BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini melakukan analisis perbandingan terhadap berbagai alat NIDS rilisan terbaru ketika penulis melakukan penelitian ini, yang diantaranya yaitu *Snort*, *Suricata*, dan *Zeek*, dengan serangan PS dan DDoS. Penelitian ini memperoleh informasi tentang performa yang berbeda-beda pada setiap NIDS yang digunakan. Hasil penelitian dapat disimpulkan sebagai berikut:

1. *Suricata* unggul dalam mendeteksi intrusi pada serangan PS dan DDoS, hal ini dapat ditunjukan dengan nilai persentase TPR yang dimiliki *Suricata* paling tinggi dibandingkan nilai persentase TPR *Zeek* dan *Snort*. *Zeek* unggul dalam kecepatan mendeteksi serangan per menit, hal ini dapat ditunjukan dengan nilai DR/m yang dimiliki *Zeek* paling tinggi dibandingkan nilai DR/m *Snort* dan *Suricata*, hal ini membuat *Zeek* sangat cocok untuk diterapkan pada lalu lintas jaringan kecepatan tinggi. Parameter *resource usage* pada penelitian ini memiliki hasil yang variatif. Pada CPU *usage*, *Snort* lebih unggul karena nilai persentasenya CPU *usage* paling minimum dibandingkan *Zeek* dan *Suricata*, sedangkan pada *memory usage*, *Snort* unggul dalam serangan PS karena memiliki nilai persentase *memory usage* yang paling minimum, pada *case* serangan DDoS *Suricata* unggul karena memiliki nilai persentase *memory usage* yang paling minimum. Kemudian, pada *network usage*, *Suricata* unggul karena memiliki nilai kb/s paling tinggi dibandingkan *Snort* dan *Zeek.*
2. Hasil perbandingan performa NIDS secara keseluruhan menunjukkan bahwa *Suricata* unggul dari *Snort* dan *Zeek*. Oleh karena itu performa *Suricata* menjadi pilihan yang solutif dan efektif.

5.2 Saran

Pada penelitian ini adapun saran yang dapat dilakukan untuk menjadi penelitian lanjutan dimasa depan, peneliti dapat menggunakan lingkungan fisik atau nyata, serta memperbanyak *tools* IDS yang digunakan seperti *OSSEC, Snort 2, Bro, OpenWIPS-ng*, dan tidak hanya membandingkan NIDS *tools*, tetapi juga

membandingkan HIDS *tools*. Kemudian, menambahkan parameter metrik QoS untuk melakukan perbandingan perfoma IDS yang lebih komprehensif, dan dapat mengintegrasikan IDS dengan *machine learning* ke dalam alat IDS untuk mengoptimalkan keakuratan deteksi sekaligus meminimalkan FP.