BAB V
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan pembahasan mengenai penelitian *Implementasi Intrusion Prevention System* (IPS) untuk Menganalisis Triad CIA terhadap Serangan Keamanan Jaringan Pada *Web Server* dapat diperoleh beberapa kesimpulan sebagai berikut:

1. Hasil pengujian IPS terhadap serangan yaitu paket yang dikirim oleh *attacker* cocok dengan *rule database* yang telah dibuat pada Snort sehingga serangan dapat terdeteksi sebagai ancaman dan menampilkan *alert* pada Snort. IPS mampu membedakan paket dari *attacker* secara tepat dan akurat dengan *option rule* yang digunakan sehingga hanya paket serangan yang akan dieksekusi dan *legal user* tidak dianggap sebagai paket serangan. Pada sisi pencegahan, serangan *Port Scanning* dan *Brute Force* dapat dengan mudah dicegah karena karakteristik serangan yang mudah dikenali dalam proses pencocokkan paket dengan *option rule* pada Snort. Hasil pengujian pada serangan DDoS, Snort hanya mempercepat waktu serangan untuk dapat diakses kembali. Serangan DDoS dengan jenis Slow HTTP tidak dapat sepenuhnya dicegah karena *option rule* yang belum mampu mengenali karakteristik dari serangan yang mengirimkan paket *header* tidak lengkap dengan jumlah yang banyak secara bertahap dan dengan mempertahankan waktu sesi koneksi.
2. Hasil pengujian pada serangan Port Scanning dan Brute Force yaitu *web server* terlindungi dan *attacker* tidak dapat mendapatkan informasi dan hak akses untuk dapat masuk ke dalam sistem *web server*. Pada serangan DDoS ketika terjadi serangan sebelum IPS diaktifkan yaitu penggunaan CPU dan RAM mengalami peningkatan dengan rata-rata penggunaan CPU sebesar 58% dan RAM sebesar 1,54GB dan terjadi penurunan dengan rata-rata penggunaan CPU sebesar 48,8% dan RAM sebesar 1,54GB atau dengan kata lain terjadi penurunan sebesar 9,2% pada penggunaan CPU pada saat Snort diaktifkan. Hasil pengujian pada serangan DDoS pada sisi *legal user* tidak dapat mengakses *web server* ketika terjadi serangan sebelum IPS diaktifkan dan pada saat IPS diaktifkan dengan *action rule drop* maka akan kembali dapat diakses pada detik

ke 160 sedangkan jika menggunakan *action rule reject* dapat diakses kembali pada detik 145 dimana normalnya *attacker* dapat memulihkan *web server* pada detik ke 165.

5.2 SARAN

Implementasi pengujian Snort dan *IPTables* sebagai IPS pada penelitian ini masih terdapat kekurangan serta keakuratan *rule* untuk mengeksekusi serangan DDoS dengan jenis *Slow* HTTP sehingga pada penelitian berikutnya diharapkan dapat merumuskan *rule* yang lebih spesifik dengan karakteristik serangan. Penelitian berikutnya juga dapat mengganti metode pendeteksian Snort yang lain seperti *anomaly-based* pada NIPS ataupun dengan penggabungan teknologi lain seperti SDN, *load balancer* atau *Cloud Computing.* Pada sisi pengamanannya dapat mengganti atau menambahkan jenis *firewall* terutama untuk pencegahan serangan *Slow* HTTP. Pada penelitian berikutnya diharapkan dapat menggunakan serangan yang lain yang berbeda karakteristiknya sehingga menambah referensi tentang analisis karakteristik serangan terhadap aspek Triad CIA.