BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dengan ditemukannya teknologi-teknologi baru maka perkembangan teknologi informasi saat ini menjadi tidak terelakkan, teknologi tersebut sebenarnya dirancang untuk membantu kehidupan masyarakat sehari-hari. Internet adalah jaringan komputer besar yang saling berhubungan yang dapat menghubungkan orang dan komputer di seluruh dunia. Untuk memungkinkan orang bertukar informasi dan data, sejumlah besar aktivitas Internet membuat pengguna Internet rentan terhadap serangan *malware*. Selain banyaknya penggunaan internet, *malware* semakin banyak memasuki komputer melalui perantara *file*. *Malware* adalah perangkat lunak yang dibuat untuk tujuan jahat dan berbahaya karena dapat mengganggu kerja sistem komputer. *Malware* memasuki sistem dan menggunakannya tanpa izin, seperti merusak data, perangkat, atau orang.

Dilansir dari reuters.com lebih dari 1,500 perusahaan di Amerika mengelami serangan ransomware yang terjadi di U.S. [1] menunjukkan semakin berkembangnya *malware* dengan cepat. Oleh karena itu, diperlukan teknologi baru yang dapat menganalisis perangkat lunak berbahaya untuk mendeteksi perangkat lunak berbahaya yang memasuki komputer. Diperlukan penggunaan sistem yang kompleks untuk analisis *malware* dan penggunaan beberapa fungsi dalam satu sistem. MALICE adalah salah satu *framework* yang dibuat untuk melakukan analisis *malware* dengan menjalankan plugin dan menentukan modul pemrosesan mana yang harus dijalankan selama setiap analisis dan menjalankan modul untuk mencapai analisis *end-to-end*.

Saat melakukan analisis *malware*, maka akan diperoleh informasi dasar tentang sampel *malware* tersebut. Informasi sampel *malware* tersebut dianalisis dengan berbagai cara, salah satunya dengan mengekstrak stringnya. Ekstraksi string adalah sepotong teks yang menampilkan informasi *file* penyusun objek. Selama proses ekstraksi ini, informasi tentang *malware* dapat diperoleh. Penelitian ini menggunakan MALICE untuk membuat sistem analisis *malware*. Keuntungan dari sistem analisis *malware* ini adalah dapat menampilkan beberapa informasi. Informasi ini dibutuhkan untuk mempelajari *malware* dan diharapkan dapat membantu menemukan *malware* secara lebih detail, sehingga didapatkan hasil yang dapat diberikan kepada pengembang antivirus sebagai hasil pembuatan materi antivirus. Sistem akan dibangun pada ruang lingkup virtual mesin.

1.2 Rumusan Masalah

Sejumlah besar aktivitas Internet membuat pengguna Internet rentan terhadap serangan *malware.* Selain banyaknya penggunaan internet, *malware* semakin banyak memasuki komputer melalui perantara *file.* Dengan menggunakan MALICE untuk membuat sistem analisis *malware,* dapat menampilkan beberapa informasi tentang sampel sebuah sampel *malware*. Informasi ini dibutuhkan untuk mempelajari *malware* dan diharapkan dapat membantu menemukan *malware* secara lebih detail.

1.3 Tujuan

Adapun tujuan yang ingin dicapai dalam penyusunan proyek akhir ini adalah sebagai berikut :

1. Merancang dan membangun sistem analisis *malware* dengan MALICE untuk deteksi malware pada sistem operasi berbasis linux.
2. Membandingkan parameter malice ratio dengan virustotal ratio.
    a. Pengujian dilakukan pada *file* sampel.
    b. Parameter ratio pada sampel sebagai pengukuran hasil analisis.

1.4 Batasan Masalah

Dari beberapa rumusan masalah di atas maka terdapat Batasan masalah, untuk membatasi meluasnya bahasan masalah yang akan diteliti, maka dibatasilah masalah yang berkaitan dalam penyusunan proyek akhir ini sebagai berikut:

1. Sistem analisis malware dijalankan pada mesin virtual.
2. Sistem tidak bisa menghapus *malware*,
3. Sampel diambil dari internet dan komputer pribadi.
4. Hasil analisis hanya menjelaskan fitur sistem yang telah dibangun dan hasil analisis sempel secara garis besar tidak terperinci.

1.5 Definisi Operasional

1. Sistem Analisis

Adalah upaya mengamati sesuatu detail dengan cara menguraikan komponen pembentuknya untuk dikaji lebih lanjut.

2. Analisis Malware

   Adalah proses membedah komponen – komponen *malware* dan mempelajari tujuan fungsi *malware* tertentu. Proses ini dapat mengetahui jenis *malware*.[2]

1.6 Metode Pengerjaan

Metode pengerjaan yang digunakan pada Proyek Akhir ini menggunakan metode waterfall, metode waterfall [3] merupakan metode yang sering digunakan oleh penganalisa sistem pada umumnya. Inti dari metode waterfall adalah pengerjaan dari suatu sistem dilakukan secara berurutan atau secara *Linear*.

1. Studi Literatur

   Mencari referensi dan sumber untuk mempelajari konsep dan teori tentang analisis *malware* dan *malware*. Hal ini dilakukan sebagai landasan untuk analisis dan perancangan sistem yang akan dibangun.

2. Analisis dan Perancangan Sistem

   Landasan konsep dan teori dasar dilakukan pada tahap studi literatur digunakan untuk menganalisis persyaratan sistem dan kemudian membuat desain sistem yang akan dirancang.

3. Implementasi dan Pengujian Sistem

   Untuk implementasi system yang akan dibangun, dilakukan dengan instalasi perangkat – perangkat lunak. Kemudian dilakukan pengujian terhadap sampel – sampel *malware* pada mesin virtual.

4. Penyusunan Laporan

   Pada tahap ini, dilakukan dokumentasi dan penyusunan laporan dari semua proses tahapan yang telah dilakukan.