BAB V

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan Penelitian mengenai kinerja Snort dalam mendeteksi serangan jaringan pada komputer diperoleh beberapa kesimpulan sebagai berikut :

1. Dalam pengimplementasian metode *Intrusion Detection and Prevention System* (IDPS), konfigurasi snort mampu mendeteksi dan melakukan pemblokiran serangan UDP *flooding* dan SYN *flooding*.
2. Dalam pengujian, dilakukan 2 skenario untuk mengukur kinerja snort yaitu ketika adanya serangan tetapi snort belum diaktifkan dan ketika snort telah diaktifkan.
3. Snort berhasil meningkatkan nilai *throughput* pada saat serangan masuk kedalam server, sehingga konektivitas dalam jaringan dalam memberikan layanan semakin baik. Snort mampu menurunkan nilai *delay* sehingga waktu dalam pengiriman data dari server menuju *client* menjadi lebih cepat. Pada pengukuran *Jitter*, ketika snort waktu yang dibutuhkan data untuk sampai tujuan dalam kualitas yang baik sedangkan snort diaktifkan terdapat nilai *packet loss* dari kedua serangan karena terjadinya kekeliruan snort dalam mendeteksi dan memblokir paket dari *client.*

5.2 SARAN

1. Pada penelitian selanjutnya, dapat menggunakan *tools* selain snort untuk menguji serangan dengan metode *Intrusion Detection and Prevention System* (IDPS)
2. Pada penelitian selanjutnya, dapat membandingkan performansi metode *Intrusion Detection and Prevention System* dengan menggunakan dua *tools*
3. Pada penelitian selanjutnya, menggunakan uji coba serangan selain SYN *flooding* dan UDP *flooding.*