# BAB V
# KESIMPULAN DAN SARAN

## 5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, peneliti dapat mengambil kesimpulan sebagai berikut:

1. *Suricata* pada platform *SELKS* dan *Security Onion* dapat mendeteksi serangan *SYN Flood* berdasarkan *rule* yang dibuat dengan baik.
2. Suricata pada platform SELKS memiliki tingkat akurasi lebih tinggi dengan rata-rata 99,91% dibandingkan Security Onion di angka 99,87% dengan selisih 0,04%.
3. Dari segi penggunaan sumber daya sistem *CPU* dan Memori, Suricata pada Security Onion menggunakan CPU lebih efisien dari SELKS dengan rata-rata penggunaan yaitu 28,99% dan standar deviasi bernilai 3,2 dibandingkan SELKS di angka 34,63% dengan standar deviasinya yaitu 5,03. Berdasarkan penggunaan memori, Security Onion sedikit kurang efisien dengan rata-rata penggunaan 2,73% dengan standar deviasi 0,38 dibandingkan SELKS yaitu sebesar 1,98% diikuti standar deviasinya di angka 0,08.
4. Meskipun penggunaan memori Suricata pada platform Security Onion sedikit kurang efisien, *Security Onion* tetap lebih unggul karena dapat mendekati tingkat akurasi deteksi *SELKS* tanpa mengorbankan penggunaan sumber daya *CPU* yang lebih tinggi dan memori yang berlebihan.
5. *Security Onion* memiliki skabilitas lebih baik karena sudah menggunakan *containerization* berbasis *docker* dan dapat dijalankan pada skala jaringan kecil maupun besar. Namun proses manajemen *ruleset* pada *Security Onion* hanya dapat dilakukan secara manual pada sistem. Berbeda dengan *SELKS*, meskipun skalabilitas nya kecil tetapi memiliki aplikasi web yang mendukung manajemen *ruleset Suricata* sehingga memudahkan admin jaringan dalam mengatur *ruleset* yang ingin diimplementasikan.

## 5.2 Saran

Adapun saran dari penelitian ini yaitu:

1. Menggunakan platform *virtual machine* lain seperti *VMware* atau bahkan *cloud computing*.
2. Menggunakan *ruleset* dari organisasi atau pengembang seperti *ET Open, Suricata PT Open*.