BAB VI

PENUTUP

6.1. Kesimpulan

Berdasarkan penelitian dan perancangan yang telah dilakukan, secara keseluruhan sebagai jawaban dari perumusan masalah, dapat ditarik kesimpulan sebgai berikut:

1. Suatu tindakan dicurigai sebagai serangan manakala tindakan tersebut menimbulkan reaksi pada server dan aplikasi dalam hal ini adalah berkas *error log*.
2. Mempelajari tingkah laku penyerangan merupakan cara lain untuk mendeteksi sebuah serangan. Meskipun terdapat banyak variasi dalam penerapannya, namun setiap teknik serangan pastilah mempunyai pola utama.
3. Ketika *Intrusion Prevention System* menemukan sebuah tindakan yang perpotensi sebagai serangan yang dapat merugikan, ia akan segera melakukan tindakan pencegahan seperti mengubah aturan firewall, menuliskan log dan mengirimkan laporan kepada pihak yang bertanggung jawab baik melalui SMS ataupun email.
4. Intrusion Prevention System menggabungkan 2 teknik yang berbeda yang sebelumnya tidak pernah dipadukan. Yaitu analisa paket data dan analisa

log server. Dengan demikian, selain mempertinggi tingkat akurasi juga diharapkan akan mengurangi *false positive* dan *false negative*.

5. Kemudahan dalam konfigurasi, administrasi dan penyajian laporan membuat *Intrusion Prevention System* menjadi salah satu tolak ukur utama pengembangan aplikasi dan server.

6.2. Saran

Dari hasil penelitian yang telah dilakukan dan untuk kepentingan penelitian selanjutnya, berikut ini beberapa point penting sebagai saran:

1. Teknik penyerangan semakin canggih seiring dengan semakin tingginya tingkat pengamanan. Untuk itu, pustaka serangan yang ada secara berkala perlu diperbaharui.
2. *Intrusion Prevention System* ini dibangun diatas system operasi berbasis Unix dengan web server Apache. Pengembangan untuk system operasi dan web server lain masih sangat terbuka, dengan cara menyesuaikan pengelolaan *error log* server.