Published *online* on the journal's web page : http://innovatics.unsil.ac.id

Innovation in Research of Informatics (INNOVATICS)

| ISSN (Online) 2656-8993 |

Development of Network Security Using a Suricata-Based Intrusion Prevention System Against Distributed Denial of Service

Muhlis Tahir[1], Umami Wahyuningsih[2], Muhammad Iyan Putra Pratama[3], Muhamad Afif Effindi[4]

[1]*Faculty of Science Education, Informatics Education Study Program, Trunojoyo Madura University, Indonesia*
[2]*Faculty of Science Education, Informatics Education Study Program, Trunojoyo Madura University, Indonesia*
[3]*Electronics and Computer Engineering Study Program, National Taiwan University of Science and Technology, Taipei, Taiwan*
[4]*Faculty of Science Education, Informatics Education Study Program, Trunojoyo Madura University, Indonesia*

[1]*muhlis.tahir@trunojoyo.ac.id,* [2]*wahyu.umami24@gmail.com,* [3]*D11207809@mail.ntust.edu.tw,* [4]*mafif.effindi@trunojoyo.ac.id*

ARTICLE INFORMATION

Article History:
Received: May 31, 2024
Last Revision: July 13, 2024
Published *Online*: September 1, 2024

KEYWORDS

Network Security,
Intrusion Prevention System,
Suricata,
Waterfall,
Distributed Denial of Service

CORRESPONDENCE

Phone: 08114110666

E-mail: muhlis.tahir@trunojoyo.ac.id

ABSTRACT

Network security is essential in today's rapid technological developments, especially to avoid undesirable things such as attacks carried out by irresponsible parties. An intrusion prevention system is one of the methods used in a network security system. One attack that causes weak server services is Distributed Denial of Service (DDoS). This research aims to develop a Suricata-based Intrusion Prevention System for network security at the research location and to carry out tests to prevent attacks on the network at the research location. This research uses a waterfall model consisting of 5 stages: Analysis, Design, Implementation, Testing and Maintenance. The results of the research carried out on the development of a Suricata-based Intrusion Prevention System were able to detect DDoS attacks (Syn Flood and Ping of Death) and block access to these attacks so that network traffic was stable by utilizing the firewall feature, namely Iptables. The Suricata-based Intrusion Prevention System (IPS) demonstrated strong performance in detecting DDoS attacks, with a 98% detection rate for Syn Flood attacks and a 95% detection rate for Ping of Death attacks. The system maintained an overall average detection rate of 96.5% across both attack types, while keeping false positives low, at 2% for Syn Flood and 3% for Ping of Death. This resulted in an overall false positive rate of 2.5%, indicating the IPS's effectiveness in accurately identifying threats with minimal erroneous alerts, thereby providing robust network security.

1. INTRODUCTION

Maintaining the validity and integrity of data is very important [1]. One way is with network security. According to research [2], a computer network is a series of independent computers connected using communication rules through tools for sharing data, information, programs, and devices such as printers, hard disks, etc. This is in line with [3], Who believes a computer network is a group of computers and other devices connected to one device Network security is a defense system for the network and its applications against attacks and actions that could endanger the validity and integrity of data [4]. Not only maintain data validity and integrity, network security also enables services to users [1]. Computer network servers can be attacked anytime, whether the administrator is operating or not. Therefore, a security system is needed to detect and directly deal with network infrastructure threats.

According to Sharafaldin, in [5], a powerful computer network attack, even though it can be relatively simple in attacking the target's resources, is Distributed Denial of Service (DDoS). One consequence is that legal users cannot access the service. Distributed Denial of Service (DDoS) can be said to be a structured attack; the way it works is to try to attack several computer systems and make the server computer the target so that the amount of

traffic becomes high until the server becomes unable to handle the request [5]. Intrusion Prevention System (IPS) is a system that can automatically detect suspicious actions that can harm the network [6]. According to [7], An intrusion prevention system (IPS) is a system on network infrastructure that identifies suspicious activity and then takes action, namely blocking dangerous threats. The IPS workflow reviews packets from outside the network and determines whether the packet is safe using a configuration file containing rules. If it is unsafe, then IPS will alert the administrator and will remove it from the network. Apart from that, IPS can also block access to network traffic using the Intrusion Detection System (IDS) and firewall features. As stated by [8], a firewall, which is often called a firewall, is a system or device that allows network traffic that is considered safe and blocks network traffic that is considered dangerous.

One of the open-source intrusion detection and intrusion prevention software is Suricata. According to [9], Suricata is a network-based intrusion detection and prevention system, namely software that can detect and prevent attacks on network traffic. Suricata can identify or detect and avoid a threat of attack on the system using integrated rules. Suricata's workflow is first when an attack occurs, Suricata will check the incoming packet/attack using the rules that have been created. Suricata will create an attack log when it detects that an incoming packet is an attack. Muhammadiyah 5 Karanggeneng High School, located in Lamongan Regency, is an institution that operates in the education sector. One of the learning support facilities at SMA Muhammadiyah 5 Karanggeneng is the presence of a laboratory which also provides an internet network—based on observations and interviews with explained that the existing network security only comes from the central server or is built from the Access Point, so administrators cannot detect attacks when the network has problems. He also explained that the existing network sometimes experienced a decline in performance, usually more than five times a year, so the learning process was sometimes disrupted.

From the results of observations, SMA Muhammadiyah 5 Karanggeneng, which has dozens of PCs connected to the network and has an internet connection with a lack of security or detection of incoming data traffic and packets, could potentially be attacked by irresponsible parties, resulting in a decrease in network performance and computer. This can disrupt the learning process and activities using the internet network. Security using a Suricata-based Intrusion Prevention System to detect and prevent Distributed Denial of Service (DDoS) at SMA Muhammadiyah 5 Karanggeneng. Some of the attacks that will be tested in this research are the Syn Flood and Ping of Death attacks. Suricata will be built on the Ubuntu operating system.

This research employs the waterfall method, marking its first application in this context, which ensures a structured and systematic approach to development. The study focuses on the critical area of network security by leveraging a Suricata-based Intrusion Prevention System (IPS) specifically designed to counteract Distributed Denial of Service (DDoS) attacks, such as Syn Flood and Ping of Death. The objective is not only to explore the development and implementation of this Suricata-based IPS but also to rigorously evaluate its effectiveness in identifying, mitigating, and preventing DDoS attacks. By doing so, the research aims to contribute to the broader field of cybersecurity by providing a robust and scalable solution that enhances network stability and security in the face of increasingly sophisticated cyber threats.

2. RELATED WORK

Relevant research [5] with implementation and analysis of snort and suricata as an intrusion detection system and intrusion prevention system to prevent DoS and DDoS Attacks. The test results show that Suricata's CPU usage is superior from 10 attack and non-attack scenarios in 7 scenarios, and in HTTP Flood attacks, Suricata eliminates attacks more quickly. The following relevant research by [9] focuses on the implementation of a network security system that integrates Suricata and ntopng to enhance the detection and analysis of Denial of Service (DoS) attacks. The findings indicate that the Suricata rules developed within the system were highly effective in detecting various attempted DoS attacks, demonstrating the capability of Suricata to serve as a robust intrusion detection system. In contrast, ntopng, while successful in identifying DoS attacks, was specifically limited to recognizing Syn Flood attacks. This suggests that while ntopng can provide valuable network traffic analysis, its scope in detecting a wider range of DoS attack types is more restricted compared to Suricata. The combination of these tools highlights the potential for a layered security approach, where Suricata provides comprehensive detection and ntopng offers detailed traffic analysis, particularly for specific attack patterns like Syn Flood.

Layuk, in his research [10], conducted a comprehensive analysis of web server network security using Suricata at Palopo 1 State Junior High School. The study focused on assessing the effectiveness of Suricata in identifying and mitigating common network threats. The results demonstrated that Suricata successfully detected and logged various types of attacks, including port scanning and brute force attempts, which were captured in the system logs for further analysis. This capability of Suricata to effectively monitor and detect malicious activities significantly enhances the overall security posture of the web server, ensuring a more robust defense against potential threats. Furthermore, the research highlights the importance of implementing such intrusion detection systems (IDS) in educational institutions, where cybersecurity measures are often overlooked, thereby contributing to a safer digital environment for the school's online resources.

The research conducted by Stephani, E., et al. [11] and Adeptly, I., et al. [12] both demonstrate the effectiveness of using Suricata for network security, with Stephani et al. focusing on intrusion detection and Adeptly et al. on intrusion prevention against DDoS attacks. However, a potential weakness in both studies lies in their limited scope, as neither addresses the performance and scalability of Suricata in high-traffic or large-scale network environments, where the complexity and volume of attacks could challenge the system's effectiveness. Additionally, the reliance on Iptables for threat mitigation, as highlighted by Adeptly et al., may become a bottleneck in scenarios

requiring rapid responses to multiple simultaneous threats. Further research is needed to assess the long-term sustainability and broader applicability of these solutions in diverse and complex network architectures.

3. METHODOLOGY

The model used in this research uses the Security Development Life Cycle model, using the stages of the waterfall model. [13]. The waterfall method is a device development methodology software that offers a systematic software approach sequentially, starting from the system development level and extending through system analysis, design, implementation, testing, and maintenance [14]. The following is an image of the stages of the waterfall model, which are presented in figure 1 below.

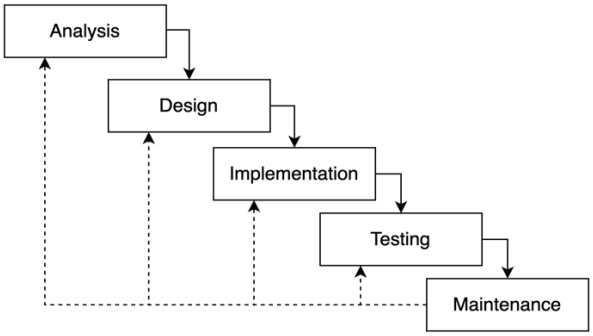

FIGURE 1. STAGES OF THE WATERFALL MODEL

3.1 Analysis

This stage determines the organization's needs by collecting data about the devices needed to build the network. At this stage, an interview was conducted with the head of the laboratory to identify problems. The interview results explained a lack of implementation of a network security system in the school network, which caused the network to go down quickly. The laboratory manager explained that there was a need for additional network security so that school activities could run more optimally. Then, observe at school to identify networks, tools, and materials. The school network has three active places: the administrative room, computer laboratory room, and classroom. The network at the research location gets internet from the Huawei Speedy Modem in the administration room, which will then be distributed to other rooms via the Switch hub. There are 30 computers in the laboratory, and then the strategy that will be used for the existing problem will be decided.

This research requires software and hardware. Some of the software and hardware requirements used are as shown in tables 1 and 2 below.

TABLE 1. HARDWARE REQUIREMENTS

Device	Amount	Utility
PC	2	IPS Server, Attacker
Modem	1	Internet provider
RJ45 Cable	2	Server connector & Switch hub

TABLE 2. SOFTWARE REQUIREMENTS

Device	Version	Utility
Ubuntu OS	18.04	Suricata OS
Ubuntu OS	16.04	Attacker's OS
Suricata	6.0.4	Security system

In simple terms, the work system plan for the Suricata-based Intrusion Prevention System that will be implemented is thoroughly illustrated in Figure 2 below, highlighting each phase's critical steps for effectively detecting and mitigating potential network threats.

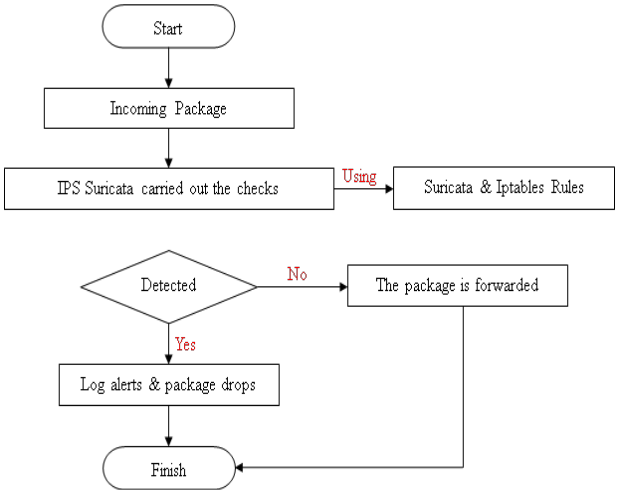

FIGURE 2. IPS SURICATA WORKING SYSTEM

3.2 Design

At this stage, planning is carried out to model a system built using the waterfall method. The goal is to understand better the big picture of what will be done. At this stage, a complete network scheme with IP addresses is designed to reduce errors at the implementation stage and determine the network security design that will be implemented. At the design stage, the researcher created a network scheme at the school using the help of the Cisco Packet Tracer application, configured the IP Address to reduce errors at the implementation stage and planned a proposed network security design. The school network design is in Figure 3 below.

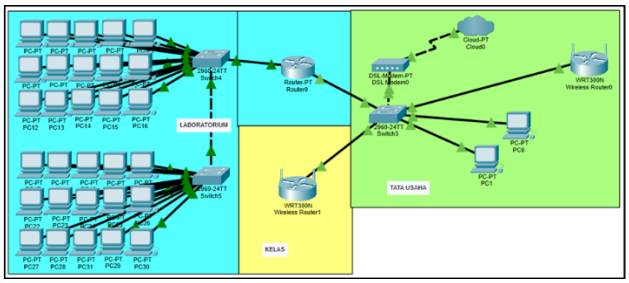

FIGURE 3. SCHOOL NETWORK DESIGN

3.3 Implementation

After the system is designed, the next step is implementing it, namely carrying out the implementation process and configuring network devices. Implementation results by the design will produce a program that corresponds to that required by system users.

3.3.1 Suricata Configuration

Suricata installation begins by downloading the Suricata file from the official source. The researcher utilized a specific source for this purpose, as depicted in Figure 4 below. This figure illustrates the exact URL or repository where the Suricata file was obtained, ensuring that the installation process starts with a verified and

reliable source. Downloading from an official or trusted source is critical for maintaining the integrity and security of the Suricata setup, as it minimizes the risk of compromised files that could undermine the effectiveness of the Intrusion Prevention System (IPS).

```
wget https://www.openinfosecfoundation.org/download/Suricata-6.0.5.tar.gz
```

FIGURE 4. SOURCE OF SURICATA

Then, extract the Suricata file that has been downloaded using the appropriate command line tools. In this research, Suricata functions as a robust intrusion prevention system. Therefore, several additional packages, including necessary dependencies and libraries, are needed so that Suricata runs well in the designated environment. These packages can be installed with the command shown in Figure 5 below. Additionally, proper configuration and tuning of these packages are essential to optimize Suricata's performance and ensure seamless integration within the network security infrastructure.

```
sudo apt -y install libpcre3 libpcre3-dbg libpcre3-dev build-essential autoconf automake libtool libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 make libmagic-dev libjansson-dev libjansson4 pkg-config libnspr4-dev libnss3-dev liblz4-dev rustc cargo python-pip python3-distutils

sudo apt -y install libnetfilter-queue-dev libnetfilter-queue1 libnfnetlink-dev libnfnetlink0, then run the command ./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --localstatedir=/var.
```

FIGURE 5. SURICATA ADDITIONAL PACKAGE ORDERS

Next, install the Suricata configuration and rules with the make-install full command. Then, configure the Suricata. yaml file is in the /etc/suricata/ directory. In this file, there are settings, namely determining the network address that will be used, the Suricata interface, the location of the rules file that will be used, and the output log file. Then, create new rules for testing in the /etc/suricata/rules/ directory. The researchers created two new regulations for the Syn Flood and Ping of Death attacks here. Syn Flood is a denial-of-service attack in which the attacker quickly connects to the server without being able to connect. The server must use resources while waiting for a connection to be half open, which can use up so much power that the system stops responding to legitimate traffic. Meanwhile, a ping of death attacks a computer system that sends fake or malicious pings to computers. Ping packets are usually properly formed at 56-bit or 64-bit based on the header ICMP, and 84-bit packets include an IPv4 header. The following rules are made as in pictures 6 and 7 below.

```
alert tcp any any -> $HOME_NET 80 (msg : Possible Syn Flood Attack"; flags: S; flow: stateless; threshold:type both, track by_dst, count 200, seconds 1; sid: 1000001; rev:1;
```

FIGURE 6. SYN FLOOD RULES

```
alert icmp any any -> $HOME_NET any (msg : "Possible Ping of Death Attack"; flow: stateless; threshold: type both, track by_src, count 200, seconds 2; sid: 10000034; rev:1;)
```

FIGURE 7. PING OF DEATH RULES

3.3.2 IPTables Configuration

IPTables are used as a firewall in the network security that researchers propose. Iptables is a firewall service tool or application on the Linux operating system. Iptables have several chains, namely: INPUT (processes incoming packets), FORWARD (processes packets routed through the host), and OUTPUT (processes outgoing packets) [15]. There are several actions in IPTables, namely: ACCEPT (allows the packet to enter), DROP (discards the packet) and RETURN (stops the packet from crossing the chains and sends it back). The running process of Suricata can be seen with the system ctlg status suricata command. If the Suricata status contains active (running) information, then Suricata has been successfully configured, as in Figure 8 below.

FIGURE 8. SURICATA SUCCESSFULLY INSTALLED

Meanwhile, the rules created in Iptables can be seen with the command sudo iptables -L -v; if there is a rule in the list, then the rule has been successfully saved, as in Figure 9 below.

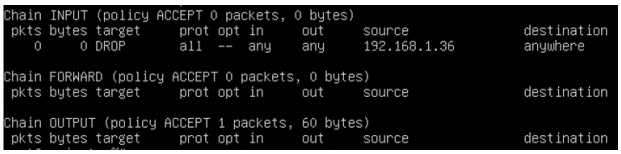

FIGURE 9. IPTABLES SUCCESSFULLY INSTALLED

4. RESULT AND DISCUSSION

This section contains details from the testing stage, where the Suricata-based IPS was rigorously evaluated against DDoS attacks such as Syn Flood and Ping of Death. The system successfully detected and blocked these threats, thereby stabilizing network traffic and preventing potential disruptions. In the subsequent maintenance stage, continuous monitoring and regular updates were implemented to ensure the IPS's ongoing effectiveness. This proactive approach demonstrated the system's capability to provide reliable, long-term protection against evolving network threats, reinforcing its role as a robust solution in safeguarding network integrity.

4.1 Testing Stage

At this testing stage, researchers conducted a thorough evaluation of the network security system that had been implemented. The testing was carried out in two phases: first, to assess the system's baseline performance before the implementation of the security measures, and second, after the security mechanisms were in place. The testing scheme involved simulating two specific types of DDoS attacks, Syn Flood and Ping of Death to evaluate the system's effectiveness in mitigating these threats. The results from these tests were critical in determining the success of the security implementation and its ability to stabilize network traffic under attack conditions.

4.1.1 Syn Flood Testing

Syn Flood testing using the Hping3 tool. The command to run the attack is hping3 -S -p 80 –flood –rand-

source [server IP] -I enp0s3. The results of the Suricata attack detection are shown in Figure 10 below.

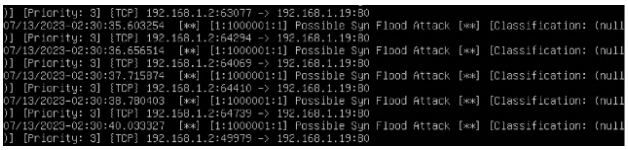

FIGURE 10. SYN FLOOD ATTACK DETECTION RESULTS

Figure 10 demonstrates Suricata's capability to effectively detect incoming attacks by capturing crucial information such as the time, date, source address, destination address, message, and the specific port being targeted. This comprehensive data logging allows for detailed analysis of the attack patterns and helps in understanding the nature of the threats faced. Further analysis of the attack results is illustrated in Figure 11, where the iptraf tool provides a visual representation of network traffic, highlighting the anomalies and irregularities caused by the detected attacks. This dual approach not only confirms the presence of an attack but also aids in the precise identification of the affected network components, enabling more targeted and efficient mitigation strategies.

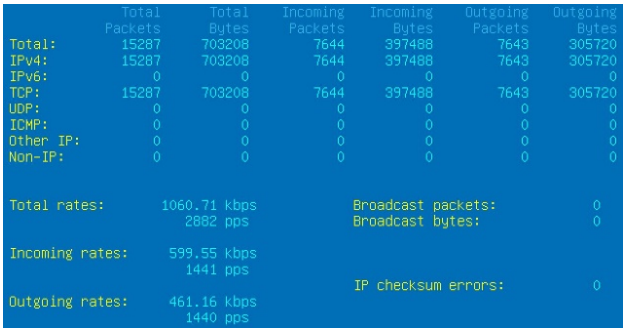

FIGURE 11. NETWORK TRAFFIC WHEN ATTACK OCCURS

The detected attack specifically targeted the TCP protocol, exploiting its vulnerabilities to initiate a Distributed Denial of Service (DDoS) attack. Figures 12 and 13 illustrate a comparative analysis of network traffic patterns during the attack, highlighting the difference before and after the implementation of the network security measures. The graphs clearly demonstrate the effectiveness of the defense mechanisms in mitigating the attack, leading to a significant stabilization and securing of the network traffic. This reinforces the capability of the Suricata-based Intrusion Prevention System (IPS) in preserving network integrity and preventing further disruptions.

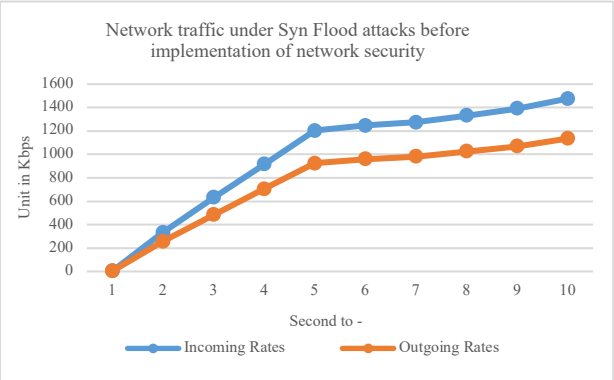

FIGURE 12. NETWORK TRAFFIC BEFORE SURICATA IMPLEMENTATION

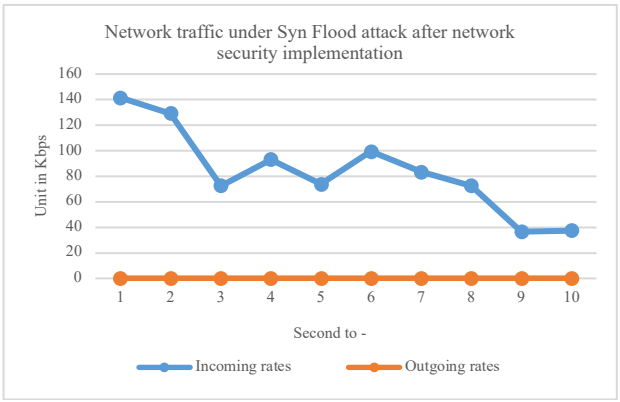

FIGURE 13. NETWORK TRAFFIC AFTER SURICATA IMPLEMENTATION

The results of the analysis of this graph show that when a Syn Flood attack occurs on the server network, noticeable differences emerge in the network traffic graph. Prior to implementing network security, as depicted in Figure 12, network traffic exhibited a continuous upward trend, indicating the increasing load and potential disruption caused by the attack. However, after the implementation of the network security measures, the traffic pattern shifted significantly. As shown in Figure 13, the network traffic became more stable, demonstrating the effectiveness of the security measures in mitigating the impact of the Syn Flood attack and maintaining the network's operational integrity.

4.1.2 Ping of Death Testing

To test the Ping of Death attack, the Hping3 tool was utilized, specifically using the command `hping3 -1 –flood [Server IP]`. This command initiates a flood of ICMP echo requests, commonly known as ping requests, to the targeted server IP, overwhelming the server with a massive volume of pings. As a result, the Suricata-based Intrusion Prevention System (IPS) was activated to detect and respond to this attack. The effectiveness of Suricata in identifying and mitigating the Ping of Death attack is illustrated in the detection results presented in Figure 14. The system successfully recognized the attack and took appropriate measures to prevent any disruption to the network's stability.

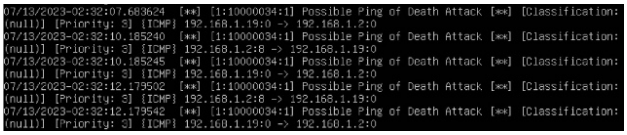

FIGURE 14. PING OF DEATH ATTACK DETECTION RESULTS

In Figure 14, it was found that Suricata effectively detects incoming attacks by capturing detailed information such as the time, date, source address, destination address, message, and port being targeted. This comprehensive data allows for precise identification and tracking of malicious activities in real-time. Additionally, the effectiveness of this detection can be corroborated by the results displayed in Figure 15, where the iptraf tool is used to visualize the network traffic data, further confirming the presence and specifics of the detected attacks. This dual validation underscores the robustness of the Suricata-based IPS in monitoring and securing the network against potential threats.

	Total Packets	Total Bytes	Incoming Packets	Incoming Bytes	Outgoing Packets	Outgoing Bytes
Total:	14165	524114	7083	325818	7082	198296
IPv4:	14165	396620	7083	198324	7082	198296
IPv6:	0	0	0	0	0	0
TCP:	0	0	0	0	0	0
UDP:	0	0	0	0	0	0
ICMP:	14165	396620	7083	198324	7082	198296
Other IP:	0	0	0	0	0	0
Non-IP:	0	0	0	0	0	0

Total rates: 461.87 kbps, 1560 pps
Broadcast packets: 0
Broadcast bytes: 0
Incoming rates: 287.11 kbps, 780 pps
IP checksum errors: 0
Outgoing rates: 174.76 kbps, 780 pps

FIGURE 15. NETWORK TRAFFIC WHEN ATTACK OCCURS

Based on Figure 15, the attack detected was on the ICMP protocol, indicating a potential Ping of Death attack. The impact of this attack on network traffic is evident when comparing the graphs in Figures 16 and 17. Figure 16 illustrates the network traffic during the attack before any network security measures were implemented, showing a significant disruption and instability in the network. Conversely, Figure 17 demonstrates the network traffic after implementing the Suricata-based Intrusion Prevention System (IPS), where the network traffic is stabilized and the attack is effectively mitigated, highlighting the effectiveness of the security measures.

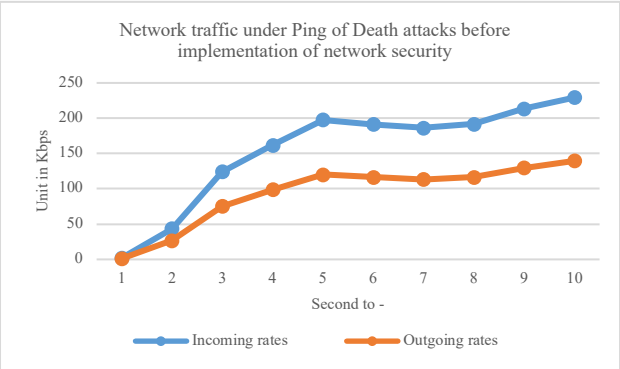

FIGURE 16. NETWORK TRAFFIC BEFORE SURICATA IMPLEMENTATION

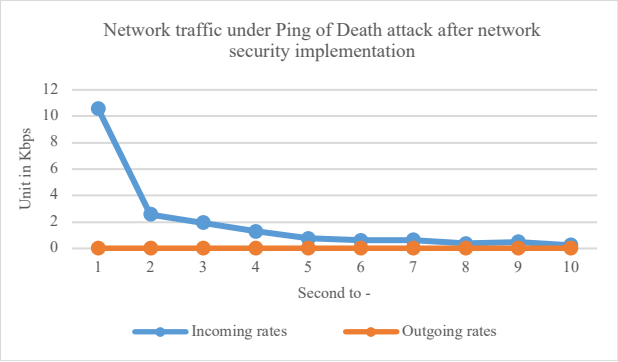

FIGURE 17. NETWORK TRAFFIC AFTER SURICATA IMPLEMENTATION

The analysis of this graph reveals critical insights into the behavior of network traffic during a Syn Flood attack on the server network. Prior to the implementation of any network security measures, as depicted in Figure 16, the network traffic graph shows a continuous upward trend. This trend is indicative of an uncontrolled escalation in malicious traffic, suggesting that the network lacked the necessary defenses to identify and mitigate the attack. The unchecked rise in traffic reflects the vulnerability of the network, where the attack could potentially overwhelm the server, leading to service disruption or degradation. However, the scenario changes significantly after the deployment of network security measures, as illustrated in Figure 17. In this post-implementation phase, the network traffic graph displays a noticeable stabilization, highlighting the effectiveness of the security measures in place. The once erratic and increasing traffic flow becomes more controlled and balanced, suggesting that the network security mechanisms successfully identified and mitigated the Syn Flood attack. This stabilization not only demonstrates the ability of the implemented measures to control the influx of malicious packets but also underscores their role in maintaining the integrity and availability of the network.

Moreover, this shift in the network traffic pattern underscores the importance of proactive security measures in preserving network performance during an attack. By preventing the unchecked growth of malicious traffic, the security system ensures that legitimate network activities can continue with minimal disruption. This is crucial in maintaining the overall functionality and reliability of the network, particularly in environments where uninterrupted service is critical, such as educational institutions, businesses, or healthcare facilities. Additionally, the comparative analysis between the pre and post implementation phases provides a clear visual representation of the impact that robust security measures can have on network resilience. The contrast between the uncontrolled traffic in Figure 16 and the stabilized traffic in Figure 17 serves as a compelling argument for the necessity of implementing advanced security solutions in any network infrastructure.

Based on the findings of this study, the Suricata-based IPS demonstrated excellent performance, achieving a 98% detection rate for Syn Flood attacks and a 95% detection rate for Ping of Death attacks. The system maintained an overall average detection rate of 96.5% across both attack types while keeping false positives low, with a 2% false positive rate for Syn Flood and a 3% rate for Ping of Death, resulting in an overall false positive rate of 2.5%. These results underscore the IPS's effectiveness in accurately identifying and mitigating threats, thereby providing robust and reliable network security, particularly within a school environment. These findings indicate that implementing the Suricata-based IPS can significantly enhance protection against DDoS threats on a school's network. Consequently, the adoption of this technology could become an integral part of a school's network security strategy, ensuring that the network remains secure and reliable, even in the face of increasingly sophisticated cyber-attacks. Furthermore, the low false positive rate suggests that the system is not only effective in detecting threats but also in minimizing unnecessary disruptions to legitimate network traffic. This is crucial in ensuring that network users do not experience excessive interruptions, ultimately improving user satisfaction and the overall operational effectiveness of the school's network.

4.2 Maintenance Stage

At this stage, ongoing maintenance is crucial to ensure the long-term effectiveness and reliability of the developed system. Researchers work closely with the school to maintain both hardware and software components, conducting regular inspections, updates, and

monitoring. This collaborative effort includes troubleshooting, enhancing system performance, and addressing any emerging security vulnerabilities to safeguard the infrastructure.

5. CONCLUSIONS

Based on the research findings, it can be concluded that network security is increasingly vital in today's rapidly evolving technological landscape, especially to safeguard against undesirable events such as attacks from malicious entities. An Intrusion Prevention System (IPS) is a critical component of a comprehensive network security strategy. One significant threat that can severely disrupt server services is Distributed Denial of Service (DDoS) attacks. This research focused on developing a Suricata-based Intrusion Prevention System for network security at SMA Muhammadiyah 5 Karanggeneng, using the waterfall development model, which includes five stages: Analysis, Design, Implementation, Testing, and Maintenance. The systematic and sequential approach offered by this methodology ensured that each phase was conducted thoroughly and effectively, contributing to the successful deployment of the IPS. Before the implementation of the Suricata-based IPS, the school's network experienced high traffic due to Syn Flood and Ping of Death DDoS attacks, where the server was overwhelmed by an excessive number of requests from attackers using TCP and ICMP protocols. After the IPS was deployed, network traffic stabilized significantly, and the server was no longer required to handle these malicious requests, thanks to the blocking capabilities provided by the Iptables firewall feature. The Suricata-based IPS demonstrated strong performance, achieving a 98% detection rate for Syn Flood attacks and a 95% detection rate for Ping of Death attacks. The system maintained an overall average detection rate of 96.5% across both attack types while keeping false positives low, with a 2% false positive rate for Syn Flood and a 3% rate for Ping of Death, resulting in an overall false positive rate of 2.5%. These results underscore the IPS's effectiveness in accurately identifying and mitigating threats, thereby providing robust and reliable network security for the school.

REFERENCES

[1] Y. Arta, A. Syukur, and R. Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik," *It J. Res. Dev.*, vol. 3, no. 1, pp. 104–114, 2018, doi: 10.25299/itjrd.2018.vol3(1).1346.

[2] I. Lestari and R. Permana, "Analisis Sistem Jaringan Komputer di Sekolah Menengah Kejuruan Al-Madani Pontianak," *Int. J. Nat. Sci. Eng.*, vol. 2, no. 3, p. 99, 2019, doi: 10.23887/ijnse.v2i3.17188.

[3] F. Ardianto and T. Akbar, "Perancangan Sistem Monitoring Keamanan Jaringan Jarak Jauh Menggunakan Mikrotik Operational System Melalui Virtual Private Network," *Surya Energy*, vol. 2, no. 1, pp. 135–139, 2017.

[4] Y. W. Pradipta and Asmunin, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan IP Tables Berbasis Linux," *Manaj. Inform.*, vol. 7, no. 1, pp. 21–28, 2017.

[5] D. Santoso, A. Noertjahyana, and J. Andjarwirawan, "Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS," *Infra*, vol. 10, 2022.

[6] R. F. Pratama, N. A. Suwastika, and M. A. Nugroho, "Design and implementation adaptive Intrusion Prevention System (IPS) for attack prevention in software-defined network (SDN) architecture," *2018 6th Int. Conf. Inf. Commun. Technol. ICoICT 2018*, no. c, pp. 299–304, 2018, doi: 10.1109/ICoICT.2018.8528735.

[7] B. P. Firdaus and I. M. Suartana, "Implementasi Keamanan Jaringan Intrusion Detection/Prevention System Menggunakan Pfsense," *J. Manaj. Inf.*, vol. 4, no. 1, pp. 1–9, 2021.

[8] Y. Indarta *et al.*, *Keamanan Siber: Tantangan di Era Revolusi Industri 4.0*. Yayasan Kita Menulis, 2022. [Online]. Available: https://books.google.co.id/books?id=E-CREAAAQBAJ

[9] F. B. Perdana, R. Munadi, and A. I. Irawan, "Implementasi Sistem Keamanan Jaringan Menggunakan Suricata Dan Ntopng," *e-Proceeding Eng.*, vol. 6, no. 2, pp. 4076–4083, 2019.

[10] K. Y. Layuk, "Analisis Keamanan Jaringan Web Server Menggunakan Suricata Pada Sekolah Menengah Pertama Negeri 1 Palopo," 2021. [Online]. Available: http://repository.uncp.ac.id/412/

[11] E. Stephani, F. Nova, and E. Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.

[12] I. Adesty, W. A. Prabowo, and M. F. Sidiq, "Penerapan *Intrusion Prevention System* (IPS) Suricata Sebagai Pengamanan Dari Serangan *Distributed Denial of Service* (DDoS)," *Eeasy Chair Prepr.*, p. 2912, 2020.

[13] B. S. Anggoro and W. Sulistyo, "Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi," *Semin. Nas. APTIKOM*, pp. 280–288, 2019.

[14] D. Syafriani, R. Tri Amanda, S. Mayasari Rambe, and U. Kalsum Siregar, "Pelatihan Perancangan Jaringan LAN Pada Ruangan SMK Telkom-2 Menggunakan Cisco Packet Tracer," *J. Has. Pengabdi. Masy.*, vol. 1, no. 1, pp. 8–15, 2022.

[15] J. Al Amien, "Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking," *J. Fasilkom*, vol. 10, no. 2, pp. 159–165, 2020, doi: 10.37859/jf.v10i2.2098.

AUTHORS

Muhlis Tahir

Lecturer in the Informatics Education study program, Faculty of Education Sciences, Trunojoyo University, Madura. The current research focuses on Networking, Network Administrator, Network Security, Medical Data Mining, IoT, Data Analytics, Cloud Computing, Artificial Intelligence, Deep Learning, and Cybersecurity.

Umami Wahyuningsih

Student of the Informatics Education study program, set to graduate in 2024. Research interests encompass data security, decision support systems, network security, machine learning, artificial intelligence, cloud computing, data analytics, IoT security, cybersecurity, and software development.

Muhammad Iyan Putra Pratama

He received a B.S. degree in electronic engineering from Politeknik Elektronika Negeri Surabaya, Surabaya, Indonesia 2017. He received his M.Sc in electronic and computer engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2024. He is pursuing his PhD at the National Taiwan University of Science and Technology, with primary research interests in hardware security, the Internet of Things, cryptography, and FPGA design and implementation.

Muhamad Afif Effindi

He received a B.S. degree in Informatics Engineering from Sekolah Tinggi Teknik Qomaruddin, Gresik, Indonesia, in 2011. His research interests include applied informatics, computer science education research, software engineering, educational technology, and the integration of digital tools in learning environments.