J-COSINE (Journal of Computer Science and Informatics Engineering)
Vol. 8, No. 2, December 2024 E-ISSN:2541-0806
Accredited Sinta-4 by RISTEKDIKTI Decree No. 79/E/KPT/2023 P-ISSN:2540-8895

Server Performance Analysis Against Distributed Denial of Service (DDoS) Attacks (Case Study: Mataram University Academic Information System)

Rafli Gunawan Hadi*, Ahmad Zafrullah Mardiansyah, Raphael Bianco Huwae
Dept. Informatics Engineering, Mataram University
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email: rafligunawanhadi@gmail.com, : [zaf, raphael.bianco.huwae]@unram.ac.id

Corresponding Author

Abstract **Information technology advancement has significantly impacted Indonesia's education sector, including the University of Mataram. The university relies on the Sistem Informasi Akademik (SIA) for various academic activities. However, increasing users has led to challenges such as excessive traffic and server downtime. This research analyzes the impact of DDoS attacks on the SIA server's performance and utilizes Zabbix for server monitoring. The results show that DDoS attacks mainly burden the network traffic component, with a significant increase compared to normal conditions. CPU and RAM resources also increased but less significantly. Monitoring with Zabbix improves the efficiency of performance management, enabling real-time monitoring and easy-to-understand visualization. The findings help administrators identify the need to increase server capacity and implement DDoS detection and mitigation systems to maintain the quality and availability of academic services.**

Key Words**: Server Monitoring, Zabbix, Distributed Denial Of Service, Cyber Security, Sistem Informasi Akademik.**

I. INTRODUCTION

Over time, information technology continues to advance and develop. Computer networks and servers are now standard in institutions, companies, or government agencies [1]. A server is one of the hardware components in a computer system that functions as a resource center for data storage and complex special services. Intensive use of servers requires serious consideration regarding the use of resources and their security [2]. Server security includes monitoring and preventing unauthorized use or attacks from external and internal parties to avoid fatal damage to services [1].

Without a real-time monitoring system, server administrators will face significant challenges when operational problems arise, such as excessive CPU usage, high memory consumption, and insufficient network bandwidth. This problem often occurs at Mataram University, especially in the Sistem Informasi Akademik (SIA), which experiences the highest access peak during the Kartu Rencana Studi (KRS) filling period [3]. In the 2023 academic year, approximately 205,000 users accessed the SIA between February and July, often causing server downtime. This research uses Zabbix, a highly effective, open-source server monitoring tool, to monitor the performance of network components and SIA server resources to avoid overloading. Zabbix offers notification and alarm features, which make it easy for administrators to manage multiple servers and systems simultaneously with minimal supervision [4].

This research tests the performance of network components and server resources using DDoS attacks. A Distributed Denial of Service (DDoS) attack is a variant of a Denial of Service (DoS) attack that uses many distributed resources to launch a significant attack against a target [5]. These attacks can disrupt or shut down services in a system, preventing legitimate users from accessing available services [6]. The main difference between DoS and DDoS lies in the scale and resources used; DDoS attacks use multiple distributed resources or networks, causing victim hosts to run out of resources such as memory, CPU, and traffic capacity [7].

According to a recent report from Arbor Networks, DDoS attacks increased by 20% in 2023 compared to the previous year. Data from Kaspersky Lab shows that the most significant DDoS attack in 2023 reached a peak traffic of 2.5 Tbps. In addition, Akamai reports that the financial and technology sectors are the most frequently targeted attacks, with each accounting for more than 30% of the total DDoS attacks detected. A case study of a significant attack in October 2022 shows how DDoS attacks significantly impact digital infrastructure. A large e-commerce company experienced more than 12 hours of downtime, resulting in financial losses of $5 million and loss of customer confidence. In another case, an attack on DNS provider Dyn in 2016 caused significant disruptions to well-known websites such as Twitter, Netflix, and Reddit.

Therefore, this research analyzes server performance against DDoS attacks using the Zabbix monitoring and hping3 testing tools. With the increasing frequency and complexity of DDoS attacks, it is crucial to understand how servers respond to such attacks and how to optimize

settings to mitigate their impact. This research will provide valuable insight into the steps that can be taken to improve resilience to DDoS attacks, which is particularly relevant for organizations looking to protect their digital infrastructure.

II. Literature Review and Basic Theory

A. Related Research

Research on system performance monitoring has been widely conducted to evaluate and improve systems. Several previous studies have been used to reference this research.

One such study is titled "Desain dan Implementasi Sistem Monitoring Sumber Daya Server Menggunakan Zabbix 4.0" conducted by Sulasno and Rakhmat Saleh in 2020. This research resulted in a system for monitoring server resource usage, which can be displayed on a real-time dashboard and accessed via the Internet by administrators [8].

In the study titled "Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary" conducted by Sri Suharti, Anton Yudhana, and Imam Riadi in 2022, research was carried out on digital evidence of various DDoS tools capable of compromising web server performance on proprietary operating systems, resulting in performance degradation. The findings revealed that DDoS attacks can disrupt and increase traffic by 92,84%, leading to a 78% decrease in server performance, ultimately causing server downtime [9].

In the study titled "Perancangan Sistem Monitoring Performa Aplikasi Menggunakan OpenTelemetry dan Grafana Stack" conducted by Guntoro Yudhy Kusuma and Unan Yusmaniar in 2022, system monitoring was conducted using Grafana tools, which can generate alerts via Slack when anomalies in the collected metric data occur. The implementation of OpenTelemetry in the application negatively impacted application performance, leading to a decrease in request throughput by an average of 23,32% [10].

In the study titled "Implementasi Zabbix Server Untuk memonitor Kondisi Jaringan Komputer Di Dinas Komunikasi dan Informatika Kabupaten Pekalongan" conducted by Arief Budi Cahyo and Tony K. Hariadi, Zabbix was implemented to monitor the computer network conditions at the Department of Communication and Informatics. Zabbix was chosen due to its flexibility and capability of reaching systems of varying scales from small to large. After researching and analyzing the network resource conditions of the system, the installation of Zabbix made it easier for administrators to perform monitoring and checks as the network resource conditions were displayed on the dashboard page in graphical form [11].

In the study titled "Website Security Analysis Against DDoS Attacks Using the National Institute of Standards and Technology (NIST) Method", conducted by Yunanri W and Yuliadi in 2023, DDoS attacks were evaluated using various open-source frameworks, tools, and source codes on terminal networks to analyze website security [12].

Based on the explanations in several previous studies that have been collected, the authors conducted research on testing attacks using Distributed Denial of Service (DDoS) on server performance at the Sistem Informasi Akademik (SIA) of Mataram University. The difference between the research conducted and previous research lies in the server monitoring tool used and the test object, which is the test objective.

B. Supporting Theory

The following are general theories that are used as support in this research:

B.1. Information System Security

Information System Security is a vital asset to maintain. Companies or agencies must pay serious attention to maintaining the security of their information because incidents of data leakage or system failure can negatively impact their finances and productivity. Aspects of factors that must be considered in Information System Security include relevance to the current environment and compliance with applicable standards and guidelines [13].

By prioritizing information system security, managers can identify potential attacks on agency data at an earlier stage. By detecting early, managing agencies can take proactive measures to prevent attacks or risks that may occur [14]. Three main aspects are often referred to by the abbreviation CIA (Confidentiality, Integrity, Availability), which has the following meaning:

- Confidentiality: This aspect of confidentiality refers to ensuring that only authorized persons with legal access rights can view the information.
- Integrity: This aspect, which means integrity (intact), focuses on ensuring that the data is not changed without permission from the authorized party to remain accurate and intact.
- Availability: This aspect, which means availability, ensures that data is always available when needed, anytime and anywhere.

B.2. Server Monitoring

Monitoring is a technology that allows a person to monitor and understand what needs to be known. The primary purpose of using a monitoring system is to obtain information more quickly when a disturbance or problem occurs [4].

A server is a computer system that provides exceptional services in a computer network. A server is needed to maximize network utilization as a container for various data and information. In its role as a server, the performance and efficiency of data processing can be influenced by the architecture and technology used [15]. A server has essential components that include hardware and software. The hardware components needed by the server consist of a CPU (Central Processing Unit), RAM (Random Access Memory), Hard Disk / Storage, and NIC (Network

Interface Card), which allows the server to connect to the network. The software components needed by the server are the server operating system and server applications, such as the web server and the database server used to store client data [16].

Server monitoring is an important activity or practice that is carried out to monitor the state and server performance. This server monitoring process is carried out regularly to ensure that the server is operating correctly. A server can be said to be good if the availability of services can be accessed without interruption, optimal performance can handle the workload as expected and has sufficient storage capacity and resources, such as CPU, RAM, and network components such as network traffic that can affect the availability of server services, in order to support the workload run by the server [17]. In this study, monitoring specific servers is carried out to maintain server performance so that it continues to run correctly without any interference in terms of CPU usage, RAM consumption, and network load generated by the server as a supporter of data transfer.

B.3. Zabbix

Network monitoring is required in an organization to monitor network or system performance and problems in real time. One of the applications used to perform network monitoring is Zabbix. Zabbix is an application that monitors the availability and performance of open-source computer code, or it can be called open source. Zabbix's advantage is that besides this software being free to use, the UI (User Interface) can be easily understood because it can produce statistics in the form of graphs. Zabbix can also create network maps (maps) and display graphs of network conditions being monitored [18].

Several main components exist in the Zabbix architecture in order to support the use of network monitoring tools, including:

- Zabbix Server, is the core component of the Zabbix system. It is responsible for receiving data from the client and displaying it on the dashboard.
- Zabbix Agent, is a component that retrieves and collects data from the client and sends it to the Zabbix server.
- Zabbix Web Interface, is where the data the Zabbix server has received will be displayed. After a configuration is made, the data will appear on the dashboard.

B.4. Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) is a series of Denial of Service (DoS) attacks involving more than one traceable address. In general, DDoS attacks use botnets/zombies as attacking entities. The attack concept or workings of a DDoS attack is to send data packets continuously with a single or joint target destination. Commonly used packet types include TCP fragments (TCP syn flood attack), ICMP (ping to death), and UDP (UDP flood attack). The primary purpose of this attack is to disrupt the availability of server services used by the target system by overloading the network so that the system can no longer serve legitimate user requests [19].

DDoS attacks target organizations or companies connected to the Internet in two primary forms: consuming network bandwidth and system resources or exploiting bugs in software. Hping3 was chosen as a tool to launch DDoS attacks due to its flexibility in sending packets using TCP, UDP, and ICMP protocols. Hping3 allows customization of parameters such as port number, packet size, and sending frequency, making it an effective tool for simulating different types of DDoS attacks. The protocol types supported by hping3 include:

- TCP (Transmission Control Protocol): Used to test connections that require reliability and sequential delivery.
- UDP (User Datagram Protocol): Used for traffic that does not require sequential delivery, such as streaming video or voice.
- ICMP (Internet Control Message Protocol) is often used to send network error messages and operational information.

Hping3 can generate network traffic in various volumes and intensities. For example, hping3 can send thousands of packets per second, varying in size from 64 bytes to tens of thousands of bytes. This flexibility enables realistic simulations of DDoS attacks, helping researchers test server capacity and resilience. For example, an attack with a packet size of 1000 bytes at a frequency of 1000 packets per second can consume bandwidth, while a 60,000 byte packet at a lower frequency can overload network traffic and increase the performance of both CPU and RAM resources.

B.5. Sistem Informasi Akademik (SIA)

An information system in an organization is designed to manage daily transactions to support organizational operations and provide information needed for decision-making by authorized parties [20]. A Sistem Informasi Akademik (SIA) system manages educational information at various levels of educational institutions, both formal and informal, from primary to tertiary levels. Data generally managed in Sistem Informasi Akademik (SIA) includes information about students, lecturers, courses for each semester, course schedule data, and other relevant information according to the needs of each educational institution. In a more straightforward framework, Sistem Informasi Akademik (SIA) can be explained as applications that aim to facilitate and simplify the management of data and information related to educational institutions [21].

III. Research Methodology

The figure shows the research flow regarding the Analysis of Server Performance Against DDoS Attacks conducted on the Sistem Informasi Akademik of the University of Mataram.

A. Research Flow

The following is a flowchart that explains the flow of this research.

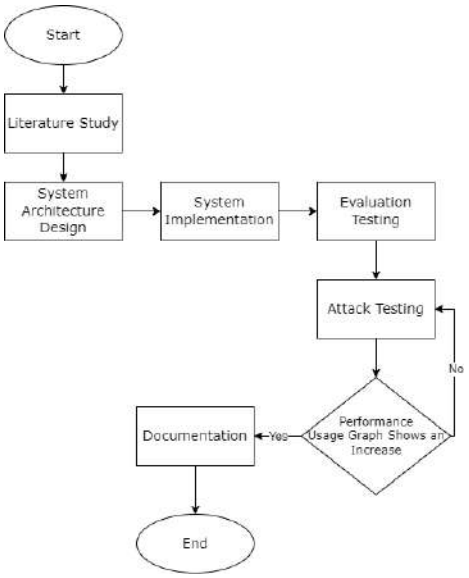

Fig. 1. Research Flow Diagram.

TABLE I. RESEARCH FLOW

Stages	Explanation
Literature Study	The initial stage of the research involved looking for previous journals related to the research topic to use as a reference for the author. The literature used includes topics related to information system security, server monitoring systems, implementation of server monitoring tools, Distributed Denial of Service (DDoS) attack algorithms, and Sistem Informasi Akademik (SIA) Universitas Mataram.
System Architecture Design	The system architecture design involves conceptualizing the architectural framework and outlining the system's workflow. This design starts with setting up the server monitoring system, Zabbix, on the University of Mataram's host server. It is then followed by installing agents on the target servers (SIA).
System Implementation	The system implementation involves creating the system based on the previously designed concept.
Evaluation Testing	The evaluation testing stage aims to verify whether the testing results align with the objectives set in the research, starting from measuring performance, checking consistency, and evaluating the conformity of the data.
Attack Testing	In the attack testing phase, a DDoS attack simulation is carried out on the target host server using the hping3 tool. The attack is carried out periodically by increasing the payload size in each experiment to observe changes in server performance. Tests are carried out until a significant increase in CPU usage, RAM, and Network Traffic is observed, as shown in the server visualization graph.
Documentation	Documentation involves recording the testing results and writing a report summarizing the overall research findings.

B. Requirements Analysis

As for the requirements analysis in this study, such as the server specifications used by the Zabbix server monitoring system, the specifications of the SIA target server, and also the specifications of the attacker's computer using the virtual server needed for testing, as follows:

B.1. Zabbix Monitoring Server

A dedicated virtual server with the following specifications is provided for installing monitoring tools using the Zabbix platform.

- Operating System : Linux Ubuntu 20.04 LTS
- RAM : 2 GB
- CPU : 1 Core
- Storage : 15 GB

B.2. SIA Target Server

The main testing target in this research is the server used by the Sistem Informasi Akademik (SIA) at the University of Mataram. With higher specifications, this server is designed to handle larger workloads, such as MIS applications that require fast and stable data processing.

- Processor : 4 x Intel(R) Xeon(R) CPU E3-1225 v5 @ 3.30GHz (1 Socket)
- RAM : 16 GB
- CPU : 4 Core
- Storage : 100 GB SSD
- Bandwidth: 5.2 Gbps

B.3. Attacker Computers

Two dedicated servers with the same specifications were used as attacker computers in launching the simulated DDoS attack.

- Operating System : Linux Ubuntu 22.04 LTS
- RAM : 4 GB
- CPU : 4 Core
- Storage : 20 GB

C. System Design

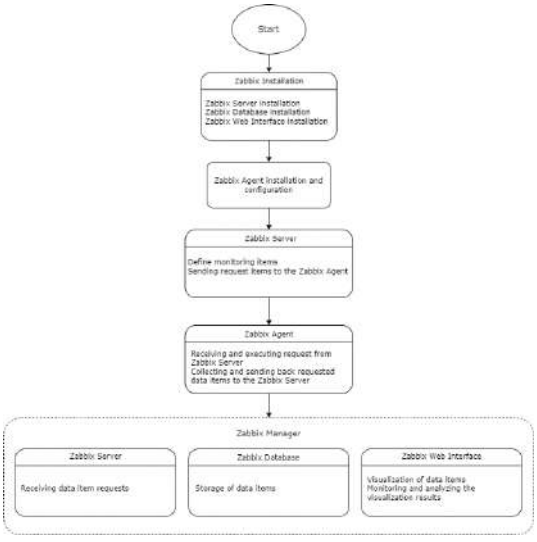

Fig. 2. System Design Diagram.

- The first stage is Zabbix Installation, which involves installing the three main components of Zabbix: Zabbix Server collects and processes monitoring data

from hosts for performance analysis and enables host management and configuration of monitoring items; Zabbix Database stores all system configuration, monitoring data history, and performance analysis needs; and Zabbix Web Interface provides a web-based interface for management, configuration, and visualization of monitoring data through graphs, reports, and tables.

- Zabbix Agent Installation and Configuration in the next step, the SIA Unram server host is installed as a client or monitoring target. The Zabbix Agent is then configured to integrate it and enable data exchange with the Zabbix Server.
- Zabbix Server determines the data items to be monitored and displayed. It sends data item requests to the Zabbix Agent on the SIA Unram server host.
- Zabbix Agent receives and promptly executes requests the Zabbix Server sends. After receiving the requested data item information, the data item is sent back to the Zabbix Server for monitoring.
- Zabbix Server receives the data items sent by the Zabbix Agent, stores them, and visualizes them in graphs. The data items can then be directly analyzed for information on the performance of the SIA Unram server.

D. Network Topology

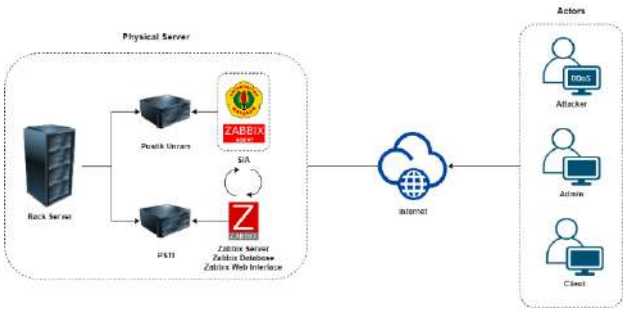

Fig. 3. Network Topology.

Figure 3 shows the architecture of the self-designed and custom-built system, especially during the installation of the system components. It can be seen that there is a server rack containing two server stacks, namely Pustik Unram and PSTI. The SIA host and Zabbix Agent installation are inside the Pustik Unram server stack. Meanwhile, the Zabbix Server, Zabbix Database, and Zabbix Web Interface, the main framework of the monitoring system, are installed on a different server stack, PSTI. Although the SIA and Manager host servers are on different server stacks, information exchange between the SIA host and Zabbix Server can still be done through the installed Zabbix Agent. This is facilitated by configuring host creation so the Zabbix Agent and Zabbix Server can integrate or connect. The attacker will perform a DDoS (Distributed Denial of Service) attack on the SIA server, the test target. The attacker will simulate a DDoS attack over the internet to disrupt the availability of services the target server provides. After that, the administrator will monitor the resources and network traffic affected by the attack using the Zabbix monitoring system, which can be accessed through the Zabbix Web Interface on the manager device.

E. Testing Scenario

In the test scenario, the Zabbix monitoring system will be installed on the dedicated host server that has been provided. After the device installation is successful, the Zabbix Agent installation configuration is carried out on the SIA host server as the client to be monitored. Host creation is then performed on the Zabbix Server to add the monitored host to Zabbix, and the monitoring graph of resources and network traffic from the client-server is displayed. The specific Test Scenario Flowchart design for this research can be seen in Figure 4.

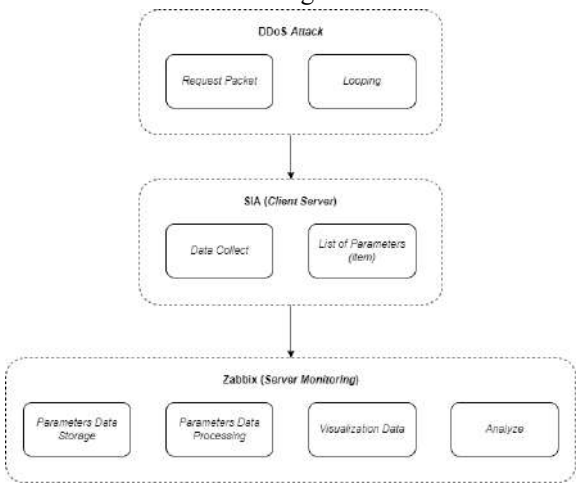

Fig. 4. Flowchart Testing Scenario.

- The test begins by simulating a DDoS (Distributed Denial of Service) attack on the SIA client server by sending excessive Request Packets. This aims to load the network traffic, impact the client-server resources, and make the service inaccessible to legitimate users, commonly called "server down." Service requests are sent continuously with increasing resources and attack duration until server service availability is compromised.
- The Zabbix agent installed on the SIA client server collects the requested parameter data (items) and sends the parameter list to the Zabbix Server for storage and processing.
- Subsequently, the Zabbix Server stores this parameter data in a database. The Zabbix Server processes the parameter data to calculate the minimum (min), average (avg), and maximum (max) usage of network bandwidth and server resources.
- Then, Zabbix Server visualizes the parameter data in graphical form. Data parameters can be visualized in the Zabbix Web Interface, making it easier for administrators to analyze performance changes on the SIA client server.

F. Evaluation Testing

DDoS attack testing uses the hping3 tool to understand the attack's impact on server performance. Parameters

monitored in this test include CPU usage, RAM usage, and network traffic. Tests were conducted using two computer attack scenarios to obtain significant results.

In the first scenario, the attack was carried out using one computer and lasted 9 minutes. The test was conducted eight times with different payload sizes, ranging from 1000, 5000, 10.000, 20.000, 30.000, 40.000, 50.000, and 60.000 bytes.

The second scenario involved attacking two computers simultaneously but with different attack durations of 6 minutes. Like the first scenario, the test was conducted eight times with the same payload size, ranging from 1000 to 60.000 bytes. Using two attacked computers is expected to obtain more comprehensive and significant data on the impact of DDoS attacks on server performance.

The results of these two scenarios will provide a clear picture of the impact of DDoS attacks with various payload sizes and attack durations on the parameters monitored, thus helping to formulate more effective mitigation strategies.

G. Report Documentation

At this documentation stage, after completing the system testing, the focus will shift to documentation and report creation. The testing results will be documented, and conclusions will be drawn based on them. The conclusions obtained will serve as a useful reference for further research.

IV. Results And Discussion

A. Normal Server Conditions

The simulation stage of attack testing in this study is carried out on the target server, the SIA server, with parameters that will be monitored for changes, namely CPU, RAM, and Network Traffic. Tests will be carried out using the test evaluation design described earlier. Table II shows data showing the use of the three parameters, ranging from CPU usage to RAM and Bits received and Bits sent on network traffic under normal conditions before the DDoS attack.

TABLE II. Normal Condition Of The Server Without DDoS Attack

Parameters		Min	Avg	max
CPU		0,498 %	1,336 %	3,377 %
RAM		7,701 %	9,647 %	11,786 %
Network Traffic	Bits received	2.15 Mbps	6.65 Mbps	13.26 Mbps
	Bits sent	2.47 Mbps	3.2 Mbps	5.67 Mbps

A.1. Normal CPU Usage

Under normal conditions, the server showed low to moderate CPU usage. The visualization of the Zabbix dashboard can be seen in the following figure.

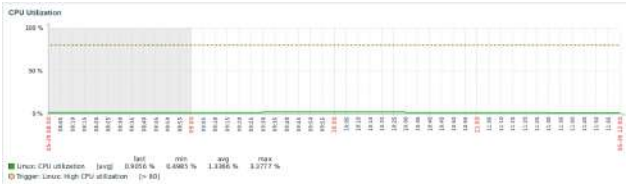

Fig. 5. Normal CPU Utilization Conditions before Attack Testing.

In Figure 5 shows, the minimum CPU usage of 0,4985% indicates that the server is very light on processor usage. In comparison, the average usage of 1,3366% indicates that a small portion of the CPU capacity is used to handle routine tasks. The maximum CPU usage of 3,3777% indicates periods of higher workload but is still within manageable limits without causing disruption to services.

A.2. Normal RAM Usage

Under normal conditions, the server showed stable RAM usage with controlled fluctuations.

Fig. 6. Normal RAM Usage Condition before Attack Testing.

In Figure 6, minimum RAM usage of 7,7012% indicates that most memory is still available for other applications or processes. The average usage of 9,6474% shows balanced memory usage. In comparison, the maximum RAM usage of 11,7869% shows increased memory usage at certain times but is still within safe limits without indicating a memory shortage.

A.3. Normal Network Traffic

Network Traffic refers to the amount of data received and sent over the network in units of megabits per second (mbps). Under normal conditions, the server exhibits stable network traffic patterns with consistent data transmission rates.

Fig. 7. Normal Conditions of Network Traffic before Attack Testing.

In Figure 7, minimum bits received of 2.15 Mbps and minimum bits sent of 2.47 Mbps show that the server can handle light network traffic steadily. An average of 6.65 Mbps of bits received and 3.2 Mbps of bits sent indicates continuous communication activity but within manageable limits. The maximum bits received of 13.26 Mbps and bits sent of 5.67 Mbps indicate a spike in traffic that occurs at certain times but can still be handled by the available network capacity without experiencing a decrease in service quality.

B. DDoS Attack Testing

During the attack testing phase of this research, the DDoS attack tool hping3 was used to create and send customized packets with various payload sizes to simulate a Distributed Denial of Service attack and observe changes

in server performance. The DDoS attack simulation involves sending TCP SYN packets continuously to the IP address of the target server. The commands used were:

```
hping3 -S -d [data size] --flood --rand-source [IP target]
```

Where the "`-S`" option sets the SYN flag on the TCP packets sent, "`-d [data size]`" specifies the size of the data in each payload. In this research, the data size has been determined according to the previous test evaluation, starting from the payload size of 1000, 5000, 10.000, 20.000, 30.000, 40.000, 50.000, and 60.000 bytes in each sent packet, "`--flood`" directs hping3 to send packets as fast as possible without waiting for a response, and "`--rand-source`" generates a random source IP address for each packet sent, to mimic attacks from different IP sources. Then, the "`[IP address]`" part is the IP of the target server to be attacked. Testing experiments with this configuration can result in network traffic on the target server becoming busy and affecting CPU and RAM resources as it continues to try to process connection requests that are never complete.

C. Testing Simulation Results

The results of testing simulations of DDoS attacks using the hping3 attack tool with the TCP SYN flood protocol using one and two attacker computers targeted at the SIA network. Then, the differences in CPU usage, RAM consumption, and network traffic between the two test scenarios can be seen.

C.1. One Attack Computer

This section shows the results of testing the attack with one computer. In each experiment, the size of the payload sent differs and increases to see the difference in CPU usage, RAM, and network traffic.

TABLE III. TEST RESULTS WITH ONE ATTACKER COMPUTER

Number of Computers	Duration (minute)	Payload Size (bytes)	Parameters		
			CPU (%)	RAM (%)	Network Traffic
One Attack Computer	9	1000	1,415	7.968	584.44 Mbps
		5000	7,007	8,734	852.18 Mbps
		10.000	5,719	7,885	925.07 Mbps
		20.000	4,822	8,170	924.17 Mbps
		30.000	3,944	7,454	923.22 Mbps
		40.000	3,802	7,533	994.12 Mbps
		50.000	3,723	6,998	1.05 Gbps
		60.000	4,043	7,404	1.04 Gbps

Based on Table III, the test results show the performance changes after a DDoS attack with one attacker computer.

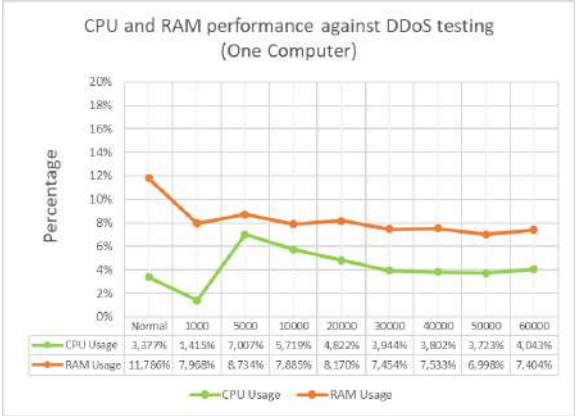

Fig. 8. Line Chart of Testing Results for One Attacker Computer.

Figure 8 shows a line chart showing the difference in CPU and RAM usage during normal conditions and during DDoS attacks. In general, DDoS attacks tend to decrease CPU and RAM usage compared to normal conditions. The detailed analysis can be seen as follows.

C.1.1. CPU Usage

The CPU usage parameter shows that at a payload size of 1000, the CPU usage is 1,415%. The increase in CPU reaches its peak at payload size 5000, with an increase of 7,007%. After payload size 5000, the increase in CPU tends to decrease, with the lowest increase of 3,723% at payload size 50,000 and slightly increasing at payload size 60.000 to 4,043%. The performance utilization rate on the CPU parameter shows a non-linear increase with increasing payload size.

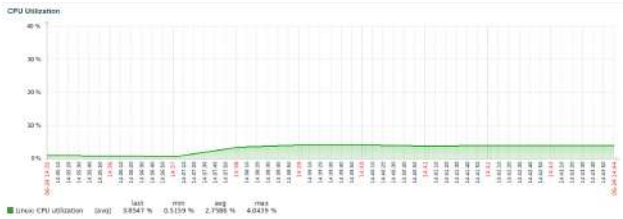

Fig. 9. CPU Usage Condition with Highest Payload Size (One Computer).

Figure 9 displays a visualization from Zabbix showing the CPU performance conditions when under attack from the highest payload size of 60,000 bytes with one attacking computer.

C.1.2. RAM Usage

Based on the test experiment results, the RAM (memory) usage parameter at payload size 1000 shows a usage of 7,968%. After payload size 5000, the increase in RAM tends to vary but generally decreases, with the lowest increase of 6,998% at payload size 50.000 and a slight increase at payload size 60.000 to 7,404%. RAM usage is similar to CPU, with a peak increase at payload size 5000. After that, RAM usage decreases, indicating that RAM is not the main bottleneck in this DDoS attack.

Fig. 10. RAM Usage Condition with Highest Payload Size (One Computer).

Figure 10 displays a visualization from Zabbix showing the RAM performance conditions when under attack from the highest payload size of 60.000 bytes with one attacking computer.

C.1.3. Network Traffic

Network traffic significantly increased as the payload size sent in each packet increased. The highest increase was recorded at payload 50.000, which amounted to 1.05 Gbps. At payload 20.000, the increase in network traffic was 924.17 Mbps, indicating that the DDoS attack affected the most affected component network.

Fig. 11. Network Traffic Conditions at the Highest Payload Size (One Computer).

Figure 11 displays a visualization from Zabbix showing the network traffic load when attacked from the highest payload size of 60.000 bytes with one attacking computer.

C.2. Two Attack Computers

Table IV shows the results of testing the attack with two computers and a shorter duration of 6 minutes. In each experiment, the size of the payload sent increases to see the difference in CPU usage, RAM, and network traffic.

TABLE IV. TEST RESULTS WITH TWO ATTACK COMPUTERS

Number of Computers	Duration (minute)	Payload Size (bytes)	Parameters		
			CPU (%)	RAM (%)	Network Traffic
Two Attack Computers	6	1000	2,270	8,457	1.27 Gbps
		5000	9,179	8,282	1.51 Gbps
		10.000	8,630	8,063	1.96 Gbps
		20.000	7,834	17,644	1.92 Gbps
		30.000	6,195	7,087	2 Gbps
		40.000	5,765	6,932	1.93 Gbps
		50.000	5,370	6,892	1.84 Gbps
		60.000	5,833	7,611	2.03 Gbps

Based on Table IV, the payload size used in this experiment is the same as the previous test, with a different attack duration of 6 minutes. The test results show the performance changes after the DDoS attack with two computers.

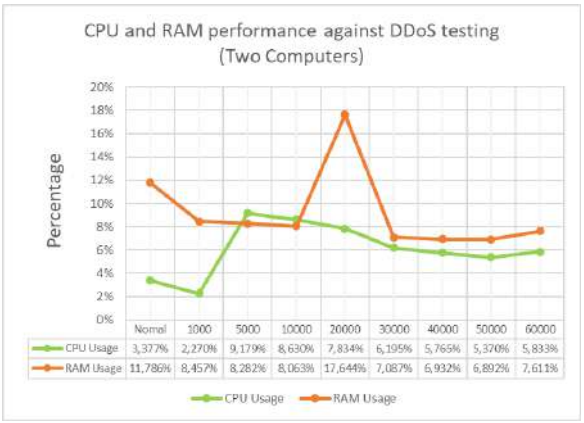

Fig. 12. Line Chart of Testing Results for Two Attacker Computers.

Figure 12 is a line chart showing the difference in CPU and RAM usage during normal conditions and a DDoS attack with two attacker computers. In general, DDoS attacks tend to increase CPU usage compared to customary conditions, while RAM usage shows inconsistent variations, with some payloads causing significant increases in RAM usage. The detailed analysis can be seen as follows.

C.2.1. CPU Usage

At a payload size of 1000, the CPU utilization is 2,270%, and the CPU increase peaks at a payload size of 5000 with an increase of 9,179%. The CPU increase tends to decrease after payload size 5000, with the lowest increase of 5,370% at payload size 50.000 and a slight increase to 5,833% at payload 60.000. CPU usage is similar to the test scenario using one attacker computer, with a significant increase at payload 5000 and a decrease after that. However, the CPU increase in this test scenario was higher than the previous test scenario. This indicates that coordinating attacks from two attacker computers is more taxing on the CPU.

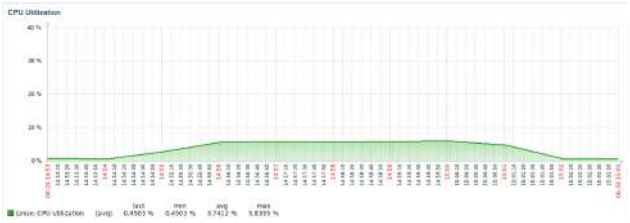

Fig. 13. CPU Usage Condition with Highest Payload Size (Two Computers).

Figure 13 displays a visualization from Zabbix showing the CPU performance conditions when under attack from the highest payload size of 60.000 bytes with two attacking computers.

C.2.2. RAM Usage

The RAM usage at payload size 1000 is 8,457%, and the increase in RAM reaches its peak at payload size

20.000 with an increase of 17,644%. After payload size 20.000, the increase in RAM tends to vary but generally decreases, with the lowest increase of 6,892% at payload size 50.000 and a slight increase to 7,611% at payload 60.000. RAM usage is different from the test scenario with one computer. At a payload size of 20.000, there is a significant spike in RAM usage, which then decreases at higher payload sizes. This shows that RAM becomes more burdened with attacks from two computers at a specific payload before stabilizing.

Fig. 14. RAM Usage Condition with Highest Payload Size (Two Computers).

Figure 14 displays a visualization from Zabbix showing the RAM performance conditions when under attack from the highest payload size of 60.000 bytes with two attacking computers.

C.2.3. Network Traffic

Network traffic increased significantly as the payload size increased. The highest increase was recorded at a payload size of 60.000 at 2.03 Gbps. At higher payload sizes (30.000 to 60.000), the increase in network traffic was relatively stable at around 2 Gbps, indicating that the network was the most affected component by the DDoS attack with two computers.

Fig. 15. Network Traffic Conditions at the Highest Payload Size (Two Computers).

Figure 15 displays a visualization from Zabbix showing the network traffic load when attacked from the highest payload size of 60.000 bytes with two attacking computers.

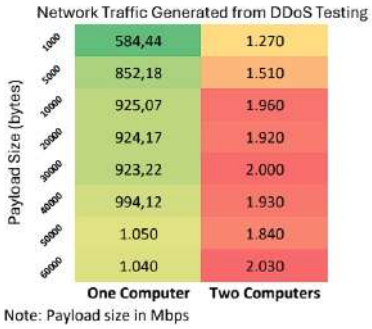

Fig. 16. Network Traffic Heatmaps.

In Figure 16, the results of network traffic testing using one and two attacker computers are displayed as a heatmap with units of Mbps, where the smallest value is colored green, and the highest value is colored red. The lowest throughput value for one attacker computer is 584,44 Mbps (payload 1000 bytes), and the highest is 1.050 Mbps (payload 50.000 bytes). As for two attacker computers, the lowest throughput is 1.270 Mbps (payload 1000 bytes), and the highest is 2.030 Mbps (payload 60.000 bytes).

D. Analysis Result

In evaluating the test results of DDoS attacks using hping3 with normal server performance conditions based on server monitoring using Zabbix, it was found that CPU usage increased compared to normal server performance conditions in attacks with one computer. The highest CPU usage occurred in payload 5000 at 7,007%, which only reached 3,377% under normal conditions. The highest RAM usage during attack testing occurred on payload 5000 at 8,734%, and when compared to normal conditions, which reached 11,786%, there was no significant increase that did not affect these parameters. The highest network traffic at payload 50.000 reached 1.05 Gbps, previously only 13.26 Mbps. Then, in the attack with two computers, CPU usage experienced the highest increase at payload 5000 of 9,179%, showing a similar increase to that of one computer. The highest RAM usage was at payload 20.000 of 17,644%, which, compared to normal conditions, experienced a relatively high increase. The highest network traffic at payload 60.000 reached 2.03 Gbps, which indicates that the parameter experienced the most significant spike. DDoS attacks that use the TCP protocol, such as SYN flood, and with more attacker resources, are effective in flooding the TCP protocol. These attacks have a significant impact, especially on network traffic, which overloads the network capacity with large amounts of data packets sent to disrupt or stop the service access on the server.

V. Conclusion and Suggestion

This research analyzes the performance changes that impact the performance of the SIA server through simulation testing of DDoS attacks that can disrupt network traffic and overload server resources. The test results found that the network traffic component was the most burdened, increasing significantly compared to the initial conditions or regular use. CPU and RAM, part of the server resources, also experienced an increase in load due to the server's efforts to handle and process massive traffic during an attack. However, the increase is not significant but indicates an additional load. It can be concluded that network traffic is the component most affected by DDoS attacks, with a significant increase in load size.

These findings show that using Zabbix server monitoring positively impacts human resource efficiency because it can provide real-time monitoring of the monitored server network by presenting visualizations in the form of detailed and easy-to-understand statistical graphs. This allows server administrators or managers to

monitor and analyze performance changes and consider increasing performance capacity, if needed, to handle CPU usage, RAM, and network traffic spikes. In addition, server managers can also implement effective DDoS detection and mitigation systems to identify and block malicious traffic before it reaches the server.

ACKNOWLEDGEMENT

The author would like to thank the University of Mataram, especially the Department of Informatics Engineering, where the author can learn a lot and get facilities during this research. Thanks also to the administrator and management team at UPT Pustik Unram, who have guided and provided research materials, and to the people closest to the author who have provided support and help during the research.

REFERENCES

[1] K. A. Marta, B. Hartawan, and S. Satwika, "Analisis Sistem Monitoring Keamanan Server dengan SMS Alert Berbasis Snort," Information System and Emerging Technology Journal, vol. 1, no. 1, pp. 25–40, Jun. 2020.

[2] R. Yulvianda and M. Ismail, "Desain dan Implementasi Sistem Monitoring Sumber Daya Server Menggunakan Zabbix dan Grafana," Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM), vol. 3, no. 1, pp. 322–329, Apr. 2023.

[3] A. Zubaidi, A. Z. Mardiansyah, W. Wedashwara, and A. H. Jatmika, "Integrasi Sistem Informasi Akademik dan Bot Telegram Sebagai Media Pengaksesan Informasi di Universitas Mataram," JTIKA, vol. 3, no. 2, pp. 253–260, Sep. 2021.

[4] S. Eko Prasetyo and Haryono, "Analisis dan Perancangan Monitoring dan Notifikasi System Web Application Firewall Menggunakan Zabbix," Conference on Management, Business, Innovation, Education and Social Science, vol. 1, no. 1, pp. 851–859, Feb. 2021.

[5] S. Geges and W. Wibisono, "Pengembangan Pencegahan Serangan Distributed Denial of Service (DDoS) pada Sumber Daya Jaringan dengan Integrasi Network Behavior Analysis dan Client Puzzle," JUTI: Jurnal Ilmiah Teknologi Informasi, vol. 13, no. 1, pp. 53–67, Jan. 2015.

[6] R. Hermawan, "Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDoS)," e-Journal Universitas Indraprasta PGRI (Persatuan Guru Republik Indonesia), vol. 5, no. 1, pp. 1–14.

[7] F. Indrajid, K. Ferdy Andika, S. Aditya Putra, K. Karisma Bramanda, A. Jude Saskara, and E. Listartha, "Analisis Hasil DoS SYN Flood Attack pada Web Server," vol. 12, no. 1, pp. 1–8, 2023.

[8] S. Sulasno and R. Saleh, "Desain dan Implementasi Sistem Monitoring Sumber Daya Server Menggunakan Zabbix 4.0," JUITA: Jurnal Informatika, vol. 8, no. 2, pp. 187–196, Nov. 2020.

[9] S. Suharti, A. Yudhana, and I. Riadi, "Forensik Jaringan DDoS Menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary," Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer, vol. 21, no. 3, pp. 567–582, Jul. 2022.

[10] G. Yudhy Kusuma and U. Yusmaniar Oktiawati, "Perancangan Sistem Monitoring Performa Aplikasi Menggunakan Opentelemetry dan Grafana Stack," Journal of Internet and Software Engineering (JISE), vol. 3, no. 1, pp. 26–35, Nov. 2022.

[11] A. Budi Cahyo, T. K. Hariadi, and Y. Ardiyanto, "Implementasi Zabbix Server untuk Memonitor Kondisi Jaringan Komputer di Dinas Komunikasi dan Informatika Kabupaten Pekalongan," Thesis, Universitas Muhammadiyah Yogyakarta, Yogyakarta, 2020.

[12] Yunanri, Yuliadi, F. Hamdani, Y. Bella Fitriana, and N. Oper, "Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST)," KLIK: Kajian Ilmiah Informatika dan Komputer, vol. 3, no. 6, pp. 1296–1302, Jun. 2023.

[13] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review Sim)," JEMSI (Jurnal Ekonomi, Manajemen, dan Akuntansi), vol. 3, no. 5, pp. 564–573, May 2022.

[14] Zulkarnain, "Analisis Implementasi Keamanan Sistem Informasi pada Perusahaan Perakitan Elektronik," Journal of Information System and Technology, vol. 1, no. 1, pp. 1–4, Jul. 2020.

[15] A. Efendi, U. Ependi, and T. Ariyadi, "Analisis Perbandingan Performa Server E-Learning Berbasis Parallel Processing dengan Server E-Learning Berbasis Tunggal," Bina Darma Conference on Computer Science (BDCCS) 2019, vol. 1, no. 1, pp. 235–243, Jan. 2019.

[16] R. Dimas Prakoso and Asmunin, "Implementasi dan Perbandingan Performa Proxmox dalam Virtualisasi dengan Tiga Virtual Server," Jurnal Manajemen Informatika, vol. 8, no. 1, pp. 79–85, 2018.

[17] A. Haykal and Siswanto, "Aplikasi Monitoring dan Controlling Server dengan Notifikasi Email Berbasis Web pada PT. Tanabe Indonesia," Sistem Komputer dan Teknik Informatika (SKANIKA), vol. 1, no. 1, pp. 193–198, Apr. 2018.

[18] A. Mardiyono, W. Sholihah, and F. Hakim, "Mobile-based Network Monitoring System Using Zabbix and Telegram," in 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), IEEE, Sep. 2020, pp. 473–477. doi: 10.1109/IC2IE50715.2020.9274582.

[19] M. Khairullah Harto and A. Basuki, "Deteksi Serangan DDoS pada Jaringan Berbasis SDN dengan Klasifikasi Random Forest," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 5, no. 4, pp. 1329–1333, Apr. 2021.

[20] H. Marcellino, I. G. P. S. Wijaya, and Gunawan, "Sistem Informasi Akademik Penjadwalan Mata Kuliah Berbasis Website FKIP Unram," JBegaTI, vol. 3, no. 1, pp. 122–132, Apr. 2022.

[21] J. Chandra W, "Implementasi Sistem Informasi Akademik (Studi Kasus : SMP Negeri 20 Bandung)," Jurnal Universitas Komputer Indonesia, pp. 1–10, 2013.