ABSTRAK

Di masa kini, hampir semua perangkat yang terhubung dengan jaringan internet memiliki kerentanan yang tinggi untuk diserang oleh *hacker*. Munculnya berbagai jenis teknik serangan yang baru di setiap tahunnya juga semakin memperburuk kondisi tersebut. *Intrusion Detection System Snort (IDS*) menyediakan cara yang handal untuk menjawab kebutuhan tersebut. Namun permasalahan yang ada yakni kemampuan dasar *Snort* sebagai IDS yang tidak mampu menyajikan notifikasi serangan secara *user-friendly* pada suatu *Dashboard Application* untuk memudahkan *monitoring*. *Snort* juga tidak memiliki kemampuan dasar untuk melakukan *blocking* alamat IP secara otomatis menggunakan *firewall* pada *hardware* yang tersedia jika terjadi suatu serangan oleh alamat IP tertentu.

Pada Tugas Akhir ini dibuat sistem yang mampu mengintegrasikan antara kemampuan *Snort* sebagai IDS, *Dashboard Application* untuk menampilkan *signature* yang terdeteksi, kemampuan *Snortsam* untuk melakukan *blocking* serangan pada berbagai jenis *firewall,* dan juga kemampuan *ClamAV* dalam melakukan *filtering* virus. Implementasi dari arsitektur ini diharapkan mampu meningkatkan performansi dan kehandalan *Snort*.

Berdasarkan hasil pengujian dan analisis terhadap sistem yang dibuat, sistem mampu melakukan fungsi deteksi serangan, menampilkan *signature* pada *Dashboard Application*, dan mampu melakukan *blocking* secara otomatis pada alamat IP yang terdeteksi sebagai *attacker*. Namun terjadi penurunan performansi IDS *Server* seiring dengan banyaknya *service* keamanan yang beroperasi pada IDS *Server*.

Kata Kunci*: **Network Intrusion Detection Prevention System, Dahsboard System, Snort , ACL Router, ClamAV.***