BAB VI
KESIMPULAN DAN SARAN

6.1 KESIMPULAN

Setelah melakukan pengujian terhadap penelitian yang telah penulis lakukan maka penulis dapat menyimpulkan, yaitu;

1. Rancangan bangun yang dibutuhkan untuk dapat melakukan implementasi IDS Suricata, Snort, dan Fail2ban pada Raspberry PI adalah Raspberry PI yang bekerja menggunakan sistem operasi berbasis *ubuntu-server* sebagai defender, yang mana pada penelitian ini dibantu juga dengan 1 buah komputer sebagai attacker dengan menggunakan software *VirtualBox* untuk dapat menjalankan sistem operasi tersebut pada komputer bekerja dengan sistem operasi Windows. Tehnik untuk mencegah intrussion berbasis jaringan (*networ based*) dapat dilakukan dengan menerapkan IDS ditempat titi yang strategis didalam sebuah jaringan untuk melakukan pengawasan *traffic*.
2. Berdasarkan table hasil pengujian, bisa diambil kesimpulan bahwa Snort hanya dapat menangkap satu kali serangan pertama dari percobaan *Scanning port*, *DDoS*, dan *BruteForce* dari 40 percobaan serangan terhadap Snort. Suricata mampu mendeteksi seluruh percobaan *Scanning port* parameter -A, tetapi Suricata tidak mampu mendeteksi adanya percobaan penyerangan *Scanning port* parameter -sS -p-, *DDoS*, *BurteForce*. Fail2ban mampu mendeteksi satu kali serangan pertama dari *Scanning Port* parameter -A, untuk *Scanning Port*, *DDoS* fail2ban tidak mampu mendeteksi bahwa adanya serangan yang dilakukan terhadapt file2ban, dan untuk serangan *BruteForce* fail2ban berhasil mendeteksi seluruh percobaan serangan yang dilakukan. IDS yang belum mampu mendeteksi adanya serangan kemungkinan disebabkan oleh pola serangan dan rules yang belum sesuai dengan yang sudah disediakan oleh masing-masing IDS,

sehingga kita perlu untuk mencocokan pola serngan dan rules agar dapat mendeteksi sebuah serangan.

6.2 SARAN

Untuk perbaikan dan kelanjutan penelitian yang telah penulis lakukan maka penulis dapat memberikan saran-saran sebagai berikut;

1. Mengupdate traffic atau pola serangan beserta rules agar saat testing berikutnya bisa lebih baik lagi.
2. Dilakukan atau diimplementasikan pada jaringan yang sesungguhnya.