# BAB V
# KESIMPULAN DAN SARAN

## 1.1 KESIMPULAN

Berdasarkan Penelitian mengenai perbandingan Snort, Suricata dan Zeek dalam mendeteksi serangan jaringan pada komputer diperoleh beberapa kesimpulan sebagai berikut :

1. Hasil pengukuran QOS yang didapatkan pada uji coba serangan ICMP *Flood* yaitu pada saat Snort diaktifkan nilai *jitter* menurun dari 7,54 ms menjadi 7,37 ms, kemudian pada serangan ICMP *Flood* yaitu pada saat Suricata diaktifkan nilai *jitter* meningkat dari 2,62 ms menjadi 6,2 ms, selanjutnya pada serangan ICMP *Flood* yaitu pada saat Zeek diaktifkan nilai *jitter* menurun dari 1,25 ms menjadi 0,88 ms. kemudian nilai *throughput* pada snort meningkat dari 24453 bit/s menjadi 26485 bit/s. selanjutnya nilai *throughput* pada suricata meningkat dari 28939 bit/s menjadi 32400 bit/s, dan nilai *throughput* pada Zeek menurun dari 25777 bit/s menjadi 18438 bit/s. dan nilai *delay* pada Snort menurun dari 245,78 ms menjadi 223,53 ms. Selanjutnya nilai *delay* pada Suricata menurun dari 207,37 ms menjadi 183,85 ms, sedangkan nilai *delay* pada Zeek menurun dari 48,85 ms menjadi 45,59 ms, untuk pengukuran *packet loss* pada Snort menurun dari 0,46% ms menjadi 0,32%, sedangkan *packet loss* pada Suricata tidak ada perubahan sama sama sebesar 0,44% dan nilai *packet loss* pada Zeek meningkat dari 0,15% menjadi 0,25%.
2. Pada pengujian serangan SYN *flooding*, saat Snort, Suricata dan Zeek diaktifkan, nilai *delay* dan *jitter* meningkat yaitu pada saat Snort diaktifkan nilai *jitter* menurun dari 2,86 ms menjadi 1,81 ms, kemudian nilai *delay* menurun dari 197,23 ms menjadi 187,17 ms. Sedangkan, pada saat Suricata diaktifkan nilai *jitter* menurun dari 7,03 ms menjadi 5,63 ms, kemudian nilai *delay* menurun dari 114,16 ms menjadi 104,59 ms. Sedangkan pada saat Zeek diaktifkan nilai jitter menurun dari 2,82 ms menjadi 2,02 ms, kemudian nilai *delay* menurun dari 32,66 ms menjadi 17,9 ms. Untuk hasil pengukuran parameter *throughput* mengalami kenaikan yaitu untuk Snort meningkat dari 29107 bit/s menjadi 29701 bit/s dan untuk Suricata *throughput* menurun dari 20325 bit/s menjadi 16029 bit/s. dan untuk Zeek *throughput* meningkat dari 14966 bit/s menjadi 21970 bit/s. Untuk pengukuran *packet loss* pada Snort meningkat dari 0,51% ms menjadi 0,56%, sedangkan *packet loss* pada Suricata menurun dari 0,32% menjadi 0,29% dan *packet loss* pada Zeek menurun dari 0,66% menjadi 0,14%.

3. Hasil perbandingan performansi QOS pada Snort, Suricata dan Zeek dalam mendeteksi serangan ICMP *Flood* yaitu Suricata lebih baik berdasarkan nilai *throughput* dibandingkan dengan Snort dan Zeek dan jika diukur dari segi parameter *delay*,*Jitter* dan *Packet Loss* Zeek lebih baik dibandingkan dengan Snort dan Suricata.
4. Pada pengujian serangan SYN *flooding* dari segi parameter *throughput* dan *jitter* Snort lebih baik dibandingkan Suricata dan Zeek dan jika diukur dari segi parameter *delay* dan *Packet Loss* Zeek lebih baik dibandingkan Snort dan Suricata.

## 1.2 SARAN

1) Pada penelitian selanjutnya, sebaiknya dapat menambahkan parameter untuk pengujian perfomansi selain menggunakan *parameter Quality of Service* (QOS).
2) Pada penelitian berikutnya dapat menggunakan Serangan selain ICMP *Flood* dan SYN *Flooding*

Pada penelitian berikutnya dapat menambahkan *tools* selain Snort, Suricata dan Zeek.