

## ABSTRAK

Nama : Nizan Muhammad Basalamah

Program Studi : Teknik Informatika

Judul Skripsi : Simulasi Sistem Monitoring Jaringan Lokal Menggunakan Snort Dengan Notifikasi Aplikasi Telegram

Dalam jaringan komputer, khususnya yang berkaitan dengan keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan. Adapun contoh masalah yang sering terjadi dalam keamanan jaringan adalah karena disebabkan oleh pihak ketiga yang mencoba mengganggu pengguna jaringan tersebut yang berupaya melakukan perusakan, penyusupan atau penyalahgunaan data maupun sistem seperti *Denial Of Service* dan *Port Scanning*. Serangan – serangan tersebut dapat bertujuan untuk memeriksa port yang terbuka dan mengirim paket yang banyak agar target *down*. Untuk itu penulis membuat simulasi sistem monitoring jaringan lokal menggunakan Snort dan aplikasi bot telegram sebagai media untuk memberikan notifikasi adanya serangan. Snort merupakan *Open Source Intrusion Detection System* (IDS) yang digunakan untuk pemantauan terhadap gangguan pada jaringan komputer. Agar mempermudah administrator dalam melihat dan membaca hasil log dari setiap paket data yang masuk atau keluar maka menggunakan *Basic Analysis and Security Engine* (BASE) dan nantinya sistem ini dapat mengirimkan notifikasi adanya serangan pada gadget administrator jaringan secara *real-time* dan berfungsi juga sebagai alat bagi administrator jaringan untuk memantau jaringan tanpa harus berada di depan server secara langsung. Pada PC Server menggunakan sistem operasi linux ubuntu 20.04. Dan Pengujian dilakukan pada Local Area Network dengan topologi Star. Kemudian hasil gangguan yang disebabkan *Port Scanning* dan *Denial Of Service* (DoS) dapat dikenali oleh Snort IDS, dapat dimonitoring menggunakan *Basic Analysis and Security Engine* (BASE), dan hasil peringatan dari dua serangan tersebut lalu disimpan di log dan dikirimkan ke *gadget* administrator jaringan menggunakan aplikasi Telegram.

**Kata Kunci** : Snort, *Intrusion Detection System* (IDS), *Port Scanning*, *Denial of Service* (DoS), *Web Monitoring*, Bot Telegram.

## ABSTRACT

Name : Nizan Muhammad Basalamah

Study Program : Teknik Informatika

Title : Simulation of Local Network Monitoring System Using Snort  
With Telegram Application Notifications

In computer networks, especially those related to network security, it is very important to pay attention to. Examples of problems that often occur in network security are caused by third parties who try to interfere with network users who try to destroy, infiltrate or misuse data or systems such as *Denial Of Service* and *Port Scanning*. These attacks can aim to check open ports and send a large number of packets to bring the target *down*. For this reason, the author makes a simulation of a local network monitoring system using Snort and the telegram bot application as a medium to provide notification of an attack. Snort is an *Open Source Intrusion Detection System* (IDS) which is used for monitoring computer network disturbances. In order to make it easier for administrators to view and read log results from each incoming or outgoing data packet, they use the *Basic Analysis and Security Engine* (BASE) and later this system can send notifications of attacks on network administrator gadgets in real-time and also functions as a tool for network administrator to monitor the network without having to be in front of the server directly. On the PC Server using the Linux Ubuntu 20.04 operating system. And the test is done on Local Area Network with Star topology. Then the results of interference caused by *Port Scanning* and *Denial Of Service* (DoS) can be recognized by Snort IDS, can be monitored using the *Basic Analysis and Security Engine* (BASE), and the warning results of the two attacks are then stored in the log and sent to the network administrator's *gadget* using Telegram application.

**Keywords:** Snort, *Intrusion Detection System* (IDS), *Port Scanning*, *Denial of Service* (DoS), *Web Monitoring*, Bot Telegram.