BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan sebagai berikut.

1. Penggunaan IDS (*Intrusion Detection Sistem*) dalam penelitian yang sudah di lakukan terbukti berhasil dalam mencegah masuknya peretas yang berusaha mengobesvasi masuk ke dalam *router* melalui *port* yang sudah di tentukan dan sering di gunakan sebagai akses masuk *administrator* untuk melakukan konfigurasi pada *routerboard mikrotik*. Dapat di terangkan bahwasanya *metode* IDS (*Intrusion Detection Sistem*) merupakan Langkah yang mudah digunakan dan juga tidak membutuhkan *source* yang banyak atau langkah yang rumit dalam penerapannya, sehingga *metode* ini sudah cukup untuk menghindari kemungkinan sebuah jaringan dapat di retas atau di salah gunakan.
2. secara keseluruhan mekanisme penerapan IDS (*intruction Detection system*) menjadi sangat penting apabila jaringan yang menjadi tolak tumpu atau distribusi koneksi hanya memiliki satu jalur saja. Maka dari itu salah satu pencegahan dan pendeteksian dini dapat di lakukan dengan beberapa fitur yang ada pada *metode* IDS itu sendiri. Selain dari pada itu, penggunaan IDS sangat berguna dalam mengendalikan *source* pada *routerboard* itu sendiri. Salah satu contoh yang di ambil yakni *load CPU* yang terjaga pada angka yang normal dengan posisi banjir *request Packet ICMP*.

5.2 Saran

Setelah menyelesaikan penelitian, penulis mencoba memberikan saran terkait kelemahan yang ditemukan dalam penerapan atau pengujian fitur fitur pada

penelitian ini untuk perancangan selanjutnya guna pengembangan dan perbaikan lebih lanjut seiring perubahan kebutuhan dan kemajuan teknologi, Adapun saran yang dapat penulis sampaikan kepada penelitian serupa di kemudian hari yakni sebagai berikut :

1. Penelitian dapat di terapkan untuk skala jaringan yang lebih besar dan kompleks. Dengan maksud melihat secara jelas dan mengukur seberapa jauh *metode* IDS dapat menagkal serangan dari peretas di jaringan yang lebih besar.
2. Pada penelitian ini respon dari salah satu *ruls* pada fitur *port scan detection* yaitu menutupnya aplikasi *winbox* setelah dilakukan *scanning port* terkadang tidak terjadi, sehingga perlunya ada pengembangan dalam *rules* yang di buat pada fitur tersebut sehingga dapat menyesuaikan situasi jaringan saat *metode* IDS (*Intrusion Detection Sistem*) di terapkan
3. Pentingnya objek dalam penelitian ini, yakni untuk dapat menerima masukan dari tempat dimana *metode* yang akan diterapkan. Dalam hal ini penulis menyarankan untuk di terapkan pada skala ISP (*internet service provider*). Dimana dalam pengelolaan internet skala besar dapat di ketahui peforma dari IDS (*Intrusion Detection Sistem*) pada jaringan berskala sedang dan besar