

BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan pembahasan pada bab-bab yang telah diuraikan sebelumnya mengenai implementasi dan evaluasi keamanan jaringan yang menggunakan sistem IDS di sekolah SMKN 1 Kota Jambi, maka dapat disimpulkan beberapa hal sebagai berikut :

1. Berdasarkan seluruh rangkaian kegiatan yang dilakukan, dapat disimpulkan bahwa penerapan sistem keamanan jaringan menggunakan *Snort* di LAB TJKT SMKN 1 Kota Jambi berjalan dengan baik. Melalui proses implementasi, *Snort* berhasil dipasang dan dikonfigurasi pada mesin sensor yang terhubung ke jaringan lokal sekolah. Sistem ini memanfaatkan *software open source* seperti Ubuntu 20.04 serta beberapa pendukung lain yang membantu proses pencatatan dan pemantauan lalu lintas jaringan.
2. Dengan adanya *Snort*, lalu lintas data yang masuk dan keluar dari jaringan sekolah dapat terpantau secara menyeluruh. Dari hasil pengujian yang dilakukan, *Snort* terbukti mampu mendeteksi berbagai aktivitas mencurigakan yang sengaja disimulasikan, seperti serangan *port scanning*, serangan DDoS, dan percobaan *brute force*. Masing-masing percobaan serangan tersebut berhasil memicu peringatan atau *alert*, sehingga *administrator* jaringan dapat mengetahui adanya potensi ancaman lebih awal.

Dengan demikian, kehadiran sistem IDS berbasis *Snort* di LAB TJKT SMKN 1 Kota Jambi memberikan manfaat nyata dalam meningkatkan keamanan jaringan. Tidak hanya dapat mendeteksi serangan lebih cepat, tetapi juga membantu pihak sekolah meminimalkan risiko gangguan dan kebocoran data di lingkungan laboratorium. Implementasi ini diharapkan dapat menjadi langkah awal bagi sekolah untuk semakin sadar pentingnya keamanan jaringan, sekaligus menjadi contoh penerapan teknologi IDS yang dapat terus dikembangkan di masa mendatang.

5.2 SARAN

Berdasarkan hasil penelitian mengenai implementasi sistem deteksi intrusi (IDS) pada jaringan SMK Negeri 1 Kota Jambi, peneliti mengajukan beberapa saran sebagai berikut:

1. Disarankan agar pengelola jaringan secara rutin melakukan pemeliharaan dan pembaruan terhadap sistem IDS guna memastikan kinerja sistem tetap optimal dalam mendeteksi dan merespons berbagai ancaman yang terus berkembang serta melakukan evaluasi dan penyesuaian secara berkala terhadap aturan (*rules*) IDS.
2. Disarankan untuk mengintegrasikan sistem IDS dengan perangkat keamanan jaringan lainnya, seperti *firewall* dan sistem pencegahan intrusi (IPS), sehingga membangun lapisan keamanan yang lebih komprehensif dan efektif