BAB V

PENUTUP

2.1. Kesimpulan

Berdasarkan hasil penelitian mengenai "Analisis Perbandingan Kinerja Snort dan Suricata Sebagai *Intrusion Detection System* dalam Mendeteksi Serangan SYN Flood pada *Web Server* Apache" yang dilakukan dengan percobaan. Penulis menyimpulkan bahwa :

1. Berdasarkan pengujian menggunakan parameter jumlah serangan terdeteksi, IDS Snort lebih banyak melakukan pendeteksian serangan dibandingkan dengan IDS Suricata setelah melakukan 30 kali pengujian. Hal ini dapat dibuktikan dari data yang telah didapat yaitu IDS Snort dapat mendeteksi serangan dengan rata-rata performa sebanyak **84,97%** dan memiliki standar deviasi **167248,43** dibandingkan IDS Suricata sebanyak **74,62%** dan memiliki standar deviasi **128160,39** dari 30 kali pengujian.
2. Berdasarkan pengujian menggunakan parameter penggunaan resource CPU Snort lebih baik dibandingkan IDS Suricata setelah melakukan pengujian sebanyak 30 kali, data yang diperoleh dari rata-rata rasio penggunaan CPU sebanyak **78,31%** dibandingkan IDS Suricata yang memperoleh rata-rata penggunaan CPU sebanyak **80,08%**. Namun dalam penggunan RAM, IDS Suricata lebih unggul dengan rata-rata rasio penggunaan RAM sebanyak **11,36%** dibandingkan Snort dengan rata-rata rasio penggunaan RAM sebanyak **23,89%**

3. Berdasarkan pengujian dengan menggunakan parameter efektifitas serangan yang diperoleh dari uncaptured paket, IDS Suricata lebih baik dibandingkan IDS Snort setelah melakukan pengujian sebanyak 30kali, data yang diperoleh dari rasio efektifitas IDS Snort memiliki rasio uncaptured paket sebanyak **68,2%** sedangkan Suricata sebanyak **3,42%.**
4. Dari segi fitur Snort lebih unggul karena dapat menampilkan infromasi data serangan dan data *outstanding* paket secara langsung, sedangkan Suricata harus membuka file log terlebih dahulu untuk melihat informasi data serangan dan Suricata tidak memiliki informasi data *outstanding* paket.
5. Maka hasil pengujian dapat disimpulkan bahwa IDS Snort lebih unggul dalam pendeteksian serangan, penggunaan resource CPU, dan fitur informasi data serangan, sedangkan Suricata lebih unggul dalam efektivitas serangan dari data uncaptured paket dan penggunaan RAM.

2.2. Saran

Berdasarkan kesimpulan yang ditarik dari hasil percobaan, maka penulis memberikan rekomendasi sebagai berikut:

1. Untuk penelitian kedepannya disarankan menggunakan IDS selain IDS Snort dan Suricata.
2. Bagi peneliti selanjutnya, disarankan untuk menggunakan serangan dan tools yang berbeda.
3. Peneliti selanjutnya, disarankan untuk menggunakan lebih banyak parameter pengujian.