BAB V

KESIMPULAN

5.1 Kesimpulan

Dari uraian dan pembahasan "Analisis dan Implementasi Keamanan Jaringan Menggunakan *Network-based Intrusion Detection System* (NIDS) study kasus SMA Negeri 11 Yogyakarta" maka dapat diambil kesimpulan sebagai berikut:

1. Dalam menerapkan IDS, administrator jaringan dapat mengetahui jika terdapat salah satu server yang diserang sesuai dengan *rule* yang telah dibuat. Administrator mendapatkan notifikasi dari NIDS melalui Telegram yang dibangun dengan menggunakan Aplikasi *instan messaging* Telegram dan diintegrasikan dengan *database* Snort secara *realtime*.
2. Dari hasil akurasi waktu dan perbandingan dari tabel 4.4 menunjukkan bahwa waktu yang diperlukan untuk mendeteksi serangan tidaklah lama, butuh maksimal 3 detik untuk mendeteksi serangan dan maksimal 17 detik untuk notifikasi bisa terkirim ke Telegram.
3. Administator belum dapat secara maksimal menganalisa intrusi yang telah Snort deteksi melalui *interface web* yang dibangun menggunakan BASE dikarenakan tidak muncul nya tampilan *interface database* di dalam BASE.

4. IDS yang dibangun dapat mendeteksi beberapa serangan seperti *Port Scanning, FTP Bad Login, SSH Brute Force,* dan *DDOS Attack*

5.2 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 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.