BAB V
PENUTUP

5.1 Kesimpulan

Dari Analisa keamanan Web Server menggunakan Suricata pada Linux Ubuntu Server yang telah dilaksanakan penulis, dapat diambil beberapa kesimpulan diantaranya :

1. Suricata mampu mendeteksi serangan serangan *client side attacks, test rules, bad traffic, fragmented packet, evasion technique, brute force, denial of service, pcap replay, normal usage* dan *shell codes* dengan waktu yang tidak terlalu lama dan dengan menggunakan resource sesuai rules yang diaktfifkan.

5.2 Saran

Saran yang dapat penulis berikan untuk penelitian selanjutnya adalah sebagai berikut :

1. Menggunakan konfigurasi yang dioptimalkan untuk suricata
2. Menggunakan rules sesuai kebutuhan sehingga tidak memakan resource terlalu banyak.
3. Mengupdate rules secara berkala sehingga suricata mampu mendeteksi terhadap pola serangan yang akan dating.
4. Menggunakan tools pengujian IDS selain pytbull.