JURNAL TEKNOLOGI REKAYASA INFORMASI DAN KOMPUTER
E-ISSN: 2797-1724, DOI: 10.30811/jtrik.v8i2.7460
Vol. 8 No. 2 September 2025 pp. 22-29

Network Security Analysis Using Snort With Intrusion Detection System (IDS) Method For Computer Network Security Optimization

Muhammad Rizki Afrizal[1], Amri[2*], Jamilah[3]

[1,2,3] Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

Coresponding Author : amri@pnl.ac.id

Article info: Received 01/07/2025, Revised 10/07/2025, Accepted 07/August/ 2025

Abstract

Information technology, particularly computer networks, enables the rapid and complex exchange of information. Proper network management is necessary to maximize the utilization of this information. However, the more extensive the network, the more difficult it is to manage. Threats to network security, such as attacks by hackers and crackers, are increasingly widespread. These attacks can disrupt normal operations and steal critical information. In response to these threats, security systems such as the Snort IDS have been developed. Snort functions to detect and prevent attacks, as well as monitor network traffic for suspicious activity. This study aims to determine the success rate of an Intrusion Detection System (IDS) in securing computer networks against various types of attacks, whether single or multiple attacks are simultaneously executed. The study used an IDS method installed on a server to monitor network traffic. Snort's success in detecting a single attack was 100%, and its success in detecting two attacks simultaneously was 100% if there were no more than two types of attacks. Based on the results of the analysis, Snort can be implemented as an intrusion detection system on the Ubuntu 22.4 Linux operating system to detect attacks in the form of port scanning, DOS, DDOS, and brute force by capturing the attacker's IP address, which produces a response and impact on the computer's CPU that exceeds capacity.

Keywords: hacker, computer, IDS, snort, server

1. Introduction

The development of information technology, particularly computer networks, enables the rapid and increasingly complex exchange of information. Proper computer network management will certainly maximize the utilization of this information. Therefore, computer networks must be managed and monitored to ensure the smooth transmission of information. The more extensive a computer network system, the more difficult it is to manage and monitor.

One reason computer networks are less than optimal is the presence of attacks by intruders, such as hackers and crackers, who seek to benefit or gain from others. Hackers or crackers consistently attempt to gain unauthorized access to a security system, compromising the computer system or network and disrupting normal user activity. Hackers often attack email delivery processes, client-server data access, and data storage on servers. System instructions are compromised when unauthorized individuals attempt to gain access or disrupt the normal operation of an information system.

Threats to network security, such as attackers, intruders, and crackers, are becoming more widespread and increasingly prevalent. With increasing knowledge of hacking and cracking, coupled with the proliferation of tools, attacks and infiltrations have become increasingly easy to execute. To counter the ever-growing number of hackers and crackers, a reliable network security system capable of detecting attacks based on their number and nature is essential.

Many security systems have been developed, including "Network Security Monitoring with Snort IDS Using Network Forensic Methods." The attack monitored in this study was Netcut, which steals internet connections from clients.[1] Despite these efforts, hackers are never satisfied and continue to attempt to disrupt the server network.

Snort is a tool used to detect and prevent network intrusions and attacks. Snort, as used in this study, functions as a detector. In this case, Snort monitors network traffic and looks for signs of suspicious activity or potential attacks. The Snort Intrusion System can also function as an Intrusion Prevention System (IPS), not only detecting attacks but also actively preventing them from occurring. Snort can also be used to detect port scanning attempts, DoS (Denial of Service) attacks, or other network attacks.

A. Intrucsion Detection System (IDS)

An IDS is a system capable of analyzing data in real-time to detect, log, and prevent misuse and attacks. An IDS is a security tool that can be used to counter hacker activity. An IDS can provide warnings to administrators if an attack or misuse occurs on a network. These warnings can even display the IP address of the attacker's system [1].

B. Snort

Snort is an open-source intrusion detection system created by Roesch and first released on December 22, 1998. Snort can analyze network traffic and log packets in real time in three main modes: packet sniffer, packet logger, and network IDS[2]. To perform its functions, Snort has four main components in its architecture. These components are as follows:

- Sniffer : A sniffer is a device that intercepts network traffic. This component's purpose is to sniff, or capture, packets traveling through the network.
- Preprocessor: The main task of this component is to filter or examine captured packets. This component determines the type of captured packet, whether it is an HTTP packet, a port scan packet, or another type of packet.
- Detection Engine: At this stage, the detection engine compares the packet against the predefined rules. If the packet matches the created rules, the packet will be forwarded to the output system to generate an alert.
- Output System: If the packet matches the rules, the output system will issue a warning or alert from the IDS. In addition to generating alerts, Snort also generates text-based logs that are stored in log files in the /var/log/snort directory. Snort IDS logs can be saved in various formats, including tcpdump, csv, and Unified2.

C. Computer Network

Computer networks are an unavoidable necessity. Generally, a computer network is a collection or group of computers interconnected using communication protocols and media to share information, applications, and hardware. Furthermore, a computer network can also be defined as a collection of communication terminals located in various locations, consisting of more than one interconnected computer [3]. Computer networks continue to evolve, both in terms of scalability, number of nodes, and technology used. Therefore, proper network management is necessary to ensure network availability. However, network management presents many challenges, including those related to network security.

Computer network security is a primary concern when building a network infrastructure. Most network architectures utilize routers with built-in firewalls, as well as network software support that facilitates access control, data packet monitoring, and the use of well-managed protocols. Network security can also be controlled by adjusting the network sharing properties on each computer, which allows for restricting the visibility of folders and files to specific users on the network.

D. *LOIC (Low Orbit Ion Cannon)*

LOIC is an application used to attack server computers. LOIC (Low Orbit Ion Cannon) is a tool or application that functions to paralyze a website server by sending as many packets as possible according to the attacker's wishes to the target server computer via the target computer's domain or server IP [4].

E. Brute Force

Brute force is an attack technique or hacker action that forces a web security system by trying to guess usernames and passwords. Hackers use brute force attacks to find hidden code and web page vulnerabilities that can be exploited. Once identified, attackers use that information to infiltrate the system and compromise data. Their ultimate goal is to cause denial-of-service attacks on web pages and extract data from the system to be directed to third parties. [5]

F. Nmap (Network Mapper)

Nmap is an open-source tool for network exploration and security auditing. Nmap uses raw IP packets to detect hosts connected to a network, their assigned services (application name and version), operating system (and version), the type of firewall/packet filter in use, and several other characteristics.
Nmap's output is a list of target hosts scanned, along with additional information depending on the options used.

Key among these is the "interesting ports table." This table lists port numbers and protocols, service names, and their corresponding statuses. The statuses are open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstruction is blocking the port, preventing Nmap from determining whether it is open or closed.[6]

2. Methods

This design is used to explain the system design description that will be created.

A. Research Stages

The first stage of network analysis involves identifying the problem to be solved, followed by the design requirements for both hardware and software. Next, the topology research stage is carried out. Testing is then carried out on a server with Snort IDS installed, and then attacks are conducted from both the local and public networks. The expected results include detecting port scanning, DOS, DDOS, and brute force attacks. The system design stages are shown in Figure 1 below.

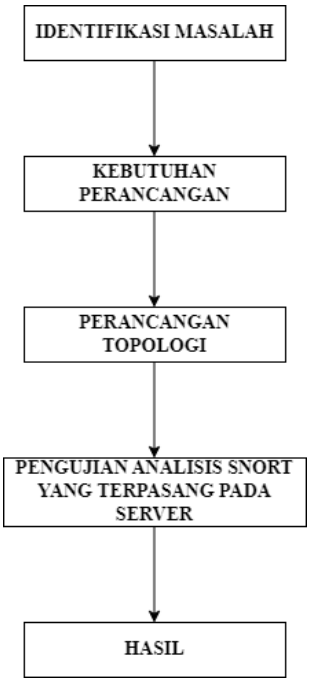

Figure.1 Research Stages

B. *Network Topology*

In this stage, the implementation of the Intrusion Detection System method is discussed, and a system is built with a network topology. The topology of the Intrusion Detection System method is illustrated in Figure 2 below.

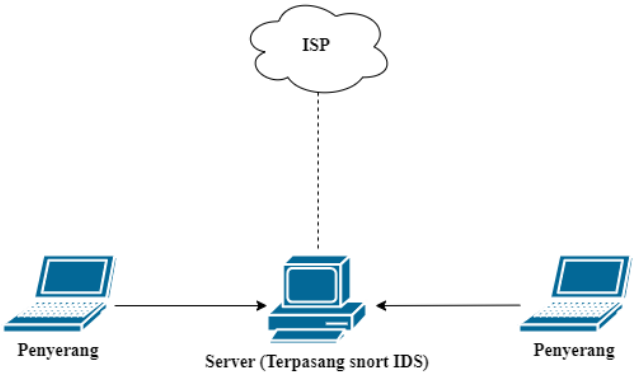

Figure 2. *Snort* IDS Topology

System design is used to explain the overall system design. An IDS method is installed on the server to detect network traffic. Attack testing is then performed on the server with the Snort IDS installed.

C. Experiments

System testing is the stage for evaluating or testing this research. This evaluation aims to determine the effectiveness of Snort as a network threat detection system, as shown below.

- Server Without Snort Installed
  This server does not have Snort installed. This will test the server's ability to detect network attacks. A model of a server without Snort installed is shown in Figure 3 below.

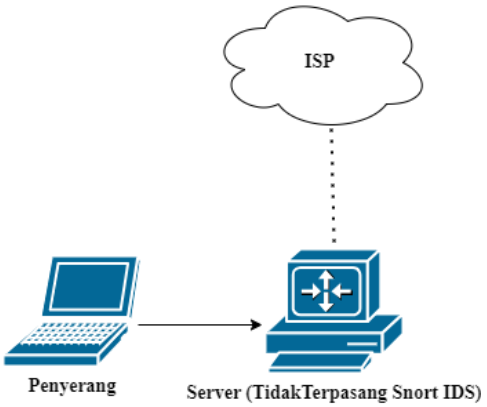

Figure 3. Snort Server Not Installed

- Server With Snort Installed :
  Snort is installed on this server. This test will test the server's ability to detect network attacks. A model of the server with Snort installed is shown in Figure 4 below.

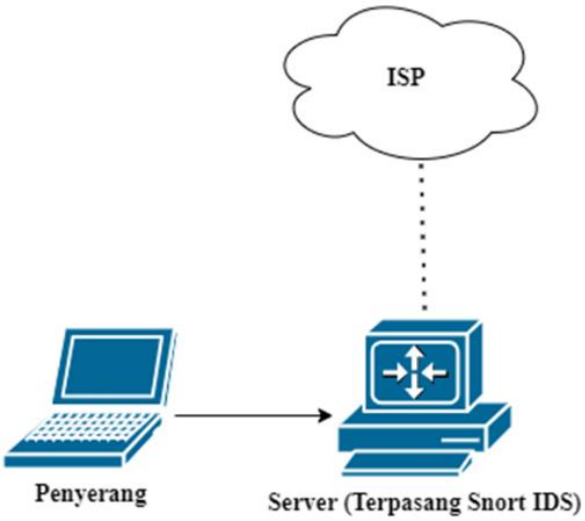

Figure 4. Snort Server Installed

3. Results and Discussion

- Experiment Results

Pengujian yang dilakukan penyerangan serangan terhadap server yang tidak terpasang snort intrucsion detection system. Hasilnya menunjukkan bahwa ketika ada serangan dan aksi-aksi berbahaya, komputer yang tidak terpasang snort tidak dapat melihat traffic lalu lintas jaringan. Hal ini disebabkan traffic dan paket-paket lalu lintas jaringan hanya dapat dilakukan bila sistem sudah terpasang snort.

Mobiledit Forensik Express adalah perangkat lunak forensik digital yang digunakan untuk mengumpulkan, menganalisis, dan mengumpulkan bukti digital dari perangkat seluler.

- Testing On Server Without Snort Installed
  The tests conducted included attacks on servers without the Snort intrusion detection system installed. The results showed that when attacks and malicious actions occurred, computers without Snort were unable to detect

network traffic. This is because network traffic and packets can only be detected if the system has Snort installed.Mobiledit Forensic Express is digital forensics software used to collect, analyze, and gather digital evidence from mobile devices. In this section, an attack was conducted on a server without Snort. It was found that when an attack was carried out, the server was unable to detect attacks or suspicious activity in network traffic because it lacked Snort. Furthermore, this server would not automatically generate detection reports, so malicious activity was not properly detected or tracked. Server security may be more dependent on other security solutions, such as firewalls or other intrusion detection systems that may have been implemented. Without a Snort IDS, this server may not detect certain threats that could compromise network and data security. In the event of an attack, this server may take longer to respond or identify an ongoing attack.

- Testing a Server with Snort Installed
  The following is how Snort installed on the server can detect attacks.
  Snort Display : This displays information about Snort successfully installed on Ubuntu, which is used as a server for detection and security. Furthermore, it generates a message or log/record display that can be generated when detection on the server is successful. A successful Snort installation can be seen in Figure 5 below.

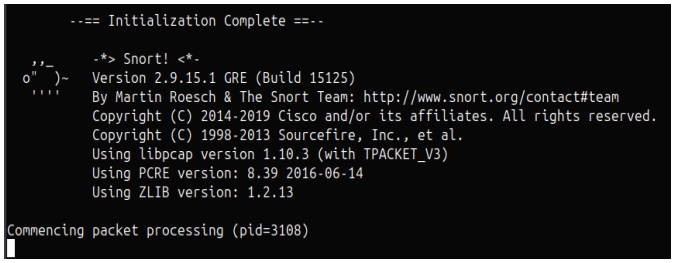

Figure 5. Snort Dasboard

- View data packet storage to log file

  The information displayed in sniffer mode is captured and then entered into a log file as shown in Figure 5 below.

Figure 6. Saving data into log files

- File Log
  After the server detects that data has entered the server, Snort will record it and save it in a log file as shown in Figure 6 below.

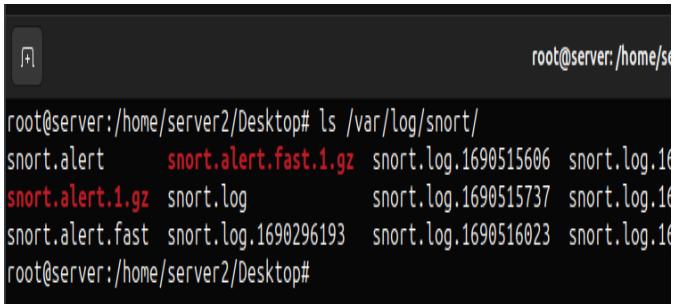

Figure 6. File log

A. Attack View

The attack on the server with Snort installed can be seen as follows.

a) TCP SYN Attack

Pinging is performed from the Attacker to the server to see the server's resistance to TCP SYN attacks as shown in Figure 7 below.

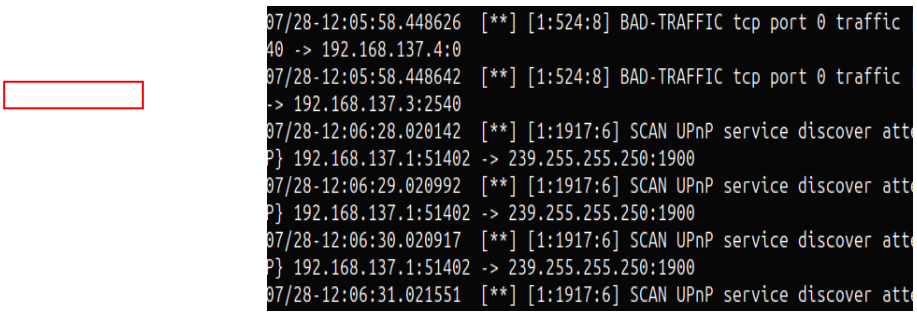

Figure 7. TCP SYN Attack

b) Spoofing attack

IP address disguise is achieved by entering a fake IP address, which prevents the server from recognizing the attacker's actual IP address, as shown in Figure 8 below.

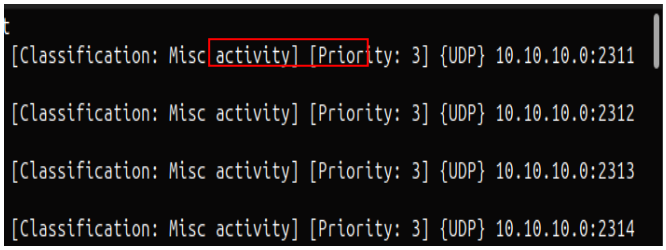

Figure 8. Spoofing attack

c) DDOS Attack Using LOIC

The attack was carried out via the attacker's computer and used the LOIC application with the Transmission Control Protocol (TCP) Flooding method, as shown in Figure 8 below.

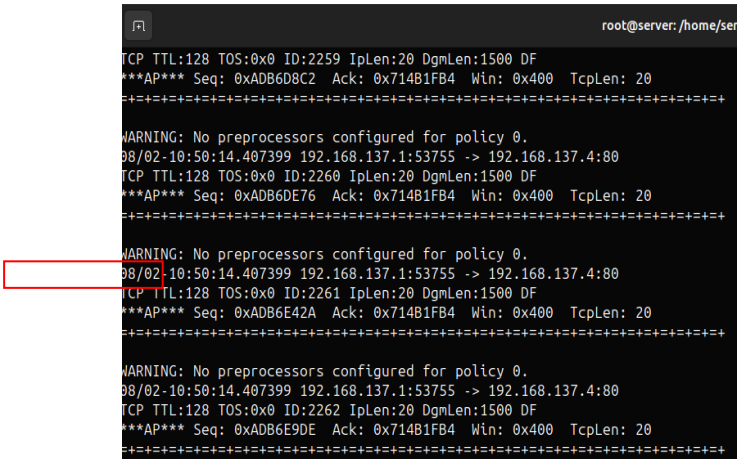

Figure 8. DDOS tipe TCP Attack

d) DDOS Attack

The DDOS attack caused the web server status to be reconnecting/unable to load the web page display because the packets in question were attacked by five computers causing the web server to be down/unable to work as usual as seen in Figure 9 below.

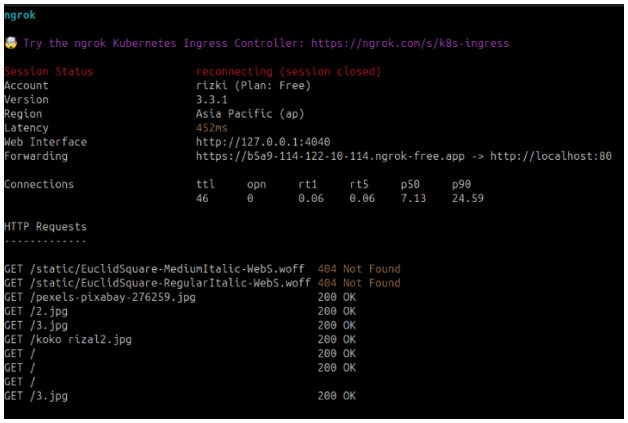

Figure 9. Web server status

e) Brute force attack

Brute force is carried out using the FTP protocol by guessing SSH so that the attacker can access the server as shown in Figure 10 below.

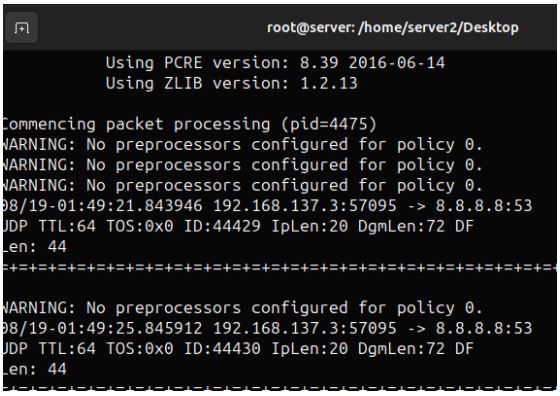

Figure 10. Brute Force Attack

B. Experiment Results

The results of the analysis of the tests carried out on the PC server include testing to activate Snort, along with Snort rules, to detect alerts that can identify when an attacker targets the server. Table 1 show attack test results.

TABLE 1
Attack test results

NO	Attacker IP Address	Target IP Address	Attack	Result
1	192.168.137.3	192.168.137.4	Port Scanning	Terdeteksi
2	192.168.137.1	192.168.137.4	Dos	Terdeteksi
3	192.168.137.1	192.168.137.4	DDOS	Terdeteksi
4	192.168.137.3	192.168.137.4	Brute Force	Terdeteksi
5		https://6f0c-114-122-22-145.ngrok-free.app/	DDOS	Tidak Terdeteksi

4. Conclusions

Based on the test results in this study it can be concluded that snort can be implemented as an intrusion detection system on the Ubuntu 22.4 Linux operating system to detect attacks in the form of port scanning, DOS, DDOS, brute force by capturing the attacker's IP address which produces a response and impact on the computer's CPU that exceeds capacity. Thus, it can be concluded that the success of Snort in detecting one attack is 100%, and the success of Snort in detecting two attacks simultaneously is 100% if there are no more than two types of attacks.

REFERENCE

[1] Atmaji, J, S, E., & Susanto, M, B. 2016 (Juli). ”Monitoting Kemanan Jaringan Komputer Menggunakan Network Intruction Detection System (NIDS)”, 118-122.

[2] Fachri, F. 2023 (Februari). "Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing". Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK), 10(1), 5158. https://doi.org/10.25126/jtiik.2023105872.

[3] Mutaqin, F, A. 2016 (Januari)." Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMSAlert dengan Snort". 12537-38133-1-Pb. 1(1).

[4] Rahadian, D, dkk. 2021 (Desember). "Perancangan Dan Implementasi Adaptive Intrusion Prevention System (Ips) Snort Menggunakan Logika Fuzzy Untuk Mencegah Serangan Pada Arsitektur Software-Defined Network". 8(6), 11697–11710.

[5] Ramadhan, I. 2019 (Mei). "Monitoring Keamanan Jaringan Dengan Snort Ids Menggunakan Metode Forensic Jaringan" (Studi Kasus: Cv.Triem Gunung Mas Sejahtera). Jurnal Ilmiah Mika Amik Al Muslim, 3(1), 13–18.

[6] Redro, B, D, dkk. 2020 (September). ”Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap”. PROSISCO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer,7(2),108-115. https://doi.org/10.30656/prosisko.v7i2.2522.

[7] Sau, T, M., & Siswantyo, S. 2021 (Agustus). "Analisis Penggunaan Hasil Deteksi IDS Snort pada Tools RITA dalam Mendeteksi Aktivitas Beacon". Info Kripto, 15(2), 97–104. https://doi.org/10.56706/ik.v15i2.21

[8] Sebayang, A., & Widiasari R, I. 2021(Juni). "Implementasi Proxy dan Snort Sebagai Gateway Antivirus". MEANS (Media Informasi Analisa dan Sistem), 6(1), 1–6. https://doi.org/10.54367/means.v6i1.1232

[9] Sugeng, W., & Mery, S, I. 2012 (April). "Analisis Jaringan Komputer” Dinas Komunikasi dan Informatika. 2013, 3(1), 8.(diakses tanggal 16 Maret 2023).

[10] Sugiyono. 2016 (Juni). "Sistem keamanan jaringan komputer menggunakan metode watchguard firebox pada pt guna karya indonesia". Jurnal CKI, 9(1), 1–8.

[11] Suhartono, D, dkk. 2015 (Februari). "Intrusion Detectin Prevention System (IDPS) pada Local Area Network (LAN)". Telematika, 8(1), 24–42. https://ejournal.amikompurwokerto.ac.id/index.php/telematika/article/download/261/236