ABSTRAKSI

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Terutama pada perusahaan-perusahaan dimana data-data penting perusahaan harus dilindungi dari segala macam serangan dan usaha penyusupan oleh pihak yang tidak berhak. Sehingga suatu sistem keamanan pada jaringan menjadi salah satu aspek yang penting untuk diperhatikan dari sebuah sistem informasi. Oleh karena itu sistem keamanan pada sebuah jaringan membutuhkan pengamanan yang kuat dalam menghadapi serangan yang dapat membahayakan jaringan dan informasi penting dari suatu perusahaan. Salah satu solusi yang dapat digunakan untuk membantu dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam jaringan tersebut menggunakan *tools* Intrusion Prevention System (IPS). Sistem yang hanya mendeteksi ini akan diimplementasikan dengan menggunakan aplikasi Snort. Sistem IPS ini yaitu sistem yang mampu memberikan alerting maupun pencegahan apabila terjadi serangan di dalam jaringan, selain itu IPS ini juga dapat memonitoring serangan melalui interface web. Sistem IPS ini menggunakan sistem operasi Ubuntu 17.04 dan dibagi menjadi beberapa modul yaitu IPS software yaitu snort, AfPacket, dan Acidbase, untuk network device yang digunakan adalah sebuah hub. Pengujian sistem dilakukan dengan menggunakan beberapa jenis serangan yaitu *Dos, Port Scan, brute force attack dan Flooding*. Skenario dalam pengujian ini berdasarkan functionality test, dengan target sebuah server.

Kata Kunci : ***IPS, Snort, Ddos, Port Scan, Flooding***

ABSTRACT

Computer network security as part of an information system is very important to maintain the validity and integrity of data and ensure the availability of services for its users. Especially in companies where important company data must be protected against all kinds of attacks and intrusion attempts by unauthorized parties. So that a security system on the network to be one important aspect to note of an information system. Therefore security systems on a network require strong security in the face of attacks that may harm the network and important information of a company. One solution that can be used to help in monitoring network conditions and analyze the malicious packets contained in the network using Intrusion Prevention System (IPS) tools. Systems that only detect this will be implemented using the Snort app. IPS system is a system that can provide alerts and prevention in case of attacks within the network, in addition to this IPS also can monitor attacks through the web interface. IPS system uses the operating system Ubuntu 17.04 and divided into several modules that IPS software is snort, AfPacket, and Acidbase, for network devices used is a hub. System testing is done by using several types of attacks that are Dos, Port Scan, brute force attack and Flooding. Scenarios in this test are based on functionality test, with the target of a server.

Keywords: IPS, Snort, Ddos, Port Scan, Flooding