ABSTRAK

Server merupakan pusat penyedia layanan dan pengolahan data dalam suatu jaringan, permintaan yang dikirim oleh *client* akan diolah *server*. Keamanan sangat dibutuhkan agar *server* dalam kondisi baik dan dapat melindungi informasi yang berada dalam jaringan dan meminimalisir terjadinya kegiatan anomali seperti serangan DoS. Berdasarkan permasalahan tersebut, maka dilakukan penelitian mengenai keamanan jaringan menggunakan aplikasi Snort sebagai *Host-based Intrusion Prevention System* (HIPS) dengan teknik deteksi *anomaly-based* untuk melindungi pelayanan yang diberikan *server* dari penyerang. Dari penelitian yang telah dilakukan HIPS dapat mendeteksi dan memblokir 72550 dari 72600 serangan *ICMP Flood*, 98418 dari 98718 serangan *UDP Flood*, 25950 dari 26950 serangan *SYN Flood*, 141 dari 151 serangan *FTP Bruteforce*. Selain itu dilakukan analisis nilai *Quality of Service* sebelum dan saat terjadi penyerangan. Pada nilai CPU mengalami peningkatan yang disebabkan karena CPU harus bekerja untuk menjawab permintaan yang masuk, pada nilai *throughput* mengalami peningkatan yang disebabkan jumlah data yang diterima lebih banyak dibandingkan waktu yang dibutuhkan. Pada *delay* dan *jitter* mengalami penurunan dikarenakan total *delay* dan *jitter* memiliki nilai yang kecil dibandingkan dengan jumlah paket yang diterima, selain itu nilai *packet loss* pada semua percobaan bernilai nol persen atau dapat dikatakan sempurna, hal ini disebabkan paket yang menuju *server* sudah tersaring oleh HIPS.

Kata kunci: *Host-based Intrusion Prevention System* (HIPS), DoS, Snort, *Quality of Service*