ABSTRAK

Perkembangan teknologi saat ini telah berkembang pesat terutama dalam penggunaan jaringan komputer, akan tetapi perkembangan ini juga memiliki dampak terhadap keamanan suatu jaringan. Oleh karena itu, sistem keamanan jaringan komputer saat ini menjadi sangat penting dalam menjaga kerahasiaan dan integritas data untuk menjaga dari penyusup yang berusaha mengubah atau bahkan merusak data yang dimiliki oleh suatu jaringan. *Intrusion Detection and Prevention System* (IDPS) salah satu solusi yang dapat digunakan untuk membantu administrator dalam memantau dan menganalisa serta dapat melakukan pemblokiran terhadap paket-paket berbahaya yang terdapat dalam sebuah jaringan. Dalam implementasinya, terdapat beberapa jenis *tools* yang dapat digunakan untuk mendukung kinerja dari *Intrusion Detection and Prevention System* (IDPS). Pada penelitian ini, akan menganalisis kinerja dari metode IDPS menggunakan snort dalam mendeteksi serta memblokir serangan UDP *flooding* dan SYN *flooding*. Untuk menguji kinerja sistem IDPS dengan snort, maka dilakukan pengujian serangan dan menggunakan parameter uji *Quality of Service* (QoS) yaitu *throughput, delay, jitter,* dan *packe*t *loss.* Berdasarkan hasil penelitian, snort berhasil meningkatkan nilai *throughput* pada saat serangan UDP *flooding* dan SYN *flooding* masuk kedalam server, sehingga konektivitas dalam jaringan dalam memberikan layanan semakin baik. Selanjutnya, snort mampu menurunkan nilai *delay* sehingga waktu dalam pengiriman data menjadi lebih cepat dibandingkan dengan sebelum snort aktif. Dari sisi *Jitter*, mengakibatkan nilai rentang antar *delay* menurun sehingga sehingga kualitas pengiriman data ketika client mengakses web server meningkat dari sebelumnya.

Kata kunci : keamanan jaringan, *Intrusion Detection and Prevention System, Quality of Service (QoS),* UDP *flooding,* SYN *flooding*