ABSTRAK

Masalah keamanan jaringan semakin menjadi perhatian dikarenakan perkembangan teknologi informasi yang semakin cepat. Hal ini membuat seseorang secara ilegal untuk masuk ke dalam sistem dan membuat lumpuh sistem tersebut. Selain itu, adanya celah dan tidak adanya sistem keamanan yang melindungi sistem menjadikan sistem rentan terhadap serangan.

Oleh karena itu, pada Tugas Akhir ini dibuatlah sebuah sistem kemanan dengan menggunakan Suricata sebagai *Network Intrusion Detection System* (NIDS) dan Ntopng sebagai alat untuk me-*monitoring* jaringan hingga ke *layer*-7. Dengan fokus pada serangan *Denial of Services* (DoS), maka akan dilihat perbandingan antara kedua aplikasi tersebut dalam menangani serangan DoS.

Dari hasil penelitian ini, berdasarkan *rule* Suricata yang penulis buat, penulis berhasil mendeteksi semua serangan yang diujicobakan. Sedangkan pada *rule default* pada Ntopng, penulis hanya mampu mengidentifikasi jenis serangan DoS berupa SYN *flood*. Untuk serangan DoS dengan tujuan *website server*, pada bagian akurasinya, *rule* Suricata yang penulis buat lebih unggul daripada *rule default* pada Ntopng untuk aplikasi LOIC sebesar 52,70%, sedangkan untuk aplikasi Hping3 sebesar 48,80%, dan aplikasi GoldenEye sebesar 52,84%. Sedangkan untuk serangan DoS dengan tujuan FTP *server*, pada bagian akurasinya, *rule* Suricata yang penulis buat juga lebih unggul daripada *rule default* pada Ntopng untuk aplikasi LOIC sebesar 52,30%, sedangkan untuk aplikasi Hping3 sebesar 59,97%. Sehingga ada perbedaan jauh antara persentase akurasi, *precision rate,* dan *recall rate* dari Suricata dan Ntopng yaitu Suricata lebih unggul dalam ketepatan akurasi *rule*-nya dalam mendeteksi serangan DoS.

Kata Kunci : *suricata, ntopng, rule, DoS.*