BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Setelah dilakukan penelitian, simulasi sistem keamanan jaringan HIPS dengan metode *anomaly detection* dapat berjalan sesuai dengan skenario pada penelitian. Dalam praktiknya sistem ini dapat mendeteksi dan memblokir serangan yang ada.
2. Dilihat dari *log* yang diperoleh dari pengujian menunjukan bahwa akurasi pendeteksian dan pemblokiran dari aplikasi Snort sudah cukup baik seperti saat pengujian *ICMP Flood* dapat mendeteksi dan memblokir 72550 dari 72600 serangan terdapat 10 serangan yang lolos diakibatkan dari aturan yang dibuat membutuhkan 10 serangan untuk menjalankan aturan *ICMP Flood*, saat pengujian *UDP Flood* dapat mendeteksi dan memblokir 98418 dari 98718 serangan terdapat 378 serangan yang lolos diakibatkan dari aturan yang dibuat membutuhkan 400 serangan untuk menjalankan aturan *UDP Flood*, saat pengujian *SYN Flood* dapat mendeteksi dan memblokir 25950 dari 26950 serangan terdapat 489 serangan yang lolos diakibatkan dari aturan yang dibuat membutuhkan maksimal 500 serangan untuk menjalankan aturan *SYN Flood*, dan saat pengujian *FTP Bruteforce* dapat mendeteksi dan memblokir 141 dari 151 serangan terdapat 10 serangan yang lolos diakibatkan dari aturan yang dibuat membutuhkan 10 serangan untuk menjalankan aturan *ICMP Flood.*
3. Performansi dari sistem keamanan jaringan HIPS dengan metode anomaly detection terhadap CPU *usage*, *throughput, delay, jitter*, dan *packet loss* didapatkan bahwa terdapat peningkatan pada CPU *usage* disebabkan adanya serangan yang lolos diakibatkan untuk menjalankan aturan serangan yang telah dibuat, perlu meloloskan beberapa serangan sesuai dengan kondisi aturan yang dibuat. *Throughput* mengalami peningkatan disebabkan serangan yang lolos untuk menjalankan aturan serangan, membuat jumlah data yang diterima saat pengujian dimulai cukup banyak dibandingkan saat keadaan

normal. *Delay* dan *jitter* mengalami penurunan disebabkan untuk menjalankan aturan serangan perlu meloloskan beberapa serangan yang membuat nilai total *delay* dan *jitter* semakin kecil dibandingkan jumlah paket yang datang. *Packet loss* memperoleh nilai nol persen disetiap pengujian dikarenakan paket sudah terfilter terlebih dahulu oleh HIPS.

5.2 Saran

1. Pada peneliti selanjutnya sebaiknya dalam pengambilan data untuk lebih teliti dikarenakan jumlah data yang banyak.
2. Pada peneliti selanjutnya sebaiknya untuk dapat melakukan pengujian dengan jenis serangan yang lain seperti *SQL Injection.*
3. Pada peneliti selanjutnya sebaiknya untuk dapat melakukan percobaan IPS dengan jenis *Network-based* atau *Wireless-based*.