BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan pada bab-bab sebelumnya maka pada bab kesimpulan ini penulis dapat mengambil kesimpulan mengenai hasil perbandingan IDS Snort, Suricata dan Ossec dalam mendeteksi serangan DoS terhadap Web Mail Server diantaranya sebagai berikut :

1. Dalam melakukan perhitungan pendeteksian serangan dengan menggunakan parameter jumlah rata-rata prosentase serangan terdeteksi *(captured packets)*, IDS Snort lebih banyak melakukan pendeteksian daripada IDS Suricata dan IDS Ossec. Selama percobaan pengujian serangan DoS terhadap Web Mail Server sebanyak 20 kali pengujian, nilai rata-rata IDS Snort dapat mendeteksi serangan sebanyak 92,4% kemudian IDS Ossec dengan 85,9%, dan yang terakhir IDS Suricata sebanyak 1,4% saja. IDS Server yang paling Efektif dalam percobaan ini adalah IDS Snort dan Efisien dalam penggunaan sumber daya ram, penjelasan tentang sumber daya di jelaskan di point 2 dan 3. IDS Server yang dapat mendeteksi serangan dengan prosentase terbanyak dan Standar Deviasi yang masih dalam standart, merupakan IDS yang paling Efektif dalam mendeteksi dan menangkal paket data DoS.
2. Dalam melakukan pengujian serangan DoS terhadap Web Mail Server, masing-masing IDS membutuhkan sumber daya cpu dan ram yang berbeda untuk mendeteksi paket serangan. Efsiensi penggunaan *cpu* dan *ram*

3. diantara ketiga IDS didapatkan dengan mencari rata-rata prosentase selisih pergerakan sebelum dan saat terjadi serangan dengan nilai terkecil. IDS Ossec merupakan IDS yang paling efisien dalam melakukan pekerjaan mendeteksi dan menanggulangi serangan DoS yaitu dengan rata-rata peningkatan sumberdaya CPU sekitar 58,4%, lalu diikuti dengan IDS Snort (66,3%) dan IDS Suricata (68,2%).
4. Efisiensi penggunaan sumberdaya RAM terbaik yaitu yang memiliki pergerakan rerata prosentasi RAM paling rendah adalah IDS Snort (8,8%), jika dibanding dengan IDS Ossec(18%) dan IDS Suricata (19,5%).

5.2 Saran

Saran yang dapat penulis berikan untuk penelitian selanjutnya adalah sebagai berikut.

1. Pengujian yang dilakukan peneliti di dokumen ini didasarkan pada IDS dengan *rule script default*, tidak terdapat kostumisasi spesifik pada protocol imap, pop dan protocol pendukung web mail lainnya. Peneliti menyarankan agar menggunakan konfigurasi yang lebih spesific terhadap rule yang digunakan disetiap IDS.
2. Pengujian yang dilakukan peneliti pada dokumen ini untuk mencari IDS yang paling efisien didasarkan pada performa sumberdaya cpu dan ram saja, penelitian selanjutnya dapat dilakukan dengan menganalisa performa peripheral lainnya seperti kartu jaringan *(lan card), badnwidth / troughput data transfer rate, storage* dan lain sebagainya.

3. Pengujian yang dilakukan peneliti pada dokumen ini menggunakan Virtual machine yang berjalan pada sebuah host, pengujian selanjutnya bisa dilakukan pada mesin server fisik independen