BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring pesatnya kemajuan teknologi informasi khususnya di bidang teknologi komputer dan jaringan, keamanan dan isu yang kerap kali dibahas. Mulai dari ancaman langsung para craker atau hacker jahat hingga acaman yang dilakukan melalui program yang disebut malcode (malicious code). Suatu program atau script apapun yang bersifat merusak atau merugikan dapat katagorikan sebagai malcode termasuk virus komputer, worm atau trojan horse.

Selama lebih dari tiga dekade yang lalu, virus komputer telah berkembang dari sekedar riset akademis menjadi masalah yang umum bagi para pengguna komputer di dunia. Masalah terbesar dari virus ini berasal dari penanggulangan efek kerugian yang ditimbulkan oleh penyebarannya. Efek kerugian ini semakin menjadi dengan maraknya penggunaan internet sebagai jalur komunikasi global antara pengguna komputer di seluruh dunia. Berdasarkan hasil survei CSI/FB sejak tahun 2004-2008 pada sekitar 433-an responden dari berbagai organisasi di Amerika Serikat, tentang kejahatan komputer dan keamanannya, menyebutkan bahwa virus menempati urutan pertama sebagai kejahatan komputer yang paling merugikan. Seiring dengan perkembangannya, virus komputer mengalami beberapa evolusi dalam bentuk, karakteristik serta media penyebarannya. bentuk evolusi tersebut dikenal dengan *Worms, Spyware, Trojan horse* dan program Malcode lain.

Perkembangan penyebaran malcode di Indonesia pada awalnya lebih banyak didominasi oleh *worms* dan *virus* yang berasal dari luar negeri. Namun pada bulan Oktober 2005, dominasi ini mulai runtuh dengan menyebarnya virus-virus lokal yang hampir ada disetiap komputer di seluruh Indonesia, virus menyebar dengan sangat cepat dan sangat membuat risih bagi pengguna komputer, dengan demikian dibuatlah anti virus sebagai salah satu solusi mencegah penyebaran.

Metode pencarian virus yang paling sering di pakai oleh anti virus yaitu metode CRC-32 (*Cyclic Redundancy Code*). Metode CRC-32 merupakan teknik yang semulanya digunakan untuk mengecek kerusakan pada file. Metode ini yang sering digunakan oleh anti virus untuk mengecek signature dari virus, tetapi teknik ini tidak efesien apabila diterapkan pada malware yang sudah mengimplementasikan teknik polymorph. Teknik Polymorph secara umum adalah teknik mereplikasi diri dan tiap signature replikanya berbeda satu sama lain. Kasus virus lokal sudah ditemukan penggunaan teknik polymorph. Baik itu secara sederhana maupun kompleks. Cara yang biasa digunakan yaitu :

1. Merubah atau mengenkripsi nama variabel dan string
2. Menambah atau mengurangi byte-byte tertentu di virus
3. Menggunakan *engine polymorph* tertentu

Jika secara normal metode *CRC-32* ini sangat gampang untuk dikelabui, hal ini dikarenakan perubahan 1 bit kode pada program maka akan menyebabkan perubahan hasil pengecekan *CRC-32*.

Hal ini yang melatar belakangi mengapa "Teknik Pembuatan Anti Virus Dengan Metode Pencarian Dengan Membaca Informasi Struktur File *Portable Executeble*(PE) Sebagai Pola Virus" diangkat sebagai judul skripsi, karena berdasarkan pengamatan penulis walaupun virus sudah melakukan modifikasi menambah atau mengurangi byte-byte tertentu tetapi Informasi Struktur File *Portable Executeble*(PE) yang berupa data optimal header dari virus yang berisi informasi *SizeOfCode* dan *AddressOfEntry*, tidak akan berubah.

1.2 Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah, maka permasalahan dalam skripsi ini, adalah bagaimana teknik pembuatan anti virus dengan metode pencarian dengan membaca informasi struktur file *Portable Executeble*(PE) yang berupa data optimal header dari virus yang berisi informasi *SizeOfCode* dan *AddressOfEntry* sebagai pola virus.

1.3 Batasan Masalah

Penulis membatasi penelitian ini dengan membahas :

1. File yang akan di jadikan sampel virus yaitu berupa file yang berekstensi *.exe.
2. *Pattern virus* dalam bentuk hexadecimal yang merupakan data *AddressOfEntryPoint* dan *SizeOfCode* yang didapat dengan membaca informasi struktur file *Portable Executeble*(PE) .

3. Menyimpan *pattern virus* pada suatu text file terpisah dimana 16 digit pertama adalah pola virus yang berupa bilangan hexa, dan diikuti oleh nama virus.

1.4 Tujuan Penelitian

Dari hasi penelitian yang dilakukan, adapun tujuan yang ingin dicapai dalam merancang suatu sistem anti virus yaitu :

1. Untuk memenuhi persyaratan dalam rangka menyelesaikan program studi S-1 Jurusan Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta
2. Untuk membuat sebuah anti virus dengan metode pencarian yang membaca informasi struktur file *Portable Executeble*(PE) yang berupa optimal header data yang berisi informasi *SizeOfCode* dan *AddressOfEntryPoint* sebagai pola virus.
3. Untuk mengetahui letak kekurangan-kekurangan dari sistem yang sedang berjalan.
4. Untuk mengetahui sejauh mana efektivitas dan efisiensi dari sebuah sistem anti virus yang menggunakan header file *SizeOfCode* dan *AddressOfEntryPoint* yang didapat dari membaca struktur file *Portable Executeble*(PE) sebagai *pattren virus* yang dirancang.

1.5 Manfaat Penelitian

1. Aplikasi dapat digunakan sebagai salah satu Antivirus pada komputer.
2. User dapat meminimalisasi pemakaian media peyimpanan yang dipakai untuk menyimpan database virus berupa text file.
3. User dapat melakukan update database virus tanpa harus melakukan koneksi ke server penyedia Antivirus.

1.6 Sistematika Penulisan

Dalam penyusunan Tugas Akhir ini penulis akan membagi dalam beberapa bab, yaitu:

Bab I : PENDAHULUAN

Pada bab ini penulis akan menerangkan tentang latar belakang masalah, batasan masalah, rumusan masalah, tujuan penelitian dan sistematika penulisan.

Bab II : LANDASAN TEORI

Pada bab ini membahas mengenai dasar teori analisis dan tinjauan pustaka, serta membahas tentang gambaran umum tentang *Virus*, *Antivirus*, *Worms* dan *Portable Executable* (HEADER FILE).

Bab III : ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini berisi analisis tentang Portable Executable (HEADER FILE) / Dos Header Virus Brontok A, Worm

Kleze, dan teknik perancangan sistem Anti Virus.

Bab IV: IMPLEMENTASI DAN PEMBAHASAN

Dalam bab ini dibahas implementasi pengujian program, hasil pengujian dan manual program.

Bab V : PENUTUP

Pada bab ini menerangkan tentang kesimpulan dan saran.