BAB 5

Penutup

5.1 Kesimpulan

Berdasarkan penelitian yang dilakukan, terkait dengan penggunaan metode *network forensic* untuk analisa data log malware yang didapatkan dapat disimpulkan sebagai berikut :

1. Menggunakan analisa network forensic dapat mengetahui jenis serangan yang terjadi pada sistem, dapat mengetahui IP dari host *Command Center* dari serangan malware tersebut, dan kapan hal tersebut terjadi pada sistem komputer. Hal ini dapat digunakan sebagai barang bukti serangan.
2. Dari data yang di analisis didapatkan bahwa :
    a. malware emotet menggunakan protokol http sebagai protokol untuk mengambil data atau file yang mengandung malware lainnya dari *Command Center*. maka dapat digunakan filtrasi http.request dan http.response pada wireshark untuk mempermudah analisa.
    b. Koneksi yang terjadi dari server malware ke komputer korban akan meminta untuk mempertahankan koneksi (*Keep-Alive*).
    c. Didalam packet yang di dapatkan dari server host malware terdapat file yang menempel (*attachment*), dan beberapa dari data file yang didapatkan hanya dapat berjalan didalam sistem operasi.

5.2 Saran

Adapun saran yang dapat diberikan untuk penelitian selanjutnya diharapkan untuk melakukan analisis terhadap malware baru yang muncul di masa yang akan datang dan sangat disarankan untuk menggunakan minimal dua. Melakukan percobaan analisa menggunakan tools log data selain wireshark.