BAB V
KESIMPULAN, IMPLIKASI, DAN REKOMENDASI

5.1. Kesimpulan

Berdasarkan hasil penelitian yang sudah dilakukan, maka kesimpulan yang dapat diambil, yaitu:

1. Proses menemukan bukti sumber serangan siber dengan metode forensik yang mengancam kerusakan pada jaringan komputer adalah dengan *triggering* konfigurasi *rules* dan *log source* pada masing-masing *tools* yang berjalan pada jaringan komputer target. Hal ini dapat dilakukan dengan menggunakan *tools* IBM QRadar dan Snort.
2. Implementasi *network forensics* menggunakan *tools* IBM QRadar SIEM *Community Edition* dan Snort yang dapat mendeteksi ancaman serangan siber memiliki tahapan persiapan *resources*, konfigurasi *rules*, respon *tools* terhadap aktivitas serangan siber, sehingga data hasil yang diperoleh atau *capture* pada *tools* sampai tahapan akhir untuk menganalisis serangan siber dapat lebih terstruktur untuk menganalisis hasil *log* dengan *tools* IBM QRadar dan Snort.
3. Perbandingan efektivitas performa dari *tools* IBM QRadar SIEM *Community Edition* dan Snort dalam mendeteksi ancaman dan serangan siber dengan metode *network forensics* menunjukkan bahwa IBM QRadar mempunyai performa lebih efektif daripada Snort dalam mendeteksi serangan siber karena lebih banyak fitur, seperti pada tab *offenses* yang dapat melakukan kustomisasi dan konfigurasi *rules* paket data serangan dan visualisasi data yang kompleks dengan informasi *magnitude*. Selain itu, dalam mendeteksi serangan siber lebih responsif dengan teknologi *Artificial Intelligence* (AI) dan hasil data yang informatif untuk dianalisis lebih lanjut. Namun, penggunaan *resources* QRadar lebih besar dan lebih berat dalam *running log* jaringan yang terdapat serangan siber.

5.2. Implikasi

Pada penelitian yang sudah dilakukan, maka implikasi yang diharapkan pada penelitian ini, yaitu:

1. Penelitian ini berdampak pada sektor *security analyst* dalam membantu mengenali jenis serangan siber yang terjadi pada jaringan.
2. Penggunaan *tools* IBM QRadar yang responsif terhadap ancaman serangan siber yang mengganggu aktivitas jaringan, sehingga lebih efektif untuk mengenali jenis serangan dan sumber serangan yang tejadi pada suatu perangkat jaringan.

5.3. Rekomendasi

Pada penelitian yang sudah dilakukan dengan kondisi perangkat keras dan waktu yang terbatas terdapat rekomendasi yang dapat diterapkan untuk kedepannya, yaitu:

1. Penggunaan *resources* RAM, HDD, dan *core* pada *processor* pada *tools* IBM QRadar yang lebih besar dari spesifikasi yang digunakan dalam penelitian dan kondisi perangkat yang mempunyai spesifikasi lebih tinggi untuk memaksimalkan fitur dari IBM QRadar dan meminimalisir terjadinya *lag* pada perangkat.
2. Spesifikasi perangkat yang *recommended* dalam menjalankan IBM QRadar SIEM adalah menggunakan memori RAM 12 GB, HDD 250 GB, dan 4 *core* pada *processor*.
3. Penelitian terhadap IBM QRadar dan Snort perlu menambahkan *tools* lain yang khusus untuk melakukan *capture* jaringan, seperti wireshark yang dapat mengukur lalu lintas jaringan yang terindikasi adanya serangan siber.