

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi dan pengujian sistem monitoring keamanan jaringan menggunakan SNORT sebagai IDS (*Intrusion Detection System*) dan notifikasi serangan melalui *instant messaging* Telegram, maka dapat diambil beberapa kesimpulan, sebagai berikut :

1. Dengan menerapkan Snort sebagai IDS (*Intrusion Detection System*) yang bekerja dalam melakukan pengawasan terhadap lalulintas (*traffic*) jaringan. Apabila ditemukan kegiatan-kegiatan mencurigakan yang berhubungan dengan lalulintas jaringan, maka Snort akan memberikan peringatan kepada administrator jaringan.
2. Memberikan fungsi *trigger send message* API kedalam konfigurasi *file web* BASE (*Basic Analysis and Security Engine*) yang telah terhubung dengan IDS (*Intrusion Detection System*) Snort, maka pada saat terjadi serangan, *trigger* akan mengeksekusi *file* tersebut untuk mengirimkan notifikasi *alert* menuju aplikasi *instant messaging* Telegram milik administrator secara *real time*.

## 5.2 Saran

Berdasarkan hasil pengujian dan pembahasan yang telah dilakukan, masih banyak terdapat kekurangan maupun kelemahan terhadap sistem. Untuk mendapatkan hasil yang lebih baik lagi, maka ada beberapa hal yang bisa dijadikan saran sebagai perkembangan kedepannya, antara lain :

1. Penambahan komponen-komponen pelengkap yang mendukung kinerja IDS (*Intrusion Detection System*) akan membantu efisiensi kerja sistem, seperti penambahan *rules* serangan sehingga pengetahuan sistem terhadap serangan jauh lebih banyak dan lebih baik, dan juga penambahan *frond-end*.
2. Adanya pelaporan data serangan kepada administrator bukan hanya dalam bentuk notifikasi Telegram, melainkan dalam bentuk rekapan dokumen lengkap dari data-data serangan yang berformat *xls*, *pdf*, *doc*, dsb.
3. Snort selain berfungsi sebagai IDS (*Intrusion Detection System*) hendaknya dapat dikembangkan lebih kompleks lagi, bukan hanya sebagai sistem pendeteksi serangan jaringan tetapi juga sebagai sistem pencegahan serangan atau yang dinamakan IPS (*Intrusion Prevention Sytem*).