BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. Berdasarkan parameter kecepatan dan akurasi deteksi, Hasil pengujian menunjukkan bahwa Suricata mampu mendeteksi serangan Slowloris yang dijalankan pada server web. Deteksi ini ditunjukkan oleh munculnya alert pada log Suricata setiap kali serangan Slowloris dilakukan, sesuai dengan aturan deteksi yang telah dikonfigurasi. Dari data hasil pengujian, Suricata menghasilkan rata-rata waktu deteksi sebesar 0,346 detik. Selain itu, tingkat akurasi deteksi menunjukkan nilai rata-rata sebesar 72,84%, yang menandakan bahwa sebagian besar aktivitas serangan Slowloris berhasil terdeteksi selama rangkaian pengujian. Dengan demikian, hasil pengujian menunjukkan bahwa performa Suricata dalam mendeteksi serangan Slowloris dapat dilihat dari parameter kecepatan dan akurasi deteksi yang diperoleh selama pengujian.

2. Berdasarkan hasil pengujian, penggunaan Suricata sebagai Intrusion Detection System (IDS) selama serangan Slowloris mempengaruhi konsumsi sumber daya sistem, namun tidak mengganggu proses deteksi yang dilakukan. Data menunjukkan bahwa rata-rata penggunaan CPU meningkat dari 2,028% menjadi 7,25% saat serangan, penggunaan RAM meningkat dari 59,85 MB menjadi 66,24 MB, dan penggunaan bandwidth meningkat dari 2,038 kbps menjadi 256,72 kbps selama serangan berlangsung. Meskipun terjadi peningkatan pada parameter

penggunaan resource tersebut, Suricata tetap mampu memberikan peringatan dini dengan tingkat akurasi deteksi rata-rata sebesar 72,84%. Hal ini menunjukkan bahwa Suricata tetap dapat menjalankan fungsi deteksinya selama serangan berlangsung dan mendukung ketahanan server dari sisi pemantauan dan deteksi, tanpa menyebabkan penggunaan sumber daya terlalu tinggi yang dapat menghambat kinerja sistem.

5.2 Saran

Berikut ini saran untuk penelitian selanjutnya :

1. Penelitian selanjutnya dapat menguji performa Suricata terhadap jenis serangan lain seperti HTTP Flood, SYN Flood, atau serangan berbasis aplikasi layer-7 lainnya. Dengan demikian, kemampuan Suricata dapat dievaluasi tidak hanya pada serangan Slowloris, tetapi juga pada pola serangan yang memiliki karakteristik berbeda.

2. Pengujian selanjutnya disarankan menggunakan perangkat dengan spesifikasi yang lebih tinggi, terutama kapasitas RAM dan CPU, atau dilakukan pada lingkungan server produksi (real server). Hal ini bertujuan untuk mengetahui performa Suricata pada beban trafik yang lebih besar dan kondisi yang lebih mendekati implementasi nyata.

3. Penelitian berikutnya dapat mengembangkan sistem dengan mengombinasikan Suricata dan mekanisme respons otomatis, seperti integrasi dengan firewall (misalnya pemblokiran IP otomatis) atau sistem Intrusion Prevention System (IPS). Dengan cara ini, sistem tidak

hanya mendeteksi serangan, tetapi juga dapat langsung melakukan tindakan pencegahan.

4. Proses pencatatan dan analisis data dapat dikembangkan menggunakan sistem monitoring atau dashboard otomatis, seperti integrasi dengan tools visualisasi log. Hal ini bertujuan agar proses evaluasi performa IDS menjadi lebih cepat, terstruktur, dan meminimalkan kesalahan pencatatan manual.