BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari implementasi dan pembahasan pada penelitian "Manajemen Log Serangan Deauthentication pada Jaringan Wireless menggunakan ELK (Elastic, Logstash, dan Kibana)" dapat diambil beberapa kesimpulan sebagai berikut :

1. Setelah melakukan penelitian mengenai mengolah dan memanajemen log serangan jaringan Wireless agar mudah dipahami oleh administrator jaringan didapatkan hasil bahwa deteksi serangan deauthentication menggunakan Raspberry Pi sebagai sensor serangan.
2. Setelah melakukan penelitian akan mempermudah administrator menganalisa, log akan dikonversi ke dalam grafik yang dapat memvisualisasi serangan pada jaringan tersebut. Sensor akan mengaktifkan mode monitor menggunakan Airmon-ng, kemudia sensor akan melakukan pemantauan dengan mengambil log dan akan di export ke berkas csv.

5.2 Saran

Dalam Analisis Log Serangan Deauthentication pada Jaringan Wireless menggunakan ELK (Elastic, Logstash, dan Kibana) ini masih memiliki banyak hal yang dapat dikembangkan untuk penelitian selanjutnya yaitu :

1. Kedepannya pengembangan konfigurasi pada sistem sehingga meminimalisir kendala yang tidak berjalan menjadi berkurang.
2. Tidak hanya menggunakan wireshark saja namun kedepannya lebih menambah tools untuk mengambil log untuk memonitoring dan melindungi sistem atau jaringan.

Demikian kesimpulan dan saran yang dapat penulis sampaikan. Penulis berharap agar Analisis Log Serangan Deauthentication pada Jaringan Wireless menggunakan ELK (Elastic, Logstash, dan Kibana) dapat bermanfaat bagi orang-orang agar dapat menjaga kerahasiaan data.