BAB V
PENUUTP

5.1. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang sudah dijelaskan pada BAB sebelumnya, maka dapat ditarik beberapa kesimpulan yaitu sebagai berikut:

1. Pengujian simulasi menggunakan aplikasi Snort3 dalam memberikan *alert* dan menccegah adanya serangan memiki efisiensi dan akurasi yang tinggi hingga mencapai 100% setiap serangan.
2. Snort dapat mendeteksi dan mencegah adanya serangan *port scanning*, SSH *brute force*, MiTM, DDoS (ICMP *flood*, TCP *flood* dan UDP *flood*). Namun, Snort3 tidak dapat melakukan penceghan terhadap serangan UDP *flood* yang bersifat anomali, dengan opsional menjalankan Snort3 dengan pengecekan terhadap semua paket masuk yang dianggap *bad checksum* lalu *drop* paket tersebut.
3. Pendeteksian Anomali pada Snort3 dapat terdeteksi dengan melakukan perbandingan *resources* menggunakan aplikasi *monitoring resources* contohnya aplikasi Zenith dan melihat *event log file* json menggunakan WUI ELK *stack*.
4. Penggunaan sumber daya pada saat terjadi serangan dengan menggunakan pengamanan membutuhkan *resources* lebih besar dibandingkan dengan tidak menggunakan pengamanan.

5.2. Saran

1. Menggunakan mode keamanan SSL pada *website* yang digunakan nantinya sebagai *target* penyerangannya.
2. Melakukan pengujian dengan praktek secara langsung menggunakan perangkat keras seperti Cisco sebagai routernya.
3. Melakukan percobaan metode IPS berbasis *Wireless-based*.