ABSTRAK

Peningkatan ancaman serangan jaringan, terutama serangan flooding yang dapat mengganggu kinerja jaringan dan layanan yang ada. Flooding dapat menyebabkan hilangnya ketersediaan dan kendala pada layanan jaringan, sehingga dapat mengganggu aktivitas dari layanan tersebut. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan dan menerapkan sistem pendeteksi serangan flooding data menggunakan Snort pada jaringan IT Telkom Surabaya. Untuk membangun sebuah sistem pendeteksi dalam mengurangi flooding data dengan snort menggunakan metode IDS, dapat dilakukan dengan *Software* Snort yang berbasis *Host-based IDS*. Penelitian ini melibatkan instalasi dan konfigurasi IDS menggunakan tools Snort pada server, penggunaan Telegram Bot API untuk mengirimkan notifikasi serangan ke pengguna, serta uji coba serangan flooding pada jaringan lokal. Pada penelitian ini penyerangan dilakukan melalui serangan TCP Flood, UDP Flood, dan ICMP Flood pada jaringan lokal. Output jika terjadinya flooding akan menghasilkan notifikasi pada telegram, Hasil percobaan menunjukkan bahwa Snort memiliki kemampuan yang baik dalam mendeteksi berbagai jenis serangan flooding. Hasil dari penelitian ini berupa analisis efektifitas Snort dalam mendeteksi dan melindungi jaringan dari serangan flooding data. Snort mampu mendeteksi serangan SYN TCP Flood dengan tingkat efisiensi sebesar 48.19%, UDP Flood sebesar 35.95%, dan ICMP Flood sebesar 56.00%. Peningkatan periode waktu pengujian menjadi 10 menit menghasilkan peningkatan efisiensi pendeteksian, yaitu 72.68% untuk SYN TCP Flood, 67.73% untuk UDP Flood, dan 89.99% untuk ICMP Flood. Kesimpulan daroi penelitian ini adalah Snort merupakan solusi yang efektif dalam mendeteksi dan melindungi jaringan dari serangan flooding data. Meskipun efisiensi pendeteksian berbeda-beda pada setiap jenis serangan, Snort dapat memberikan perlindungan yang memadai dan dapat diandalkan untuk mengatasi ancaman serangan jaringan.

Kata Kunci : ***Snort, Flooding Data, Snort Efisiensi***.

ABSTRACT

Increased threat of network attacks, especially flooding attacks that can disrupt the performance of existing networks and services. Flooding can cause loss of availability and constraints on network services, so that it can disrupt the activities of these services. Therefore, this research aims to develop and implement a data flooding attack detection system using Snort on the Telkom Surabaya IT network. To build a detection system in reducing data flooding with Snort using the IDS method, it can be done with Snort Software based on Host-based IDS. This research involves the installation and configuration of IDS using Snort tools on the server, the use of Telegram Bot API to send attack notifications to users, as well as testing flooding attacks on local networks. In this research, the attack was carried out through TCP Flood, UDP Flood, and ICMP Flood attacks on the local network. The output if flooding occurs will produce a notification in telegram, The experimental results show that Snort has a good ability to detect various types of flooding attacks. The results of this study are an analysis of the effectiveness of Snort in detecting and protecting networks from data flooding attacks. Snort is able to detect SYN TCP Flood attacks with an efficiency rate of 48.19%, UDP Flood of 35.95%, and ICMP Flood of 56.00%. Increasing the test time period to 10 minutes resulted in an increase in detection efficiency, namely 72.68% for SYN TCP Flood, 67.73% for UDP Flood, and 89.99% for ICMP Flood. The conclusion of this research is that Snort is an effective solution in detecting and protecting networks from data flooding attacks. Although detection efficiency varies with each type of attack, Snort can provide adequate and reliable protection against network attack threats.

Keywords: Snort, Flooding Data, Snort Efficiency