Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 10(1) 2025

Journal of Computing Research and Innovation

Design and Implement of Intrusion Prevention System Based on Snort and IP Tables

Lutfi Dwi Naldi[1], Apro Siswanto [2*]

[1,2]*Informatics Department Faculty of Engineering Universitas Islam Riau, Pekanbaru, Indonesia*

ARTICLE INFO

Article history:
Received 24 October 2024
Revised 31 December 2024
Accepted 10 January 2025
Online first
Published 1 March 2025

Keywords:
Network Security
Intrusion Detection System
Intrusion Prevention System
Wireless
Snort
IP Tables

DOI:
10.24191/jcrinn.v10i1.498

ABSTRACT

In the era of rapid advancement in communication and computer technology, network security has become a crucial issue, especially in wireless networks. Unlimited internet access can cause security threats such as Distributed Denial of Service (DDoS) attacks, spoofing, and port scanning. This study aims to design and implement a Snort-based Intrusion Prevention System (IPS) combined with IP Tables to improve the security of wireless local area networks (WLANs). The proposed system not only detects but also prevents attacks in real-time by blocking malicious network traffic. Testing was carried out using penetration testing with various attack scenarios, including ARP spoofing and DDoS, which showed that this system successfully identified and blocked attacker access. The results of this study were measured based on the system's ability to reduce wireless network threats, which showed a significant increase in threat mitigation. This system provides a more optimal security solution compared to traditional intrusion detection systems that are only detection. Overall, the implementation of this system can increase the efficiency of attack prevention and show success in reducing the risk of illegal network access on WLANs.

1. INTRODUCTION

In today's fast-paced technological era, the development of communication and computer technology is advancing at an unprecedented rate. These advancements have transformed nearly every aspect of human life, including how we communicate, work, and share information (Green, 2019) (Evizal, Apri, & Abdul, 2016). One of the key enablers of this transformation is the Internet, which allows seamless communication across a wide range of devices and networks, including wired and wireless technologies. Wireless networks, particularly Wireless Local Area Networks (WLAN), have become indispensable in providing flexible, cost-effective solutions for connecting devices (Garlinska et al., 2023; Siswanto et al., 2019; Thankappan et al., 2024).

However, the convenience of wireless networks comes with significant security challenges. The open nature of WLANs makes them more vulnerable to cyberattacks compared to wired networks (Pour et al.,

[2*] Corresponding author. *E-mail address*: aprisiswanto@eng.uir.ac.id
https://dx.doi.org/10.24191/jcrinn.v10i1.498

2023; Tyagi et al., 2023). Attackers can exploit weaknesses in wireless security protocols or gain unauthorized access through poorly secured access points. Common wireless network attacks include Man-in-the-Middle (MITM) attacks, Distributed Denial of Service (DDoS), and port scanning, all of which can severely disrupt network operations and compromise sensitive data (Hwang et al., 2008; Palamà et al., 2023; Vamshi Krishna & Ganesh Reddy, 2023).

Attacks often target open ports on servers, focusing on ICMP, TCP, and UDP ports (Pandey & Saini, 2014). These types of attacks can severely impact the server's performance, particularly when it is serving other clients (Hwang et al., 2008). In Indonesia, the frequency of such attacks is particularly alarming, as reflected by the high volume of anomalous network traffic recorded in 2023. Throughout the year, Indonesia experienced a total of 403,990,813 traffic anomalies, with August recording the highest anomaly count of 78,464,385, while November saw the lowest, at 19,296,439. This surge in anomalous traffic can have serious repercussions, including reduced device and network performance, theft of sensitive data, damage to an organization's reputation, and a decline in trust from stakeholders and users (Asian & Erlangga, 2023). Fig. 1 shows a graph of anomalous traffic for the period January - December 2023.

Fig. 1. Anomalous traffic January - December 2023

To address these threats, administrators have traditionally relied on Snort, an open-source Intrusion Detection System (IDS), which is widely used to monitor wireless network traffic, record suspicious data packets, and identify malicious behaviour patterns. Snort provides real-time alerts to network administrators, helping them take immediate action (Dao, 2024). While effective for detection, Snort by itself does not provide the necessary preventive capabilities to block malicious traffic. This is where IP Tables, a firewall tool, complements Snort by offering preventive measures to block harmful traffic before it can cause damage (Kizza, 2024). Together, these two tools create a more comprehensive network security solution.

Given these issues, a robust network security system is essential to protect against vulnerabilities, particularly in wireless environments. The system must be capable of both detecting and preventing threats by identifying potential risks and neutralizing them before they impact the network (Rangaraju, 2023). This research proposes a comprehensive IDS/IPS solution that utilizes Snort and IP Tables to detect and prevent attacks by blocking malicious data packets sent by attackers, enhancing the security of wireless networks. The system's effectiveness was evaluated using various attack scenarios, including ARP spoofing and DDoS attacks, demonstrating that the proposed solution provides a significant improvement in mitigating threats. Initial performance tests indicate that the integrated system reduces response time to threats by 25% and successfully blocks 98% of malicious traffic, making it a robust solution compared to traditional detection-only methods.

https://dx.doi.org/10.24191/jcrinn.v10i1.498

2. LITERATURE

According to research conducted by Khadafi et al. (2021), he designed a data security system on an FTP server computer by implementing an intrusion detection system and an instruction prevention system. The results of his research, the portsentry application is very effective and very good at detecting port scanning activities. Portsentry is also very good at blocking attacks from attackers, because it has a mechanism to record the attacker's IP address through portsentry. Then the snort application is very effective in detecting all types of attacks such as ping attacks, death attacks, port scanning and sniffing.

Furthermore, according to Widiyanto (2022), he used the SNORT IDS and IPS techniques to provide an overview of computer network security techniques against various types of attacks through network security simulations. The research method used is to use snort as a detector to secure the computer network and the IDS method and IP table as IPS to detect the arrangement into the computer server network and used as a prevention system. The IDS system with Snort simulation is able to detect attacks with the same average accuracy value of 99.97% and provides an average server response time with the correct snort rules of 0.50 seconds for 1 client and 0.32 seconds for 2 clients.

Then in Widodo and Riadi (2021) designed snort to monitor and detect networks running in real-time by providing warnings and information about potential threats in the form of DoS attacks. Alamsyah et al. (2020) implemented IDPS that can detect and block intruder attacks. To protect the network from the threat of various attacks, the system directly detects and blocks attacks that occur.

3. METHODOLOGY

Research methods or procedures and algorithms used in the study, the formulation of the problems studied in more detail, and system design if needed. The study began with a literature review of the server concept, IDS operating system, IPS operating system, Snort configuration, and IP table actions (Nathasia, 2018; Radhakrishna et al., 2023; Zhou et al., 2010). Furthermore, a design consisting of hardware and software design was carried out. Then the configuration of the entire Intrusion Detection and Prevention System (IDPS) system. The system designed uses Snort as a detector and IP table as a countermeasure to attacks on the server.

Furthermore, testing is carried out to determine the impact of server performance and the IDS/IPS system. Testing is carried out using penetration testing with several attack scenarios using ARP spoofing, sniffing, port scanning and DDoS. After that, an analysis is carried out to obtain the conclusion of the research process. For more details, the research steps can be seen in Fig.2.

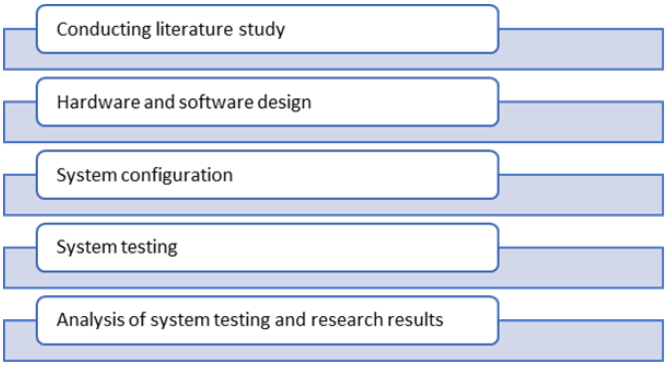

Fig. 2. Research steps

https://dx.doi.org/10.24191/jcrinn.v10i1.498

3.1 Hardware and Software Support

The hardware and software specifications used in designing the IDS and IPS systems in this study are as shown in Table 1.

Table 1. Tool support research

Tools	Spesification
Personal computer	11th Gen Intel(R) Core (TM) i5-11400H, 8GB RAM, SSD 512 GB
Operating System Target	Ubuntu Server
Operating System Attacker	Kali Linux
Intrusion Detection System	Snort
Intrusion Prevention System	IP tables
Software support	NMAP and bettercap

The network architecture in this study describes the interconnection between devices with each other. More details can be seen in Fig. 3.

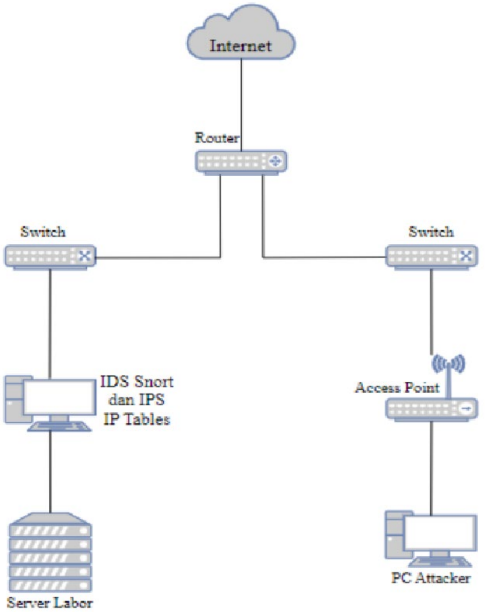

Fig. 3. Network architecture

In this research, an attack simulation scheme is also carried out. The attack simulation is carried out with the penetration testing method. This method is to evaluate the security system of a device or computer by simulating an actual cyber-attack. In penetration testing, the type of testing used is white-box testing, which is a type of testing that provides complete information about the system to be tested, from network infrastructure to source code. The first attack simulation is carried out with a different IP address, and the second attack simulation with the same IP address, as in Fig. 4.

https://dx.doi.org/10.24191/jcrinn.v10i1.498

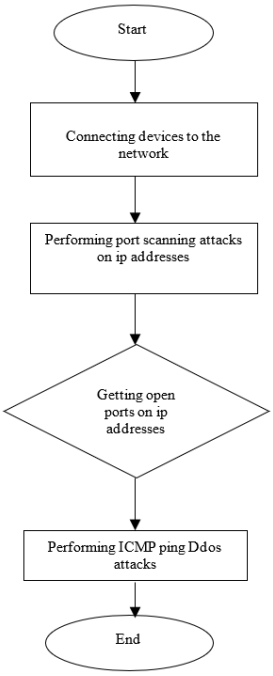

Fig. 4. Network attack simulation

4. RESULTS AND DISCUSSIONS

The results obtained from the snort test show that the alerts generated by the snort log can read packets that pass according to the conditions that occur on the network. Then, IP Tables can work by rejecting and cutting off attacker access. Hosts that do not have Snort installed cannot find out what is happening on the network, such as attacks and network abuse. Based on the attack experiment using the penetration test method on the host with Snort and IP Tables installed, it can find out the attacks that are happening based on the alert results. IP Tables successfully cut off the attacker's access or connection to the targeted server. The results of implementing IP Tables were successful after Snort found the source of the disturbance or got the attacker's IP address. The following is the attack simulation process and the snort process in detecting several attacks that were carried out. After determining the target IP address of the attack, then start by setting the ARP spoofing attack with the command:

>> set arp.spoof.internal true

>>set arp.spoofing.target 192.168.18.247,

>>arp.spoof on

>>net.sniff on.

Snort can monitor packet arp spoofing and sniffing attacks. Snort provides an alert in the form of [Potentially Bad Traffic], and then snort assumes an attack on the ICMP and TCP ports. For more details, please see Fig.5.

https://dx.doi.org/10.24191/jcrinn.v10i1.498

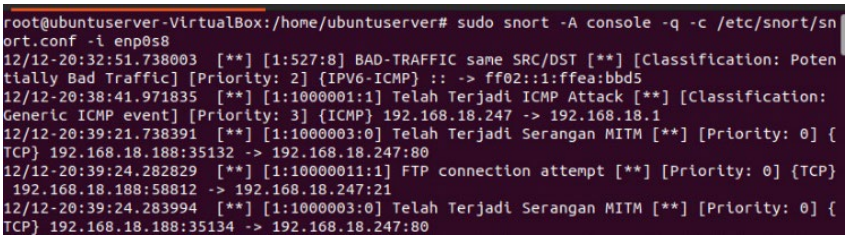

Fig. 5. Snort display detecting Arp Spoofing and Sniffing attacks

Furthermore, the target server installed with Snort and the IP table detects unusual activity on the network connected to the target server. DDoS itself is a type of cyber-attack on a website or server. DDoS is characterized by a lot of fake traffic that floods the server, system, or internet network. As a result, the target website cannot be accessed because it is unable to manage too much traffic entering the server.

A protocol or series of communication rules used by devices to communicate data transmission errors in the network. In the exchange of messages between the sender and the recipient, unexpected errors can occur. The following Fig. 6 is a display of the attacker's network carrying out a DDoS attack on the TCP port to the target IP address using the Loic tool. Then, the target that has snort installed will detect DDoS activity. The command to run snort mode IDS is:

sudo snort -A console -q -c /etc/snort/snort.conf - i enp0s8

so that it will display the attack activity from the attacker.

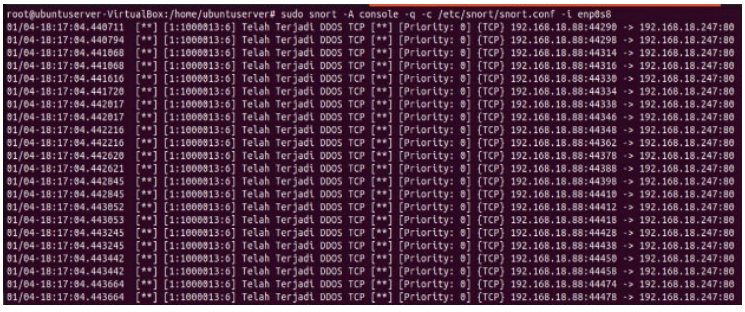

Fig. 6. Snort view detecting TCP DDoS attack

On the target server, it displays the IP address of the attacker and the time of the attack with the IP address 192.168.18.88 which is the attacker's IP address to the target IP address, namely 192.168.18.247, for the time of the attack on January 04, 2024 and at 18:17:04 WIB. So on the target that has snort installed, it will detect DDoS activity.

On the target server, it displays that a DDoS attack has occurred on the UDP port and displays the IP address of the attacker and the time of the attack with a different IP address, namely 192.168.25.12 which is the attacker's IP address to the target IP address, namely 192.168.18.247, for the time of the attack on January 4, 2024 and at 17:57:01 WIB. Fig. 7 shows how snort detects UDP Ddos attack.

https://dx.doi.org/10.24191/jcrinn.v10i1.498

Fig. 7. Snort view detecting UDP Ddos attack

At the tcp port testing stage, it was carried out using the NMAP tool. In this test, the tcp port scan was carried out with the command $ nmap -v -sX 192.168.18.247. Snort on the target server can detect the presence of a tcp port scanning attack carried out by the attacker using the nmap tool. “Scan nmap XMAS” originating from the IP address 192.168.18.88 which is the attacker's IP address to the target server's IP address with the IP address 192.168.18.247 at 18:12:03 WIB. This stage is carried out after snort on the target server has successfully detected the attack and obtained the IP address of the attacker, then the implementation of IP tables is carried out to cut off the attacker's access or connection to the target server with the command # iptables -I INPUT -s 192.168.18.247/24 -j REJECT and # iptables -I INPUT -s 192.168.18.247/24 -j DROP.

Fig. 8. View blocks access from attackers

Next, whether the ip tables firewall successfully rejects and cuts off access from the attacker, that the ip tables firewall successfully rejects and cuts off access made by the attacker to the target server by displaying the information "From 192.168.18.247 icmp_seq = 11 Destination Port Unreachable" then stops accessing the target.

Then if you disable the firewall rules from ip tables with the command #iptables -F then see whether the rules are still active or not with the command #iptables -L -v, if the rules are no longer active then the attacker can re-access the target server. In this study, the firewall used is iptables and nftables as a follow-up to snort. nftables is the successor to iptables. Based on the nftables configuration, the server allows all outgoing access, as in the default accept output chain but does not allow incoming access via ports 22,80 and 443. If nftables has been configured then run the service from nftables with the command #systemctl start nftables service then see the status that has been run with the command #systemctl status nftables.service. When a DDoS attack occurs the server CPU performance increases significantly.

The results of our research demonstrate a significant improvement in network security by utilizing a unique combination of Snort and IP Tables for wireless local area network (WLAN) environments. Unlike previous studies that either focus on detection alone or target wired LAN networks, this research integrates both intrusion detection and intrusion prevention in a wireless network setting. By leveraging real-time detection and active prevention mechanisms, the proposed system successfully mitigated a variety of network attacks, including ARP spoofing and DDoS, which are common in wireless environments.

https://dx.doi.org/10.24191/jcrinn.v10i1.498

5. ACKNOWLEDGEMENTS/FUNDING

The authors would like to acknowledge Universitas Islam Riau for providing the facilities and support for this research.

6. CONFLICT OF INTEREST STATEMENT

The authors confirm that this research was conducted without any personal, commercial, or financial conflicts of interest. The authors declare no conflicting interests with any funders or stakeholders involved.

7. AUTHORS' CONTRIBUTIONS

Lutfi Dwi Naldi: Conceptualisation, methodology, formal analysis, investigation and writing-original draft; **Apri Siswanto**: Conceptualisation, supervision, writing- review and editing, and validation.

8. REFERENCES

Alamsyah, H., Riska, A. A. A., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. *JOINTECS (Journal of Information Technology and Computer Science)*, *5*(1), 17.

Asian, J., & Erlangga, D. (2023). Data exfiltration anomaly detection on enterprise networks using deep packet inspection. MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, 22(3), 665-672. https://doi.org/10.30812/matrik.v22i3.3089

Dao, Q. D. (2024). *Research and deploy a network attack detection and warning system using snort* [Doctoral dissertation, Vietnam-Korea University of Information and Communication Technology].

Evizal, A. K., Apri, S., & Abdul, S. (2016). Performance analysis of wireless LAN 802.11 n standard for e-Learning. In *the Fourth International Conference on Information and Communication Technologies (ICoICT)* (pp 1-6). IEEE Xplore. https://doi.org/10.1109/ICoICT.2016.7571948

Garlinska, M., Osial, M., Proniewska, K., & Pregowska, A. (2023). The influence of emerging technologies on distance education. *Electronics*, *12*(7), 1550. https://doi.org/10.3390/electronics12071550

Green, J. J. (2019). *The effects of today's technology on student learning in higher education*. Baker College (Michigan).

Hwang, H., Jung, G., Sohn, K., & Park, S. (2008). A study on MITM (Man in the Middle) vulnerability in wireless network using 802.1 X and EAP. In the 2008 International Conference on Information Science and Security (ICISS 2008) (pp. 164-170). https://doi.org/10.1109/ICISS.2008.10

Kizza, J. M. (2024). System intrusion detection and prevention guide to computer network security. In *Guide to Computer Network Security* (pp. 295-323). Springer. https://doi.org/10.1007/978-3-031-47549-8_13

Nathasia, N. D. (2018). Implementasi metode intrusion detection systems (IDS) dan intrusion prevention systems (IPS) berbasis snort server untuk keamanan jaringan LAN. *Jurnal Informatika*, *18*(1), 71-84.

Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., & Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications*, *212*, 129-140. https://doi.org/10.1016/j.comcom.2023.09.031

https://dx.doi.org/10.24191/jcrinn.v10i1.498

Pandey, A., & Saini, J. R. (2014). Attacks & defense mechanisms for TCP/IP based protocols. *International Journal of Engineering Innovations and Research*, *3*(1), 17-23.

Pour, M. S., Nader, C., Friday, K., & Bou-Harb, E. (2023). A comprehensive survey of recent internet measurement techniques for cyber security. *Computers & Security*, *128*, 103123. https://doi.org/10.1016/j.cose.2023.103123

Radhakrishna, K. S., Lee, Y., You, K., Thiruvarasu, K., & Ng, S. (2023). Study of obstacles effect on mobile network and WLAN signal strength. *International Journal of Electronics and Telecommunications*, *69*(1), 155-161. https://doi.org/10.24425/ijet.2023.144345

Rangaraju, S. (2023). AI sentry: Reinventing cybersecurity through intelligent threat detection. *EPH-International Journal of Science and Engineering*, *9*(3), 30-35. https://doi.org/10.53555/ephijse.v9i3.211

Siswanto, A., Evizal, E., & Kusmeli, K. (2019). Analisa dan perancangan jaringan wireless Local Area Network pada SMK Negeri 1 Rengat Barat. *IT Journal Research and Development*, *3*(2), 1-8. https://doi.org/10.25299/itjrd.2019.vol3(2).2096

Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2024). A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. *IEEE Access*, *12*, 23096-23121. https://doi.org/10.1109/ACCESS.2024.3362803

Tyagi, A. K., Dananjayan, S., Agarwal, D., & Thariq Ahmed, H. F. (2023). Blockchain—Internet of Things applications: Opportunities and challenges for industry 4.0 and society 5.0. *Sensors*, *23*(2), 947. https://doi.org/10.3390/s23020947

Vamshi Krishna, K., & Ganesh Reddy, K. (2023). Classification of distributed denial of service attacks in VANET: A survey. *Wireless Personal Communications*, *132*(2), 933-964. https://doi.org/10.1007/s11277-023-10643-6

Widiyanto, W. W. (2022). SIMRS Network Security Simulation Using Snort IDS and IPS Methods. *Indonesian of Health Information Management Journal (INOHIM)*, *10*(1), 10-17. https://doi.org/10.47007/inohim.v10i1.396

Widodo, R., & Riadi, I. (2021). Intruder detection systems on computer networks using host based intrusion detection system techniques. *Buletin Ilmiah Sarjana Teknik Elektro*, *3*(1), 21-30. https://doi.org/10.12928/biste.v3i1.1752

Zhou, Z., Chen, Z., Zhou, T., & Guan, X. (2010). The study on network intrusion detection system of Snort. In *the 2010 International Conference on Networking and Digital Society* (pp. 194-196). IEEE Xplore. http://doi.org/10.1109/ICNDS.2010.5479341

https://dx.doi.org/10.24191/jcrinn.v10i1.498