BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan internet saat ini tidak lepas dari perkembangan teknologi yang semakin canggih dan meningkatnya infrastruktur jaringan internet secara public membuat akses informasi semakin mudah dan semakin cepat.. Informasi yang diakses oleh seorang pengguna melalui media internet dengan penyedia layanan secara real time dan full time dari komputer *server*. Aktivitas pengguna pada sebuah jaringan dapat dicatat dan dideteksi kedalam sebuah log. Dengan banyaknya pengguna internet dapat menimbulkan suatu masalah, mulai dari kasus perbuatan yang tidak menyenangkan hingga terjadi kejahatan.

Tujuan dicatatnya aktivitas dari pengguna yang mengakses informasi yang tersimpan pada komputer adalah untuk mengetahui apabila ada aktivitas yang tidak sesuai atau kejahatan siber seperti serangan *ARP Spoofing, DDoS, SQL Injection, XSS dan Malware*. Data Log tersebut dapat digunakan sebagai barang bukti apabila insiden merugikan dari sisi penyedia. Informasi yang dapat dianalisa seperti informasi tentang jenis serangan yaitu informasi IP Address, informasi waktu dan tanggal akses dan kegiatan yang dilakukan dalam sistem komputer.

Malware emotet muncul kembali pada akhir tahun 2020 dengan *payloads* yang telah diperbaharui dan kampanye yang mencapai 100.000 target perhari (Tara Seals 2020, h.1), "Maldoc Emotet baru mencakup perubahan yang terlihat, kemungkinan dimaksudkan untuk menjaga agar korban tidak menyadari bahwa mereka baru saja terinfeksi," katanya. “Dokumen tersebut masih berisi kode makro berbahaya untuk menginstal Emotet, dan masih mengklaim sebagai dokumen yang “dilindungi” yang mengharuskan pengguna mengaktifkan makro untuk membukanya.

Pada bulan desember 2020 malware emotet muncul kembali menjadi ancaman malware teratas (Emilie Beneitez L, 2020, h.1), “Emotet awalnya dikembangkan sebagai malware perbankan yang menyelinap ke komputer pengguna untuk mencuri informasi pribadi dan sensitif. Namun, ia telah berkembang dari waktu ke waktu dan sekarang dilihat sebagai salah satu varian malware yang paling mahal dan merusak,” kata Maya Horowitz, Director, Threat Intelligence & Research, Products at Check Point. “Sangat penting bahwa organisasi menyadari ancaman yang ditimbulkan Emotet dan bahwa mereka memiliki sistem keamanan yang kuat untuk mencegah pelanggaran signifikan terhadap data mereka. Mereka juga harus memberikan pelatihan yang komprehensif bagi karyawan, sehingga mereka dapat mengidentifikasi jenis email berbahaya yang menyebarkan Emotet.”

Untuk mendapatkan informasi dari serangan yang terjadi pada sebuah sistem komputer perlu dilakukannya analisis terhadap Log. Metode yang digunakan saat melakukan analisis adalah *Network Forensic*, *Network Forensic* merupakan salah satu metode yang dapat digunakan untuk kegiatan investigasi dan analisis log untuk mencari aktivitas yang tidak sesuai atau siber *crime*, dimana bukti yang didapatkan berdasarkan dari pengamatan. Dalam investigasi terhadap file sistem Log, kita dapat menggunakan aplikasi management log untuk memudahkan analisis data log.

Network Forensic adalah kegiatan menangkap , merekam, dan menganalisis kejadian di dalam jaringan untuk menemukan sumber dan melakukan analisis jenis serangan yang dilakukan terhadap sebuah komputer *server*. *Network Forensic* jika dilakukan secara manual akan membutuhkan waktu yang lama dalam mengumpulkan data dan melakukan Analisa jenis serangan dan mencari IP address sumber dari serangan. Maka digunakan *tool* untuk mengumpulkan log.

Pengumpulan data Log sistem untuk *Network Forensic* menggunakan *tool* manajemen log, aplikasi atau *tool* yang digunakan dalam melakukan *Network Forensic*, dan Wireshark, Wireshark merupakan *tool open source* untuk menganalisa paket yang masuk di dalam jaringan, wireshark juga merupakan *tool cross platform* dapat diinstall pada sistem operasi Windows, Linux.

Berdasarkan latar belakang diatas, penulis ingin melakukan Analisa pada serangan yang dilakukan terhadap sistem komputer dengan *tool* wireshark untuk menentukan jenis serangan dan sumber dari serangan. Karena hal tersebut maka Penulis memberi judul "Analisis Serangan Siber dengan Wireshark untuk *Network Forensic*"

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan diatas maka penulis merumuskan masalah seperti berikut :

1. Apakah dengan menggunakan metode *Network Forensic* dapat mengetahui jenis serangan yang dilakukan ?
2. Bagaimana ciri-ciri dari malware emotet ?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini yaitu untuk mengimplementasikan Wireshark serta menganalisis Log dengan menggunakan *Network Forensic*, yaitu melakukan investigasi dari data serangan yang tersimpan pada Log.

1.4 Manfaat Penelitian

Berdasarkan latar belakang masalah yang telah diuraikan diatas, maka penulis mengharapkan manfaat sebagai berikut :

1. Dapat menganalisis serangan pada data Log dengan menggunakan metode *Network Forensic*.
2. Dapat dijadikan sebagai referensi untuk penelitian terkait dengan pembahasan pada tulisan ini.

1.5 Batasan Masalah

Berdasarkan latar belakang masalah yang telah penulis uraikan, maka Batasan masalah sebagai berikut :

1. Penelitian dilakukan dengan menggunakan serangan *Malware Emotet.*

2. Sistem komputer yang digunakan untuk dilakukan infeksi malware emotet menggunakan sistem operasi windows.
3. Malware yang digunakan sudah ada di dalam sistem.

1.6 Luaran Yang Diharapkan

Berdasarkan latar belakang masalah yang telah penulis uraikan diatas maka luaran yang diharapkan adalah untuk pembaca mengetahui bagaimana cara menggunakan metode *Network Forensic* untuk menentukan jenis serangan dan sumber dari serangan tersebut untuk dijadikan sebuah bukti.

1.7 Sistematika Penulisan

Penulis akan memaparkan gambaran sistematika penulisan laporan penelitian ini yang terdiri dari beberapa bagian sebagai berikut :

BAB 1 Pendahuluan

Pendahuluan yang berisi latar belakang penelitian, tujuan, permasalahan, ruang lingkup penelitian, sistematika penulisan.

BAB 2 Landasan Teori

Landasan teori (kajian pustaka) berisi mengenai teori-teori, metode, prosedur dan *tool*s yang digunakan dalam penelitian.

BAB 3 Metodologi Penelitian

Metodologi Penelitian berisi antara lain langkah-langkah apa yang dilakukan dalam penelitian serta metode/teknik/prosedur yang digunakan dalam setiap langkah penelitian berikut keluaran yang diharapkan.

BAB 4 Pembahasan

Pembahasan berisi penjelasan tentang rumusan masalah yang sudah dibuat sebelumnya dan melakukan pengujian penelitian.

BAB 5 Penutup

Penutup berisi tentang kesimpulan dan saran dari hasil penelitian yang telah dilakukan sebelumnya.

DAFTAR PUSTAKA