows and Ubuntu operating systems. The topology used consisted of a server with SIEM Wazuh Server installed, a client PC (Wazuh Agent) and an attacker PC (penetration testing).

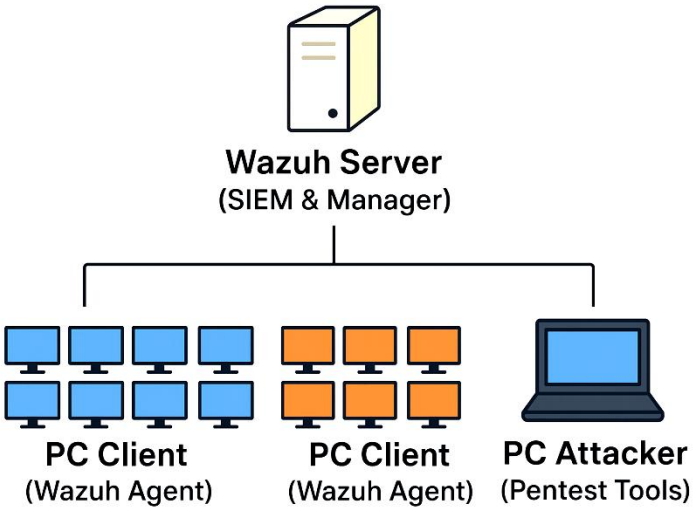


Figure 1. Network Topology Design

Based on Figure 1, the simulation uses the main component of Wazuh Server (SIEM & Manager), a central server that is responsible for managing agents, receiving logs, performing security analysis, and displaying monitoring results on the dashboard. Functions as a core SIEM on a PC Client system with Wazuh Agent. Consisting of 20 endpoints divided into 10 Windows installed. Wazuh Agent specifically for the Windows operating system. This agent sends system logs, event logs, application processes, and user activities to the 10 Ubuntu/Linux servers installed. Wazuh Agent for Linux. This agent records kernel logs, system services, SSH logins, and other activities. All clients are connected to the Wazuh Server via an internal network using the default protocol. PC Attacker (Pentest Tools) acts as an attacker or penetration tester. Used to simulate attacks (e.g., port scanning, SSH/SMB brute force, SQL injection, malware injection). Attacks are directed at the PC Client (Windows/Ubuntu) so that its activities will be recorded by the Wazuh Agent, then forwarded to the Wazuh Server.

Wazuh Indexer

Perform the installation of the Wazuh Indexer server which acts as a storage and processor of security data and logs obtained from the Wazuh Server.

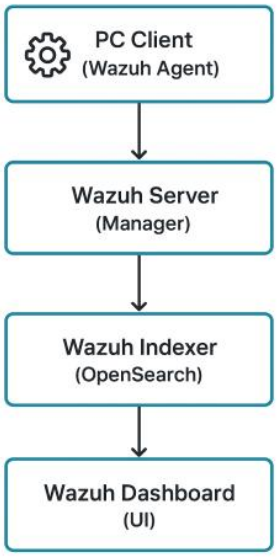


Figure 2. Initial Configuration

Make changes to the Wazuh Indexer configuration file by looking at the server IP address.

```
[root@wazuh-server wazuh-user]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 08:00:27:91:ba:af brd ff:ff:ff:ff:ff:ff
    altname enp0s17
    inet 10.22.66.236/24 metric 1024 brd 10.22.66.255 scope global dynamic eth0
       valid_lft 3543sec preferred_lft 3543sec
    inet6 fe80::a00:27ff:fe91:baaf/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@wazuh-server wazuh-user]#
```

Figure 3. Wazuh IP Configuration

Enable and start the Wazuh Indexer and initialize the cluster on any indexer node. Wazuh loads the new certificate information and starts the cluster.

Wazuh Server

Run the assistant with the wazuh-server option followed by the node name to install the Wazuh server.

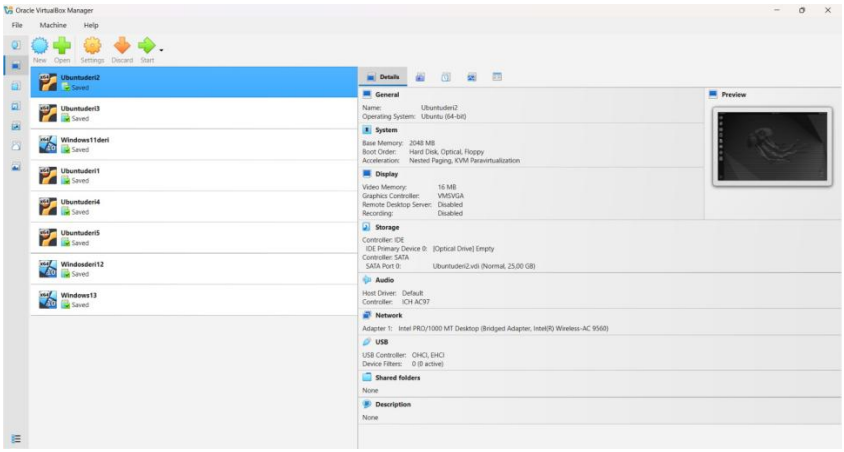


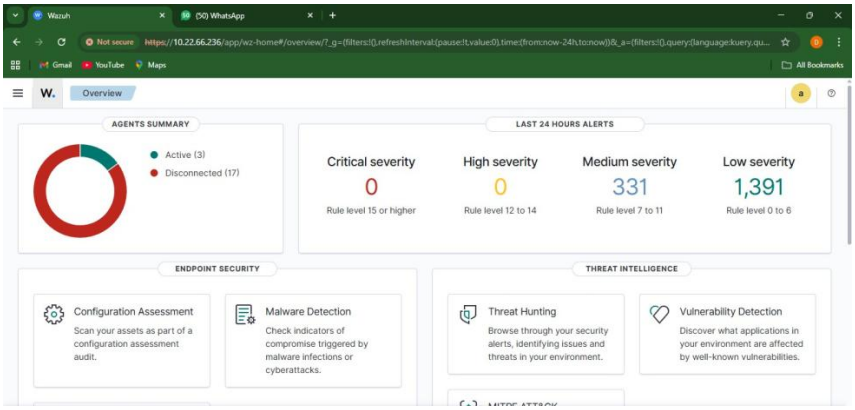
Figure 4. Wazuh Server Installation

Wazuh Dashboard

Install the Wazuh Dashboard as a user interface to display security data reports obtained from the Wazuh Indexer and analyzed by the Wazuh Server. Activate and start the Wazuh Dashboard. Access the Wazuh Dashboard using the IP address of the previously configured server.

Figure 5 Wazuh Login Page

Here is the Wazuh Dashboard display:



Fugure 6. Wazuh Dashboard View

Wazuh Agent

Installing Wazuh Agent on the monitored server to obtain security data, such as logs, system activity and other security information. Here are the steps for installing Wazuh Agent on a Windows endpoint.:

First, select the operating system on which the wazuh agent will be installed.

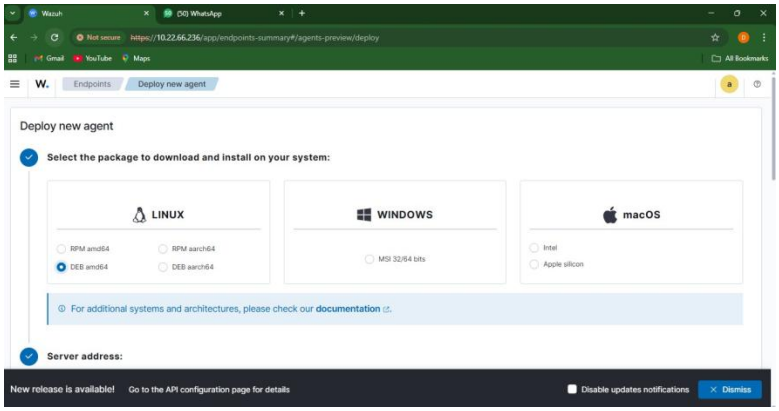


Figure 7. Wazuh Agent Deploy View

After successfully installing the Wazuh Agent on a server, it collects information and data on system and network activity on that server. This information can include system logs, files, open ports, user activity, and more.

Wazuh Integration with Telegram

To simplify system administrators' work, attack notifications were created using a Telegram chatbot to send real-time notifications when an attack occurs. Here are the steps for integrating Wazuh into the Telegram chatbot.

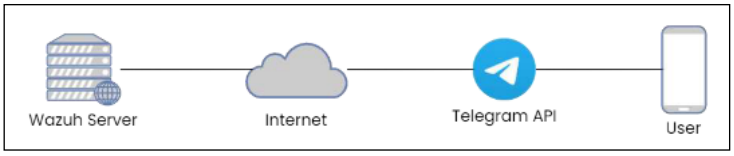


Figure 8. Telegram Bot Integration System

First, create a Telegram Bot using API KEY and CHAT ID using BotFather Telegram.

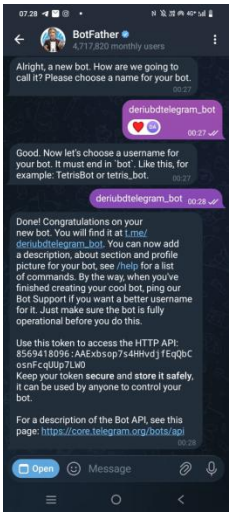


Figure 9. BotFather Telegram

Start a BotFather chat with the /start command, then BotFather will reply by asking for a name for the bot it will create. Once the name is correct and approved, BotFather will send an API key, which we will use to integrate with the Wazuh server..

Security Attack Testing

BruteForce

Bruteforce testing was applied to the Wazuh Agent to attack username and password combinations (login failures). The login failure process was carried out by randomly changing usernames and passwords through trial and error, resulting in user access to the server being blocked. In this test, a bruteforce attack was carried out on the gateway of one of the agents that had a web server installed. The first step was to open the DVWA website previously installed on the Wazuh agent and attempt to log in using various login combinations, such as usernames and passwords.

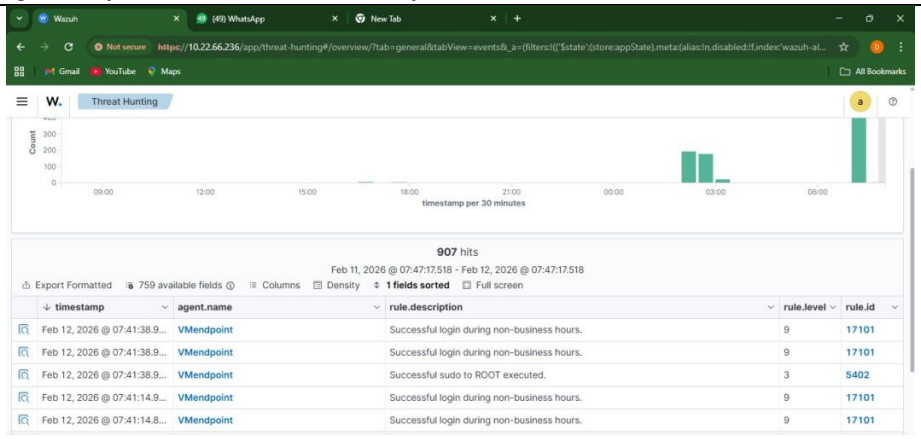


Figure 10. Bruteforce Test Results

The image above shows the results of a brute force attack test, namely a failed login attempt using an invalid username or password.

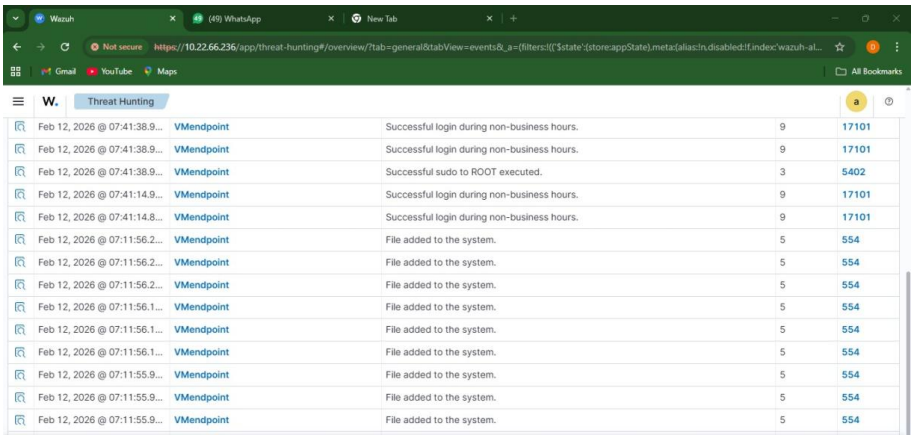


Figure 11. Request Time Out (RTO) Test Results

The image above shows the test results which indicate a Request Time Out (RTO), which is a condition where the internet connection is interrupted when the user tries to access the server.

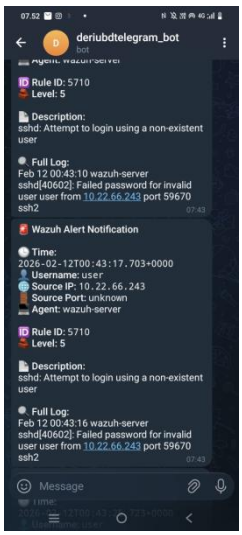


Figure 12. Wazuh Telegram Bot Notification

The image above shows the notification results on the Telegram bot that has been integrated with Wazuh.

DoS Attack (SYN Flood)

SYN Flood is a DoS attack that aims to disrupt server performance by sending fake SYN requests. In this test, a SYN Flood attack was carried out against the Wazuh Agent. This attack was carried out using Ubuntu using the command:
hping3 -S –flood -p 22 102266236

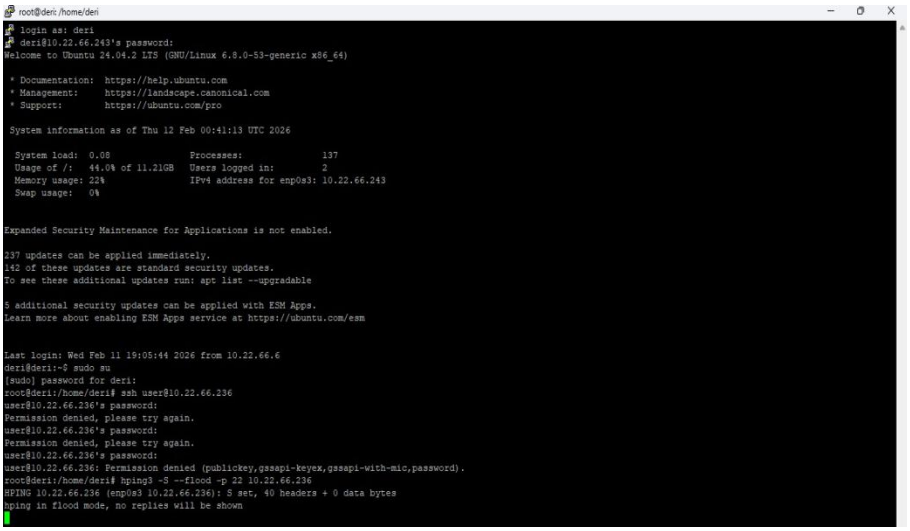
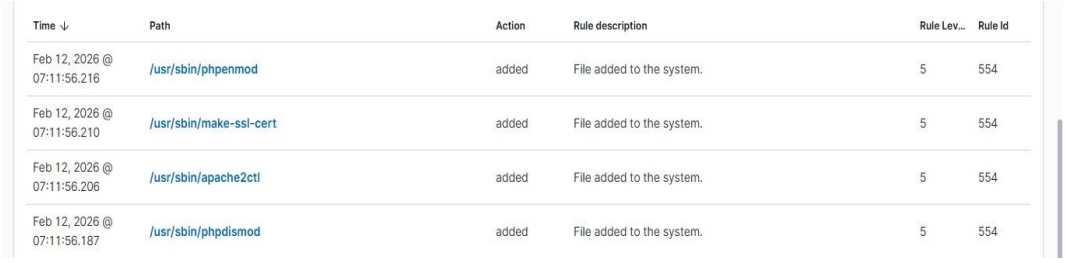


Figure 13. SYN Flood Attack

Below are several explanations regarding the function of each word in the command:

1. "sudo" is a command to give access permission to the superuser to execute commands..
2. “hping3” is used to send network packets and test attacks on the network..
3. “-S” is used to send SYN-signed packets in the TCP protocol. This command can also be used to perform SYN flooding attacks.
4. “--flood” is a command to activate flooding mode on hping3 which sends a high number of network packets at high speed to a specified target.
5. “-p” is a command to display detailed information about each packet sent and received.
6. “-p 20” is the command to determine the target port for the attack.
7. “102266236” is the IP address of the wazuh agent that was the target of the attack.



Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Feb 12, 2026 @ 07:11:56.216	/usr/sbin/phpenmod	added	File added to the system.	5	554
Feb 12, 2026 @ 07:11:56.210	/usr/sbin/make-ssl-cert	added	File added to the system.	5	554
Feb 12, 2026 @ 07:11:56.206	/usr/sbin/apache2ctl	added	File added to the system.	5	554
Feb 12, 2026 @ 07:11:56.187	/usr/sbin/phpdismod	added	File added to the system.	5	554

Figure 14. SYN Flood Test Results

The image above shows the test results that the Wazuh Dashboard has detected a DoS attack that detects attacks against MySQL.

SQL Injection

SQL Injection is an attack that intentionally inserts an SQL query command to obtain data from a database. To increase the effectiveness of the attack, attackers typically use tools such as SQLmap, available in the Kali Linux operating system, which allows for automated SQL injection attacks. In this test, an attack was carried out on the Wazuh Agent, the DVWA website installed on the local server https://102266243/DVWA, using the command:
sqlmap -u "http://102266243/DVWA/vulnerabilities/sqli/?id=1&Submit= Submit" --

cookie="security=low; PHPSESSID=ISI_SESSION_KAMU" --dbs

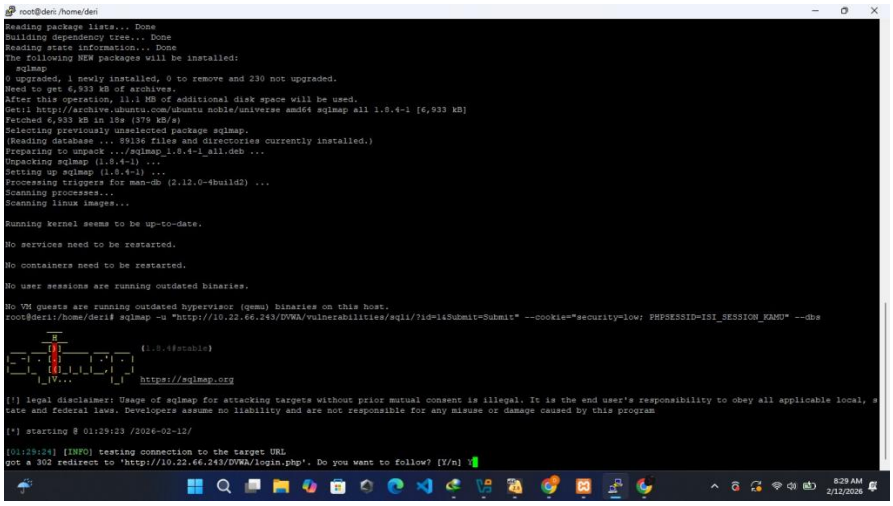


Figure 15. SQL Injection Attack

Below are several explanations regarding the function of each word in the command:
1. “Sqlmap” is a command to automatically exploit SQL Injection vulnerabilities.
2. “-u” is the command to set a URL Address.
3. "https://102266243" is the URL address of the website you want to test.
4. “–dbs” is a command to count available databases.

Vulnerabilities Software

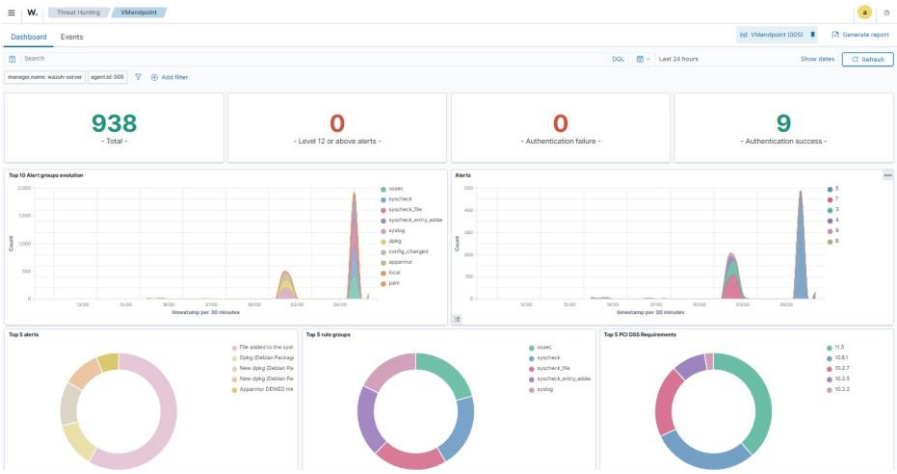


Figure 16. Vulnerabilities Software

The image above shows the results of software vulnerabilities which state that the Wazuh Dashboard detected software that has vulnerabilities, namely the VCL media player which has high/critical vulnerabilities with the highest CVSS (Common Vulnerability Scoring System) score of 98..

Performance Testing

Performance testing is performed to measure the state of the device when receiving an attack, and compare it with the state before the device received the attack. Performance testing is performed on two different devices, namely CPU and Memory. Based on the analysis and discussion of CPU performance under normal conditions or before the attack occurred, it is in the range of 00% to 15%, this percentage indicates that the CPU is in normal condition. Then, after several different attack attempts, the percentage of CPU usage is known to increase to 60%. This indicates that CPU performance increases due to attack activity from users. The increase in CPU load occurs following the large number of events (attacks) that occur at one time against the agent, including several attacks from the public that are detected based on monitoring results on the Wazuh agent and considering several other factors that may occur in the operating system.

5. Conclusion

Conclusion

This research aims to implement and analyze SIEM in the Bina Darma University server ecosystem using Wazuh to manage and monitor security on a network, thus providing convenience in obtaining and collecting network traffic information in real time.

a. This research successfully implemented Wazuh as a tool to effectively manage and monitor security on the studied network. Using Wazuh, the research demonstrated the system's ability to detect and respond to potential security threats. Several attacks, such as brute force attacks, DoS attacks, and SQL injections, were successfully detected by Wazuh, meeting the research's expectations.
b. Visualization based on network incident logs provides a better understanding of security patterns. Thus, the research has achieved its goal of producing a graphical representation of incident logs that can help users identify security threats more effectively.
c. The integration of Wazuh app findings with a Telegram bot as an alert system provides real-time responses to potential security threats. This increases efficiency in responding to detected security incidents.
d. During the attack, the CPU performance percentage increased from 00%-15% to 00%-60%. This was influenced by the number of activity events occurring within the server, which increased the CPU workload. Meanwhile, memory performance measurements under normal conditions ranged from 00%-400%. This indicates that memory performance remained normal, with the same write speed, regardless of server conditions.

Suggestions

The suggestions given in this research are as follows:

a. Wazuh functionality enhancements are recommended for further research. Developing new features or customizing them to meet the specific needs of a particular network environment could be a focus of research..
b. Log Visualization Optimization: Further research is needed to optimize incident log visualization. Improvements in graphical representation and data analysis can help users more easily understand and respond to security threats..
c. Integration Expansion with Other Platforms, research may involve further exploration regarding Wazuh integration with other platforms besides Telegram Integrating the system with various platforms can increase the flexibility and usability of the application.

d. Further Case Studies: As an additional suggestion, further research could involve further case studies with more complex scenarios or larger networks. This could help test and develop the Wazuh application in a broader context.

Reference

[1] B. W. Aulia, "Peran krusial jaringan komputer dan basis data dalam era digital," *JUSTINFO Jurnal Sistem Informasi dan Teknologi Informasi*, vol. 11, pp. 9–20, 2023.

[2] M. H. Rumlus and H. Hartadi, "Kebijakan penanggulangan pencurian data pribadi dalam media elektronik," *Jurnal Ham*, vol. 11, no. 2, p. 285, 2020.

[3] C. Arfanudin, B. Sugiantoro, and Y. Prayudi, "Analisis Serangan Router Dengan Security Information and Event Management Dan Implikasinya Pada Indeks Keamanan Informasi," *CyberSecurity dan Forensik Digit*, vol. 2, no. 1, pp. 1–7, 2019.

[4] E. Soesanto, D. P. Aprillia, N. D. Anjani, and H. D. Halimatusa'diah, "Pengaruh Sistem Pengamanan Objek Vital, File Dan Cyber Terhadap Manajemen Sekuriti," *Cross-border*, vol. 6, no. 1, pp. 705–714, 2023.

[5] L. A. Saputra, F. M. Akbar, F. Cahyaningtias, M. P. Ningrum, and A. Fauzi, "Ancaman keamanan pada sistem informasi manajemen perusahaan," *Jurnal Pendidikan Siber Nusantara*, vol. 1, no. 2, pp. 58–66, 2023.

[6] Z. Munawar and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J-SIKA*, vol. 2, no. 1, pp. 14–20, 2020.

[7] A. Safitri, D. Mafulla, M. W. Nichlah, R. M. Roykhan, S. Devi, and U. Absor, "Analisis Identifikasi Risiko, Penilaian Risiko Dan Pengendalian Risiko," *Jurnal Ilmiah Keuangan Akuntansi Bisnis*, vol. 3, no. 2, pp. 513–518, 2024.

[8] F. A. Saputra, T. R. Dharmawan, and A. Rustianto, "Implementasi Wazuh SIEM untuk Manajemen Log Event," *Jurnal Informatika Terpadu*, vol. 10, no. 2, pp. 146–155, 2024.

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

[10] S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, and A. Setiawan, "Implementasi konfigurasi firewall dan sistem deteksi intrusi menggunakan Debian," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 12, 2024.

[11] C. ARFANUDIN, B. Sugiantoro, and Y. Prayudi, "ANALYSIS OF ROUTER ATTACK WITH SECURITY INFORMATION AND EVENT MANAGEMENT AND IMPLICATIONS IN INFORMATION SECURITY INDEX," *Cyber Security dan Forensik Digital*, vol. 2, no. 1, pp. 1–7, Jul. 2019, doi: 10.14421/csecurity.2019.2.1.1388.

[12] H. Khotimah, F. Bimantoro, R. S. Kabanga, and I. B. K. Widiartha, "Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat," *Jurnal Begawe Teknologi Informasi*, vol. 3, no. 2, 2022.

[13] F. A. Saputra, T. R. Dharmawan, and A. Rustianto, "Implementasi Wazuh SIEM Untuk Manajemen Log Event di Pesantren Teknologi Informasi dan Komunikasi Jombang," *Jurnal Informatika Terpadu*, vol. 10, no. 2, pp. 146–155, 2024.

[14] M. S. Hadi, D. A. P. Putri, and S. Kom, "Implementasi Security Information And Event Management (SIEM) Untuk Deteksi Dan Analisa Insiden Keamanan Pada Web Server," 2023.

[15] M. R. Kamal and M. A. Setiawan, "Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII," *Automata*, vol. 2, no. 2, 2021.

[16] Afridon, M., et al. "Optimizing Data Security in Computer-Assisted Test Applications Through the Advanced Encryption Standard 256-Bit Cipher Block Chaining." *International Journal of Advanced Computer Science & Applications* 15.8 (2024).