BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan mengenai penerapan *intrusion detection system* pada *web server* menggunakan metode *signature based* , maka dapat diperoleh kesimpulan sebagai berikut :

1. Jenis serangan XSS dan SQL *injection* adalah jenis serangan yang memanfaatkan celah dari sebuah website yang tidak memvalidasi inputannya.
2. Dengan *intrusion detection system* pada jaringan, administrator dapat melihat *history log* dari paket-paket data yang mencurigakan pada jaringan.
3. *Intrusion detection system* memiliki dua metode dalam mendeteksi serangan yaitu *anomaly based* dan *signature based*. *Signature based* merupakan jenis metode pendeteksian yang menggunakan *rule*. *Intrusion detection system* menggunakan *signature based* dapat mendeteksi beberapa serangan pada web server.
4. Dengan menerapkan aplikasi snortbow sebagai *user interface* IDS, administrator dapat dengan mudah mengkonfigurasi IDS dan melihat notifikasi jika terjadi serangan.
5. Dengan diterapkannya *intrusion detection system* pada jaringan, tidak mempengaruhi kecepatan akses komunikasi antara *client* dan *server*.

5.2 Saran

Berdasarkan penelitian mengenai penerapan *instrusion detection system* pada *web server,* hasil yang telah dicapai saat ini masih memiliki beberapa kekurangan khususnya pada implementasi rule pada berbagai macam serangan dan aplikasi snortbow. Disarankan untuk menambahkan hal-hal yang dapat melengkapi rule dan aplikasi snortbow ini yang akan datang. Diantaranya adalah :

1. Pengembangan *rule* dalam mendeteksi berbagai macam serangan yang memungkinkan terjadi pada *server* khususnya *web server*.
2. Pengembangan aplikasi snortbow yang mampu menyediakan *wizard* dalam pembuatan rule untuk snort.
3. Pengembangan aplikasi snortbow yang mampu mengirimkan notifikasi melalui SMS.
4. Pengembangan aplikasi snortbow yang mampu mengecek status dari setiap *server* yang ada pada jaringan contohnya status koneksi, kecepatan, *storage*, dan lain-lain