Bit-Tech (Binary Digital - Technology)
Vol.6, No.2, December 2023
Available online at: http://jurnal.kdi.or.id/index.php/bt

Network Attack Detection Using Intrusion Detection System Utilizing Snort Based on Telegram

Juan Adi Dharma[1)*], Rino[2)]

[1)2)]*Buddhi Dharma University*
Imam Bonjol No.41, Tangerang, Indonesia
[1)]juanadi412@gmail.com
[2)]rino@ubd.ac.id

Article history:

Received 20 Sept 2023;
Revised 07 Oct 2023;
Accepted 14 Oct 2023;
Available online 28 Dec 2023

Keywords:

Cybercrimes
Intrusion Detection System
Network Attack Detector
Snort
Telegram

Abstract

The constantly evolving of information technology landscape has made information security something of paramount importance, yet the development of information technology is not met with a corresponding advancement in its security systems. As a result, in the current era, there is a multitude of cybercrimes in the realm of the internet. Therefore, this research aims to create a computer network attack detector using the Linux operating system by leveraging the Telegram-based Snort application and employing the Intrusion Detection System (IDS) method through an IDS-based application, namely Snort. Additionally, this study incorporates features for blocking IP addresses and changing the Linux server password through the Telegram application for initial response when an attack is detected, accomplished by sending specific commands within the Telegram application. Furthermore, this paper also introduce a feature for categorizing the risk of computer network attacks into three categories: Low, Medium, and High within the Telegram application. The results of this research demonstrate that Snort can detect predefined rules and send alerts to the Telegram application for every attack occurring within the Wireless Local Area Network (WLAN). Successful IP address blocking is achieved through Telegram integration with the Iptables application, and changing the Linux server password is also accomplished through Telegram by integrating the bash shell programming language found in the Terminal of the Linux operating system. Finally, the risk of attacks can be viewed within the Telegram application.

I. INTRODUCTION

The ever-evolving information technology landscape has made information security a matter of utmost importance, especially in the context of networks connected to the internet. Unfortunately, it is regrettable that each technological advancement is not accompanied by a corresponding development in information security systems. This has resulted in many systems remaining vulnerable and in need of enhanced security. Attacks against servers and services within organizations, or any form thereof, pose a significant detriment to both organizations and individuals.

Computer network security is a vital component of the system that upholds competence and integrity, ensures service availability to its users, and identifies unauthorized computer network usage[1], [2]. The Intrusion Detection System (IDS) functions as a network attack detector when attacks are initiated. IDS is capable of detecting harmful packets and suspicious activities within the network [3]. Snort is open-source security software or a tool based on Intrusion Detection System (IDS) designed to detect intrusion attempts within computer networks in real-time[2]. Snort is open source, meaning it can be used without the need for licensing fees[4]. Snort's features are valuable for network and system administrator, as it can alert potential intruders who may pose a threat to a system or network.

The types of attacks that can be detected in this research include Distributed Denial-of-Service (DDoS), Telecommunication Network (Telnet), File Transfer Protocol (FTP), Secure Shell (SSH), SQL Injection, and Cross-Site Scripting (XSS).

* Corresponding author

ISSN 2622-2728 (online) 2622-271X (print)
doi: 10.32877/bt.v6i2.943

The results of this research can detect the attacks mentioned previously. In addition, Telegram notifications or messages display the number of detected attacks, allowing identification of the most frequently targeted attack types, as well as additional risk assessments categorized as Low, Medium, and High. So that network administrators can determine vulnerabilities on servers. In this research, initial handling is also added when an attack is detected to prevent further attacks, such as blocking the attacker's IP address via Telegram if an attack occurs, such as DDoS, SQL Injection, and Cross Site Scripting on a website. In addition, changing server passwords for FTP, SSH, and Telnet services via Telegram. So that networks administrators can reduce the impact of attacks so that losses can be minimized.

II. Related Works/Literature Review

Several studies have been conducted to support understanding in this field. Researcher Lasma Feronika Nainggolan et al. [3], in the Scientific journal of Computer Engineering Volume 2 No 2 from the institution of the University of Methodist Indonesia, conducted a study on "Monitoring Network Security on Ubuntu Servers from DDoS Attacks Using Snort IDS." This study employed the Intrusion Detection System (IDS) method. The research concluded that Snort's Bash Shell implementation is capable of recording DDoS attacks, which are then forwarded to Telegram bots in real-time.

Furthermore, researcher Rudy Suwanto et al. [9] from the institution of Tanjungpura University have published their research findings in the journal Komputer dan Aplikasi. They conducted a study on the "Implementation of an Intrusion Prevention System (IPS) Using Snort and Iptables in Website-Based Local Network Monitoring" using the Intrusion Prevention System (IPS) method. The results indicated that the system's success rate in detecting attacks was 90% for pong of death attacks and 85% for port scanning attacks. The study also showed that avoiding attacks on Internet Control Message Protocol (ICMP), User Data Protocol (UDP), and Transmission Control Protocol (TCP) ports can be mitigated by using Iptables.

III. Methods

A. Intrusion Detection System

Intrusion Detection System (IDS) is a framework that filters network traffic to recognize suspicious activities[5]. The operation of IDS is not significantly different from antivirus programs as a whole. Therefore, the way IDS works is by filtering and coordinating traffic with a set of interrupt servers that store various information about different types of interruptions or attacks, assuming that IDS detects a match, after which IDS will send an alert[5].

B. Snort

Snort is an illustration of an Intrusion Detection System (IDS) program capable of identifying attempted intrusions within a computer network framework[2]. This application is an open-source application, making it available for securing server system at no cost, without the need for licensing fees[3]. The Snort rules are a database that stores attack patterns. These rules are then used by the detection engine to compare network traffic with the existing rules. If network traffic matches the rules, it is considered an intrusion attempt, and an alert will be issued[4].

C. Telegram

Telegram not only provides features for online chatting but also adds bot functionally with specific functions that operate automatically in response to user commands or requests[6]. The operation of a chatbot on the Telegram application involves users entering relevant commands, upon which the bot provides automatic responses based on its existing database. If the command is not suitable, the bot will not send any response[7]. The telegram bot is an applications with an interface based on the Hypertext Transfer-Transfer Protocol (HTTP)[8].

D. Iptables

Iptables is an application or tool that functions to provide a layer of protection for data within a device in a Linux operating system[9]. Iptables works by reading network traffic and then comparing it to rules created by the user[10]. The filter table is commonly used to manage network traffic on a server. There are several rules for the filter table: the first one is 'Accept,' which means accepting incoming packets; rejecting incoming the seconds is 'Reject,' which means rejecting incoming packets; the third is 'Drop,' which terminates the packet's connection; and; the last one is 'Log' for logging packets[10]. Iptables users can manage network traffic within a server, allowing, blocking, and managing ports, as well as controlling incoming and outgoing connections[9].

E. Bash Shell Programming Language

Bash programming Language is a scripting language used in both Linux and Unix operating systems. It is used to execute the ping application to determine network connectivity, and the ping process uses the Internet Control Message Protocol (ICMP)[11]. Bash was designed as a replacement for the Bourne Shell (SH) by providing additional features and several quality improvements[11]. Bash continues to be updated with improvements and

the addition of new features. This shell continually evolves with extensive community support, making it one of the most widely used shell scripting languages to this day.

F. Python Programming Language

Every programming language evolves with the emergence of new ideas and technologies, an Python developers continue to make this language more flexible and powerful[12]. The advantage of the Python language is that it is considered easy to learn, at least for beginners[13]. The code is not difficult to read carefully, and Python offers many powerful capabilities due to its extensive standard library. Python can even make projects of a very complex scale seem simple[12].

G. File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is an internet protocol used as means to exchange data between a client and a server within a network[14]. FTP is defined as a protocol for sending and receiving files between hosts used on the Advanced Research Project Agency Network (ARPANET) system. The primary function of FTP is to facilitate the easy and efficient transfer of data file between hosts, as well as to store and retrieve files remotely. FTP employs a client-server system that utilizes FTP to enable computer and smartphone users to access an FTP server, exchange data over a wireless network, and exchange data more efficiently[14].

H. Secure Shell

Secure Shell (SSH) serves as secure data transfer medium and can also be used remotely[15]. Network administrators are required to work harder to secure the computer network they manage. One form of network administrator in server management is through remote login[15]. The remote server access serves the purpose of monitoring and supervising the centralized internet server network, making it easier for internet network administrators to manage it through remote server access[15].

I. Telecommunication Network (Telnet)

Telecommunication Network (Telnet) is an network protocol used to access and control distant gadgets over an network protocol with Telnet, the device can associate with gadgets, such as servers, switches, or distant PCs and communicate with them as though they were before the gadget[16]. Telnet can be attacked by utilizing telecommunication technology and computer network information systems as transmission media with the aim of defrauding other people to obtain public and private property[16].

J. SQL Injection

SQL injection is a technique of attack that exploits security vulnerabilities on a website by injecting malicious code[4]. Assailants alter SQL Injection to get data and the information base server, permitting them to enter the framework without a record. Accordingly, aggressors can control information inside the data set[17]. The security vulnerability is exposed when an attacker inputs string values and other control characters into SQL statements by modifying the SQL commands stored in the client application's memory. This allows the attacker to inject SQL code to gain access to information and the database server[4].

K. Cross Site Scripting (XSS)

Cross Site Scripting (XSS) is one of the types of injection attacks with the different script code into a website[4]. This attacks will appear to originate from the affected website the consequences of this attacker potentially bypassing client-side security, obtaining sensitive information, acquiring user cookies, or delivering malicious applications[4]. The annihilation delivered by the XSS injection susceptibilities is particularly critical since the aggressor can take touchy information, for example, the put away client's treats and tokens or control the host from a distance by utilizing remote code execution of XSS[18].

L. Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) attack is an attack that floods the victim's computer with an overwhelming amount of information requests[3]. As a result, the computer system is unable to function normally and cannot provide its services[3]. A commonly used form of DDoS is the ping of death, where the attack leverages Internet Control Message Protocol (ICMP) communication to be inundated with requested data packets. Another type of attack is TCP flooding and UDP flooding, which flood TCP and UDP packets continuously through fictitious clients, eventually causing the server to go down[3].

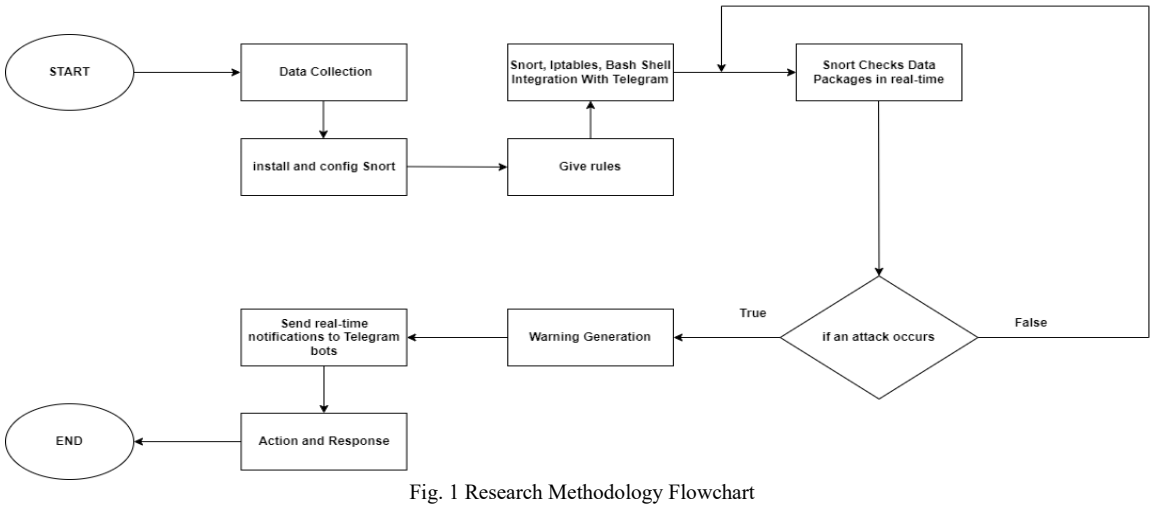

Fig. 1 Research Methodology Flowchart

The following is an explanation of the Figure 1 above:

a. the first step is data gathering to perform network attack detection, we collected network traffic data that would be analysed by the system. This data could be in the form of network packet streams, activity logs, or network traffic data stored in the appropriate format.
b. The next step is install and configure Snort on the network that will be monitored. After all the configuration are completed.
c. the next step is to create rules that Snort will use to detect potential attacks.
d. And then integrate Snort using Bash Shell language, Iptables, Bash Shell with the Telegram application.
e. Subsequently, Snort will continuously check for any signs of an attack. If no attack is detected, Snort will keep monitoring new data packets. However, if an attack occurs, Snort will issue a warning and send it to a Telegram bot. In addition to issuing warnings, this research also includes actions and responses to attacks.

The first action is to block the IP addresses involved in the attack via Telegram by integrating Iptables using python language. Furthermore, other measures taken include changing the passwords for File Transfer Protocol (FTP) service, Secure Shell (SSH) service, and Telecommunication Network (Telnet) service via Telegram by integrate the Bash Shell language using python language. Additionally, a network attack risk assessment is divided into 3 categories, namely, Low for the number of attacks from 1 to 10, Medium for the number of attacks from 11 to 20, and finally High for the number of attacks exceeding 21 this feature is still input manually into the language python script. So the number of attacks must be calculated manually.

This features allow network administrators to assess vulnerabilities in various parts of the server by displaying those risks in the Telegram application using the python language. Thus, the above steps form a crucial framework in this research for detecting, responding to, and mitigating network attacks. Although significant progress has been achieved in the development of IDS and utilization of Snort, there are still contradictions in research regarding the integration of Snort-based IDS with Telegram for universal network attack detection and immediate reply. This study attempts to overcome this contradiction by proposing a new system that leverages the capabilities of Snort and Telegram to improve network security.

IV. RESULTS

The testing of the Intrusion Detection System, using Snort, involves the use of pre-defined rules to identify more specific attacks and ensure that Snort can detect these rules. Snort is deployed on the target/victim laptop, which is used as the device being attacked to detect prepared attacks. The following is figure 2 of the Snort warning display in the Telegram application.

Figure 2 explains results of logs Snort on the Telegram bot with a type of SQL Injection attack where the attacker's IP address is 192.168.1.14 and the target IP address is 192.168.1.15, but all types of attacks are more or less the same in structure. They include a warning message, date and time of the attack, the attacker's IP, the target IP, and the type of attack. The only difference is the text describing the type of attack.

Fig. 2 Snort Logs On Telegram Bot

Testing the blocking of IP addresses via Telegram. After the attack is detected, the research adds simple mitigation to prevent the attack from continuing. This research integrates Telegram-based Iptables to block the attacker's IP address using the Telegram application. Figure 3 displays the blocking of the attacker's IP address via the Telegram application.

Fig. 3 Blocking an IP address through the Telegram

Figure 3 explains that the command /blockip and then enter the IP address that you want to block, as in Figure 3 the blocked IP address is 192.168.1.14.

The research integrates a Telegram-based Shell to change the password of the Ubuntu Linux operating system via Telegram. This is done to mitigate attacks on FTP, SSH, and Telnet services where the attacker has knowledge of the passwords. Figure 4 displays a Telegram bot message and commands for changing the passwords through Telegram.

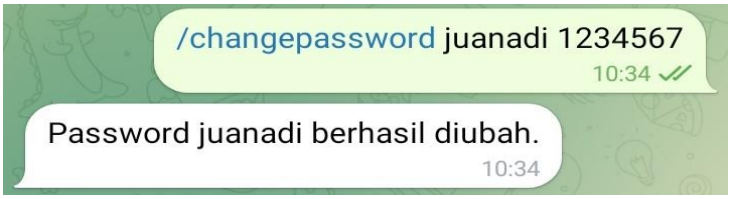

Fig. 4 Changing The Password Through the Telegram

Figure 4 explains that the way to input the command is simply by entering /changepassword username new password.

Testing computer network attack risks will be displayed via Telegram. Computer network attack risks are divided into three categories: Low, Medium, and High. These three categories are determined based on the number of detected attacks for each type. If the number of detected attacks is from 1 to 10, it will be categorized as Low. If the number of detected attacks is from 11 to 20, it will be categorized as Medium. If the number of detected attacks is more than 21, it will be categorized as High. Please note that the number of attacks is calculated manually, so it must be entered into the script manually. For more clarity, you can refer to Figure 5, which shows the message displayed in the Telegram chat bot by entering /risikoserangan.

Fig. 5 Computer Network Attack Risk Messages on The Telegram

Figure 5 explains that attacks with a count below 10 are categorized as Low, for the Medium category, the number of attacks ranges from 11 to 20, and High category includes attacks exceeding 21. Keep in mind that the detected number of attacks is calculated manually, so it must be entered into the script manually.

V. DISCUSSION

In this discussion, the results of the research on detecting computer network attacks using Snort based on Telegram will be explained. Below is a brief description of the results of this research:

a. Telegram successfully displayed a warning note from Snort. In the Telegram display, there is a warning sentence containing the attack date and time, the attacker's IP address, and the target IP address.
b. Telegram is able to block IP addresses that need to be blocked by integrating Telegram-based Iptables. It can be seen in Figure 6 that Iptables has already blocked the IP address 192.168.1.14.

```
root@SnortHoneypot:/home/juanadi# sudo iptables -L INPUT -n | grep DROP
DROP       all  --  192.168.1.14         0.0.0.0/0
root@SnortHoneypot:/home/juanadi#
```

Fig. 6 The IP Address 192.168.1.14 has been blocked

As shown in Figure 6, there is a "DROP 192.168.1.14", so the IP address 192.168.1.14 is prevented from launching further attacks.

c. Telegram is able to change the password of a Linux Ubuntu operating system by integrating the Bash Shell programming language.
d. Telegram is capable of displaying computer network attack risks, such as the detected number of attacks, attack categories: Low, Medium, High, and attack types. Here is Figure 7, which shows the script for the manually entered number of attacks.

```
@bot.message_handler(commands=['risikoserangan'])
def handle_risikoserangan(message):
    jumlah_rule_1 = 100
    jumlah_rule_2 = 100
    jumlah_rule_3 = 30
    jumlah_rule_4 = 25
    jumlah_rule_5 = 10
    jumlah_rule_6 = 15
    jumlah_rule_7 = 100
    jumlah_rule_8 = 5
```

Fig. 7 Script for The Detection Number of Attacks

The explanation in Figure 7 is that the "jumlah_rule_1" indicates a DDoS attack using Transmission Control Protocol (TCP) port that has been detected or counted 100 times. The "jumlah_rule_2" indicates a DDoS attack using Internet Control Message Protocol (ICMP) port that has been detected or counted 100 times. The "jumlah_rule_3" indicates a Telnet login attack that has been detected or counted 30 times. The "jumlah_rule_4" indicates a SQL Injection attack that has been detected or counted 25 times. The "jumlah_rule_5" indicates SSH login attack that has been detected or counted 10 times. The "jumlah_rule_6" indicates a FTP login attack that has been detected or counted 15 times. The "jumlah_rule_7" indicates a DDoS attack using User Data Protocol (UDP) port that has been detected or counted 100 times. The "jumlah_rule_8" indicates a Cross Site Scripting (XSS) attack that has been detected or counted 5 times.

VI. CONCLUSIONS

Snort can detect computer network attacks within the Telegram-based. It also effectively handles computer network attacks within the Telegram application, such as blocking IP addresses and changing the password of the Linux Ubuntu operating system. The response is also fast. The computer network attack risks displayed on Telegram are also accurately calculated. Suggestions that can be provided in this research, it is hoped that the study can be further develop, for the computer network attack risk section, it can be further developed by automating the calculation of the detected attack counts. This way, there's no need to input the counts manually.

REFERENCES

[1] R. Pangestu and A. Solichin, "Klasifikasi Serangan Jaringan Menggunakan Metode Decision Tree Berbasis Website," *Jurnal Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, vol. 1, no. 1, pp. 614–620, Apr. 2022, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/

[2] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort," *SISFOKOM(Sistem Informasi dan Komputer)*, vol. 09, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9.i1.770.

[3] L. F. Nainggolan, N. F. Saragih, and F. G. N. Larosa, "Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS," *Jurnal Ilmiah Teknik Informatika* , vol. 2, no. 2, pp. 1–10, Apr. 2022, [Online]. Available: http://ojs.fikom-methodist.net/index.php/METHOTIKA

[4] I. G. W. Bangga and S. M. Ladjamuddin, "SIMULASI SNORT SEBAGAI ALAT PENDETEKSI INTRUSI PADA WEB DAMN VULNERABLE WEB APPLICATION," *Jurnal Rekayasa Informasi*, vol. 11, no. 2, pp. 160–167, Apr. 2022.

[5] P. S. Fat, Khairil, and E. P. Rohmawan, "Perancangan Dan Implementasi Intrusion Detection System (IDS) Untuk keamanan Wireless Local Area Network (WLAN) Pada SMKN 5 Kota Bengkulu," *Jurnal Media Computer Science*, vol. 2, no. 1, pp. 1–8, 2023.

[6] B. Pasaribu and W. Susanti, "Sistem Informasi Pengajuan Rancangan Usulan Penelitian Menggunakan PHP Native dan Bot Telegram," *Jurnal Mahasiswa Aplikasi Teknologi Komputer dan Informasi*, vol. 3, no. 1, pp. 29–38, 2021, [Online]. Available: http://www.php.net.

[7] A. Fathurrozi and F. Karimah, "Pelayanan Dan Informasi Customer Service Berbasis Bot Telegram Dengan Algoritma Forward Chaining Pada CV.Primguard Indonesia," *Journal of Information and Information Security (JIFORTY)*, vol. 2, no. 2, pp. 211–226, 2021, [Online]. Available: http://ejurnal.ubharajaya.ac.id/index.php/jiforty

[8] Murtopo, Khairil, and Gunawan, "Perancangan Media Pembelajaran Agama Islam Secara Interaktif Berbasis Aplikasi Telegram Bot pada Politeknik Negeri Media Kreatif," *ANALYTICA ISLAMICA*, vol. 11, no. 2, pp. 311–326, Jun. 2022, [Online]. Available: https://balitbangsdm.kominfo.go.id

[9] R. Suwanto, I. Ruslianto, and M. Diponegoro, "IMPLEMENTASI INTRUSION PREVENTION SYSTEM(IPS) MENGGUNAKAN SNORT DAN IPTABLE PADA MONITORING JARINGAN LOKAL BERBASIS WEBSITE," *Jurnal Komputer dan Aplikasi*, vol. 7, no. 1, pp. 97–107, 2019.

[10] Desmira, "SISTEM KEAMANAN OPERASI LINUX UBUNTU IPTABLES SEBAGAI FIREWALL DI DINAS PENDIDIKAN KABUPATEN SERANG," *Jurnal Khatulistiwa Informatika*, vol. 9, no. 1, pp. 17–22, 2021.

[11] Nurhanif and Z. Maizi, "PEMBUATAN PETA JARINGAN UNTUK MEMONITORING KONEKSI KOMPUTER MENGGUNAKAN PEMROGRAMAN BASH SCRIPT," *Journal of Informatics and Computer Science*, vol. 5, no. 2, pp. 164–173, Jun. 2019.

[12] Runimeirati, A. Muis, and F. Muhammad, "Pelatihan Text Mining Menggunakan Bahasa Pemrograman Python," *Jurnal Pengabdian Kepada Masyarakat*, vol. 3, no. 1, pp. 37–46, 2023, [Online]. Available: https://pusdig.web.id/index.php/abdimas/index

[13] F. Caccavale, C. L. Gargalo, K. V. Gernaey, and U. Krühne, "SPyCE: A structured and tailored series of Python courses for (bio)chemical engineers," *Education for Chemical Engineers*, vol. 45, pp. 90–103, Oct. 2023, doi: 10.1016/j.ece.2023.08.003.

[14] M. I. Rafi and Saudi, "Rancang Bangun Jaringan FTP Server dengan Menggunakan Windows Server," *NetPLG Journal of Network and Computer Applications*, vol. 1, no. 2, pp. 34–49, 2022, [Online]. Available: https://jurnal.netplg.com/jnca

[15] Desmira and R. Wiryadinata, "Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking," *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 5, no. 1, pp. 28–33, 2022.

[16] T. Shi, J. Fu, and X. Hu, "TSE-Tran: Prediction Method of Telecommunication-network Fraud Crime Based on Time Series Representation and Transformer," *Journal of Safety Science and Resilience*, vol. 4, pp. 340–347, Dec. 2023, doi: 10.1016/j.jnlssr.2023.07.001.

[17] R. Hermawan, "TEKNIK UJI PENETRASI WEB SERVER MENGGUNAKAN SQL INJECTION DENGAN SQLMAP DI KALILINUX," *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)*, vol. 6, no. 2, pp. 210–216, 2021.
[18] Q. Abu Al-Haija, "Cost-effective detection system of cross-site scripting attacks using hybrid learning approach," *Results in Engineering*, vol. 19, Sep. 2023, doi: 10.1016/j.rineng.2023.101266.