BAB V
SIMPULAN, IMPLIKASI DAN REKOMENDASI

5.1 Simpulan

Berdasarkan hasil penelitian yang telah penulis lakukan didapat kesimpulan sebagai berikut:

1. Snort berhasil diimplementasikan sebagai sistem keamanan *server* dengan diintegrasikan menggunakan telegram sebagai media penerima laporan serangan, hal ini dibuktikan dengan kemampuan deteksi serangan *Slow http, POP3, Port Scanning,* DDoS, SNMP, ICMP, *SQL Injection*, XSS, dan *IP Spoofing* dan berhasil melaporkannya pada media telegram.
2. Hasil dari pengujian performa pendeteksian snort menunjukkan bahwa *rules* yang dibuat untuk mendeteksi serangan siber pada *server* bisa bekerja dengan baik yang dibuktikan dengan tingkat keberhasilan pengujian mencapai 100% dengan waktu deteksi serangan rata-rata 1 detik.
3. Hasil pengujian pengiriman notifikasi serangan yang dideteksi oleh snort bisa diterima oleh telegram. Hasil ini menunjukan telegram bisa digunakan sebagai media penerima laporan serangan, dengan waktu penerimaan rata-rata notifikasi 4 detik.

5.2 Implikasi

Implikasi dari penelitian yang dibuat antara lain sebagai berikut:

1. Pada penelitian yang telah dilakukan dan hasil yang sudah didapat instansi atau industri bisa menggunakan snort untuk menambah sistem keamanan pada *server* yang mereka miliki, dari hasil yang didapat snort memiliki tingkat efektifitas dalam mendeteksi dan melakukan tindakan pada serangan siber yang tinggi, dan memiliki integrasi dengan notifikasi telegram. Hasil dari penelitian ini dapat digunakan oleh administrator pada suatu instansi atau industri sebagai sistem peningkatan kewaspadaan terhadap serangan siber yang sedang marak saat ini.
2. Pada pengembangan sistem kedepannya bisa dilakukan kombinasi antara sistem keamanan snort dengan sistem keamanan lainnya seperti sistem

keamanan *firewall, Security Information and Event Management* (SIEM), sistem Pemantauan Lalu Lintas Jaringan (*NetFlow, sFlow*), dan sistem keamanan lainnya.

5.3 Rekomendasi

Berdasarkan penelitian yang sudah dilakukan dan temuan yang ditemukan ada beberapa saran yang bisa penulis sarankan untuk penelitian selanjutnya. Beberapa saran yang bisa diambil antara lain:

1. Pengujian sistem keamanan snort dapat dilakukan pada skala jaringan yang lebih luas dan lebih kompleks, ujicoba juga bisa dilakukan dengan melibatkan perangkat yang lebih beragam dan lebih banyak. Dengan melakukan uji coba seperti itu kinerja snort akan lebih teruji.
2. Penambahan jenis serangan yang diujikan kepada sistem keamanan snort bisa diilakukan agar snort bisa mendeteksi serangan yang lebih beragam terutama *rules* untuk mendeteksi virus yang saat ini sedang marak terjadi.
3. Pengujian sistem keamanan snort dilakukan dengan beban lalulintas serangan yang lebih besar, pada pengujian yang dilakukan dengan menambahkan beban lalu lintas serangan yang lebih besar kehandalan snort akan lebih teruji.
4. Penelitian snort dilakukan dengan memfokuskan sistem snort untuk mengurangi kesalahan yang dbuat oleh manusia sehingga kerentanan yang disebabkan oleh *human error* dapat di antisipasi oleh sistem.
5. Pengujian yang dilakukan menggunakan ip public ditambahkan lagi agar sistem bisa bekerja maksimal dalam melakukan pendeteksian dan pencegahan serangan melalui ip publik.