BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil penelitian mengenai "Analisis Dan Implementasi Bentuk Serangan Pada Jaringan Dengan *Wifislax* Dan *Fluxion* Menggunakan Metode *Evil Twin Attack*" yang dilakukan dengan dilakukannya percobaan (metode eksperimental). Penulis menyimpulkan bahwa:

1. *Wifislax* mampu digunakan dalam bentuk *live* USB dan berjalan dengan baik serta memiliki tingkat ketepatan dalam melakukan serangan menggunakan *Fluxion* yang cukup tinggi dengan rata – rata waktu proses perintah adalah 33 detik.
2. *Evil twin attack* dapat berjalan dengan baik dan bisa menciptakan serangan akses poin palsu dengan cara mendapatkan handshake dari akses poin yang asli serta memberi paket deauth kepada akses poin yang sah untuk memutuskan jaringan antar klien agar dapat terhubung ke jaringan yang telah dibuat oleh *evil twin attack*.
3. Snort dapat menjadi WIDS (*wireless intrusion detection system*) di sistem operasi windows dan berjalan dengan baik serta mampu menjalankan perintah yang sudah penulis rancang.
4. Ketepatan Snort dalam menganalisis lalu lintas jaringan nirkabel pada penelitian ini adalah 80% dari 10 kali percobaan anomali aneh dapat terdeteksi dengan baik melihat indikasi yang di hasilkan melalui protokol

tcp, udp, dan icmp serta dapat mendeteksi protokol baru yang diciptakan melalui ipv6 multicast.

5.2. Saran

Berdasarkan kesimpulan yang ditarik dari hasil percobaan, maka penulis memberikan rekomendasi sebagai berikut:

1. *Wifislax* dapat digunakan secara optimal dengan kekuatan sinyal lebih dari 40% untuk mendapatkan hasil yang diharapkan.
2. Untuk menambah wawasan tentang jenis serangan jaringan nirkabel sehingga jika nantinya terjadi serangan *evil twin attack*.
3. Dengan penelitian ini diharapkan snort dapat dikembangkan untuk mengatasi jenis serangan *evil twin attack* bukan hanya sebagai media analisis saja.