

BAB I PENDAHULUAN

1.1. Latar Belakang

Perangkat dengan teknologi canggih saat ini sudah menjadi kebutuhan yang harus dipenuhi bagi beberapa kalangan masyarakat di seluruh dunia, seperti perangkat komputer dan *handphone* cerdas (*smartphone*).

Kecanggihan perangkat ini tidak dapat dipisahkan dari perangkat lunak yang mengoperasikannya. perangkat lunak merupakan perantara bagi pengguna dengan perangkat keras (*hardware*), khususnya komputer. Perangkat lunak dapat bekerja secara otomatis dan dapat melakukan tugas sesuai yang diperintahkan penggunanya. Akan tetapi perangkat lunak hanya dapat bekerja sesuai sumber daya yang disediakan oleh perangkat keras (*hardware*).

Berbagai macam perangkat lunak telah dikembangkan untuk memenuhi kebutuhan pengguna komputer. misalnya perangkat lunak untuk perkantoran, hiburan, game dan lain-lain. Saat ini sangat banyak perangkat lunak yang ditawarkan secara gratis (*freeware*), namun ada juga yang berbayar. Perangkat lunak *freeware* biasanya dapat di-*download* di-*internet* secara gratis.

Perangkat lunak yang di-*download* secara gratis biasanya memiliki banyak resiko. Mengapa demikian, karena saat ini sangat banyak perangkat lunak gratisan yang dengan sengaja dibuat lalu diberikan secara cuma-cuma. Tetapi perangkat lunak tersebut adalah sebuah *Malware*

Malware (Malicious Software) adalah jenis perangkat lunak yang dikembangkan dengan tujuan kejahatan. Di anggap melakukan kejahatan, karna *malware* ini sendiri dapat melakukan hal - hal yang merugikan pengguna computer. Beberapa contoh aktivitas malware pada komputer pengguna ialah: mencuri data dan informasi penting, menghapus data, dan merusak *system*.

Karena *Malware* ini adalah jenis perangkat lunak yang menyusup ke dalam *system* komputer pengguna, bisa dikatakan malware adalah perangkat lunak yang canggih, karna kemampuannya untuk menyusup serta menyembunyikan diri agar tidak terdeteksi oleh pengguna komputer. Untuk itu dibutuhkan proses serta teknik untuk mempelajari cara kerja *Malware* di dalam sebuah *system*. Pada penelitian ini penulis mengambil judul "Analsis Malware Trojan" sebagai judul skripsi.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah di atas dapat dirumuskan masalah sebagai berikut:

1. Bagaimana melakukan analisis statis terhadap sebuah *malware trojan*?
2. Bagaimana melakukan analisis dinamis terhadap sebuah *malware trojan*?

1.3. Ruang Lingkup

Ruang lingkup yang akan dibahas pada penelitian ini, sebagai berikut:

1. *Malware trojan* yang dianalisis tidak terenkripsi.
2. Analisis dilakukan dalam dua teknik yaitu statis dan dinamis.
3. Analisis dilakukan pada sistem operasi windows xp 32 bit.
4. File type *Trojan* adalah *PE32 executable Intel 80386 (EXE)*
5. Analisis menggunakan *tools kali linux* versi 1.6

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk memberikan informasi tentang bagaimana sebuah *malware* bekerja pada sebuah sistem, khususnya *malware* jenis *trojan*

