Online Version Available at: https://jurnal.ubd.ac.id/index.php/te

JOURNAL OF TECH-E

| 2581-1916 (ONLINE) | 2598-7585 (PRINTED) |

Article

Implementation of Tarpit Firewall for Network Security Optimization with The NIST SP800-86 Method in KP Room

Rahmat Novrianda Dasmen[1], *Ardiansyah*[2], *Timur Dali Purwanto*[3], *Marlindawati*[4]

[1, 2, 3, 4] *Bina darma University, Computer Technique, Palembang, Indonesia*

SUBMISSION TRACK

Recieved: 09, 30, 2024
Final Revision: 01, 07, 2025
Available Online: 02, 03, 2025

KEYWORD

Brute Force, DdoS, Mikrotik, Port Scanning, Snort IDS

CORRESPONDENCE

E-mail:
rahmat_novrianda@binadarma.ac.id
ardi10062@gmail.com
timur.dali.purwanto@binadarma.ac.id
marlindawati@binadarma.ac.id

A B S T R A C T

Network optimization is one of the important aspects that aims to improve the performance, efficiency and reliability of network systems and security on the network, but if the optimization is not carried out effectively it will pose a security threat to the network, one of the real threats is DdoS Attack, DdoS attack is a dangerous attack because this attack can paralyze the network server, Therefore, optimization needs to be carried out in the KP Room in order to avoid the threat of DdoS attacks, so the initial stage of this research will test the network to find out how optimal the network is in the KP room so that optimization is needed. The research method used is NSIT, which includes collection, examination, analysis, and reporting, the results after the research is carried out where, on the network in the kp room after testing at the examination stage and then by identifying the test results, it can be concluded that the network is not optimal enough against DdoS attacks and connection type attacks which, The optimization step taken is to apply a Tarpit firewall on the router. The implementation of Tarpit Firewall successfully overcomes DdoS attacks by slowing down incoming connections and stopping attacks, thereby improving network security from Port Scanning, DDoS, and Brute force attacks.

DOI: 10.31253/te.v8i2.3277

I. INTRODUCTION

KP Room Has a Computer Network that Facilitates Network Services for Practical Work Participants, but on the network the network security is not optimal against threats that can make the network disrupted so that it cannot be accessed, the attack is none other than a DDoS attack, DDoS attacks are the most popular technique and are the weapon of choice for hackers because they have been proven to be a threat on the internet, In recent years, the number of network-based threats including the volume and intensity of DdoS has increased significantly [1].This attack has been around since 1990 [2]. These attacks allow them to access all the resources that their victims have. The perpetrators of these DDoS attacks usually make DDoS part of the crime [3]. As a result, the system is unable to function optimally, thus hindering other users from accessing services from the attacked system [4]. So, to anticipate the abuse of the network by hackers, it is necessary to increase the security of the network [5].

The optimization of the network in the kp room is carried out so that the network can be optimal against attacks that threaten the network, the optimization carried out is by applying a firewall, namely a tarpit firewall found in mikrotik, a service tarpit firewall on a computer system that deliberately slows down incoming connections or a protocol that will block or stop attacks [6]. The optimization carried out on the network makes the network more optimal so that attacks on the network can be minimized and make network connectivity will be safer without fear of the threat of attacks on the network on mikrotik routers, routers are one of the network devices that allow other devices to connect to the internet network, besides that the router can also store the identity of data packet traffic that passes through it along with its movement [7]. Additionally, the researchers will implement an Intrusion Detection System (IDS) within the network. The IDS to be employed is Snort IDS, which runs on Ubuntu. Snort is an open-source, rule-based intrusion prevention and detection system used for passively monitoring network traffic and issuing alerts when threats are detected. The system is logically divided into several components that work together to identify specific attacks [8]. Snort can also generate output in various formats, such as log data that records detection alerts. Once deployed, Snort will actively monitor the network, capturing any incoming attacks. Research conducted by [9] demonstrated the successful implementation of a tarpit firewall as a network security measure at STIA Lancang Kuning Dumai. Building on this research, the present study introduces an innovation by combining the tarpit firewall with Snort IDS. In this system, the IDS serves as an intrusion detection mechanism, while the tarpit firewall ensures network security. This integrated approach aims to provide both detection and prevention capabilities, creating a robust defense mechanism for the network.

II. LITERATURES REVIEW

FIREWALL TARPIT

Firewall tarpit is a firewall action contained in and is a service on a computer system that deliberately slows down incoming connections or a protocol that will block or stop attacks [6].Tarpit Firewall can be used as Network security from connection-based attacks such as Ddos, brute force.

SNORT IDS

Snort is an open-source, rule-driven, network intrusion prevention and detection system that is used to passively monitor network traffic and provide alerts when threats are detected. The system can logically be divided into several components that work together to detect a specific attack. Snort is also able to produce outputs in the required format, such as log data that records detection alerts [8] is IDS Snort log data can be used by network administrators to analyze the performance of network security systems. The data recorded in the log consists of information about attack alerts that have been successfully detected by Snort, such as the type of attack, the time of the attack, the attacker's address and port, and the attacker's target address and port. Snort gives and records the alert according to the rules or rules that have been configured.

DOI: 10.31253/te.v8i2.3277

III. METHODS

The method that will be used by this researcher is the National Institute of Standard and Technology (NSIT) The NIST Forensic Method is a guide that assists forensic experts in collecting, analyzing, and securing digital evidence scientifically, This method is used to describe how to go step by step in detail and systematically, so that it can solve existing problems, The method used aims to maintain the results obtained, so that it can be used as evidence [10].

Figure 1. NSIT Method

Based on figure 1 above, this study uses the NSIT SP800-86 Method, in this method has four stages in the process, namely.

Collection

Collection is the stage of data collection where at this stage the researcher will collect data in the kp room in the form of IP address data on the network, network topology and devices contained in the room, and the results obtained are the ip address on the network 10.10.19.0/24, the devices contained in the room are in the form of microtic routers, hubs and several connected PCs and laptops, the following is the topology in the KP room.

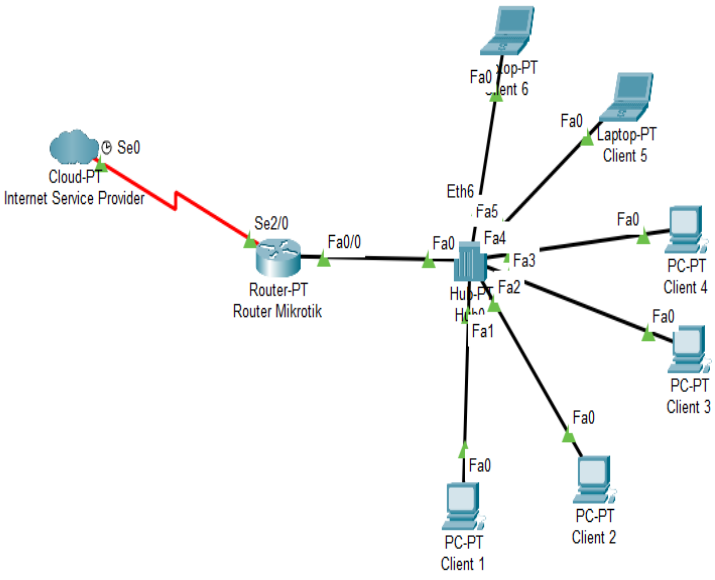

Figure 2. Network Topology

Examination

At this stage, the researcher conducts an investigation of the network before making optimizations, the scheme carried out by the researcher is that the researcher applies an intrusion detection system (IDS) contained in the Snort IDS tool, Snort is a software to detect intruders and analyze packets that cross the computer network in real-time traffic and logging into the database and is able to detect various attacks from outside network [11]. The snort tools are found on the ubuntu operating system, then the researcher conducts an attack test, the attack test carried out is a

DOI: 10.31253/te.v8i2.3277

Port Scanning attack test, Port Scanning aims to scan a certain host port whether it is open. If the port of an application in the computer network is open, then anyone will be able to log in [12]. The scanning process is carried out with Zenmap tools, Zenmap is used to get information gathering in the form of ports and systems used by the target website [13]. DdoS with pentmenu tools found in Kali Linux, Kali Linux open-source operating system (OS), Kali Linux was first released in 2013 by Offensive Security and is a derivative of Debian Linux, a Linux distribution operating system developed with a focus on penetration testing tasks. The times linux was previously known as backtrack [14]. The testing process is carried out using the slowloris technique, Slowloris is a highly targeted attack, allowing one web server to bring down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server as possible. Brute force attacks are one of the most common tactics used by hackers to access unauthorized networks [15]. with the ncrack tools available on Ubuntu. The following is the flowchart from this study.

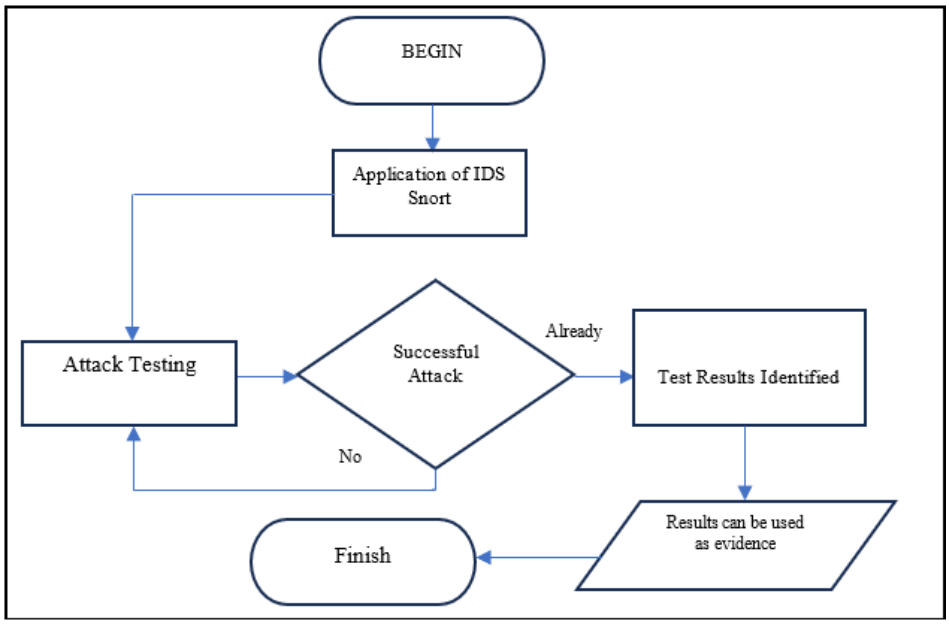

Figure 3. Stages of Examination

Application of IDS Snort

At this stage, the researcher applies Snort IDS on the network, which will be used as an instrument detection system, the researcher installs Snort IDS On the ubuntu server, the following is the process of applying it to the network.

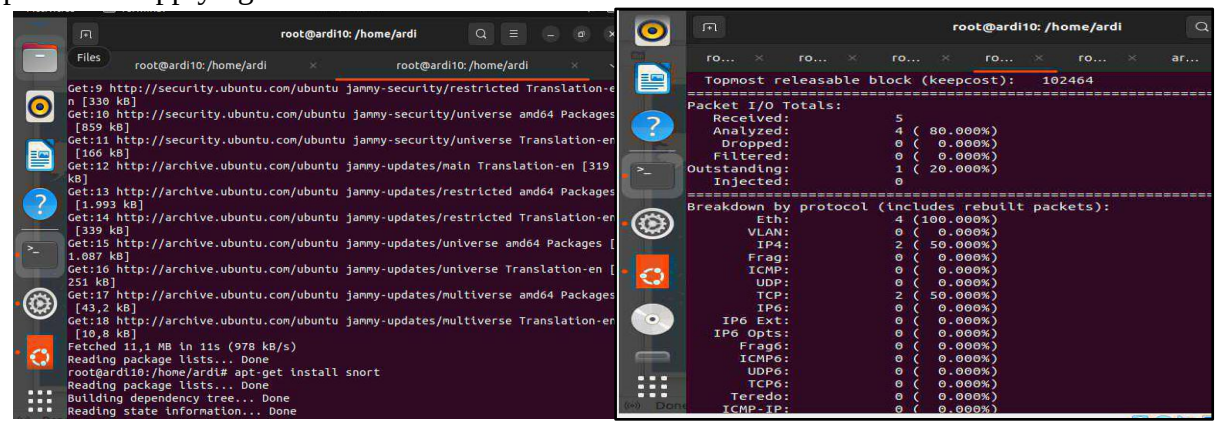

Figure 4. Install and Deploy Snort IDS on The Network

Attack Testing

At this stage, the researcher conducted a Port Scanning test on the network using nmap tools with the destination IP address of 10.10.19.185, following the results of the port scanning test.

DOI: 10.31253/te.v8i2.3277

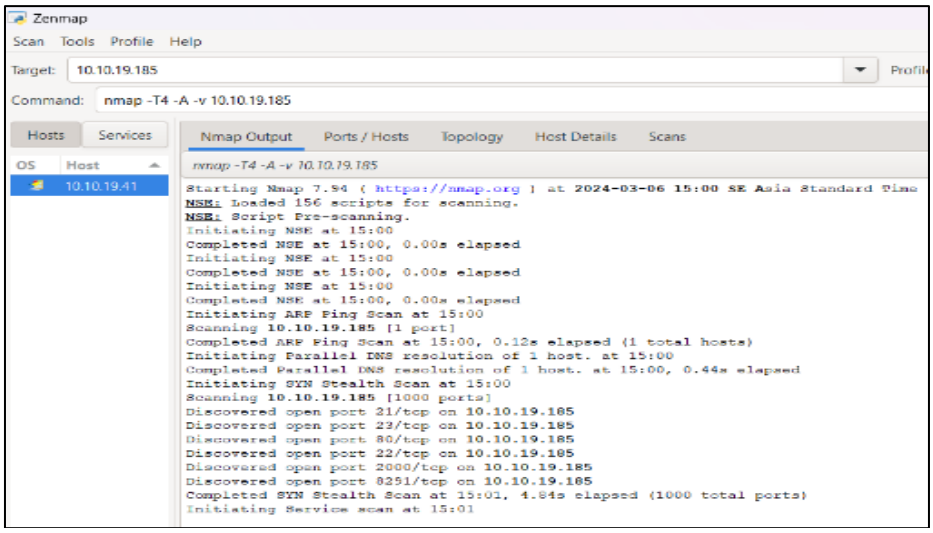

Figure 5. Results of Scanning Open Ports with NMAP Tools

In figure 5 above is the nmap scanning process that is carried out, and with the results of the open ports are 21.22.23 and 80, these open ports are the beginning of an attack if network security is not implemented it will result in a threat to the network. Next, the researcher will carry out attacks, namely Ddos and brute with the aim of IP Address 10.10.19.185 and open ports on the network, namely 21, 22, 23 and 80 along with the test.

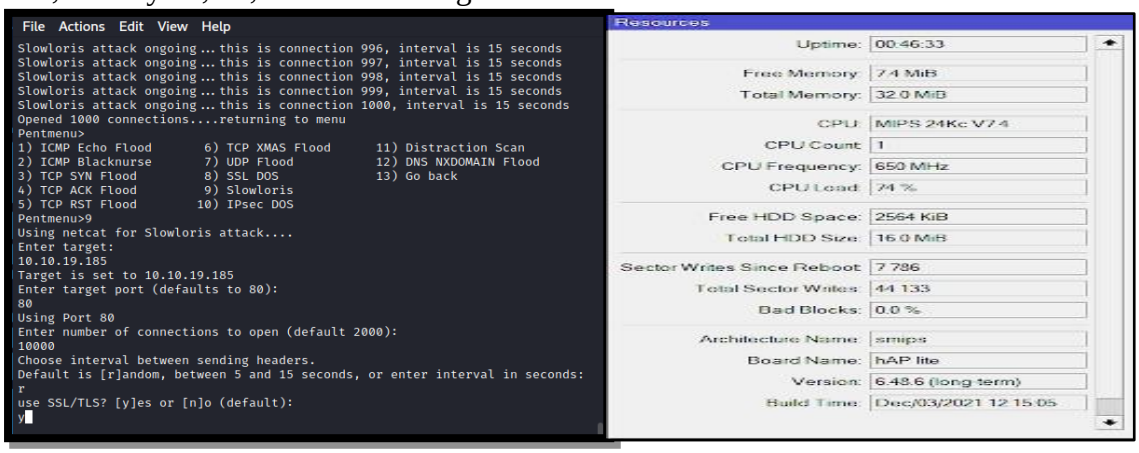

Figure 6. Ddos Attack Detection and Attack Result Display on Winbox

In figure 6 is an attack test carried out using the pentmenu tool on linux with an IP address of 10.10.19.185, successfully carried out with the result of an increase in CPU by 74%, causing the router to become abnormal and inaccessible, this shows that the security on this network is not optimal.

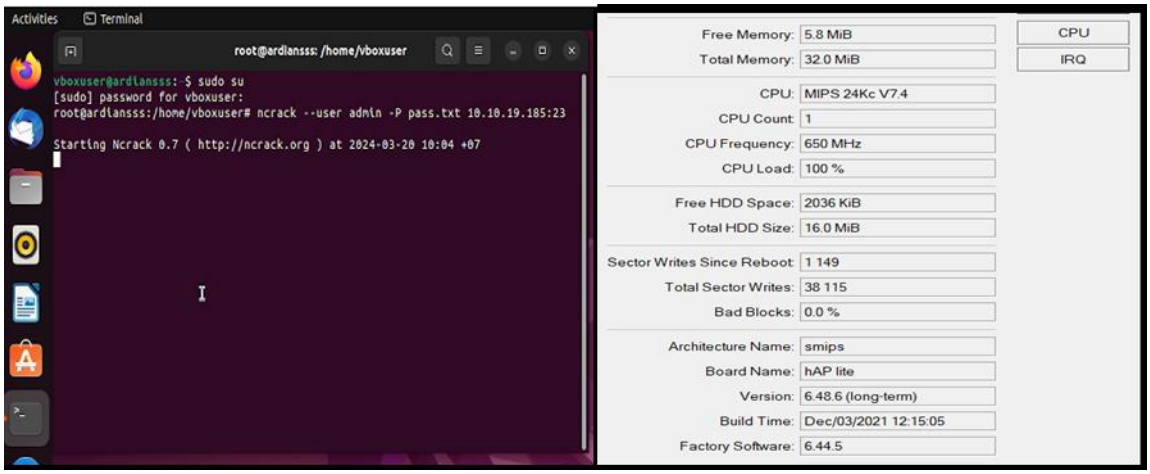

Figure 7. Brute Force Testing and Display of Test Results on Winbox

DOI: 10.31253/te.v8i2.3277

In Figure 7 is the result of a brute force test with ncrack tools on the IP address 10.10.19.185 with Port 24, the results on the CPU have increased to 100% and the router becomes abnormal and the network is inaccessible. Furthermore, the researcher managed to get results on snort ids when applied, namely there were results when attack testing was carried out, here are the results.

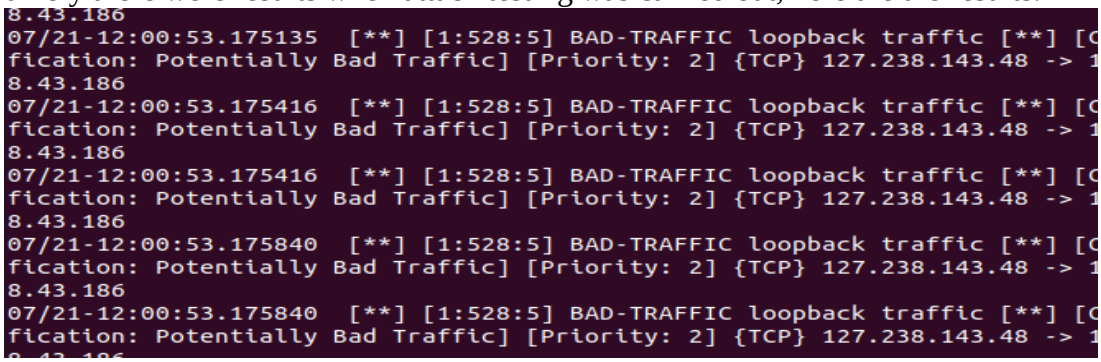

Figure 8. Results of Snort IDS Scanning on The Network

In the image above are the results contained in the snort ids during the real time scanning process and with the results showing the data of the Attacker's IP address, time and attack protocol used, namely TCP, which shows that the network is really vulnerable to attacks so optimization is needed so that the network is safe from attacks.

IV. RESULT

Analysis

At this stage, the researcher analyzed the results obtained in the examination process after testing port scanning with nmap tools, DdoS with pentmenu tools found in linux, and brute force with ncrack tools found in ubuntu. The following are the results of the investigation of the security vulnerability of the Kp Room network in Table 1.

Table 1. Results of Network Security Vulnerability Investigations

NO	Types of Attacks	Testing Tools	Attack Identification Tools	Router Condition	Description
1	Port Scanning	Nmap dan putty	-	-	Successfully found open ports on the network by scanning on nmap tools and successfully testing on putty tools
2	Ddos	Pentmenu	Snort IDS	Abnormal	The test was successful and the attack was successfully identified through the results of the IDS Scanning Snort
3	Brute force	ncrack	Winbox	Abnormal	Successfully conducted the test and the attack was successfully identified via the winbox terminal

Based on table 1, the test carried out is port scanning using nmap tools by scanning on the network successfully found open ports with port details, namely 21, 22, 23, 80. Continued in the second test, namely testing the Ddos attack with the slowloris technique where this attack uses the TCP protocol and the type of slowloris attack is attacking slowly but never stopping which interferes with network traffic, the attack succeeded in making the state of the mikrotic router experience disruption with an increase in Cpu load so that the service is down, the test of the attack was successfully identified using the Snort IDS tool with the results namely there is the attacker's IP address and the protocol used, namely TCP, then the next test, namely the Brute force attack test using ncrack tools was successfully carried out and the test was successfully identified on the winbox when the test took place, the Brute force attack is an attack that tries to make a large number of unauthorized logins with an impact on the network, namely the network will go down.

Reporting

DOI: 10.31253/te.v8i2.3277

At this stage is the final result of the stages that have been carried out, the final stage is to report the test results carried out to the relevant parties, namely reporting that the network is still vulnerable to DDoS attacks and other connection-based attacks such as brute force, where in the analysis results based on attack testing, DDoS attacks are able to disrupt network services by flooding the target with very large network traffic so that The condition of the router is down, therefore the researcher will take steps to take security by Implementing a Firewall to Prevent the attack from recurring by Applying a tarpit firewall found in the microtic. Mikrotik is a software-based operating system (OS) that serves as the basis of a network router and uses a linux-based system. It is ideal for developing small to large-scale computer network administration. The following implementation of the tarpit firewall is shown in the following figure:

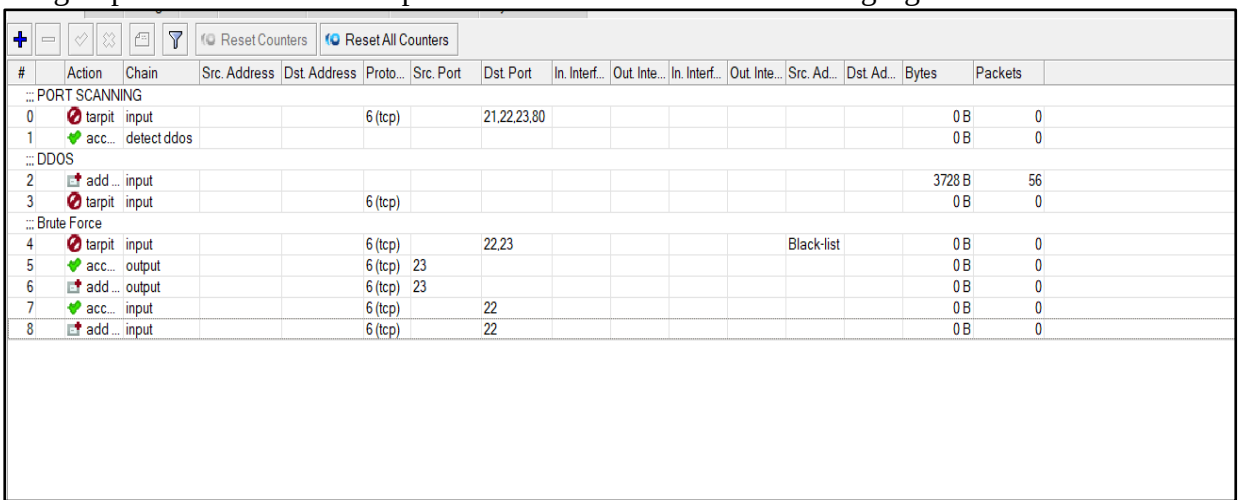

Figure 9. Tarpit Firewall Configuration Results

In Figure 9 is the application of the tarpit firewall found in Mikrotik, and After applying the tarpit firewall, the researcher will conduct an attack test to see the effectiveness of the tarpit firewall that has been applied to the network, followed by the attack test after the tarpit firewall is applied.

Attack Testing After Deploying a Tarpit Firewall

At this stage, the researcher after implementing the firewall will test the attack as before applying the tarpit firewall on the network, along with the experiments carried out including port scanning, Ddos and Brute force experiments.

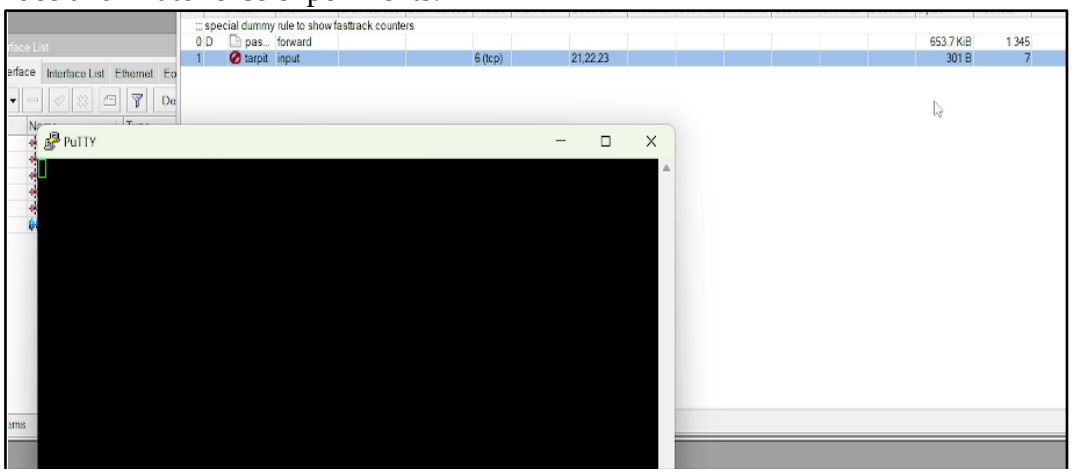

Figure 10. Test Results Using Putty Tools After Applying Tarpit Firewall

Based on figure 10 above, when the researcher will try to re-access the open port using the putty tool but it does not succeed because the firewall has been activated, it can be seen in the amount of incoming packets during the access attempt, this shows that the firewall is very effective. Furthermore, the researcher will test Ddos and Brute Force attacks on networks with tarpit firewalls that have been implemented, following the results of the DdoS and Brute Force tests.

DOI: 10.31253/te.v8i2.3277

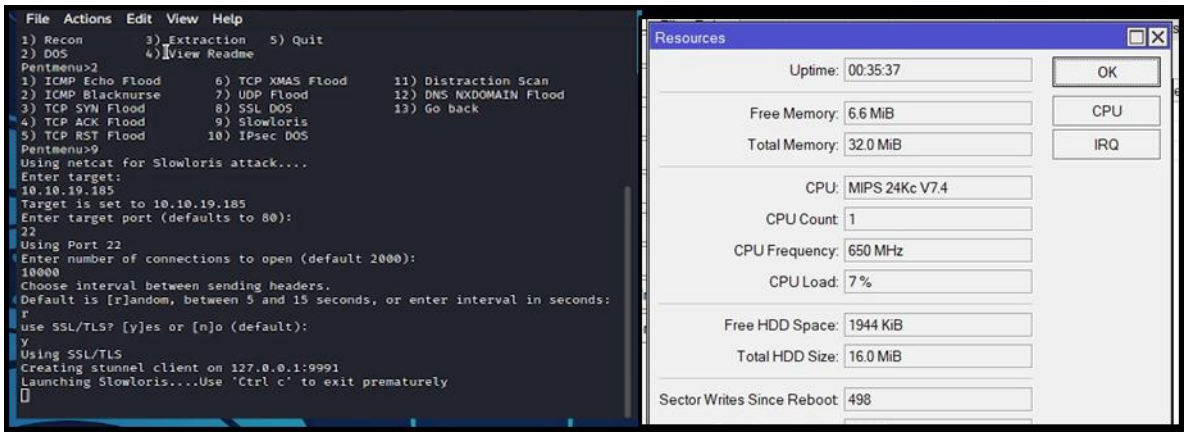

Figure 11. Results of Testing Ddos Attacks with Slowlor Techniques on The Pentmenu Tools After Applying a Tarpit Firewall

In figure 11 above is the result of an attack test carried out after applying a tarpit firewall with a cpu load result of 7% which indicates the condition on the normal cpu and the tarpit firewall successfully blocked the attack.

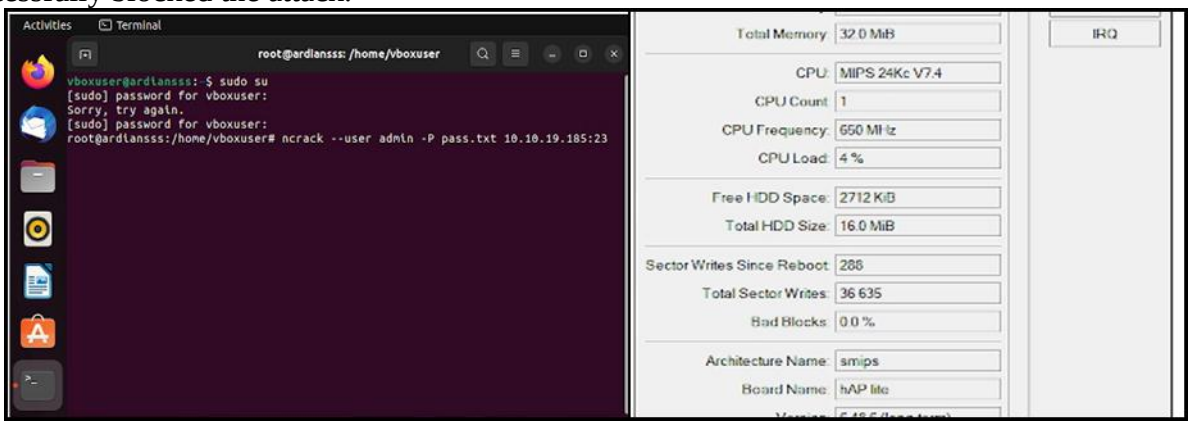

Figure 12. Brute Force Attack Test Results with Ncrack Tools After Applying a Tarpit Firewall

Based on figure 12 above, there are attack test results, namely with a cpu load result of 4% with router conditions at the time of the attack test taking place under normal conditions, this result indicates that the attack test carried out was successfully blocked using a tarpit firewall.

V. DISCUSSION

At this stage, the researcher will collect the results of the implementation of the Firewall tarpit on the network with several attack tests, including port scanning, Ddos and Brute force tests with the indicators seen, namely the cpu load on the router, the condition of the router at the time of testing attacks on the router, the following results can be seen in the table below.

Table 2. Results of Network Security Vulnerability Investigations

NO	Types of Attacks	Tools Used	CPU	Router Condition	Description
1	Port scanning	Nmap dan Putty	Normal	Normal	The testing process was carried out using putty tools with the remote experiment successfully blocked by the tarpit firewall.
2	Ddos	Pentmenu	Normal	Normal	The process of testing the Ddos attack using the pentmenu tool with the slowlor technique was successfully blocked by the tarpit firewall
3	Brute force	Ncrack	Normal	Normal	The process of testing the Brute force attack using ncrack tools was successfully blocked by the Firewall tarpit

DOI: 10.31253/te.v8i2.3277

Based on table 2, the attack test carried out is with the type of port scanning attack using nmap tools and putty tools with a remote test on the open port on the IP Router successfully blocked by the Firewall tarpit with normal router conditions and normal cpu load, then in the Ddos testing process which is carried out using the pentmenu tools with the Ddos slowlor attack technique the test of the attack was successfully blocked using the Firewall tarpit with the results on normal CPU load and during the testing process the conditions on the router with normal results, then in the third attack test, namely the Brute force test using ncrack tools with the type of attack that tries to make many and unauthorized login attempts, the attack test was successfully blocked using the Firewall tarpit with normal Cpu load results and the router condition during the attack test process with normal results.

So with the results that have been obtained after the implementation of the tarpit firewall, with the results of the tarpit firewall has proven to be effective in blocking various types of attacks, including port scanning, Ddos Slowloris, and Brute force login. All attacks were successfully blocked, During the testing process, the router's condition remained normal without any indication of interruption or degradation of performance. This shows that the tarpit firewall is capable of handling attacks without significantly overloading the system. On all attack tests, the CPU load remains normal. This indicates that the use of the tarpit firewall does not place a significant additional load on the CPU, so the system continues to run efficiently. From the overall results, the tarpit firewall showed good performance in mitigating attacks and maintaining the stability and performance of the network system.

VI. CONCLUSION

The application of Snort IDS on Networks shows that this IDS is very effective in detecting attacks on networks, proving that Snort IDS can be used as a reliable tool in detecting network threats in real-time, providing real evidence from attack testing. The Tarpit Firewall was successfully implemented on the Mikrotik Firewall and was effective in optimizing network security, demonstrating that Tarpit can be used as an effective security strategy to protect the network from attacks, specifically in reducing the ability of attackers to continue their attacks.

The advice that researchers can give is for the network so that network security is always improved, considering that in an era where everyone can connect to the internet, it is likely that crimes such as sabotage, data theft and other crimes are very vulnerable, therefore it is very important to have network security, with the security of the Firewall, of course it can create a sense of security and comfort, and it is hoped that in the future there will be more network security additions in addition to IDS (Instrusion Detection System), Firewall tarpit and Port scanning, namely IPS (Intrusion Prevention System) to improve detection on the network and prevent attacks that can endanger network security.

VII. ACKNOWLEDGEMENT

The authors would like to express our gratitude for the support provided by Faculty of Science and technology. The financial assistance from Research, Publication and Community Service Department Buddhi Dharma University is also greatly acknowledged.
(Use acknowledgement if research uses UBD financial assistance)

DOI: 10.31253/te.v8i2.3277

REFERENCES

[1] Y. I. Mahendra and R. E. Putra, "Penerapan Algoritma Gradient Boosted Decision Tree (GBDT) untuk Klasifikasi Serangan DDoS," *JINACS (Journal Informatics Comput. Sci. ISSN*, vol. 06, pp. 158–166, 2024.

[2] M. A. Ridho and M. Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, pp. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.

[3] J. Hansen and T. Sutabri, "Mendesain Cyber Security Untuk Mencegah Serangan DDoS Pada Website Menggunakan Metode Captcha," *Digit. Transform. Technol.*, vol. 3, no. 1, pp. 289–298, 2023.

[4] K. Ruswandi, M. R. Z. Pohan, K. V. Halim, and S. N. Neyman, "Strategi Pencegahan Efektif terhadap Serangan DDoS Slowloris menggunakan Kali Linux dan Linux Mint," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/jtsi.v1i4.2645.

[5] S. P. Putra and Y. Ramdhani, "Memanfaatkan Fitur Firewall Rules Pada Mikrotik Untuk Keamanan Jaringan Di Hotel Lenora Bandung," *eProsiding Tek. Inform.*, vol. 2, no. 1, pp. 122–126, 2021, [Online]. Available: https://eprosiding.ars.ac.id/index.php/pti

[6] R. Aulianita, N. Musyaffa, and R. Martiwi, "PENGGUNAAN METODE IDS DALAM IMPLEMENTASI FIREWALL PADA JARINGAN UNTUK DETEKSI SERANGAN Distributed Denial Of Service (DDoS)," *Jusikom J. Sist. Komput. Musirawas*, vol. 6, no. 2, pp. 94–104, 2021.

[7] M. Nadhir, U. Radiyah, and M. Qomarudin, "Optimalisasi Keamanan Wide Area Network Menggunakan Raw Firewall Mikrotik pada PT. Permata Graha Nusantara," *Inti Nusa Mandiri*, vol. 17, no. 1, pp. 16–23, 2022.

[8] I. A. S. Dewi Paramitha, G. M. A. Sasmita, and I. M. S. Raharja, "Analisis Data Log IDS Snort dengan Algoritma Clustering Fuzzy C-Means," *Maj. Ilm. Teknol. Elektro*, vol. 19, no. 1, p. 95, 2020, doi: 10.24843/mite.2020.v19i01.p14.

[9] M. Suhaidi and Nurhadi, "Implementasi dan Analasis Keamanan Jaringan Pada STIA Lancang Kuning Dumai Menggunakan Port Scanning dan Firewall Tarpit permasalahan serupa dan selanjutnya dijadikan tinjauan pustaka . Adapun jurnal yang satu ke pihak lain buat menghindari terbentuknya p," *Arcitech J. Comput. Sci. Artif. Intell.*, vol. 3, no. 2, pp. 110–123, 2023.

[10] A. Ahmadi, T. Akbar, and H. Mandala Putra, "Perbandingan Hasil Tool Forensik Pada File Image Smartphone Android Menggunakan Metode Nist," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 2, pp. 92–97, 2021, doi: 10.33387/jiko.v4i2.2812.

[11] M. R. Sumar, A. Wahid, and J. M. Parenreng, "Sistem Keamanan Jaringan Terhadap Serangan DOS (Denial Of Service) Menggunakan Snort Dan Firewall Berbasis Linux OS," *Pinisi J. Sciene Techonolgy*, vol. 0, pp. 1–15, 2024.

[12] A. F. D. Suryawan, F. G. D. Putra, V. A. Lovely, and A. Setiawan, "Keamanan IoT dan Sistem Terdistribusi," *J. Internet Softw. Eng.*, vol. 1, no. 3, p. 10, 2024, doi: 10.47134/pjise.v1i3.2619.

[13] D. Cunong, M. Saputra, and W. Puspitasari, "Analysis of Oros Modeler Data Reporting Process to SAP HANA in Activity based Costing for Indonesia Telecommunication Industry," 2019, pp. 246–252. doi: 10.5220/0009908602460252.

[14] N. A. Santoso, M. Ainurohman, and R. D. Kurniawan, "Penerapan Metode Penetration Testing pada Keamanan Jaringan Nirkabel," *J. Responsif*, vol. 4, no. 2, pp. 162–167, 2022.

[15] S. Bahri, "Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 136–147, 2023, doi: 10.60076/indotech.v1i3.239.

DOI: 10.31253/te.v8i2.3277

BIOGRAPHY

Rahmat Novrianda Dasmen is the Director of Innovation and Intellectual Property at Bina Darma University. He also serves as a lecturer at the Faculty of Vocational Studies at Bina Darma University, Palembang, Indonesia, especially in the Computer Engineering Study program. His dedication to innovation and education has led him to become one of the 10 Innovative Lecturer Award Nominees in South Sumatra.

Ardiansyah, is a Computer Engineering student at Bina Darma University, Palembang, Indonesia. With a focus on Networks and Network Infrastructure

Timur Dali Purwanto, Served as the Head of Computer Engineering Study Program at the Faculty of Vocational Studies, Bina Darma University, Palembang, Indonesia. currently he is actively teaching at the Faculty of Vocational Studies, Bina Darma University Palembang.

Marlindawati, He is an active lecturer at Bina Darma University, namely in the Informatics Management Study Program, Faculty of Vocational Studies, Bina Darma University, Palembang, Indonesia.

DOI: 10.31253/te.v8i2.3277