BAB V
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan penelitian mengenai analisis performansi *Intrusion Detection Prevention System* (IDPS) pada *tool* Snort dalam mendeteksi serangan *port scanning* dan *Denial of Service* (DOS) diperoleh beberapa kesimpulan sebagai berikut :

1. Pengujian dan implementasi dari *rules* Snort yang dibuat oleh penulis berhasil menjalankan fungsi *Intrusion Detection And Prevention System* (IDPS) untuk mengatasi serangan *port scanning* dan UDP *flooding*.
2. Penambahan fungsi *Intrusion Prevention System* (IPS) pada Snort, perlu dilakukan konfigurasi pengaktifan mode *inline* dengan *data acquisition* (daq).
3. Cara kerja dari Snort saat menjankan fungsi sebagai *Intrusion Detection And Prevention System* (IDPS) mempengaruhi nilai *Quality of Service* (QOS) dari sisi *client* yang mengakses web server.
4. Nilai *throughput* yang dihasilkan dari uji coba serangan UDP *flooding* mengalami peningkatan saat Snort berhasil mendeteksi dan memblokir serangan yang masuk.
5. Hasil pengukuran *delay* saat skenario serangan UDP *flooding* mengalami penurunan nilai saat Snort menjalankan fungsi IDPS. Hal ini menunjukkan bahwa Snort mampu meningkatkan kualitas nilai *delay* yang diperlukan saat pengiriman data.
6. Pada hasil nilai *jitter* saat serangan UDP *flooding* dijalankan mengalami peningkatan saat Snort melakukan pendeteksian dan pemblokiran serangan. Hal ini menunjukkan bahwa Snort tidak mampu meningkatkan kualitas nilai *jitter* pada sisi *client*.
7. Hasil pengukuran *packet loss* pada saat uji coba serangan UDP *flooding* sebesar 4,75% saat Snort diaktifkan. Selain skenario tersebut, nilai *packet loss* seluruhnya bernilai 0%.

5.2 SARAN

1. Pada penelitian selanjutnya, sebaiknya dapat menambahkan uji coba serangan yang diberikan saat Snort menjalankan fungsi sebagai IDPS agar dapat mengetahui performansi dari Snort dalam mengatasi berbagai serangan pada jaringan komputer.
2. *Quality of Service* (QOS) hanya mengukur performansi dari sisi *client* yang sedang mengakses web server atau berkomunikasi dengan server. Sebaiknya, pada penelitian selanjutnya dapat menambahkan parameter pengujian selain menggunakan QOS.
3. Pada penelitian ini, menggunakan jangkauan jaringan *Local Area Network* (LAN). Sebaiknya, pada penelitian selanjutnya dapat direalisasikan dalam cakupan jaringan yang lebih luas lagi.