BAB 5

PENUTUP

5.1. Kesimpulan

Setelah melakukan hasil dan pembahasan penelitian yang telah dilakukan, maka diperoleh hasil kesimpulan sebagai, berikut:

1. Berdasarkan hasil pengujian yang telah dilakukan IDS Suricata memperoleh hasil yaitu Sistem mampu mendeteksi serangan berupa Slowloris, *Nmap* scan, DoS, dan PingFlood.
2. IDS Suricata bekerja dengan baik dalam mendeteksi paket-paket ancaman untuk waktu yang dibutuhkan kurang lebih 4 menit tergantung dari koneksi internet yang digunakan.
3. Intrusion Detection System bersifat pasif, Sistem ini hanya akan bekerja jika terjadi serangan saja.

5.2. Saran

Untuk pengembangan penelitian ini, ada beberapa saran yang dapat diberikan :

1. Penting untuk menganalisis kinerja sistem IDS Suricata dalam skenario yang melibatkan jaringan yang lebih besar dan lebih kompleks. Uji coba yang melibatkan beban lalu lintas yang tinggi dan berbagai jenis serangan akan memberikan wawasan tentang skalabilitas sistem dan bagaimana itu mempengaruhi waktu respons dan kehandalan deteksi.
2. Melakukan perbandingan yang lebih luas antara Suricata dan sistem deteksi intrusi lainnya akan membantu dalam memahami keunggulan dan kelemahan masing-masing sistem. Ini dapat dilakukan dengan mengimplementasikan beberapa IDS populer dan membandingkan kinerja, akurasi, dan kemudahan penggunaannya. Perbandingan semacam ini akan memberikan wawasan yang berharga dalam memilih dan mengembangkan solusi IDS yang optimal.