BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi dan pengujian *Snort* sebagai *Intrusion Detection System* dan notifikasi melalui *telegram*, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. *Intrusion Detection System* (IDS) dapat dengan lancer berjalan pada sistem operasi berbasis Linux.
2. Dengan menerapkan IDS, *administrator* jaringan dapat megetahui dan memantau aktifitas jaringan pada *Web Interface Base* yang telah terpasang pada Server IDS.
3. *Intrusion Detection System* (IDS) akan melakukan pemeriksaan pada semua paket data yang masuk ke dalam jaringan server, bila paket tersebut ter-*sniff* dan sesuai dengan *rules* yang telah dibuat maka paket data tersebut terindekasi sebuah intuisi dan akan langsung di kirim melalui *log* dan diteruskan ke dalam *Web Interface*.
4. IDS yang dibangun dapat memberikan notifikasi ke administrator melalui aplikasi *instant messaging telegram* jika terjadi serangan terhadap *server* yang di kelolah terlebih dahulu pada *web interface* lalu diteruskan kepada *bot telegram* secara *real time*.

5.3 Saran

Untuk mendapatkan hasil yang lebih baik lagi, maka ada beberapa hal yang bisa dijadikan saran sebagai perkembangan kedepannya, antara lain:

1. *Snort* sebagai salah satu sistem keamanan jaringan hendaknya dapat dikembangkan tidak hanya sebagai sistem pendeteksi gangguan keamanan jaringan, tetapi juga sebagai sistem pencegahan keamanan.
2. Penambahan modul-modul tambahan yang mendukung kinerja IDS akan membantu efisiensi kerja sistem, seperti pengaturan *rule-rule* dan juga penambahan front end.
3. Penambahan fitur pada Telegram bot sehingga administrator dapat berkomunikasi dua arah dengan sistem.
4. Adanya pelaporan rekapan data Intrusi kepada administrator bukan hanya dari bentuk notifikasi Telegram, tetapi juga dalam bentuk dokumen seperti .pdf, .xls, dsb.