BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis dan pengujian dari *Intrusion Detection System* yang telah dilakukan, maka dapat diambil kesimpulan bahwa:

1. IDS yang dibangun telah berhasil mendeteksi pola serangan *ICMP Large Attack, Port Scan,* dan *Bruteforce Attack*.
2. Informasi dari adanya percobaan penyerangan dapat dilihat tanpa perlu memantau monitor atau log dari Snort IDS secara terus menerus karena bisa diketahui dengan adanya *email* ke admin baik melalui PC maupun *smartphone*.
3. Dan tidak semua alamat *email* dapat terkirim *email alert*. Sebagai contoh yang tidak bisa digunakan adalah *gmail* dan *yahoo*.

5.2 Saran

Berikut hal yang mungkin bisa dijadikan saran untuk mendapatkan hasil yang lebih baik kedepannya:

1. Masih banyak *rule* pada Snort yang bisa digunakan untuk mengoptimalkan kinerja dari IDS tersebut untuk melindungi aset yang terdapat pada komputer yang menjadi tujuan dari penyerangan.

2. IDS hanya mampu untuk mendeteksi serangan, akan lebih baik lagi apabila mampu untuk mencegah serangan atau memblokir *ip* penyerang secara otomatis apabila terjadi usaha penyerangan.