BAB V
PENUTUP

Pada bab ini akan dijelaskan tentang kesimpulan berdasarkan kepada bab-bab sebelumnya, dan juga saran 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 maka peneliti mencoba membuat kesimpulan, sebai berikut :

1. Sistem IDS (*Intrusion Detection System*) yang diterapkan telah berhasil dibangun dan dikembangkan dengan baik. Keseluruhan sistem sensor IDS dapat bekerja dengan efektif sebagai sistem keamanan jaringan komputer yang berbasis *open source* dalam mendeteksi sebuah *intruder* atau penyusup pada *server*, dimana dalam mendeteksi suatu serangan dianalisis pada BASE (*Basic Analysis And Security Engine*). Untuk lebih jelasnya dapat dilihat pada gambar 4.22
2. Sistem IDS (*Intrusion Detection System*) dalam mendeteksi serangan yang terjadi adalah dengan melakukan scanning terhadap sejumlah source dan lalu-lintas yang terjadi dalam jaringan, sehingga seluruh kejadian yang dianggap sah maupun tidak sah dapat dilihat melalui kegiatan monitoring dengan menggunakan aplikasi yang digunakan untuk melakukan pemantauan jaringan, dapat dilihat pada gambar 4.3 yang merupakan hasil dari *captuce* dalam pengujian *snort*.

3. Mekanisme sistem kerja *snort* dan BASE (*Basic Analysis And Security Engine*) yang telah berhasil di implementasi dengan baik. Dalam pengujian sistem *snort* dan BASE (*Basic Analysis And Security Engine*) yaitu dengan menggunakan ping attack, port scanning (Nmap), dan DDos. Untuk lebih jelasnya dapat dilihat pada gambar 4.19, gambar 4.20, dan gambar 4.21.
4. Pemblokiran IP *address* yang dapat dilakukan terhadap penyerang adalah dengan menggunakan *iptables*. Untuk mengatasi serangan dari *intruder* yaitu dengan cara *ping attack* dan *Nmap* ke sebuah *server*, maka peneliti membuat sebuah *rule iptables*, dimana *rule* tersebut untuk memblok berdasarkan alamat IP *address*. Saat *rules* dimasukkan ke dalam *rule iptables* maka akan terlihat pada laptop penyerang yaitu *request time out*, seperti yang terjadi pada gambar 4.25 dan gambar 4.26.
5. Kelebihan dalam menggunakan IDS (*Intrusion Detection System*) ini adalah suatu jaringan komputer dapat dipantau hanya dengan sebuah komputer yang bertindak sebagai sensor didalam jaringan dan terhubung kedalam sebuah jaringan, itu dapat melihat suatu kejadian yang sedang terjadi didalamnya. Selain keuntungan didapat dalam penerapan IDS (*Intrusion Detection System*) ini, peneliti juga mendapatkan hasil dari sistem IDS (*Intrusion Detection System*) dalam mengamankan jaringan, yaitu jika terdapat sebuah masalah pada jaringan (proses intrusi) maka dapat diketahui secara langsung oleh IDS (*Intrusion Detection System*) ini yang menggunakan *snort*, dari mana serangan itu datang, melalui port berapa, dan protocol apa yang digunakan.

6. Mendapatkan hasil dari analisa kinerja WIDS (*Wireless Intrusion Detection System*) yang ditampilkan oleh BASE (*Basic Analysis And Security Engine*) dengan total *alert* 987 x (kali), pada saat pengujian pendeteksi serangan yang dilakukan dengan proses *ping attack* (ICMP attack), *port scanning nmap* (zenmap gui), dan DDos (Digital Blaster) yang dilakukan masing – masing 1 x (kali) tes serangan.

5.2 Saran

Saran – saran yang diberikan pada penelitian ini adalah sebagai berikut:

1. Dalam segi pendeteksi dapat dilakukan dengan baik karena dapat melihat lalulintas jaringan yang sedang terjadi, akn tetapi dari sis pencegahan masih harus dilakukan pengembangan lagi dalam melindungi aset yang terdapat pada komputer *server*.
2. IDS (*Intrusion Detection System*) hanya bisa melakukan monitoring jaringan, akan lebih baiknya IDS (*Intrusion Detection System*) yang diterapkan dapat melakukan pencegahan dari serangan yang etrjadi secara otomatis.
3. Akan lebih baik jika IDS (*Intrusion Detection System*) saat mendeteksi terjadinya serangan memberi tahu administrator jaringan melalui *notif* di *smartphone*.