

BAB V KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan dari hasil pengujian *Intrusion Detection System (IDS)* Snort dengan bot telegram, sehingga dapat diambil kesimpulan sebagai berikut :

1. Dengan menerapkan IDS Snort di server laboratorium SMK Pancasila 8 Slogohimo dengan menggunakan sistem operasi ubuntu 22.04 LTS ,administrator jaringan dapat memonitoring server jaringan ketika terjadi serangan dan dapat terhubung mengirimkan notifikasi ke administrator jaringan lewat aplikasi Telegram. IDS Snort merupakan metode yang perlu diterapkan dalam jaringan yang dapat mendeteksi serangan ,sehingga administrator dapat melakukan pencegahan.
2. IDS Snort dapat melakukan pendeteksian ping yang menuju ke server dengan metode pengujian icmp , Port Scanning dengan metode pengujian menggunakan tools nmap dan dapat mendeteksi serangan *DDoS Attack* (TCP,UDP) dengan aplikasi LOIC dan TCP Syn Flood dengan tools hping3 yang telah disesuaikan dengan rules yang dibuat. Sehingga snort dapat mengirimkan alert pendeteksian serangan ke administrator lewat aplikasi telegram. Pada pengiriman alert dari snort ke administrator lewat aplikasi telegram ada jeda waktu pengirimannya yaitu pada pengujian ping ke server jeda waktu untuk mengirimkan alert selama 30 detik dari waktu pendeteksian, 44 detik dari waktu pendeteksian dari ip berbeda. Pengujian yang dilakukan port scanning terdapat jeda waktu pengiriman kepada pihak administrator selama 3 detik dari waktu pendeteksian , 2 detik dari waktu pendeteksian yang berbeda ip. Sedangkan pada pengujian serangan *DDoS attack* dengan metode TCP ,UDP dan TCP Syn Flood terdapat jeda waktu pada *DDoS attack* TCP dan UDP selama 1 detik dan jeda waktu 1 detik pada pengujian serangan *DDoS attack* TCP dari ip berbeda.

5.2. Saran

Berdasarkan hasil pengujian dan pembahasan yang telah dilakukan ,masih banyak kekurangan dari sistem .Dalam penelitian ini penulis berharap lebih dikembangkan mengenai penelitian IDS sehingga sistem dapat berfungsi secara optimal adalah sebagai berikut:

1. Penginstallan snort versi terbaru supaya fitur-fitur yang didalamnya dapat dioptimalkan dengan baik.
2. Penambahan rules untuk pendeteksian sehingga sistem dapat mendeteksi serangan-serangan yang terjadi.
3. Secara default snort berjalan sebagai IDS maka dari itu bisa dikembangkan kembali ke Intrusion Prevention System (IPS).
4. Ditingkatkan lagi pendeteksian jaringan bukan hanya skala LAN tetapi dapat mencakup skala MAN dan WAN.
5. Dan dikembangkan lagi untuk peringatan ke aplikasi telegram .Mulai dari fitur notifikasi dan pengaktifan snort otomatis untuk mengirimkan notifikasi dari snort.