Journal of Nesia Engineering Science (JNESc)
JNESc, Vol. 2, No. 1, March 2025
ISSN : 3032-2642

Modification of Local Area Network Security Monitoring System Based on Telegram Notification with Snort and Honeypot at Surabaya Aviation Polytechnic

Indra Al-Rasyid Candrawimba[1], Nyaris Pambudiyatno[2]*, Bambang Bagus Harianto[3], Meita Maharani Sukma[4]
[1,2,3,4)]Politeknik Penerbangan Surabaya, Jl. Jemur Andayani 1 No. 73, Surabaya, Indonesia
Correspondent Author, Email : nyaris@poltekbangsby.ac.id

Article Info

Article history:
Submitted: February 28, 2025
Final Revised: March 15, 2025
Accepted: March 21, 2025
Published: March 27, 2025

Keywords:
Cybercrime
cloud computing
network security,
NIDPS
Snort
Honeypot

ABSTRACT

The development of technology makes networking more complex and opens up opportunities for cybercrime. Indonesia has become the target of cyber attacks, one of which is the WannaCry ransomware. The online education system plays an important role in the operation of institutions, with an example of cloud computing technology used by the Surabaya Aviation Polytechnic campus. This study uses R&D and ADDIE to develop an NIDPS network security system with Snort and Honeypot. The results of the study show that monitoring and network security systems can detect anomalous activity and are integrated with Telegram for alarm notifications. Evaluations were also carried out for the addition of fail2ban features and less than optimal network performance.

1. INTRODUCTION

The development of technology in this era has had a significant positive impact, especially in the field of networking, which is marked by the advancement of increasingly complex tools and features. This development, although making it easier for users to access the internet, also opens up wide opportunities for cybercrime. In 2015, Indonesia ranked second in cyber attacks, showing vulnerability and ease of exploitation by hackers. The WannaCry ransomware attacked computers in 150 countries in 2017. In 2022, 8,831 cases related to cybercrime were recorded, with 12.74 million accounts experiencing data leaks. The threat of cyber attacks such as port scanning, brute force attacks, phishing, denial of service (DoS), malware viruses, and others cannot be ignored. Currently, most education is done online, showing that internet technology plays an important role in the operation of institutions. Surabaya Aviation Polytechnic is one of the campuses that uses cloud computing technology, or computer technology that uses the internet as its medium. (Saut Parsaoran Tamba et al., n.d.). Intrusion data stored in the database includes information about the origin of the attack, time of occurrence, type of attack, and its impact that can be used for network forensic analysis. (Khadafi et al., 2017)

2. LITERATURE REVIEW

2.1. Snort

Snort is an Intrusion Detection System (IDS) that was first created by Martin Roesch in 1998 as an answer to the market need for an effective and affordable detection tool for computer networks and is open-source. Snort combines pattern detection, packet flow detection, and payload detection. Snort integrates pattern detection, packet flow detection, and payload detection and combines various detection technologies with the ability to prevent attacks by blocking packets identified as threats (Purba & Efendi, 2020). How Snort works is divided into 3 packet modes:

1. Sniffer Packet. This mode is responsible for monitoring or viewing data traffic on a computer network.
2. Logger packet. Records all packets passing through the network and analyzes them to find evidence in the network forensics process.
3. Intrusion detection mode. In this mode, Snort is used to detect attacks that occur through a computer network. To run this mode, IDS must set various rules that allow it to distinguish between normal data packets and packets that carry threats.

2.2. Honeypot

Honeypot is a system developed by Lance Spitzner in 1999 that was built to resemble the original server with the aim of fooling attackers. So as a Network Administrator, you can Honeypot is a system developed by Lance

Spitzner in 1999 that was built to resemble the original server with the aim of fooling attackers. So as a Network Administrator, you can analyze the attack patterns or methods used by attackers (Akshay et al., 2020).

2.3. Quality of Service (QoS)

Quality of Service is a service in a computer network that can be defined as the ability of a network to provide services with quality according to user desires and expectations through the management and prioritization of data flow. Some of the main components of QoS are as follows (Rasudin, 2014):

1. Throughput
   Throughput is the effective data transfer rate, measured in bps. This refers to the number of packets successfully received at the destination during a given time period, divided by the duration of that period.
2. Delay
   Delay is the time it takes to send data from the source to the destination. Too long a delay can cause inconvenience to users, especially for services that require fast reaction times, such as video streaming and online gaming.
3. Jitter
   Jitter is a variation in delay caused by differences in the time in which data packets are sent, which can disrupt the quality of service, especially in multimedia applications such as video and voice.
4. Packet Loss
   Packet loss is the loss of data packets when data is sent from the source to the destination. Too high a packet loss can result in poor quality of service, especially for applications that require fast and consistent data transfer.

2.4. Linux

Linux is an open-source UNIX-based operating system developed by Linus Torvalds in 1991. Linux is widely used by developers and administrators because it is lightweight, has guaranteed security, and is free. The Linux operating system has many distributions or derivatives; among the famous ones are Kali Linux, Ubuntu, Debian

2.5. Telegram

Telegram is a cloud-based instant messaging application released in August 2013 and can be used on various operating systems today. Telegram officially uses operating systems both on the desktop (Windows, GNU/Linux, macOS) and mobile levels (Android, iOS) (Fernández-Álvarez & Rodríguez, 2021). Telegram also offers a developer API that allows developers to create animated stickers, widgets, appearance changes, and bots. Bots can be interpreted as programs that work automatically. Telegram Bot is a special Telegram account designed to send messages automatically (Arfianto, 2017).

3. METHODOLOGY

This study includes four main stages: data collection, network architecture design, system creation, and implementation and evaluation, followed by quality of service measurements. Data collection is carried out to obtain information related to network security system needs, types of intrusions to be attempted, and functions and how Snort and Honeypot work; in this case, the author uses HoneyDB as its Honeypot.

Data collection focuses on identifying attack patterns and vulnerabilities in the network. Honeypots, such as Cowrie and Dionaea, are used to capture and record malicious activity, providing insight into attack methods and frequencies (Adnyana et al., 2024). The VoIP-based honeypot captured over 105,000 events, revealing common attack protocols such as Telnet (Altunay, 2024). The design phase integrates the honeypot with existing security measures, enhancing proactive defense strategies against evolving cyber threats (Dang et al., 2024). The architecture must accommodate real-time data processing and visualization tools, such as the ELK Stack, to effectively analyze attack trends (Adnyana et al., 2024). Implementation involves deploying honeypots and monitoring their interactions with potential attackers, while evaluation assesses the effectiveness of the system in detecting and mitigating threats (Faldi et al., 2023). The performance of honeypots is compared to traditional systems such as Snort, highlighting their limitations in identifying certain types of attacks, such as DDoS (Faldi et al., 2023).

Network architecture design involves the stages of designing the infrastructure that will be used to build the IDPS system. This includes placing the IDPS system on a network server by selecting the type or method of the Network Intrusion Detection and Prevention System (IDPS). The creation of the system begins by installing the IDPS system, namely the Snort configuration, including Snort rules and Honeypot, by installing and configuring it on the administrator's computer. Then create a Telegram bot as a notification sender by requesting the official Telegram bot account from the @BotFather account to get a token. The token is needed to get the chat_id so that the notification is received. The alert data sent by the Telegram bot is completely taken from the Snort database.

This honeypot recorded more than 1,000 attacks in a few minutes, highlighting their efficiency in data collection. Similarly, Paper 2 emphasizes the use of honeypots to capture web attack information, which is then analyzed to understand the methods and intentions of hackers (Wang, 2024). Snort's ability to detect malicious network activity by matching packets with predefined rules (Kaushik et al., 2024). This makes Snort an essential tool for data collection in network security systems. the importance of optimizing IDS using Snort and firewalls to prevent unauthorized access and protect network infrastructure (Durahman et al., 2024). This multi-layered approach ensures comprehensive security coverage.

The Snort working process begins with configuring and selecting the network interface to be monitored directly. Once the setup is complete, Snort is activated to analyze data packets passing through that interface, comparing them with predefined detection rules. (Purba & Efendi, 2020). In addition to security reporting and further analysis, Snort is also designed to send logs directly via Telegram bot API messages. (M.R. & P., 2022)

The HoneyDB work process is carried out by configuring the ID provided by the HoneyDB server and then setting the service that will be used as a clone of the original server. After that, HoneyDB can be run and can display a clone server so that attackers can be fooled. (Akshay et al., 2020).

The design stage is the design phase of a security monitoring system for a Local Area Network that uses Telegram notifications with Snort and Honeypot with the following steps:

a. Installing and setting up the Snort application on an Ubuntu server
b. Installing and setting up the HoneyDB application on an Ubuntu server
c. Creating a Telegram Bot
d. Setting up Snort for integration with Telegram

After the system is ready to operate, the next step is to implement it in a local network. The author will display attack data detected by Snort and HoneyDB, as well as monitoring information that appears in Telegram during testing.

4. RESEARCH RESULTS

In this study, the author conducted a trial using IP ping, Nmap, and bad traffic to simulate a backdoor. The warning notification generated from this trial will be sent via the Telegram bot. As well as conducting an attack trial on a fake server that has been created with HoneyDB.

4.1. Analysis

The results of the author's analysis by conducting observations that will use this security monitoring system are, namely:

1. Monitoring is carried out during working hours and as needed by utilizing the security system provided by the server
2. Repairs are made when damage or suspicious activity is detected on the server.
3. Identify potential hazards to recognize risks that can cause damage, defects, or other hazards so that they can be anticipated early.
4. Use the Telegram application as a network security monitoring system so that the hazard identification process can run optimally.
5. Collect references from journals, websites, and videos that are relevant to the project to support further development.

4.2. Design

In the image belowthere is a Telegram-based network security system monitoring workflow

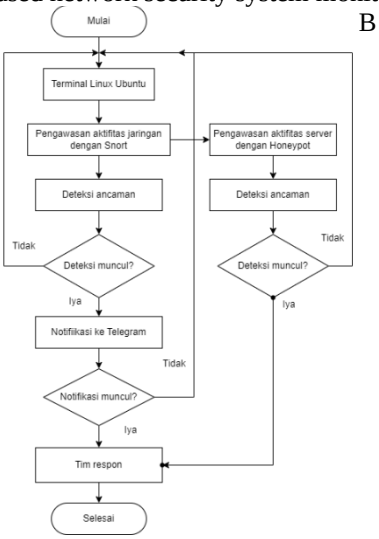

Figure 1 .Workflow for creating a network security monitoring system

The workflow in Figure 1 begins by opening the Ubuntu Linux Terminal. In Linux, 3 terminal pages will open, namely: a page to run Snort, a page to run the Telegram bot. Then open another terminal window to run Honeypot. After network monitoring by Snort and Honeypot is run, the attack detection will display the detected attacks. To send a snort alert to Telegram, run the telegram bot on another terminal page, then a Telegram notification will appear when the bot has been activated

4.3. Development

4.3.1. Install and Configure the Snort application

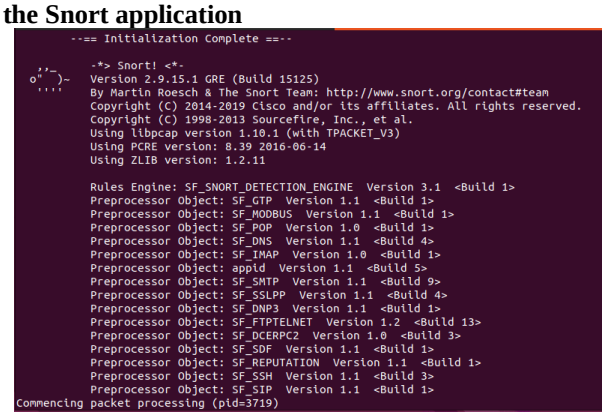

Figure 2 Snort application view

The Snort application used in this study is version 2.0 To get this program, you can visit the official Snort website: https://www.snort.org/ .

4.3.2. Install and Configure the Honeypot application

Then install Honeypot with the HoneyDB type. The HoneyDB software used in this study is version 2.2.0

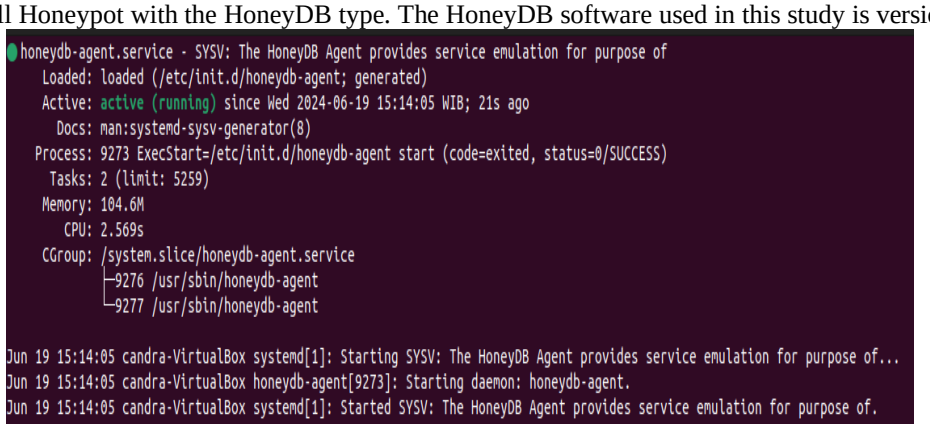

Figure 3. HoneyDB Application View

The software can be downloaded through the official HoneyDB website and can also be a stored log storage in graphical form.

4.3.3. Creating a Telegram Bot

Then create a Telegram bot so that notification alerts can be sent from Snort.

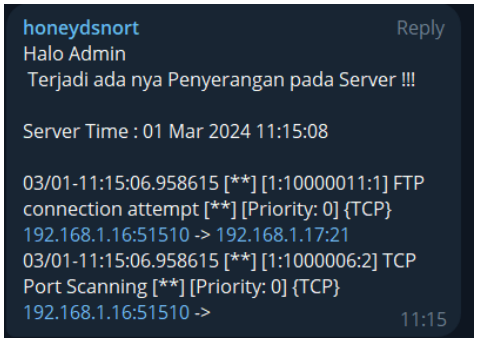

Figure 4. Telegram Bot view sending notifications

The Telegram bot created and configured on Ubuntu can send notifications from the Snort application.

4.4. Implementasi

4.4.1. Snort attack testing and notification delivery test

The purpose of this test is the success of the application to detect and send attack warning notifications from Snort to the Telegram Bot. This test was conducted in the Integrated Lab. The test was conducted by connecting the server and client laptops to the same Wi-Fi (local). The test results show that the Snort application can be connected, and Telegram notifications can be sent, as shown in the image below.

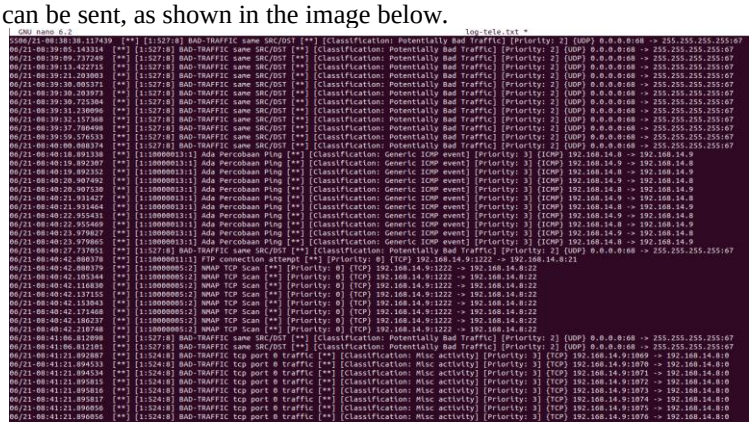

Figure 5 Attack log on Snort

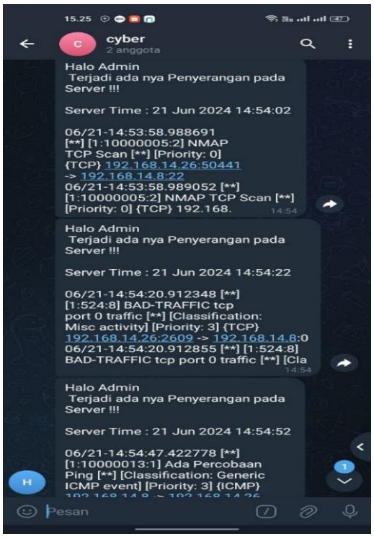

Figure 6 .Warning sent to Telegram Bot

4.4.2. Testing on HoneyDB server

The purpose of the HoneyDB server attack test is to prove that HoneyDB can manipulate the original server so that the attacker can only attack the fake server and the original server is not affected.

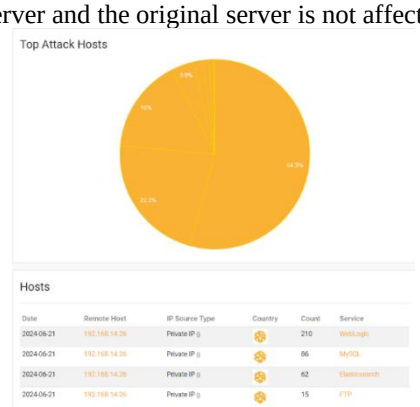

Figure 7. Attack log on HoneyDB server

The following image shows the test results from the HoneyDB server that can be viewed through the HoneyDB website.

 ISSN : 3032-2642

4.4.3. Quality of Service Testing

Quality of Service testing aims to evaluate the quality of the local network before and after the installation of the security monitoring system, as well as when tested with attacks. The table below shows the results when testing the network quality before and after the security monitoring system.

Table 1. QOS measurement results (1)

NO	PARAMETER	TIME	SCORE	INDEKS	CATEGORI
1	*Throughput (bps)*	(March 2024) 60 minutes	459k	4	Very good
2	*Packet Loss (%)*		0,3	4	Very good
3	*Delay (ms)*		14	4	Very good
4	*Jitter (ms)*		1,2	3	Good

Table 2. QOS measurement results (2)

NO	PARAMETER	TIME	SCORE	INDEKS	CATEGORI
1	*Throughput (bps)*	(April 2024) 60 minutes	704k	4	Very good
2	*Packet Loss (%)*		0,3	4	Very good
3	*Delay (ms)*		10	4	Very good
4	*Jitter (ms)*		21	3	Good

Table 3. QOS measurement results (3)

NO	PARAMETER	TIME	SCORE	INDEKS	CATEGORI
1	*Throughput (bps)*	(May 2024) 60 minutes	683k	4	Very good
2	*Packet Loss (%)*		0,1	4	Very good
3	*Delay (ms)*		3	4	Very good
4	*Jitter (ms)*		3	3	Good

Table 4. QOS measurement results (4)

NO	PARAMETER	TIME	SCORE	INDEKS	CATEGORI
1	*Throughput (bps)*	(June 2024) 60 minutes	1.026k	4	Very good
2	*Packet Loss (%)*		1	4	Very good
3	*Delay (ms)*		8	4	Very good
4	*Jitter (ms)*		5	3	Good

Quality of Service (QoS) measurement in this study is used to assess the quality of the internet network in transferring packets or data. The parameters tested include throughput, packet loss, latency, and jitter. Tables 1 and 2 show data sequentially (March and April) before the network security system was installed on the server with throughput parameters getting a value of 459 kbps and 704 kbps with an index of 4 (very good), delay getting a value of 14 ms and 10 ms with an index of 4 (very good), jitter getting a value of 1.2 ms and 21 ms with an index of 3 (good), and packet loss getting a value of 0.3% and 0.3% with an index of 4 (very good). Tables 3 and 4 show sequential data (May and June) after the network security system was installed on the server with throughput parameters getting a value of 683 kbps and 1,026 kbps with an index of 4 (very good), delay getting a value of 3 ms and 8 ms with an index of 4 (very good), jitter getting a value of 3 ms and 5 ms with an index of 3 (good), and packet loss getting a value of 0.1% and 1% with an index of 4 (very good).

4.5. Evaluation

At this stage, the system will be evaluated to ensure that the security monitoring objectives have been achieved and are in accordance with the initial needs. The implementation of a Telegram-based network security monitoring system in the Local Area Network at the Surabaya Aviation Polytechnic will be checked to ensure its success. The features lacking in this network security system monitoring are fail2ban, which is useful for blocking attacks or anomalous activities on the network, as well as sending snort alert notifications to Telegram botsis not fast enough due to the network conditions, which are not fast enough (in this case, the local network) with the calculation

$$Availability = \frac{\text{Uptime}}{\text{Uptime} + \text{Waktu downtime}} \; x \; 100\%$$

$$Availability = \frac{3.615\ s}{3.615\ s + 2.987\ s} \; x \; 100\% = 54{,}75\%$$

The installation of the fail2ban feature and the performance of sending notifications due to the network do not change the success of the system in monitoring network security. If there are deficiencies or problems found later, improvements will be made to improve the system.

5. DISCUSSION

Based on the description above, it can be seen that the way this security monitoring system works is by starting by running Snort on the Ubuntu terminal, then running the Telegram Bot script on another terminal, and running HoneyDB on another terminal. Then if there is an anomalous activity on the network that tries to attack, it will be detected on Snort and will immediately send a notification to Telegram, and HoneyDB runs according to its role, namely to manipulate the original server and show the fake server to the attacker. Then the results of the attack on the fake server created by HoneyDB can be seen in the graph on the official HoneyDB website.

6. CONCLUSION AND RECOMMENDATIONS

Snort and Honeypot are designed to monitor Local Area Network (LAN) network traffic at the Surabaya Aviation Polytechnic. By setting and adding special rules, the system uses Snort to detect potential threats. Honeypot functions to trick the original server so that attackers will attack servers that are not original. The data obtained from the attack is then analyzed. The system is also equipped with Telegram-based notifications to provide updates on suspicious activity or attacks detected in real-time.

Quality of Service (QoS) measurements were carried out to evaluate network performance before and after the installation of the monitoring system.

The measurement results showed that there was no significant difference in local network performance despite attacks on the network, which was still categorized as good.

FURTHER RESEARCH

This network security monitoring system can be developed to be more complex; it is expected to be able to add rules to Snort and services to Honeypot in order to detect more varied attacks. And additional prevention facilities can be added, namely fail2ban, to block anomalous activities on the network.

REFERENCES

[1] Adnyana, I. G., Dirgayusari, A. M., & Atmaja, K. J. (2024). Data Visualization for Building a Cyber Attack Monitoring Dashboard Based on Honeypot. *Sinkron : Jurnal Dan Penelitian Teknik Informatika*, *8*(4), 2510–2518. https://doi.org/10.33395/sinkron.v8i4.14144

[2] Akshay, A. D., Bhushan, A., Anand, N., Khemka, R., & Devi K.A, S. (2020). HONEYPOT: Intrusion Detection System. *International Journal of Education, Science, Technology, and Engineering*, *3*(1), 13–18. https://doi.org/10.36079/lamintang.ijeste-0301.66

[3] Altunay, H. C. (2024). Analysis of Cyber Attacks Using Honeypot. *Black Sea Journal of Engineering and Science*, *7*(5), 954–959. https://doi.org/10.34248/bsengineering.1531420

[4] Arfianto, A. Z. (2017). *Penggunaan Bot Telegram Sebagai Announcement System pada Intansi Pendidikan*. https://www.researchgate.net/publication/321845746

[5] Dang, F., Yan, L., Wang, J., Li, S., & Лю, Б. (2024). *Research on Network Intrusion Detection Technology Based on Honeypot*. 171–175. https://doi.org/10.1109/ispds62779.2024.10667558

[6] Durahman, Y., Nanang, H., & Arifin, V. (2024). *Anticipating Computer Security Using the Snort Intrusion Detection System*. 1–4. https://doi.org/10.1109/citsm64103.2024.10775522

[7] Faldi, F., Romadoni, D., & Sumadi, M. T. (2023). The implementation of network server security system using honeypot. *JIKO (Jurnal Informatika Dan Komputer)*. https://doi.org/10.33387/jiko.v6i2.6385

[8] Fernández-Álvarez, P., & Rodríguez, R. J. (2021). *Extraction and Analysis of Retrievable Memory Artifacts from Windows Telegram Desktop Application*.

[9] Kaushik, Y., Athmaraman, A., John, A. M., & Raj, S. (2024). *Signature-based Intrusion Prevention System for Software Defined Networks using SNORT*. https://doi.org/10.1109/aiiot58432.2024.10574719

[10] Khadafi, S., Meilani, D., Arifin, S., Komputer-Institut, S., Adhi, T., Surabaya, T., Rahman, J. A., & 100 Surabaya, H. N. (2017). *SISTEM KEAMANAN OPEN CLOUD COMPUTING MENGGUNAKAN IDS (INTRUSION DETECTION SYSTEM) DAN IPS (INTRUSION PREVENTION SYSTEM)*.

[11] M.R., A., & P., V. (2022). Review of Cyber Attack Detection: Honeypot System. *Webology*, *19*(1), 5497–5514. https://doi.org/10.14704/web/v19i1/web19370

[12] Patil, D. (2025). *Artificial Intelligence In Cybersecurity: Enhancing Threat Detection And Prevention Mechanisms Through Machine Learning And Data Analytics*. https://doi.org/10.2139/ssrn.5057410

[13] Purba, W. W., & Efendi, R. (2020). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI: Jurnal Teknologi Informasi*, *17*(Agustus), 143–158.

[14] Rasudin. (2014). *QUALITY OF SERVICE (QOS) PADA JARINGAN INTERNET DENGAN METODE HIERARCHY TOKEN BUCKET Rasudin*.

[15] Saut Parsaoran Tamba, M. K., Yonata Laia, M. K., & Saut Dohot Siregar, S. Pd. , M. P. (n.d.). 1974-Article Text-6394-1-10-20211007. *2021*.

[16]

[17] Wang, S. (2024). Design and Implementation of a Web Attack Analysis System Based on Honeypot Technology. *International Journal of Computer Science and Information Technology*. https://doi.org/10.62051/ijcsit.v4n2.09