BAB 1
PENDAHULUAN

1.1 Latar Belakang

Penggunaan komputer dalam berbagai aspek kehidupan semakin meningkat pada beberapa dekade ini. Sejak pertama kali pembuatan komputer, dibutuhkan sebuah perangkat yang dapat menginstruksikan komputer dengan tugas yang diberikan, maka dibuatlah sebuah program komputer atau *software*. Semakin berkembangya kinerja komputer, semakin berkembang pula tingkat kompleksitas pemrograman *software*. Hal ini menyebabkan munculnya kerentanan – kerentanan dalam *software*.

Dari kerentanan – kerentanan tersebut terciptalah perangkat lunak yang menyimpang atau disebut *malware*. Hal ini diawali dengan menyebarnya sebuah program yang dapat mereplikasi dirinya sendiri secara otomatis di jaringan ARPANET pada tahun 1971. Program ini bernama Creeper yang dibuat Bob Thomas.

Semakin berkembangnya *malware* ditunjukan dalam artikel yang berjudul *"Top 5 Malware Trends on the Horizon"* pada situs *tripwire.com*. Dalam artikel tersebut menyatakan bahwa perilaku *malware* 2000% lebih agresif pada tahun 2014. *Trend malware* di masa yang akan datang diprediksikan akan semakin mutakhir, agresif, dan tidak dapat terhindarkan. Langkah selanjutnya untuk mengatasi masalah tersebut, teknologi baru harus mampu untuk menganalisis *malware* secara otomatis.

Berdasarkan fakta – fakta di atas, studi untuk mempelajari *malware* perlu dilakukan untuk memahami motif dan tujuan kerusakan yang diakibatkan oleh *malware*. Terdapat 3 metode yang dapat dilakukan untuk menganalisis *malware* yaitu analisis statis, analisis dinamis, dan analisis memori.

Dalam pengerjaan proyek akhir akan dilakukan analisa *malware* dengan menggunakan ketiga metode tersebut menggunakan aplikasi Cuckoo Sandbox. Cuckoo Sandbox adalah sebuah aplikasi analisis *malware* yang dapat melakukan ketiga metode analisis tersebut. Cuckoo Sandbox melakukan analisis *malware* dengan menjalankan *file malware* pada ruang lingkup yang terisolasi dari jaringan luar. Arsitektur Cuckoo Sandbox yang modular memungkinkan kustomisasi Cuckoo Sandbox sesuai dengan kebutuhan pengguna. Kelebihan – kelebihan inilah yang menjadi alasan penggunaan Cuckoo Sandbox untuk menganalisis *malware* pada proyek akhir ini.

Diharapkan dengan dibangunnya *Server* Analisis *Malware* ini mampu menghasilkan informasi – informasi penting tentang *malware* yang dapat digunakan oleh pengguna biasa maupun peneliti *malware*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, permasalahan yang dihadapi dirumuskan sebagai berikut :

1. Bagaimana membangun *server* analisis *malware* menggunakan Cuckoo Sandbox ?
2. Bagaimana melakukan analisis *malware* menggunakan Cuckoo Sandbox ?
3. Apa saja informasi yang didapatkan dari hasil analisis *malware* ?

1.3 Tujuan

Tujuan Adapun tujuan dari pembuatan Proyek Akhir ini adalah:

1. Membangun *server analisis malware menggunakan Cuckoo Sandbox.*
2. Melakukan Analisis analisis *malware* pada ruang lingkup mesin virtual menggunakan Cuckoo Sandbox.
3. Mendapatkan informasi hasil analisis *malware* tentang karakteristik *malware* dan efek yang diakibatkan oleh *malware* .

1.4 Batasan Masalah

Untuk menghindari meluasnya pokok pembahasan, maka pengerjaan penelitian ini terbatas pada :

1. Sistem operasi *host* yang digunakan adalah Linux Mint 17.3 .
2. Aplikasi virtualisasi yang digunakan adalah VMWare Workstation 12.
3. Sistem operasi mesin virtual dimana *file malware* dijalankan diantaranya adalah Windows XP SP3, Windows 7, dan Ubuntu 14.10.
4. *Tools* analisis *malware* yang digunakan yaitu Cuckoo Sandbox 2.0-RC1 untuk mesin virtual Ubuntu 14.10. Cuckoo Sandbox 1.3 Optiv/Accuvant untuk mesin virtual Windows XP dan Windows 7.
5. Terdapat 3 sampel yang akan diujikan untuk masing – masing *platform*. Sampel tersebut terdiri dari sampel yang bukan *malware*, sampel yang belum diketahui terkait *malware* atau bukan *malware*, dan sampel yang positif terdeteksi sebagai *malware*.
6. Sampel – sampel *yang* akan dianalisis didapatkan dari contagiodump.blogspot.com , *tekdefense.com*, dan sampel yang diambil dari komputer pribadi.
7. Sampel – sampel yang akan diujikan hanya berbentuk *file binary*.
8. Konfigurasi pada *server* dibatasi hanya meliputi :
    a. Instalasi *package dependencies* untuk Cuckoo Sandbox.
    b. Instalasi mesin *virtual* pada VMWare sebagai ruang lingkup pengujian *malware*.
    c. Konfigurasi Cuckoo Sandbox versi 1.3 Optiv / Accuvant dan 2.0 RC1 untuk diintegrasikan dengan VMWare dan mesin *virtual*.

d. Pengaturan iptables pada *server* untuk mengatur IP *forwarding* dan *filtering* mesin *virtual*.

9. Analisis hasil *report* hanya menjelaskan fitur sistem yang telah dibangun dan analisis sampel secara garis besar, tidak terperinci secara spesifik.

10. Dokumentasi hasil analisis Cuckoo Sandbox berupa HTML dan PDF.

1.5 Definisi Operasional

1. *Server* adalah sebuah komputer yang ditujukan untuk menyediakan layanan khusus [5].

2. *Malware* merupakan singkatan dari *malicious software* adalah perangkat lunak berbahaya yang dirancang untuk merusak sebuah komputer independen atau sebuah jaringan komputer [1].

3. Analisis *malware* adalah studi tentang *malware* dengan membedah komponen – komponen nya yang berbeda dan mempelajari perilakunya pada Sistem operasi komputer *host* [4].

4. Istilah *sandboxing* dipakai untuk menjelaskan konsep dari pembatasan sebuah aplikasi pada sebuah ruang lingkup yang tertutup dimana aplikasi tersebut mempunyai kekuasaan penuh (terhadap ruang lingkup yang terbatas tersebut). Sebuah *sandbox* adalah sebuah mekanisme keamanan untuk memisahkan program yang dianalisis dengan program – program lain yang sedang berjalan. Hal ini biasanya dilakukan untuk menjalankan kode yang belum teruji, atau program pihak ketiga yang belum teruji [2] .

5. Cuckoo Sandbox adalah sebuah aplikasi sistem analisis *malware* terotomatisasi *open source* yang memungkinkan analisis *malware* dalam ruang lingkup *sandbox*. Aplikasi ini digunakan untuk menjalankan dan menganalisis *file* secara otomatis dan mengumpulkan hasil analisis komprehensif yang menjelaskan secara garis besar perilaku *malware* ketika sedang berjalan di dalam Sistem operasi yang terisolasi [3].

1.6 Metode Pengerjaan

1. Studi Literatur

   Pencarian referensi dan sumber – sumber untuk mempelajari konsep dan teori yang berkaitan dengan *malware* dan analisis *malware*. Hal ini dilakukan sebagai landasan untuk analisis dan perancangan sistem yang akan dibangun.

2. Analisis dan Perancangan Sistem

   Landasan konsep dan teori yang telah dilakukan pada tahap studi literatur digunakan untuk menganalisis kebutuhan sistem kemudian membuat rancangan sistem yang akan dibangun.

3. Implementasi dan Pengujian Sistem

   Untuk implementasi sistem yang akan dibangun, dilakukan dengan instalasi perangkat – perangkat lunak pada *server*. Kemudian dilakukan pengujian dari implementasi sistem yang sebelumnya telah dilakukan. Pada tahapan ini dilakukan pengujian terhadap sampel – sampel *malware* pada masing – masing mesin virtual. Hal ini dilakukan untuk memastikan sistem yang telah dibuat dapat berjalan dengan baik.

4. Penyusunan Laporan

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

1.7 Jadwal Pengerjaan

Tabel 1-1 Jadwal Pengerjaan

Kegiatan	Tahun 2016																			
	Januari				Februari				Maret				April				Mei			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Studi literatur																				
Analisis kebutuhan sistem dan perancangan sistem																				
Instalasi, konfigurasi, dan pengujian sistem																				
Penyusunan laporan hasil pengerjaan																				