ABSTRAK

Meningkatnya penggunaan halaman *web* menyebabkan *web server* rentan terhadap berbagai serangan yang menganggu kinerja *web server*. Salah satu serangan pada *web server* yaitu *data flooding* yang membuat akses dari user ke *web* menjadi terganggu karena kinerja *web server* yang terhambat. Maka diperlukan sistem keamanan jaringan yang menerapkan *Intrusion Prevention System* (IPS) untuk mencegah serangan *data flooding*.Terdapat beberapa s*o*ftware yang dapat menerapkan metode IPS seperti Snort dan Suricata. Penelitian ini menganalisis performansi IPS Snort dan Suricata dalam mencegah serangan *data flooding* berdasarkan parameter QoS layanan *web server*. Perbandingan performansi Snort dan Suricata dilihat melalui 4 skenario pengujian. Pada skenario pertama sistem tidak mengalami serangan *data flooding* untuk mengukur kinerja normal dari *web server*. Pada skenario kedua sistem mengalami serangan *data flooding* tanpa IPS. Sedangkan pada skenario ketiga dan keempat sistem mengalami serangan *data flooding* dengan menerapkan IPS Snort dan Suricata secara bergantian. Berdasarkan pengujian tersebut, maka diperoleh nilai dari parameter Qos (*delay*, *packet loss*, *throughput*, RTT). Hasil pengukuran parameter QoS pada skenario 1 yaitu *throghput* 1,898 Mbps, *packet loss* 0,029 %, *delay* 3,409 ms, dan RTT 0,028 s. Pada skenario 2 *throughput* 0,0007 Mbps, *packet loss* 64,854 %, *delay* 3475,518 ms, RTT 14,642 s. Pada skenario 3 *throughput* 0,725605455 Mbps, *packet loss* 0,018 %, *delay* 7,885 ms, dan RTT 0,064 s. Pada skenario 4 *throughput* 0,748 Mbps, *packet loss* 0,017 %, *delay* 7,669 ms, dan RTT 0,062 s.

Kata kunci : *Web server, Data flooding*, IPS, Snort, Suricata