BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari perancangan dan pengujian IDS berbasis Snort, maka dapat diambil beberapa kesimpulan sebagai berikut:

a. Dalam melakukan pendeteksian menggunakan parameter efektifitas waktu serangan terdeteksi, IDS yang diserang dengan tools Nmap pada Debian lebih cepat terdeteksi. Hal ini dapat dibuktikan dari data yang didapat dalam 30 percobaan yaitu IDS Snort dalam mendeteksi port scanning yang dilakukan dengan Zenmap pada Windows 8 memiliki rata-rata 13,52 detik dan standar deviasi 5134,685 detik. Sedangkan IDS Snort dalam mendeteksi port scanning yang dilakukan dengan Nmap pada Debian 7.11 memiliki rata-rata 1 dan standar deviasi 28,02.
b. Penyebab efektivitas IDS yang diserang dengan sistem operasi Debian lebih cepat, dikarenakan sistem operasi tersebut stabil dalam melakukan proses port scanning walaupun dengan spesifikasi yang minimum.

5.2 Saran

Berdasarkan hasil pengujian dan pembahasan yang telah dilakukan, masih banyak terdapat kekurangan pada maupun kelemahan pada sistem ini. Saran dari penulis apabila pembaca ingin melakukan pengemangan penelitian mengenai IDS sehingga meningkatkan kinerja sistem adalah sebagai berikut:

a. Selain sebagai IDS, sistem yang dibuat dapat dikembangkan menjadi Intrusion Prevention System (IPS) untuk menangani serangan sehingga

sistem dapat memberikan peringatan sekaligus menagani serangan tersebut.

b. Penambahan fitur notifikasi secara otomatis dengan media social supaya lebih mudah jika terjadi intrusi.
c. Melakukan pengujian serangan dengan tipe serangan yang berbeda.
d. Melakukan pengujian dengan tool yang berbeda dan sistem operasi yang berbeda