# BAB V
# PENUTUP

## 5.1 KESIMPULAN

Kesimpulan yang dapat diperoleh berdasarkan hasil dari pengujian dan pembahasan yang telah dilakukan secara keseluruhan pada penelitian implementasi Suricata untuk menghadapi serangan SQL *Injection* yaitu sebagai berikut:

1. Suricata pada penelitian ini berhasil berperan sebagai IPS sehingga dapat melakukan pendeteksian dan juga pemblokiran terhadap serangan SQL *Injection* dengan melakukan pengecekan terhadap *rules* yang diterapkan. Setiap terjadinya serangan SQL *Injection* yang ditujukkan ke webserver dideteksi oleh Suricata dengan pengecekan terhadap *rules* apakah terdapat kecocokan atau tidak.
2. Ketika Suricata belum aktif, penyerang berhasil masuk kedalam database dari DVWA web dan menemukan data paling sensitive dari database dvwadb. Namun ketika Suricata telah diaktifkan, penyerang berhasil terblok ketika akan masuk kedalam webserver
3. Berdasarkan hasil pengujian dari ketiga *rules* yang diterapkan hanya *rule* nomor 3 yang dinilai efektif untuk menghadapi berbagai jenis serangan SQL *Injection* karena mampu mendeteksi dan memblokir tiga jenis serangan tersebut (*Blind SQL Injection, Error SQL Injection,* dan *Union SQL Injection*) baik menggunakan *tool* SQLMap maupun serangan SQL secara manual.
4. Berdasarkan nilai *response time* yang telah diperoleh, Suricata membutuhkan waktu rata-rata 4,260633 *milliseconds* untuk menanggapi serangan yang masuk. Waktu respons tertingginya yaitu 4,863 *milliseconds* pada pengujian ke-30.

## 5.2 SARAN

Saran yang dapat diberikan agar tugas akhir ini menjadi lebih baik lagi yaitu:

1. Penggunaan Suricata untuk menghadapi serangan SQL *Injection* pada penelitian ini menggunakan metode *signature-based* pada NIPS sehingga dapat

dikembangkan lagi seperti menggunakan metode *anomaly-based* atau juga dapat diterapkan untuk jaringan yang lebih luas seperti MAN.

2. Pada penelitian selanjutnya dapat membandingkan kinerja dari Suricata dengan *tools* sistem keamanan yang lain seperti Snort dan lainnya dalam melindungi *webserver* dari serangan SQL *Injection* maupun serangan yang lainnya.