ABSTRAK

Masalah dalam penelitian ini adalah ditemukannya banyak celah keamanan jaringan internet, diantaranya yang sering terjadi dan muncul ialah *Port Scanning*, Ddos, Bruteforce. Tujuan penelitian ini adalah mendeteksi setiap serangan yang terjadi dan melakukan *block* sehingga mampu menangkal/mencegah terjadinya akses masuk pada server. Hipotesis dalam penelitian ini adalah dapat mendeteksi dan melakukan pencegahan terhadap serangan menggunakan *default rules* yang dimiliki oleh Suricata 6.0.4.

Metode yang diusulkan adalah penelitian eksperimen yang bersifat kuantitatif untuk dapat mengamankan suatu sistem jaringan menggunakan *Intrusion Prevention System* (IPS) yang dikombinasikan antara fitur *blocking* dari Firewall dan fitur *detection capabilities* dari *Intrusion Detection System* (IDS) berdasarkan *traffic behavior* atau *anomaly* yang ditemukan selama dalam pengamatan dan pengujian yang telah dilakukan. Untuk membangun sistem keamanan ini dibutuhkan sistem jaringan yang sudah yang terpasang aplikasi pfSense yang memiliki *service* Suricata sebagai IPS.

Hasil dari penelitian ini menunjukan bahwa IPS dapat melakukan *detection* dan *blocking* terhadap serangan Scanning Port, Bruteforce dengan 3 kali pengujian dan Ddos dengan pengujian selama durasi waktu 30 detik, 1 menit dan 3 menit.

Kata Kunci: *Intrusion Prevention System* (IPS), *Security, Port Scanning,* Ddos, Bruteforce

ABSTRACT

The problem in this research is the discovery of many internet network security gaps, among which often occur and appear are Port Scanning, Ddos, Bruteforce. The purpose of this study is to detect every attack that occurs and block it, so that it can prevent incoming access to the server. The hypothesis in this study is that IPS can detect and prevent attacks using the default rules by Suricata 6.0.4

The proposed method is experimental research that is quantitative in nature to be able to secure a network system using the Intrusion Prevention System (IPS) which is a combination of the blocking features of the Firewall and the detection capabilities of the Intrusion Detection System (IDS) based on traffic behavior or anomalies found during the operation. observations and tests that have been carried out. To build this security system, you need a network system that is already installed with the pfSense application that has the Suricata service as IPS.

The results of this study indicate that IPS can detect and block Scanning Port attacks, Bruteforce with 3 tests and Ddos with tests with a duration of 30 seconds, 1 minute and 3 minutes.

Keyword: *Intrusion Prevention System* (IPS), *Security, Port Scanning,* Ddos, Bruteforce