ABSTRAK

Keamanan jaringan komputer semakin dibutuhkan seiring maraknya serangan yang dilakukan oleh *hacker* dengan tujuan tertentu. Serangan yang sering terjadi dan umumnya mudah dilakukan oleh *hacker* adalah *port scanning* dan *Denial of Service* (DOS). Pada penelitian ini akan dilakukan uji implementasi Snort dalam menjalankan fungsi sebagai *Intrusion Detection Prevention System* (IDPS) ketika mendeteksi serangan *port scanning* dan UDP *flooding* menggunakan metode *afpacket*. Uji performansi pada penelitian ini menggunakan parameter pengukuran *Quality of Service* (QOS) pada sisi *client* yang sedang mengakses web server pada saat uji coba serangan UDP *flooding*. Serangan *port scanning* tidak dilakukan pengukuran menggunakan QOS, karena hanya berfungsi untuk melihat *port* yang terbuka. Hasil pengukuran *throughput* pada kondisi normal sebesar 57081 bit/s kemudian turun saat ada serangan UDP *flooding* menjadi 56194 bit/s dan kembali meningkat saat Snort berhasil mendeteksi dan memblokir serangan menjadi 64397 bit/s. Nilai *delay* yang dihasilkan pada web server normal yaitu 47,04 ms dan naik saat serangan UDP *flooding* menjadi 50,63 ms dan turun menjadi 33,52 ms saat Snort diaktifkan. *Jitter* yang dihasilkan saat web server normal sebesar 0,087 ms dan turun saat serangan UDP *flooding* menjadi 0,065 ms, kemudian naik menjadi 2,619 ms saat Snort diaktifkan. Nilai *Packet loss* sebesar 4,75% saat UDP *flooding* dan Snort aktif.

Kata Kunci : *Denial of Service, Intrusion Detection Prevention System, Port Scanning, Quality of Service,* Snort