BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan dari seluruh tahapan dari perancangan hingga proses pengujian dari penelitian Skripsi ini maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Untuk membangun Sistem IDS Suricata dibutuhkan beberapa modul tambahan agar *administrator* lebih mudah dalam me*monitor* dan menganalisa packet, yaitu Logstash, Elasticsearch dan Kibana.
2. Modul tersebut bekerja sama untuk mentranslasikan log mentah dari Suricata menjadi bentuk yang mudah dipahami.
3. Sistem dapat mendeteksi serangan atau tidak tergantung dengan pola serangan yang dikonfigurasi didalam *file rules*.
4. Instalasi Kibana sebagai *Web Interface* dapat mempermudah *administrator* dalam me*monitor* dan menganalisa setiap *log* yang dihasilkan oleh Suricata.

5.2 Saran

Penulis menyadari bahwa penelitian ini masih memiliki banyak kekurangan dan jauh dari sempurna. Harapan penulis agar nantinya pembaca dapat mengembangkan dan memperluas penelitian ini. Oleh karena itu penulis memberikan beberapa saran sebagai berikut:

1. Pengujian masih dilakukan dalam lingkup jaringan lokal dan menggunakan IP *Private*, diharapkan agar pengujian berikutnya dilakukan pada lingkup jaringan yang lebih luas seperti internet dengan menggunakan VPS.
2. Suricata pada penelitian ini menggunakan mode IDS yang hanya mampu memonitor *traffic* dijaringan dan melaporkan *traffic* kepada *administrator*. Diharapkan pada penelitian selanjutnya, Suricata dapat dikembangkan menjadi IPS agar sistem juga dapat melakukan tindakan preventif jika terjadi serangan pada jaringan.
3. Jenis pengujian serangan yang dilakukan masih terlalu sedikit, diharapkan agar pada penelitian berikutnya, jenis pengujian dapat dibuat lebih beragam.