# BAB V

# PENUTUP

## 5.1 Kesimpulan

Berdasarkan hasil penelitian pada bab-bab sebelumnya, maka dapat disimpulkan bahwa:

1. Penelitian ini menghasilkan sebuah sistem keamanan jaringan yang aman dengan melakukan implementasi *firewall Intrusion Detection System* Suricata dengan *signature-based* yang selalu di-*update* pada sebuah *server* lokal dan jaringan internal menggunakan perangkat *Router* Mikrotik terhadap serangan-serangan berbahaya dari jaringan penyusup.
2. Berdasarkan hasil penelitian dengan rancangan yang telah dibuat, sistem IDS (*Intrusion Detection System*) yang diimplementasikan telah berhasil dibangun dan dikembangkan dengan baik. Keseluruhan sistem mesin sensor IDS dapat bekerja dengan efektif sebagai sistem keamanan jaringan komputer yang berbasis *open source* dalam mendeteksi sebuah serangan.
3. Berdasarkan hasil pengujian, penggunaan Suricata sebagai *Intrusion Detection System* (IDS) dapat mendeteksi serangan berupa *Port Scanning*, Ping *Attack*, dan DoS (*TCP SYN Flood Attack* dan *UDP Flood Attack*) pada *computer host* dan *computer client* (*web server*).
4. Penggunaan *tools Elasticsearch*, *Kibana*, dan *Filebeat* dengan Suricata yang dapat mempermudah administrator dalam memonitoring jaringan. Dengan *Web Interface* yang dapat

memvisualisasikan setiap data atau *log* yang masuk sangat membantu dalam mendeteksi penyusup dengan cepat.

## 5.2 Saran

Saran untuk pengembangan dari penelitian ini dapat berupa:

1. Sistem IDS Suricata yang diimplementasikan sudah baik, namun itu hanya dari segi pendeteksian atau monitoring jaringan saja sehingga untuk pencegahannya membutuhkan *tools* tambahan. Alangkah baiknya jika *Intrusion Detection System* dapat dikembangkan lagi dari segi pencegahannya, agar serangan dari DoS dan *Port scanning* yang masuk dapat langsung dicegah atau diblokir secara otomatis tanpa *tools* tambahan.
2. Jika memiliki biaya lebih untuk merancang suatu jaringan lokal, disarankan untuk menggunakan Mikrotik *RouterOS* level 4 yang sudah memiliki lisensi gratis. *RouterOS* dengan level 0 atau *trial version* hanya bertahan selama 24 jam dan untuk bisa menggunakannya lebih lama harus membeli lisensi baru dan menambahkannya di *RouterOS* yang diinstall pada VirtualBox.
3. Untuk pengembangan kedepannya dianjurkan menggunakan notifikasi sebagai pemberitahuan jika terjadi serangan DoS dan *Port Scanning*.