Tarpit Firewall Implementation for Network Security Optimization in the IT Service Division of PT Pusri Palembang Using the NIST SP 800-86 Forensic Method

Ardiansyah[1*]

Abstract

The KP Room of the IT Service Division at PT Pusri Palembang has experienced recurring network disruptions that frequently lead to downtime, adversely impacting the performance of interns and employees. The underlying cause of these disturbances had not been determined, necessitating an investigation using an Intrusion Detection System (IDS) through Snort IDS. This study applies the NIST SP 800-86 forensic method consisting of collection, examination, analysis, and reporting to identify the source of attacks. The collection phase successfully detected indications of Distributed Denial-of-Service (DDoS) attacks. Subsequent examination and attack simulations validated that these vulnerabilities resulted from DDoS activities. To address this issue, a Tarpit Firewall was implemented on the router. The Tarpit Firewall effectively reduced the impact of DDoS attacks by slowing incoming malicious connections and terminating attack attempts, thereby improving the network's resilience against DDoS, brute-force, and port-scanning attacks.

Keywords

Brute force, DDoS, Mikrotik, port scanning, Snort IDS.

Article History

Received 21 April 2025
Accepted 25 June 2025

How to Cite

Ardiansyah. (2025). Tarpit Firewall Implementation for Network Security Optimization in the IT Service Division of PT Pusri Palembang Using the NIST SP 800-86 Forensic Method. ***Jurnal Jaringan Komputer dan Keamanan***, *6*(2), 69-77.

[1*] Universitas Bina Darma, Indonesia, Corresponding email: ardi10062@gmail.com

Introduction

In today's digital landscape, the reliability of network infrastructure has become a fundamental requirement for organizational productivity. Within the IT Service Division of PT Pusri Palembang, the KP Room serves as a critical facility providing internet connectivity and network services for both employees and interns. However, recurring network disruptions and unexpected downtime have hindered operational stability. These disturbances exhibited traffic anomalies and service degradation patterns that align with symptoms commonly associated with Distributed Denial-of-Service (DDoS) attacks. According to Ridho & Arman (2020), DDoS represents one of the most prevalent cybersecurity threats worldwide, increasingly sophisticated in frequency and intensity. Such attacks exploit system vulnerabilities and overwhelm network infrastructure, rendering essential services inaccessible to legitimate users.

The rising complexity of DDoS attacks correlates with broader criminal motives, including extortion, espionage, and sabotage. As described by Hansen et al. (2023), modern DDoS attacks are often executed using botnets and advanced automation tools capable of generating massive artificial traffic streams. When targeted systems—such as routers, servers, or gateways—are forced to process abnormal traffic loads, their resources become exhausted, resulting in service failures. This aligns with observations in the KP Room, where intermittent outages significantly disrupted workflow and temporarily halted access to business-critical applications. The operational impact of such disruptions is consistent with findings by Ruswandi et al. (2024), who emphasize that DDoS attacks severely reduce system availability and reliability.

Given these conditions, strengthening network security in PT Pusri Palembang is essential to mitigate unauthorized access and prevent malicious exploitation. Cybersecurity initiatives must focus on early threat detection, vulnerability mitigation, and rapid incident response. As asserted by Putra & Ramdhani (2021), maintaining robust security measures is crucial for preserving data integrity, confidentiality, and system availability. Against this backdrop, this study aims to identify the root causes of the network disruptions suspected to be DDoS-related, offering evidence-based insights into the nature and sources of the attacks.

To achieve these objectives, the research employed a network forensic approach, which systematically examines digital evidence derived from network traffic. Network forensics—as defined by Surya Kusuma (2023)—involves monitoring, capturing, logging, and analyzing packet flows to identify suspicious patterns, unauthorized access attempts, or malicious payloads. This method allows investigators to reconstruct events leading up to an attack, thereby distinguishing between routine anomalies and actual attack indicators. By integrating forensic techniques with controlled testing, the study ensures objective and accurate findings.

The forensic investigation used Snort Intrusion Detection System (IDS) as the primary monitoring tool. Snort provides real-time traffic analysis and rule-based alerting, making it suitable for detecting attack signatures. Several controlled attack simulations were conducted, including DDoS attacks, brute-force attempts, and port scanning. These attack types were selected because they frequently generate symptoms similar to the network disturbances observed in the KP Room. DDoS simulations were executed using Pentmenu on Kali Linux, while brute-force attacks were performed with Ncrack on Ubuntu. Port scanning was included

to evaluate potential vulnerabilities, as attackers often exploit open ports as initial footholds before launching more severe intrusions.

To mitigate identified vulnerabilities, this study implemented a Tarpit Firewall on the Mikrotik router. Tarpit technology intentionally slows down malicious incoming connections by trapping them in half-open states, preventing attackers from establishing active sessions. According to Aulianita et al. (n.d.), Tarpit is effective for delaying automated attack tools, reducing the attacker's ability to complete reconnaissance or disrupt services. The Mikrotik Tarpit configuration is particularly advantageous in environments like the KP Room, where open ports and unfiltered traffic increase the risk of exploitation. By deploying Tarpit-based protection, the network becomes more resistant to intrusive activities while maintaining stability for legitimate users.

Methodology

This study employed the NIST SP 800-86 forensic method, a widely recognized guideline for collecting, analyzing, and securing digital evidence (Ahmadi et al., n.d.). The method consists of four stages: collection, examination, analysis, and reporting. This structured approach ensures effective identification of network vulnerabilities and supports the formulation of appropriate mitigation strategies.

Collection

The collection phase involved gathering detailed information about the KP Room network, including IP addressing, network topology, and connected devices. The network uses the IP range 10.10.19.0/24 and includes a Mikrotik router, hub, PCs, and laptops

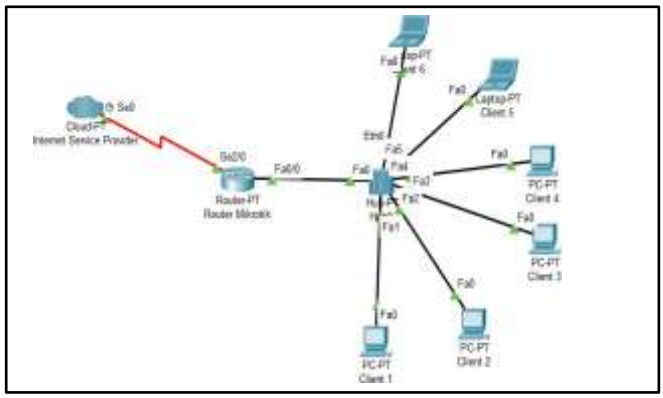

Figure 1. NIST Method Workflow

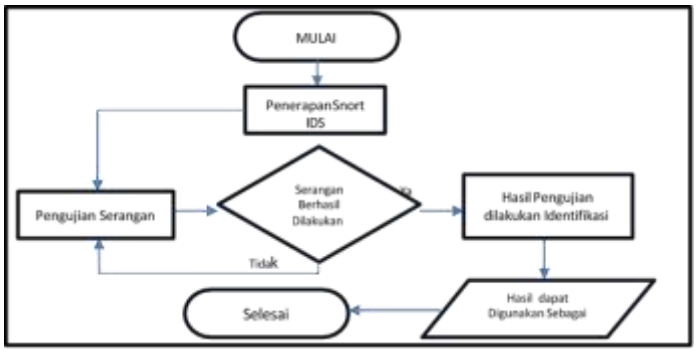

Figure 2. Network Topology

Examination

The examination phase analyzed the network's condition before deploying security enhancements. Snort IDS was installed on an Ubuntu Server to detect intrusion attempts and analyze traffic in real time (Sumar et al., n.d.).

Three attack simulations were conducted:

Port Scanning

Port scanning was conducted using Zenmap/Nmap to identify vulnerable open ports. The scan revealed open ports 21, 22, 23, and 80 on IP 10.10.19.185, indicating potential security risks (Firman et al., 2024; Cunong et al., 2020).

DDoS Attack Simulation

A Slowloris-based DDoS attack was executed using Pentmenu on Kali Linux. Slowloris maintains numerous open HTTP connections to exhaust server resources (IMPLEMENTASI + WAZUH + DASHBOARD + …, n.d.). During the attack, CPU load increased to 74%, rendering the router inaccessible.

Brute-Force Attack Simulation

A brute-force login attack was conducted using Ncrack (Bahri, 2023). The attack caused CPU load to spike to 100%, resulting in network failure and router instability. Snort IDS successfully identified attack signatures, including attacker IP addresses, timestamps, and TCP protocol usage.

Results

Analysis

Network vulnerabilities identified during the examination phase are summarized in Table.

Table 3.1. Network Security Vulnerability Findings

No	Attack Type	Testing Tools	Identification Tools	Router Status	Description
1	Port scanning	Nmap, Putty	–	Normal	Open ports detected: 21, 22, 23, 80
2	DDoS	Pentmenu	Snort IDS	Not normal	CPU overload; attack detected
3	Brute force	Ncrack	Winbox	Not normal	Unauthorized login attempts detected

The port-scanning test successfully revealed open ports that pose a security risk. The Slowloris DDoS attack caused significant CPU load spikes, and Snort IDS detected malicious traffic. The brute-force attack further demonstrated the network's susceptibility to unauthorized access attempts.

Reporting

The reporting phase concluded that the KP Room network was highly vulnerable to DDoS and brute-force attacks due to open ports and inadequate firewall protection. To mitigate these vulnerabilities, the Tarpit Firewall was implemented on the Mikrotik router.

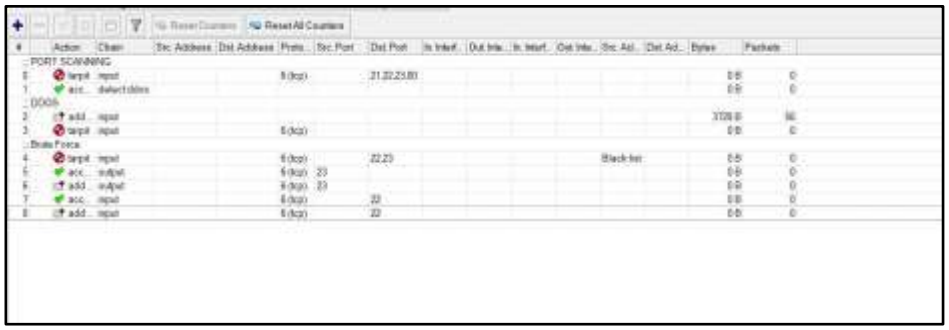

Figure 3. Tarpit Firewall Configuration

Port Scanning After Firewall Implementation

Attempts to remotely access open ports using Putty were blocked by the Tarpit Firewall. Firewall logs confirmed drops in incoming packets.

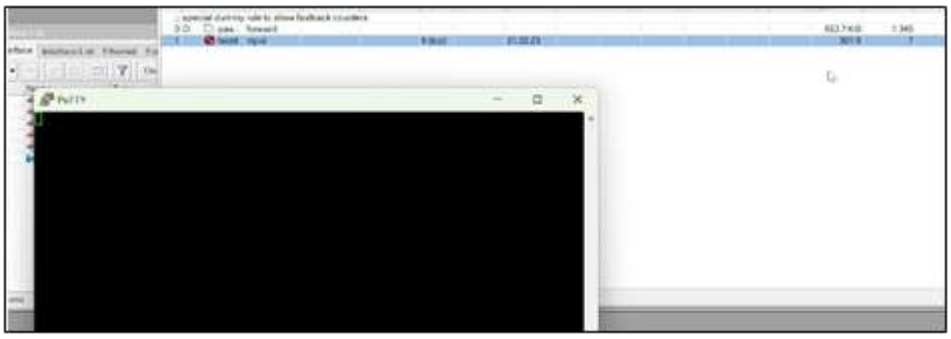

Figure 4. Putty Access Attempts After Tarpit Activation

DDoS Attack After Firewall Implementation

Post-implementation testing showed that the Tarpit Firewall kept CPU load at 7% during DDoS simulations, preventing router crashes.

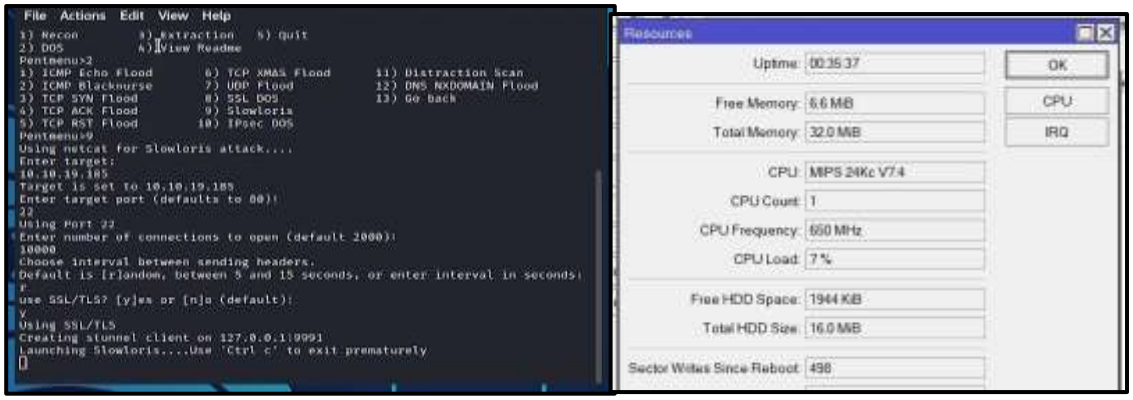

Figure 5. Slowloris DDoS Test After Tarpit

Brute-Force Attack After Firewall Implementation

The Tarpit Firewall successfully blocked brute-force attempts, maintaining CPU load at 4% and normal router operation.

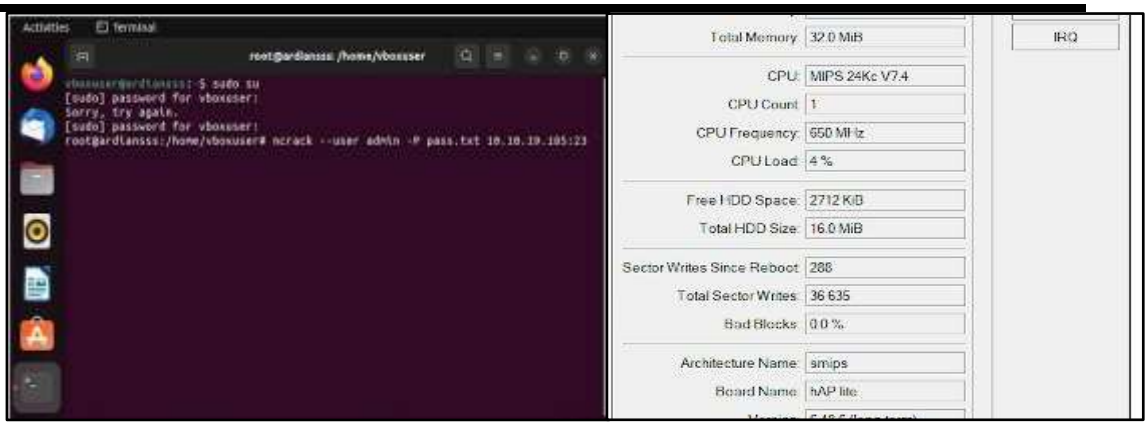

Figure 6. Brute-Force Test After Tarpit Activation

Discussion

The effectiveness of the Tarpit Firewall against simulated attacks is summarized in Table 3.2.

Table 3.2. Effectiveness of Tarpit Firewall Implementation

No	Attack Type	Tools Used	CPU Load	Router Status	Conclusion
1	Port scanning	Nmap, Putty	Normal	Normal	Attack blocked
2	DDoS	Pentmenu	Normal	Normal	Slowloris attack mitigated
3	Brute force	Ncrack	Normal	Normal	Unauthorized login blocked

The Tarpit Firewall consistently maintained CPU load within normal ranges and prevented all attempted attacks. This indicates that the firewall effectively mitigates malicious activities without imposing significant overhead on the network. The results demonstrate that Tarpit technology enhances system resilience, stabilizes router performance, and provides an efficient defense mechanism against connection-based attacks.

Conclusion and Recommendations

Snort IDS demonstrated strong performance in detecting network attacks by identifying attacker IP addresses, protocols used, and timestamps in real time. This confirms its suitability as a reliable intrusion detection tool. The implementation of the Tarpit Firewall on the Mikrotik router effectively optimized network security by blocking port-scanning attempts, DDoS Slowloris attacks, and brute-force login attempts. Furthermore, the Tarpit Firewall reduced the attacker's ability to overburden the system, maintaining low CPU usage throughout testing.

Future improvements should include regular reinforcement of network security measures due to the increasing sophistication of cyberattacks. It is recommended to

complement IDS and Tarpit firewall protection with an Intrusion Prevention System (IPS) to enhance both detection and proactive mitigation of network threats.

Disclosure Statement

The authors declare no conflict of interest related to this study.

Acknowledgments

The authors express their appreciation to PT Pusri Palembang and Universitas Bina Darma for providing support, access, and research facilities throughout the study.

References

Ahmadi, A., Akbar, T., & Putra, H. M. (n.d.). *Comparison of forensic tool results on Android smartphone image files using the NIST method*. https://doi.org/10.33387/jiko

Aulianita, R., Musyaffa, M., & Martiwi, R. (n.d.). *Use of IDS methods in implementing firewalls on networks for detecting Distributed Denial of Service (DDoS) attacks*. *Jusikom: Jurnal Sistem Komputer Musirawas*.

Bahri, S. (2023). Designing network security to prevent brute-force attacks on routers. *INDOTECH: Indonesian Journal of Education and Computer Science, 1*(3).

Cunong, D. N., Saputra, M., & Puspitasari, W. (2020). *Analysis of OROS modeler data reporting to SAP HANA in activity-based costing for the Indonesian telecommunications industry*, 7(1).

Firman, A., Suryawan, D., Graha, F., Putra, D., Lovely, V. A., Setiawan, A., & others. (2024). IoT and distributed system security. *Journal of Internet and Software Engineering, 1*(3), 1–10. https://doi.org/10.47134/pjise.v1i3.2619

Hansen, J., Sutabri, T., & Universitas Bina Darma. (2023). Designing cybersecurity to prevent DDoS attacks on websites using CAPTCHA. *Digital Transformation Technology (Digitech), 3*(1). https://doi.org/10.47709/digitech.v3i1.2764

Putra, S. P., & Ramdhani, Y. (2021). Utilizing Mikrotik firewall rules for network security at Lenora Bandung Hotel. *E-Proceedings of ARS*, 2(1). https://eprosiding.ars.ac.id/index.php/pti

Ridho, M. A., & Arman, M. (2020). Analysis of DDoS attacks using artificial neural networks. *Jurnal Sisfokom (Sistem Informasi dan Komputer), 9*(3), 373–379. https://doi.org/10.32736/sisfokom.v9i3.945

Ruswandi, K., Pohan, M. R. Z., Halim, K. V., & Neyman, S. N. (2024). Effective strategies for preventing Slowloris DDoS attacks using Kali Linux and Linux Mint. *Journal of Technology and System Information, 1*(4). https://doi.org/10.47134/jtsi.v1i4.2645

Santoso, N. A., Ainurohman, M., & Kurniawan, R. D. (2022). Application of penetration testing methods in wireless network security. *Jurnal Responsif, 4*(2), 162–167. https://ejurnal.ars.ac.id/index.php/jti

Sumar, M. R., Wahid, A., & Parenreng, J. M. (n.d.). Network security system against DOS attacks using Snort and Linux-based firewalls. *Creative Commons Attribution 4.0 (CC BY) International License.*

Surya Kusuma, R. (2023). Forensics of Ryuk ransomware attacks on cloud networks. *Jurnal Multinetics, 9*(2).

Biographical Notes

Ardiansyah is a researcher specializing in network security, digital forensics, and intrusion detection at Universitas Bina Darma. His research focuses on cybersecurity optimization, network threat analysis, and forensic investigation.