ABSTRAK

KOMPARASI KINERJA *INTRUSION DETECTION SYSTEM (IDS)* *SNORT* DAN *SURICATA* DALAM MENDETEKSI SERANGAN *FLOODING*

Oleh :

REXY FAHREZI
18312079

Permasalahan tentang serangan terhadap suatu jaringan sering terjadi, hal tersebut dikarenakan semakin berkembangnya jaringan maka semakin berkembang juga ancaman dan resiko terhadap jaringan tersebut salah satu contoh serangan terhadap jaringan yang sering terjadi adalah serangan *Flooding* yang dilakukan untuk membanjiri perangkat atau *server* dengan banyak paket dan permintaan yang berlebihan. *Snort* dan *Suricata* adalah beberapa contoh dari Intrusion *Detection System (IDS)* populer yang mampu mendeteksi serangan didalam jaringan agar dapat mendeteksi sehingga mencegah dampak lebih lanjut dari serangan tersebut.

Oleh sebab itu, penulis melakukan komparasi untuk membandingkan kinerja dari *Snort* dan *Suricata* dalam mendeteksi serangan *Flooding* agar dapat menentukan mana yang lebih baik dari segi kecepatan deteksi, banyak serangan yang dapat dideteksi dan penggunaan sumber daya *RAM* dan *CPU*. Hasil dari analisis komparasi nilai kinerja kedua *IDS* menunjukkan *Snort singlethread* lebih unggul di nilai rata-rata "CPU *usage*" sebesar 31,789% dan kecepatan deteksi sebesar 1,3107222 detik. *Snort multithread* dapat mendeteksi serangan lebih banyak sebesar 99,5754%. Sedangkan *Suricata* menggunakan sumberdaya "RAM *usage*" lebih sedikit unggul yaitu sebanyak 2,876%.

Kesimpulan dari penelitian yang telah dilakukan berdasarkan semua pengujian setiap IDS tersebut dapat menunjukkan bahwa *Snort* lebih unggul daripada *Suricata* untuk mendeteksi serangan *Flooding* dalam hal kecepatan deteksi, banyaknya serangan yang dapat dideteksi dan penggunaan sumber daya CPU. Sedangkan dalam penggunaan sumber daya RAM, *Suricata* lebih baik daripada *Snort*.

Kata Kunci : Kinerja *Intrusion Detection System (IDS), Snort, Suricata*