BAB V

KESIMPULAN

5.1 Kesimpulan

Berdasarkan analisa dan pengujian yang telah dilakukan dengan adanya laporan skripsi yang berjudul "Intrusion Detection System Host Based Pada Web Server Berbasi Linux Backbox" dapat diambil kesimpulan :

1. Sebuah intrupsi dapat di deteksi tergantung pola serangan tersebut ada di dalam rule Intrusion Detection System atau tidak. Administrator Intrusion Detection System harus mengupdate rule terbaru pada snort.conf agar selalu bisa melakukan pencegahan apabila ada serangan dengan pola baru.
2. Rule yang diterapkan sudah bisa mendeteksi adanya serangan ICMP Attack, Port Scanning, dan SSH Detection.
3. Semua software yang digunakan dapat bekerja dengan baik, yaitu snort, snorby, dan barnyard2.
4. Apabila sistem IDS terkoneksi dengan internet akan banyak ip yang terdeteksi oleh snort sehingga jumlah event yang terekam oleh snorby akan sangat banyak.
5. Setiap serangan mempunyai waktu terdeteksi berbeda-beda, yaitu ICMP Attack , Port Scanning ,dan SSH Detection .
6. Dengan menggunakan snorby log yang terekam oleh snort akan ditampilkan menjadi event yang mudah dibaca. Pekerjaan administrator

memeriksa log akan semakin mudah karena semua event sudah dikelompokkan menjadi beberapa bagian seperti jumlah rule event yang terjadi, ip sumber, ip target interupsi dan lain sebagainya.

7. Serangan *ICMP Attack* rata-rata terdeteksi dalam 1.24 detik, Serangan *Port Scanning* rata-rata terdeteksi dalam 0.44 detik, dan *SSH Detection* rata-rata terdeteksi dalam 0.42 detik.
7. Pada web server yang diterapkan sistem IDS mengalami kenaikan penggunaan CPU sebanyak sebanyak 23,475% sedangakan penggunaan memory mengalami kenaikan sebanyak 13.9%.

5.2 Saran

Pada penelitian skripsi ini tentu masih banyak terdapat kekurangan, yang mungkin dapat disempurnakan lagi pada pengembangan selanjutnya, terdapat saran yang dipergunakan kedepannya, yaitu:

1. Dalam segi pendeteksian dapat dilakukan dengan baik karena dapat melihat lalulintas jaringan yang sedang terjadi, akan tetapi dari sisi pencegahan masih harus dikembangkan lagi dalam melindungi aset yang terdapat pada komputer yang menjadi tujuan dari penyerangan.
2. Intrusion Detection System hendaknya dapat dikembangkan untuk mendeteksi dan mencegah serangan-serangan mebahayakan lain yang mungkin terjadi pada web server seperti Password Guessing, SQL Injection, dan lain sebagainya.

3. Penambahan modul-modul lain yang dapat mendukung kinerja Intrusion Detection System sehingga dapat bekerja menjadi lebih efisien, seperti update rule secara otomatis dan juga pemberitahuan kepada administrator ketika tidak di tempat kerja dan terjadi sebuah intrusi.