PERBANDINGAN METODE PENDETEKSIAN *WORM* PADA KOMPUTER *FILE NAME SCANNING* DAN *STRING SCANNING*

Mario Florentino Makang

Jurusan Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonrsia
Jln. Dipati Ukur No.112 Bandung 40132
marioflorentinomakang@yahoo.co.id

ABSTRAK

Banyaknya jenis malware (malicious software) yang terdapat pada komputer dan dampak yang ditimbulkan dari malware tersebut sangatlah merugikan bagi pengguna komputer. Salah satu jenis dari malware tersebut adalah worm.

Seperti layaknya malware yang lain virus atau Trojan dan sebagainya, worm memiliki daya rusak yang dapat sangat mnerugikan baik bagi pengguna pribadi maupun pengguna dalam kapasitas yang besar (jaringan sampai internet).

Untuk mengatasi hal tersebut terdapat dua metode yang dapat dilakukan untuk mendeteksi keberadaan worm pada suatu komputer. Yaitu metode scan File Name Scanning dan String Scanning. Dimana metode yang pertama berorientasi pada nama dari sebuah file dan kedua berorientasi pada sederetan string hexa dalam melakukan pendeteksian (scan) pada suatu file worm.

Tujuan dari tugas akhir ini adalah untuk mengimplementasikan kedua metode tersebut, dan juga untuk menguji dengan beberapa parameter uji, untuk mengetahui metode mana yang lebih optimal dalam melakukan pendeteksian file worm.

Tools yang digunakan untuk membangun aplikasi ini adalah MS. VB 6.0. Tools pembantu yang digunakan adalah HxDen (hexa decimal editor).

Hasil yang akan dicapai dari aplikasi ini adalah selain untuk dapat mendeteksi file worm yang nantinya akan diuji coba yaitu mengetahui waktu dan ketepatan dalam mendeteksi file worm yang diujikan.

Aplikasi ini telah berhasil menguji kedua metode di atas. Selain untuk mendeteksi keberadaan file worm, dapat diketahui juga kelebihan dan kekurangan melalui uji parameter. Sehingga dapat berguna bagi user dalam melakukan pendeteksian dan juga dapat mengetahui metode mana yang terbaik atau sama antara kedua metode.

Kata Kunci : File Name Scanning, String Scanning.

1. PENDAHULUAN

1.1 Latar Belakang

Komputer adalah mesin yang perkembangannya dari masa ke masa telah mengalami kemajuan yang sangat pesat. Fungsi dari komputer itu sendiri ialah untuk mengolah data, dimana data disini adalah sesuatu yang belum mempunyai arti bagi penerimanya dan masih memerlukan adanya suatu pengolahan. Data bisa berwujud suatu keadaan, gambar, suara, huruf, angka, bahasa

ataupun simbol-simbol lainnya yang bisa kita gunakan sebagai bahan untuk melihat suatu keadaan.

Informasi merupakan hasil pengolahan dari sebuah model, formasi, organisasi, ataupun suatu perubahan bentuk dari data yang memiliki nilai tertentu, dan bisa digunakan untuk menambah pengetahuan bagi yang menerimanya. Dalam hal ini, data bisa dianggap sebagai objek dan informasi adalah suatu subjek yang bermanfaat bagi penerimanya. Informasi juga bisa disebut sebagai hasil pengolahan ataupun pemrosesan data.

Sehingga kita bisa melihat bahwa fungsi utama dari sebuah komputer adalah mengolah suatu data yang telah disebutkan diatas menjadi sebuah informasi yang berguna atau bermanfaat bagi penerimanya.

Namun dalam perkembangannya komputer tidak lepas dari suatu tindak kejahatan terhadap suatu program komputer. Salah satu tindak kejahatan dalam program yaitu *worm*. *Worm* komputer dapat menimbulkan dampak yang sangat fatal dan merugikan. Contohnya komputer yang menjadi lambat, disk drive terakses secara berkala, konfigurasi komputer berubah dan lain sebagainya.

Berdasarkan hal di atas, untuk mengantisipasi perkembangan dan makin banyaknya worm, maka diperlukan suatu program yang dapat mendeteksi dan menghapus program-program berbahaya tersebut. serta perbandingan diantara kedua metode tersebut.

1.2 Identifikasi Masalah

Bagaimana membangun **PERBANDINGAN METODE PENDETEKSIAN WORM PADA KOMPUTER FILE NAME SCANNING DAN STRING SCANNING**.

1.3 Maksud dan Tujuan

Dari latar belakang yang telah diuraikan maka penulis bermaksud membangun program aplikasi Pembuatan Aplikasi Pendeteksian *Worm* Komputer Dengan Metode File Name Scanning Dan String Scanning.

Sedangkan tujuan yang akan dicapai dalam penelitian ini adalah :

1 Mengimplementasikan metode *File Name Scanning* dan *String Scanning* pada aplikasi *infector file removal*.
2 Mendeteksi *file infector* worm pada komputer.
3 Menghapus *file infector* worm dari sistem komputer.
4 Mengatahui performa berdasarkan waktu yang ditempuh oleh masing-masing metode.
5 Mengetahui keakuratan dari masing-masing metode dalam hal pencarian file worm.
6 Dapat mengetahui metode mana yang baik dari segi waktu dan hasil pencarian *file worm.*

1.4 Manfaat

Manfaat yang didapat dalam pembangunan aplikasi ini antara lain :

1 Mendeteksi *file infector* worm pada komputer.
2 Menghapus *file infector* worm dari sistem komputer.
3 Mengatahui performa berdasarkan waktu yang ditempuh oleh masing-masing metode.
4 Mengetahui keakuratan dari masing-masing metode dalam hal pencarian file worm.
5 Dapat mengetahui metode mana yang baik dari segi waktu dan hasil pencarian *file worm.*

2. MODEL, ANALISA, DESAIN, DAN IMPLEMENTASI

2.1 Model

1. Tahap pengumpulan data
   a. Studi Kepustakaan.
   b. Observasi.
2. Tahap pembuatan perangkat lunak.
   a. *Requirements analysis and definition*
   b. *System and software design*
   c. *Implementation and unit testing*
   d. *Integration and system testing*
   e. *Operation and maintenance*

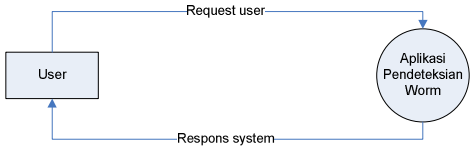
2.2 Analisis Masalah

Analisis sistem dapat didefinisikan sebagai penguraian dari suatu sistem informasi yang utuh ke dalam bagian-bagian komponennya untuk mengidentifikasikan masalah-masalah, dan hambatan-hambatan sehingga dapat diusulkan kebutuhan-kebutuhan untuk

perbaikannya. Tahap analisis merupakan tahap yang paling kritis dan sangat penting, karena kesalahan didalam tahap ini akan menyebabkan juga kesalahan di tahap selanjutnya. Analisis sistem ini diperoleh melalui observasi yang akan ditemukan beberapa data dan fakta yang akan dijadikan bahan uji dan analisis menuju penerapan dan pengembangan sebuah aplikasi sistem yang diusulkan.

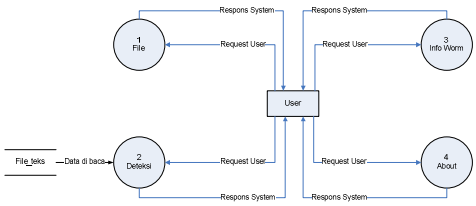
2.3 Desain

1. Diagram Konteks



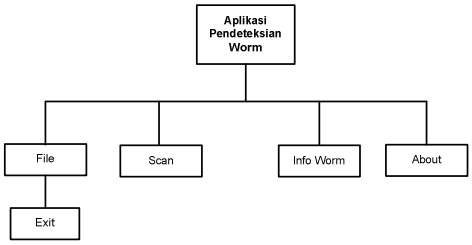
Gambar 3.7 Diagram Konteks Aplikasi Pendeteksian *Worm*

2. DFD Level 0



Gambar 3.8 DFD Level 0

3. Struktur Menu



Gambar 3.15 Struktur Menu Aplikasi

2.4 Implementasi

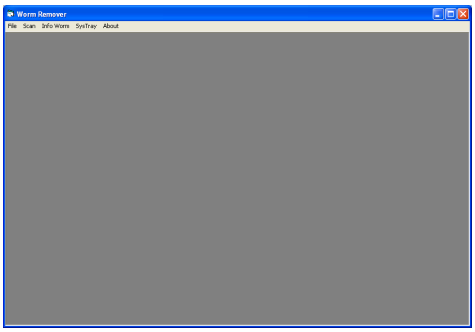
Perangkat lunak yang digunakan pada sistem komputer yang digunakan untuk membangun Aplikasi pendeteksian *worm* pada komputer adalah sebagai berikut:

1. Sistem Operasi *Windows XP Profesional SP 2*.
2. *Visual Basic* 6.0.
3.

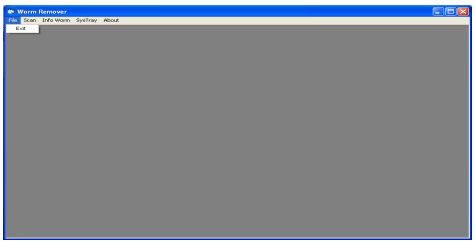
Kebutuhan minimum perangkat keras (*hardware*) yang diperlukan untuk mengimplementasikan program aplikasi yang dibuat adalah perangkat keras komputer PC *kompatibel* dengan spesifikasi yang disebutkan di bawah ini.

Kebutuhan minimumnya yaitu :

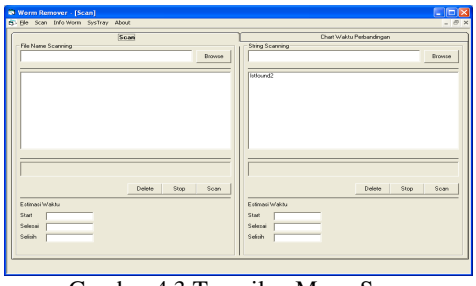
1. Processor : CPU Minimum 1.0 GHZ
2. Memory : Minimum 512MB RAM
3. Hardisk : Minimum Kapasitas 20 GB
4. VGA : Dengan Kecepatan Minimum 32 MB



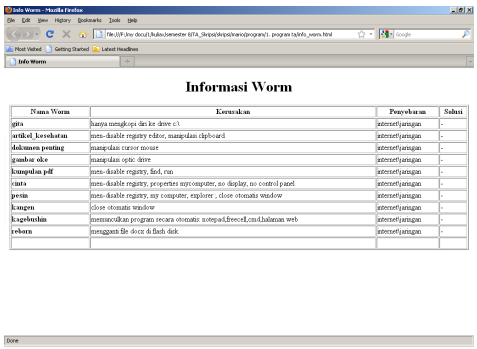
Gambar 4.1 Tampilan Menu Awal



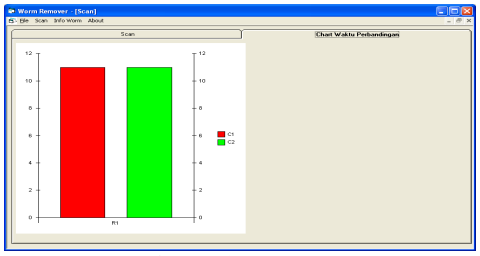
Gambar 4.2 Tampilan Sub Menu File



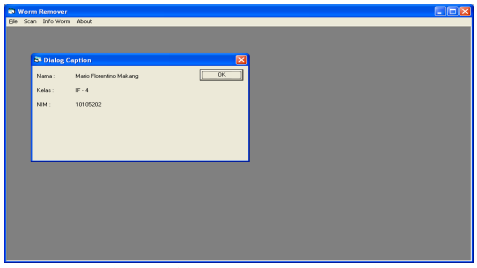
Gambar 4.3 Tampilan Menu Scan



Gambar 4.4 Tampilan Menu Info Worm



Gambar 4.5 Tampilan Sub Menu Chart



Gambar 4.6 Tampilan Menu About

3. HASIL DAN DISKUSI

3.1 Fasilitas Aplikasi

Aplikasi yang dibangun mempunyai kemampuan sebagai berikut:

1. Menerapkan dua metode yaitu *file name scanning* dan *string scanning*.

2. Dapat mendeteksi keberadaan worm pada suatu system computer (*known worm*).

3. Dapat menghapus *worm* yang terdeteksi.

4. Mengetahui performansi dari setiap metode dengan parameter waktu dan ketepatan hasil deteksi.

3.2 Perangkat Lunak

Aplikasi ini akan berjalan normal pada spesifikasi software sebagai berikut :

a. Sistem Operasi Windows

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

1. Aplikasi Pendeteksian Worm ini dibangun sudah mengimplementasikan dua metode yaitu *File Name Scanning* dan *String Scanning* pada aplikasi *infector file removal*.
2. Aplikasi Pendeteksian Worm ini dengan menggunakan dua metode yaitu *File Name Scanning* dan *String Scanning* pada aplikasi *infector file removal* telah mengidentifikasi file worm pada sistem komputer.
3. Aplikasi Pendeteksian Worm ini dengan menggunakan dua metode yaitu *File Name Scanning* dan *String Scanning* pada aplikasi *infector file removal* telah mampu menghapus file worm pada sistem komputer.
4. Perbandingan yang dilakukan terhadap dua metode menunjukan bahwa kedua metode memiliki kesamaan waktu deteksi dan keakuratan dari masing-masing metode adalah sama.

4.2 Saran

1. Teknologi scanning yang digunakan memudahkan untuk proses pendeteksian worm pada sistem komputer oleh siapa saja. Oleh karena itu, masalah keamanan harus selalu diperhatikan agar sistem dapat tetap terjaga dari pihak lain yang tidak berkepentingan, terlebih keamanan aplikasi pendeteksian ini.
2. Program aplikasi yang sudah dibangun hanya dapat mendeteksi worm yang sudah diketahui.
3. Data uji untuk kedua metode masih sangat minim. Jadi sangat dianjurkan untuk dikembangkan data uji yang lebih baik lagi.

5. DAFTAR PUSTAKA

[1]. Achmad Dharmal, (2006), *Computer Worm 1*, Jasakom, Jakarta.

[2]. Achmad Dharmal, (2006), *Computer Worm 2*, Jasakom, Jakarta.
[3]. Ilham Perdana, (2008), Petunjuk Penulisan Ilmiah, Perumusan Masalah, Pengumpulan Data Penelitian, Petunjuk Tata Tulis Ilmiah, *Handout Metodologi Penelitian*.
[4]. Wikipedia. (03 May 2009), *Visual Basic 6.0*, www.wikipedia.org/id
[5]. Wikipedia. (03 May 2009), *BASIC*, www.wikipedia.org/id
[6]. Indoskripsi. (03 May 2009), *Worms*, www.indoskripsi.com
[7]. Vbtutor. (03 May 2009), *Visual Basic 6.0*, www.vbtutor.net
[8]. Vb-bego. (03 May 2009), *Visual Basic 6.0*, www.vb-bego.com