BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada Perkembangan kemajuan teknologi komputer dalam hal keamanan semakin meningkat. Tetapi kelebihan ini juga digunakan untuk hal-hal yang bersifat merugikan, akibatnya kerugian yang diderita akibat penyalahgunaan atau kejahatan menggunakan komputer/jaringan komputer (*cyber crime*) mencapai milyaran setiap tahunnya. Serangan terhadap komputer/jaringan di seluruh dunia seperti *virus*, *worms*, *spam* dan malware semakin meningkat. Salah satunya adalah virus makro. File yang terinfeksi Virus Makro atau dikenal dengan maldoc adalah virus yang dibuat dengan pemrograman pada program aplikasi *seperti Microsoft Word, Microsoft Office, dan lainnya*. Maldoc sendiri artinya adalah *Malicious Office documents* atau dokumen office berbahaya. Makro virus memiliki kemampuan untuk menggandakan dan menyebarkan dirinya, dan juga dapat menghapus dokumen words, mengubah pengaturan komputer, *reset password*, ,dan menyelipkan perintah berbahaya di CONFIG.SYS atau AUTOEXEC.BAT. Dokumen microsoft *office* menyumbang pengiriman hampir setengah dari semua makro berbahaya pada Agustus 2018, menurut Cofense.com. Pada web tersebut dilaporkan bahwa lampiran email merupakan salah satu pilihan yang sering digunakan untuk mengirimkan virus makro yang berbahaya. Dari semua mekanisme yang dianalisis, 45% dari penyerang menggunakan dokumen-dokumen ini untuk mengirimkan makro jahat, termasuk contohnya seperti virus makro Geodo, Chanitor, AZORult, dan GandCrab.

Menurut para peneliti keamanan, makro adalah pilihan utama karena itu diaktifkan pada mesin atau hanya membutuhkan satu klik mouse untuk diaktifkan. Virus makro dijalankan sangat mudah dengan hanya dengan 1 kali klik.

ViperMonkey adalah *software* yang ditulis dengan Bahasa Phyton, yang dirancang untuk mendeteksi virus makro yang berbahaya yang terdapat dalam file

Malicious Document. ViperMonkey mengecek file tersebut aman atau tidak terinfeksi virus makro yang berbahaya bagi komputer user. Jika ternyata *file maldoc* yang dianalisa terinfeksi virus makro, maka *file* tersebut harus segera dihapus.

Berdasarkan hal tersebut penulis akan melakukan deteksi dan analisa virus makro pada file *doc* atau dokumen dengan menggunakan *ViperMonkey*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang terdapat diatas, maka rumusan masalah pada proyek akhir ini adalah cara mendeteksi virus makro pada file atau dokumen terinfeksi virus makro/*maldoc*.

1.3 Tujuan

Tujuan dari proyek akhir ini adalah menggunakan Vipermonkey untuk mendeteksi pada *file* dokumen yang dicurigai terinfeksi virus makro/*maldoc.*

1.4 Batasan Masalah

Batasan masalah yang digunakan adalah :

1. Menggunakan Vipermonkey sebagai alat untuk mendeteksi virus makro.
2. Menggunakan Operasi sistem Ubuntu.
3. Menggunakan *Virtual Machine* sebagai *software* pendukung untuk pengujian.
4. Menguji 4 sampel virus makro/*Maldoc*.

1.5 Definisi Operasional

Definisi operasional pada proyek akhir ini adalah :

1. **Keamanan**. keadaan bebas dari bahaya. Istilah ini bisa digunakan dengan hubungan kepada kejahatan, segala penyalahgunaan, dan lain-lain**.**
2. **Aplikasi.** dapat diartikan sebagai suatu program berbentuk perangkat lunak yang berjalan pada suatu sistem tertentu yang berguna untuk membantu berbagai kegiatan yang dilakukan oleh manusia.

3. **Virus Makro.** virus yang dibuat denganpemrograman pada suatu program aplikasi seperti Microsoft Word, Microsoft Excel dan sebagainya

4. **ViperMonkey.** ViperMonkey adalah Emulator Visual Basic for Applications yang ditulis dengan Phyton, yang dirancang untuk mendeteksi dan menyamarkan virus makro yang berbahaya yang terdapat dalam file Microsoft *Office* (Word, Excel, PowerPoint, Publisher, dll).

1.6 Metode Pengerjaan

Metode pengerjaan yang digunakan pada Proyek Akhir ini menggunakan metode SDLC (*Software Development Life Cycle)*. SDLC adalah siklus hidup pengembangan system. Dalam sebuah rekayasa perangkat lunak, SDLC adalah proses pembuatan dan pengubahan suatu sistem maupun model serta metode yang digunakan untuk mengembangkan sistem tersebut. Dalam pengerjaan tugas akhir ini terdiri dari beberapa tahap sebagai berikut

1. **Inisiasi**

   Pada tahap ini dilakukan pembuatan proposal.

2. **Pengembangan Konsep Sistem**

   Pada tahap ini dilakukan manajemen rencana dan mempelakari cara kerja sistem.

3. **Perencanaan (planning)**

   Pada tahap ini akan melakukan installasi ViperMonkey dan mengkonfigurasinya pada ubuntu.

4. **Analisis kebutuhan**

   Pada tahap ini dilakukan Analisa kebutuhan pengguna baik perangkat lunak dan keras maupun fungsional.

5. **Desain (design)**

   Pada tahap ini dilakukan design terhadap sistem yang dibutuhkan untuk menjalankan ViperMonkey.

6. **Pengembangan *(Development)***

   Pada tahap ini dilakukan pengubahan perancangan ke sistem informasi yang kompleks. Melakukan penginstalan ViperMonkey dan menyiapkan sampel yang akan diuji.

7. **Pengujian**

   Pada tahap ini dilakukan pengujian pada berbagai sistem yang digunakan untuk ViperMonkey .

8. **Implementasi**

   Pada tahap ini dilakukan implementasi dan analisis pada hasil.

9. **Pemeliharaan (Maintenance)**

   Pada tahap ini dilakukan operasi untuk menjalankan dan maintenance sistem pada ViperMonkey, setelah itu ditinjau mengenai hasil akhirnya.

10. **Disposisi**

    Pada tahap ini mendeskripsikan aktifitas dari pengembangan sistem dan membangun data yang telah dikumpulkan.

1.7 Jadwal Pengerjaan

Adapun jadwal pengerjaan dalam penelitian ini adalah sebagai berikut :

Tabel 1.1 Jadwal Pengerjaan Proyek Akhir

No	Kegiatan	Waktu Pelaksanaan Tahun 2018-2019																			
		Agustus				September				Oktober				November				Desember			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Inisiasi																				
2	Pengembangan Konsep Sistem																				
3	Perencanaan (Planning)																				
4	Analisis Kebutuhan																				
5	Design																				
6	Pengembangan																				
7	Pengujian																				
8	Implementasi																				
9	Pemeliharaan (Maintenance)																				
10	Inisiasi																				