BAB 5

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan pada penelitian ini, didapatkan kesimpulan sebagai berikut:

1. Berdasarkan pengujian yang dilakukan , *Intrusion detection system* bisa sangat efektif terhadap serangan tertentu. Terbukti dari hasil pengujian , dari 5 metode serangan dengan masing masing 35 percobaan , hanya terdapat 2 metode serangan yang dapat terdeteksi semua pengujian yang dilakukan.
2. Dalam mendeteksi sebuah *anomaly* , *Intrusion detection system* membandingkan sebuah traffic pada sebuah server dalam kondisi normal dengan kondisi saat terjadinya serangan. Jika perubahaan *traffic* pada penerimaan paket pada waktu tertentu melebihi 1000% dari kondisi normal dan paket perdetiknya mencapai 500 paket, maka *intrusion detection system* akan menganggap itu sebagai *anomaly* dan mendeteksi sebagai suatu serangan.
3. Dengan adanya Intrusion detection system pada sebuah server , dapat membantu *administrator* dalam mendeteksi adanya serangan dengan waktu pendeteksian yang cepat, sehingga *administrator* dapat melakukan Tindakan terhadap serangan tersebut dengan cepat.

5.2 Saran

Saran dalam melakukan penelitian terkait kedepannya yaitu, diperlukan pengembangan lebih lanjut dalam metode anomaly-based ataupun metode anomaly-based ini dapat dikombinasikan dengan algoritma yang lain sehingga pendeteksian yang dilakukan sangat efektif dan efisien

Dalam penggunaan pendeteksian anomaly, diperlukan adanya optimasi baseline atau meminimalkan perbedaan traffic pada saat normal dengan traffic pada saat terjadinya serangan, sehingga dalam mendeteksi sebuah anomaly akan lebih sensitive.