ABSTRAK

Jaringan komputer sangat erat dengan internet dan telah menjadi satu kebutuhan utama pada suatu instansi/perusahaan. Hal ini menjadi sangat berbahaya apabila sebagai pengguna tidak meningkatkan juga keamanan pada jaringan yang saat ini banyak oknim/orang yang mencari celah pada sistem jaringan pada suatu instansi/perusahaan yang bisa dimanfaatkan untuk hal yang tidak baik. *Denial of service* (Dos) menjadi salah satu bentuk serangan yang mengakibatkan suatu sistem akan terbanjiri oleh data-data terus menerus dalam waktu singkat. Hal ini mengakibatkan lalu lintas jaringan menjadi sangat padat sehingga lalu lintas dari pengguna yang terdaftar tidak terdeteksi oleh sistem jaringan. Permasalahan tersebut diperlukan tools-tools untuk mendeteksi dan pencegahan terjadinya peretasan, diantaranya menggunakan *snort* dan *suricata* sebagai *Instrusion Detection System* (IDS).

Tugas akhir ini diselesaikan dengan melakukan analisis pebandingan dari tools *Intrusion Detection System* Snort dengan *Intrusion Detection System* Suricata. Analisis dilakukan setelah mendapatkan hasil dari simulasi pengujian yang akan dilakukan. Metode *Intusion Detection System* (IDS) akan diterapkan pada OS Linux yang sudah terinstal *web* server.

Hasil dari Tugas Akhir ini berupa analisis perbandingan kinerja dari *Instrusion Detection System* (IDS) Snort dan Suricata dalam mendeteksi serangan *Denial of Service* (DoS). Dari kedua tools IDS tersebut mempunyai cara dan keunggulan masing-masing dalam hal penanganan serangan *Denial of Service* (DoS).

Kata Kunci : *Kinerja, Server Linux, Flooding data, Snort, Suricata, Denial of Service*

ABSTRACT

Computer networks very closely with the Internet and has become a major requirement in an agency / company. It becomes very dangerous if a user does not improve also security on the network that is currently widely oknim / people looking for loopholes in the system network on an institution / company that can be used for things that are not good. *Denial of Service* (DoS) be one form of attack which resulted in a system will be flooded by the data continuously in a short time. This results in network traffic becomes so dense that traffic from unregistered users are not detected by the network system. These problems required tools-tools for the detection and prevention of hacking, including using Snort and Suricata as Instrusion Detection System (IDS).

The final task is accomplished by performing comparing analysis of tools Intrusion Detection System Snort Intrusion Detection System with Suricata. The analysis was conducted after getting the results of the simulation tests to be performed. Intusion Method Detection System (IDS) will be applied to the Linux OS pre-installed web server.

The end result of this final analysis of the comparative performance of Instrusion Detection System (IDS) Snort and Suricata in Detecting DoS attack. From both the IDS tools have a way and their respective advantages in terms of handling of *Denial of Service* (DoS).

Keywords : *Kinerja, Server Linux, Data flooding, Snort, Suricata, Denial of Service*