

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan analisa dan perbandingan yang telah dilakukan baik dari sisi implementasi maupun pengujian menggunakan parameter pengukuran tingkat akurasi, penggunaan CPU dan memori, dan respon waktu tindakan oleh IPS terhadap serangan dapat diambil kesimpulan sebagai berikut.

1. Dalam hal penggunaan CPU dan memori, IPS Snort lebih unggul dengan persentase penggunaan CPU sebesar 4,5 % dan RAM sebesar 30,0 % dibandingkan dengan IPS Suricata yang menggunakan CPU sebesar 6,2 % dan RAM sebesar 30,9 % ketika IPS dijalankan secara normal tanpa ada serangan yang terjadi.
2. IPS Suricata lebih baik dibandingkan dengan IPS Snort dalam mendeteksi dan memblokir aktifitas serangan berupa *port scanning* menuju server, dengan perbandingan jumlah paket yang di *drop* oleh IPS Suricata sebanyak 2122 dan jumlah paket yang di *drop* oleh IPS Snort sebanyak 1009. Sedangkan aktifitas serangan berupa *ping of attack* keduanya memiliki kemampuan deteksi dan memblokir paket data yang sama.
3. Dalam hal respon waktu, IPS Snort lebih baik dibandingkan dengan IPS Suricata dalam hal kecepatan waktu antara mendeteksi dan memblokir aktifitas serangan berupa *ping of attack* dan *port scanning*. IPS Snort memblokir serangan *ping of attack* dalam waktu 1 detik sedangkan IPS

Suricata 2 detik dan untuk serangan *port scanning* dalam waktu 3 detik sedangkan IPS Suricata 5 detik.

5.2 Saran

Adapun saran yang dapat dikembangkan penelitian selanjutnya antara lain adalah sebagai berikut.

1. Pengujian dilakukan dengan lebih banyak jenis serangan sehingga didapatkan hasil performa yang lebih baik.
2. Implementasi dan pengujian dilakukan pada jaringan yang lebih luas seperti WAN atau jaringan internet.

