

ABSTRAK

Keamanan jaringan dibutuhkan server untuk menjaga performansi yang diberikan untuk pengguna, suatu serangan dapat terjadi kapan saja dan dimana saja. Serangan yang sering ditemui yaitu Denial of Service (DoS), serangan ini mengganggu layanan yang disediakan server, menghambat kinerja, gangguan jaringan, mengurangi kinerja server, dan merusak reputasi perusahaan. Penelitian ini akan mengimplementasikan metode IDPS menggunakan tools Snort dalam mendeteksi serangan DoS yang tertuju ke server. Penelitian ini mengukur performansi IDPS Snort berdasarkan parameter Quality of Service (QoS) yang diberikan server kepada pengguna. Nilai Throughput menurun, Packet Loss meningkat, Delay meningkat, dan Jitter meningkat pada saat serangan DoS dijalankan. Pada saat Snort sudah aktif Nilai Throughput meningkat, Packet Loss menurun, Delay menurun, dan Jitter menurun pada saat serangan DoS dijalankan. Dengan adanya Snort sebagai IDPS dapat meningkatkan kualitas QoS yang diberikan server saat serangan terjadi dibandingkan dengan saat belum mengimplementasikan *Snort*. *Snort* pada penelitian ini berhasil berperan sebagai *Intrusion Detection Prevention System (IDPS)* sehingga dapat mendeteksi dan mencegah serangan yang masuk menuju *server*.

Kata kunci: *Intrusion Detection System (IDS)*, *Intrusion Prevention System (IPS)*, *Snort*, *Quality of Service (QoS)*