

BAB V

KESIMPULAN

Pada bab ini akan dijelaskan tentang kesimpulan berdasarkan bab-bab sebelumnya, dan juga tentang apa yang harus dikembangkan lagi terhadap masalah sistem IDS (*Intrusion Detection System*) ini.

5.1 Kesimpulan

Rumusan kesimpulan dari keseluruhan proses penelitian yang telah dilakukan dari pembahasan yang sudah diuraikan dengan kesimpulan sebagai berikut:

1. Sistem IDS yang telah dibangun dalam mendeteksi serangan yang terjadi adalah dengan melakukan *scanning* terhadap sejumlah *source* dan lalu lintas yang terjadi didalam jaringan.
2. Keseluruhan sistem mesin sensor IDS dapat bekerja dengan efektif sebagai sistem keamanan jaringan komputer yang berbasis *open source*, dan didalam mendeteksi sebuah intruder atau penyusup pada mesin sensor IDS akan dianalisis pada BASE (*Basic Analysis and Security Engine*).
3. Mekanisme sistem ketja snort dan BASE yang telah berhasil di implementasikan dengan baik, dalam pengujian sistem snort dan BASE yaitu dengan menggunakan *Ping Attack*, *Port Scanning(Nmap)*, dan DDOS.
4. Pencegahan yang dapat dilakukan terhadap penyerangan adalah dengan menggunakan *iptables*. Untuk mengatasi serangan dari *intruder* yaitu dengan cara *ping attack* dan Nmap ke sebuah *server*, maka dilakukan konfigurasi *rule iptables*, dimana *rule* tersebut untuk memblock berdasarkan alamat *IP Address*.
5. Kelebihan dalam menggunakan IDS ini adalah suatu jaringan komputer dapat dipantau dengan mesin atau komputer yang bertindak sebagai

sensor didalam jaringan tersebut dan dapat melihat suatu kejadian yang sedang terjadi didalamnya. Selain keuntungan yang didapatkan penulis juga mendapatkan hasil dari sistem IDS dalam mengamankan jaringan, yaitu apabila terdapat suatu masalah pada jaringan(proses intrusi) maka dapat diketahui secara langsung oleh IDS ini yang menggunakan snort, dari mana serangan itu datang.

5.2 Saran

Saran-saran yang diberikann pada penelitian ini adalah sebagai berikut:

1. Sistem keamanan dengan WIDS snort dapat memberikan manfaat lebih apabila snort diintegrasikan dengan firewall. Snort efektif untuk mendeteksi adanya sebuah serangan terhadap sistem, akantetapi snort bukanlah sebuah intrusion Prevention sistem(IPS) yang dapat mencegah atau meblokir usaha-usaha penyusupan kedalam sistem.
2. IDS hanya melakukan monitoring jaringan, akan lebih baiknya IDS yang diterapkan dapat melakukan pencegahan dari serangan yang terjadi secara otomastis.