Overcoming Network Security on Host-Based Intrusion Detection System (HIDS) With IP and PORT Blocking Methods

Muhammad Abdurrohman[1], Nugroho Suharto[2], Putri Elfa Mas'udia[3]
[1]Digital Telecommunication Network Study Program, Department of Electrical Engineering,
State Polytechnic of Malang, 65141, Indonesia
[2,3]Telecommunication Engineering Study Program, Department of Electrical Engineering,
State Polytechnic of Malang, 65141, Indonesia

[1]abdurrohmaan99@gmail.com , [2]nugroho.suharto@polinema.ac.id , [3]putri.elfa@polinema.ac.id

***Abstract*— Network security is important to maintain security on a network, the data and information contained in it. Based on the protection of data/information security in a network, generally all data-based security theories are created and applied to secure a particular network. Network security methods that have emerged such as using IDS (*intrusion detection system*), Intrusion Detection System (IDS) or intruder detection system are computer systems (can be a combination of software and hardware) that attempt to detect intrusions. At this time DOS attacks or *software* that occur to the general public in the form of (browsers, files, videos or images) that often occur with the aim that *the server* or network is unable to accommodate the traffic, causing the website/service *down* and cannot operate. Therefore, to assist in these attacks, it is necessary to apply *blocking* IP and PORT by using *blocking* so as to be able to add researchon network protection in the internet world.**

Keywords*— DOS, IDS, IP blocking, Network Security, PORT

I. INTRODUCTION

Network security is important to maintain the security of a network, the data and information in it. Based on the protection of data/information security in a network, generally all data-based security theories are created and applied to secure a particular network. Network security methods that have emerged such as using IDS (intrusion detection system) [1-5].

One of the security methods to secure a network is to use IDS, IDS is a security system where if there is something suspicious behavior that is not appropriate to be applied to the network, the IDS will provide identification and if possible, block the IP address and PORT that carried out the attack. There are two techniques used in IDS, namely, NIDS and HIDS, HIDS is able to carry out examinations additional systems that can only be performed when the IDS application is installed on the host, such as file integrity checking, registry monitoring, log analysis, rootkit active response. detection and. The activity of an individual network host will be monitored whether there is an attempted attack or intrusion into it or not [6-10].

According to Syani & Ropi (2018), at this time DOS attacks or software-based attacks that occur in the general public in the form (browser, file, video or image) are aimed at preventing the server or network from being able to accommodate the traffic, causing the website/service to be down and unable to operate. According to Dar & Harahap's research (2018), using the implementation of the Snort Intrusion Detection System (IDS) on a computer network system can only detect DOS attacks that occur without overcoming these attacks [11-15]. Therefore, this study applies the IP and PORT blocking method to be able to detect and overcome DOS attacks1 automatically. In addition, by using the IP and PORT blocking methods so as to be able to add research on network protection in the internet world.

II. METHOD

A. *Research*

Stages The stages of the research carried out are the stages in the research which will later be compiled with the intention that the research is carried out in detail as shown in Fig. 1. The following explanation is a description of Fig. 1:

1. The first stage, literature study, is to understand the problem so that it can determine the right solution.
2. The second stage, system requirements analysis, is in the form of stages to learn all the tools and materials that will be used in making the system such as component characteristics, component requirements.
3. The third stage, system design, is the process of makinga work design of the system to be made.
4. The fourth stage, system implementation, is the stage in making the system in accordance with the system design that has been made.
5. The fifth stage, system testing, is the stage when thesystem will be tested to see whether the system is running as previously designed. If the system is running but is notin accordance with the system design that has been made, it will return to the third stage, namely system design. If the system is in accordance with the system design, it can go to

the next stage.

6. The sixth stage, data retrieval, is the stage of the data collection process on the object that is carried out when the system is working.
7. The seventh stage, the analysis and report writing stageis the stage that analyzes the work system including the program running as planned, starting from sensordetection to sending data to the web and other systems then if the system is in accordance with the plan, conclusions can be drawn.

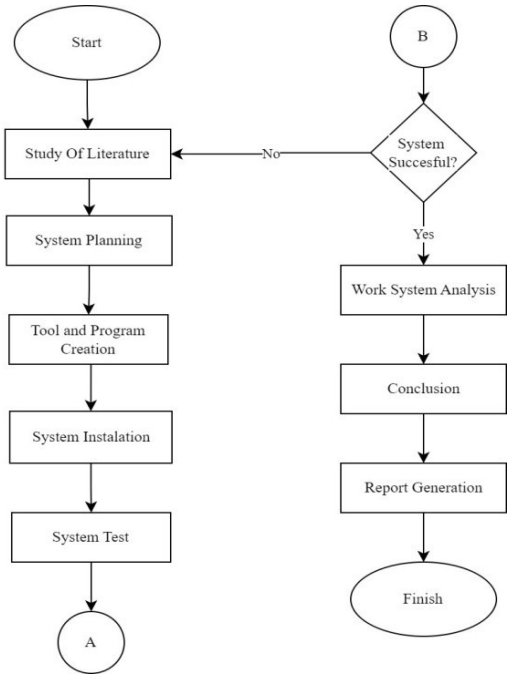

Figure 1. Research Stages

B. System design

The design that will be made to facilitate system design requires a system design drawing on the network, in this study shown in Fig. 2 which is the network design that will be carried out.

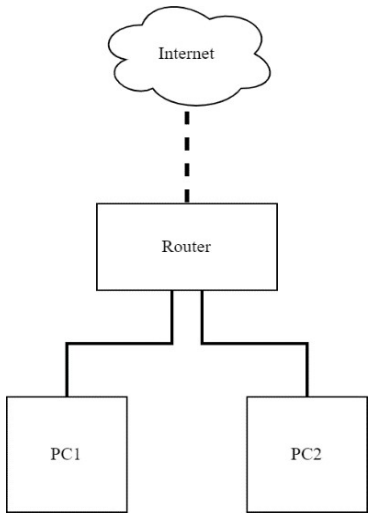

Figure 2. Drawing of Compilation Design

The following is a description of each function of the device designed based on Fig. 2:

1. A client/PC is a certain customer who uses network access that has been provided by the server.
2. The server can provide website access services to the client. If the incoming data is unexpected data, the server must be able to take action, namely by blocking the originating IP.
3. The Internet as a means of data communication to carry out daily routines, will be convenient in terms of communication and data transfer.

The device system design diagram is shown in Fig. 3 as follows:

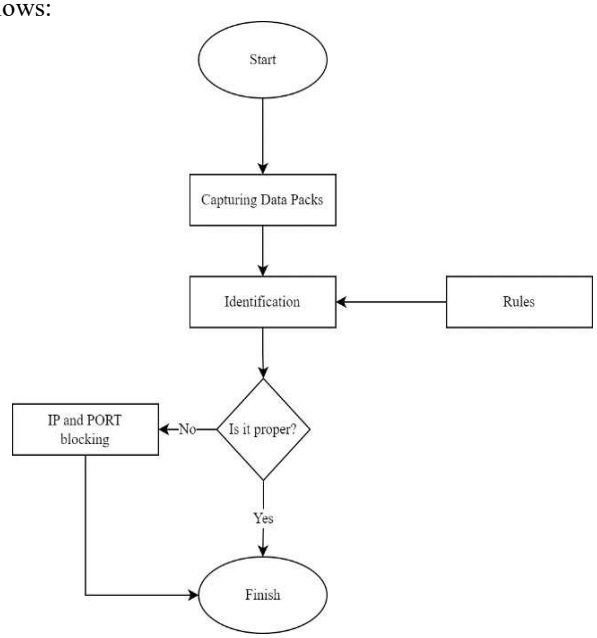

Figure 3. System Design

The following is a description of Fig. 3:

1. The first stage is entering data.
2. The second stage is to capture all data packets carried out between the client and server.
3. The third stage is the detection of data packets that have been carried out, whether the packet is in accordance with the rules that have been determined.
4. The fourth stage is packet selection, whether the packet isa normal packet or not, if the packet is a suspicious and dangerous packet, the server will block IP and PORT.

C. Attack Flow

The attack flow to be carried out in this study is shown in Fig. 4. From Fig. 4 it will be described how the steps for the attack and how the type of DOS attack works on the server, the first thing the *attacker* by scanning all ports that is on the server if there is an open port then the *attacker* will try to access a website service or other site with DOS continuously to the server, then the server will be exposed to DOS attacks so that server performance in serving other clients is disruptedand cannot perform its functions properly, then the next step is to

make a rule and the Blocking method IP and PORT to the attacker so that it can prevent attacks.

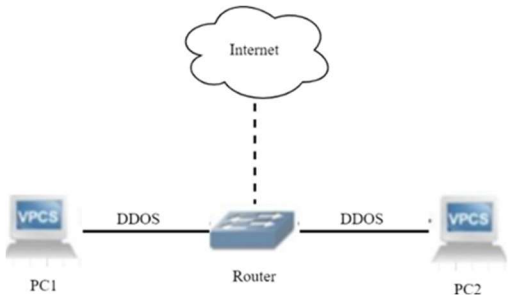

Figure 4. Attack Flow

III. RESULTS AND DISCUSSION

A. *Monitoring Port*

The process of scanning the port using nmap on the client to the server is shown in Fig. 5.

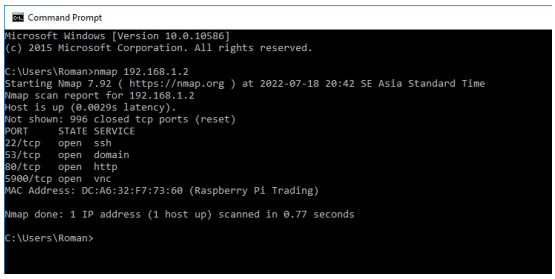

Figure 5. Scan Port

In Fig. 5 the *capture* Scan the Client port that there isa TCP protocol being open with the source IP address of the server, meaning that the server is serving the TCP protocol to the client.

B. *Configuration Rules*

Rules configuration is done by adding rules on each port used and filtering service access so that it can minimize the occurrence of an attack through website services, ports and others. The configuration of the is shown in the image below:

1. Enabling and adding the port ssh rule to fail2ban

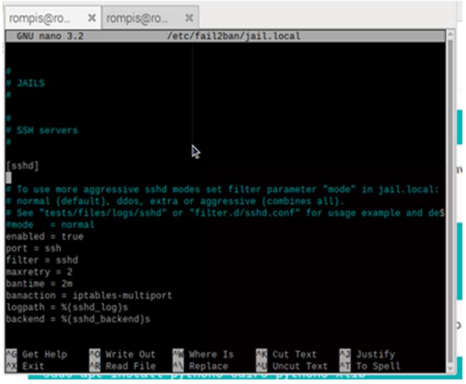

Figure 6. Configuring the sshd rules

In Fig. 6 above it can be explained that the ssh port has been enabled and added the ssh port rules with the following description:
Enabled = true (the ssh port has been enabled)
Port = ssh
Filter = sshd (filter port)
Maxretry = 2 (limit the number of accesses on the port)
Bantime = 2m (number of ip and port blocking times)

2. Activate and add apache-auth rules to fail2ban

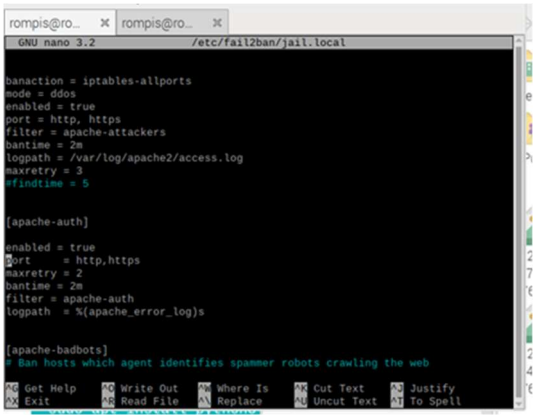

Figure 7. Apache-auth configuration

In Fig. 7 above it can be explained that apache-auth has been enabled and adds apache-auth rules with the following information:
Enabled = (apache-auth has been enabled)
Port = http,https
Maxretry = 2 (limit number of access failures on port)
Bantime = 2m (number of blocking time ip and port)
Filter = apache-auth (filter port)

3. Activate and add apache-attackers rule on fail2ban

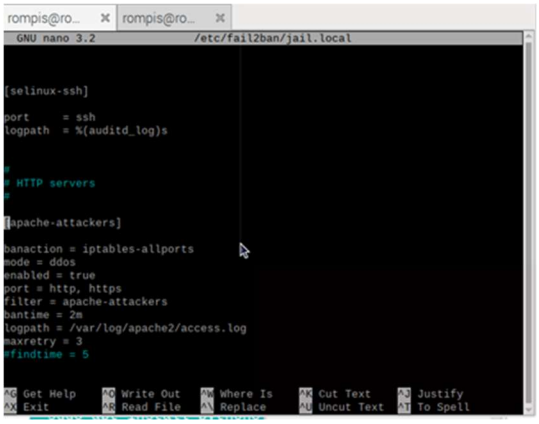

Figure 8. Apache-attackers configuration

In Fig. 8 above it can be explained that apache-attackers has been enabled and added apache-auth rules with the following information:
Enabled = true (apache-attackers have been activated)
Mode = ddos (type of attack mode that will block ip and port)

Port = http, https
Maxretry = 3 (limit the number of access failures on the port)
Bantime = 2m (sum of ip and port blocking time)
Filter = apache-attackers (filter ports)

C. *Network Security*

Testing Network security testing is done by accessing ports or website services by trying to violate the system security on the server. Denial of Service (DOS) is a type of attack on a computer or server on the internet network by spending resources owned. For network security testing can be shownin the image below:

1. Testing ssh login from the attacker to the server

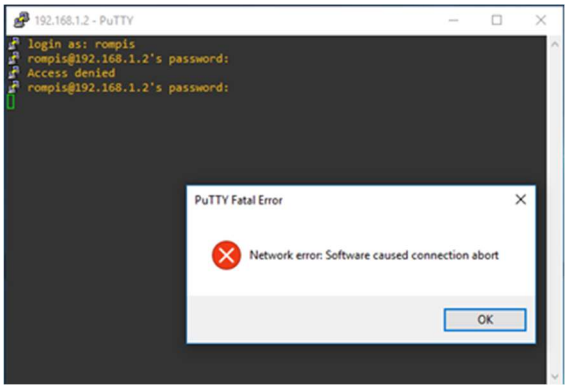

Figure 9. Process attacker Performing attacks via ssh

Fig. 9 above can be explained that the attacker's computer attempted an attack via the ssh port to the server byexceeding the specified access service limit.

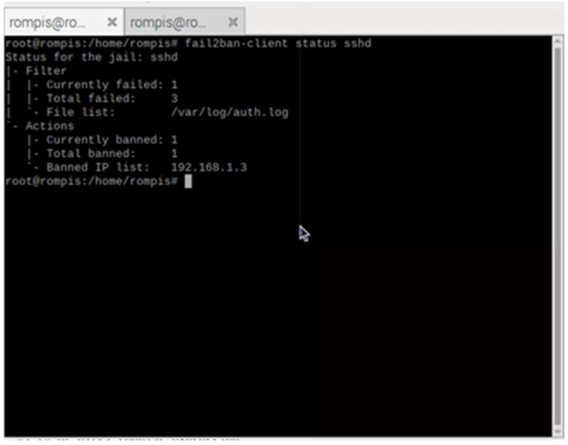

Figure 10. Logging blocking

Fig. 10 shows that there is an ip blocking and access rights for the ssh port service for a long period of time. a predetermined blocking time, if you want to see the results or IP records of the attacker who was blocked on the ssh port. doit with the following command:

Fail2ban-client sshd status

2. Testing website login from the attacker to the server

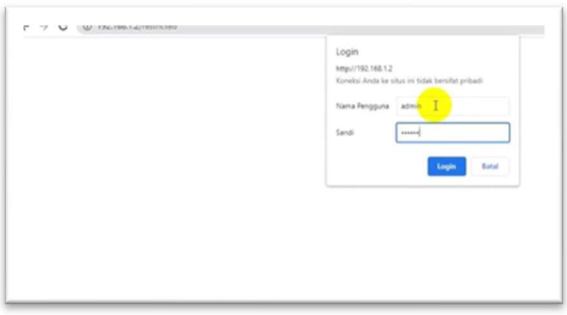

Figure 11. The process of the attacker carrying out an attack through the Website Login

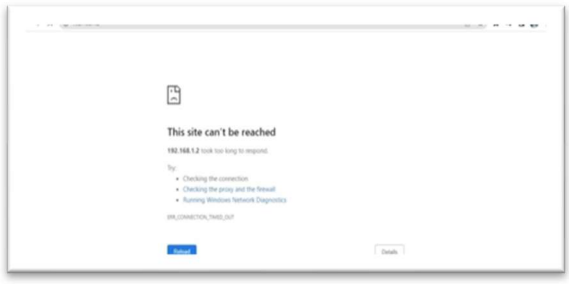

Figure 12. The results of blocking the login website

Fig. 11 and Fig. 12 above show an *attacker* conducting an attack experiment by logging in many times to the website server. If the *attacker* exceeds the limit on the number of logins that have been determined on the server rule, the server will automatically close the website service and block the ip and port on the *attacker*.

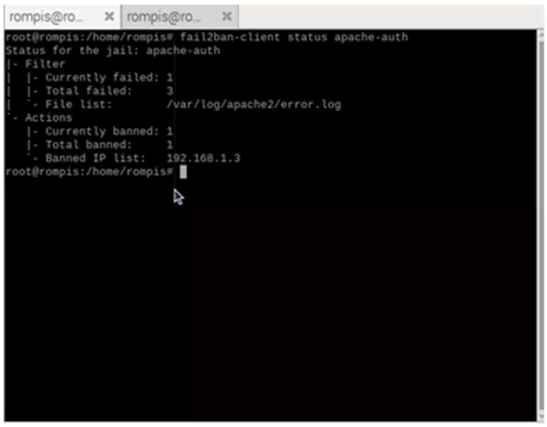

Figure 13. Logging Blocking

Fig. 13 above shows the results of blocking ip and port logging on the server that the attacker has failed to log in 3 times, the server automatically blocks the attacker with a predetermined blocking period, if you want to see the results or the attacker's IP record is blocked on the website. do it withthe following command:

Fail2ban-client status apache-auth

3. Testing access services through the website from the attacker to the server

Figure 14. The attack process through the webserver

Fig. 14 above shows that the attacker when accessing a website server, DDOS is one type of *cyber-attack* that targets websites, online services, and networks by flooding them with *fake traffic*. The main motive is for *server* or network to be unable to accommodate this traffic, causing your website/service to be *down* and inoperable.

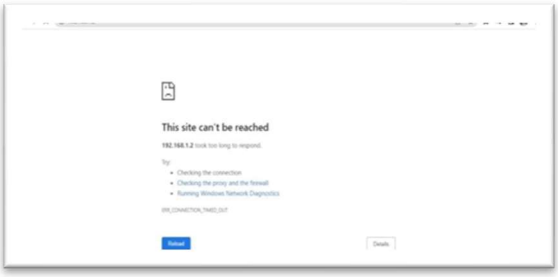

Figure 15. Results of blocking webserver

Fig. 15 above shows that the results when the website server service is when the *attacker* has attempted a DDOS attack, the server automatically blocks IP and website access services with a predetermined time so that the *attacker* can no longer access services from the server.

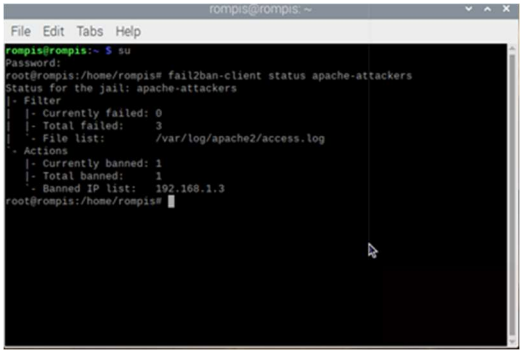

Figure 16. Logging Blocking

Fig. 16 shows the results of blocking ip and port logging on the server that attacker when carrying out a DDOS attack by flooding the website with *fake traffic* so that server performance decreases in serving other clients. So, in this study the server blocked automatically on the attacker. To see the results of blocking on the server do the following command:

Fail2ban-client status apache-attackers

D. Discussion

From the results of research that has been done on the research system "Overcoming Network Security on Host-Based Intrusion Detection System (HIDS) with the method This IP and PORT Blocking can be explained that with the IP and port blocking method the server performance is more efficient in serving each client so that it can minimize the existence of a DDOS attack or software-based attack that occurs in the general public in the form of (browser, file, video or image). The advantages of the system that has been created are:

1. Can filter every ip and port that is trying to do DDOS attacks or software-based attacks.
2. Giving access rights to website services effectively due to the maximum limit in logging in or accessing website.
3. Raspberry pi 4b server is able to become a server with fairly good performance with specifications that are smaller than the server computer.

IV. CONCLUSION

The discussion in the closing is an explanation of the conclusions of this study are as follows:

1. Implementation of fail2ban on the server in detecting and overcoming an attack that occurs in an intrusion on an Intranet network is carried out effectively.
2. IP and PORT blocking on the server can be done automatically with rules that have been determined by the server and provide a maximum time limit in providing website services to clients when conducting attack experiments. To minimize the occurrence of DDOS attacks or software-based attacks.
3. The quality of IP and PORT blocking systems with attacks on servers based on DDOS (Distributed Denial of Service) can make the server performance regularly in providing access services to clients. So that the server is more effective in its performance process.
4. For further research, it is hoped that the authors can use network security with a wider scope such as MAN and WAN. As well as with this research being able to become a basic reference for further research.

REFERENCES

[1] P. P. Putra, "Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort," *SATIN – Sains dan Teknologi Informasi,* vol. 2, no. 1, pp. 15 - 21, 2016.

[2] M. S. d. A. M. Ropi, "Analisis dan Implementasi Network Security System," *Seminar Nasional Telekomunikasi dan Informatika,* pp. 199 - 204, 2018.

[3] M. H. D. &. S. Z. Harahap, "Implementasi Snort Intrusion Detection System (IDS)," *Informatika : Fakultas Sains dan Teknologi,* vol. 6, no. 3, pp. 14 - 221, 2018.

[4] M. Arman, "Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack," *Jurnal Teknik Informatika dan Sistem Informasi,* vol. 7, no. 1, pp. 56-70, 2020.

[5] Y. W. P. d. Asmunin, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan IP Tables Berbasis Linux," *Jurnal manajemen Informatika,* vol. 7, pp. 21-28, 2017.

[6] B. Triandi, "Sistem Keamanan Jaringan Dalam Mencegah Flooding Data dengan Metode Bloking IP dan Port," *Seminar Nasional Teknologi Informasi dan Multimedia 2015,* pp. 49-54, 2015.

[7] O. K. Sulaiman, "Analisis Sistem Keamanan Jaringan dengan Menggunakan Switch Port Security," *CESS (Journal Of Computer Engineering, System And Science),* vol. Vol.1, pp. 9-14, 2016.

[8] N. d. W. N. A. Dwi Bayu Rendro, "Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus di Smk Negeri 1 Kota Serang)," *Jurnal PROSISKO,* vol. 7, no. 2, pp. 108 - 115, 2020.

[9] Y. Pramitarini, R. H. Y. Perdana, T. Tran, K. Shim, and B. An, "A Hybrid Price Auction-Based Secure Routing Protocol Using Advanced Speed and Cosine Similarity-Based Clustering against Sinkhole Attack in VANETs," Sensors, vol. 22, no. 15, pp. 1–22, 2022.

[10] R. O. d. M. Ryansyah, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen," *Jurnal Sistem dan Teknologi Informasi,* vol. 7, no. 1, pp. 52-59, 2019.

[11] D. d. 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.

[12] R. A. T. Sumardi, "Rancang Bangun Sistem Keamanan Jaringan Dengan Metode Blocking Port Pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali," *Indonesian Jurnal on Networking and Security (IJNS) - ijns.org,* vol. Vol. 2, pp. 16-21, 2013.

[13] A. Josi, "Penerapan Metode Prototiping dalam Pembangunan Website Desa (Studi Kasus Desa Sugihan Kecamatan Rambang)," *Jurnal Teknologi Informasi,* vol. 9, no. 1, pp. 50-57, 2017.

[14] N. T. d. A. Eka, "Analisis DNS Amplification Attack," *JOEICT (Jurnal of Education and Information Communication Technology),* vol. 1, no. 1, pp. 17-22, 2017.

[15] H. A. dkk, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," *JOINTECS (Journal of Information Technology and Computer Science),* vol. 5, no. 1, pp. 17-24, 2020.