BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil evaluasi implementasi sistem IDS pada jaringan nirkabel STMIK AMIKOM Yogyakarta, maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Sistem IDS sudah berjalan dengan baik dalam mengamati lalu-lintas paket data dengan memberikan informasi total paket tiap protokol pada jaringan nirkabel STMIK AMIKOM Yogyakarta dengan akurat.
2. Sistem IDS mampu memberikan informasi total paket baik yang keluar maupun masuk melalui tiap *port* (TCP dan UDP), sehingga memudahkan pengguna untuk mengetahui *port – port* mana saja yang *traffic*-nya terlalu tinggi dari keadaan normal dan yang bekemungkinan mengganggu kinerja keseluruhan sistem pada jaringan ataupun ancaman lainnya.
3. Sistem IDS mampu untuk menangkap dan menampilkan informasi setiap paket yang dianggap sebagai serangan atau berbahaya sesuai dengan *rules* yang sedang aktif.
4. Sistem IDS dibuat berbasiskan *web* sehingga pengguna dapat dengan mudah mengakses sistem ini dimanapun dan kapanpun.
5. Sistem IDS dapat berjalan selama 24 jam penuh pada jaringan tanpa mengganggu kinerja sistem lain dan juga aktivitas para pengguna Wi-Fi STMIK AMIKOM Yogyakarta karena sistem IDS ini hanya

mengambil *mirror packet* yang dikirim maupun diterima oleh para pengguna *hotspot* untuk kemudian dianalisis.

6. Sistem IDS menggunakan sistem deteksi *knowledgebase* dalam menentukan paket – paket *event*, oleh karena itu masih banyak ditemukan *event* yang bersifat *false positive*.
7. Mekanisme sistem kerja snort dan BASE yang telah berhasil diimplementasikan dengan baik. Dalam pengujian sistem snort dan BASE yaitu dengan menggunakan *ping attack*, *port scanning*, dan Digital Blaster.

5.2 Saran

Berdasarkan hasil evaluasi sistem IDS yang telah diimplementasikan, maka penulis memberikan saran yang diharapkan dapat berguna dalam meningkatkan sistem keamanan jaringan nirkabel STMIK AMIKOM Yogyakarta untuk menjadi lebih optimal. Saran – saran yang dapat disampaikan antara lain :

1. Sistem IDS saat ini menggunakan metode deteksi *knowledgebase* yaitu mengenali *malicious packet* dari *database rule* yang berisi *signature* serangan. Untuk pengembangannya, sistem IDS sebaiknya dilengkapi dengan metode pendeteksian serangan lebih lanjut dimana sistem dapat mengenali pola – pola serangan baru tanpa membandingkannya dengan *database rule*.
2. Sistem IDS hanya bisa melakukan *monitoring* jaringan, akan lebih baiknya IDS yang diterapkan dapat melakukan pencegahan dari serangan yang terjadi secara otomatis.