UNIVERSITAS
MERCU BUANA

ANALISA DAN PERANCANGANGAN APLIKASI ANTIVIRUS BACKDOOR DENGAN MENGGUNAKAN VISUAL BASIC 6.0

EKA DIFA ANDIKA

01502- 021

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2009

UNIVERSITAS

MERCU BUANA

ANALISA DAN PERANCANGAN APLIKASI ANTIVIRUS BACKDOOR MENGGUNAKAN VISUAL BASIC 6.0

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Disusun oleh

EKA DIFA ANDIKA

01502-021

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2009

LEMBAR PENGESAHAN

Yang bertanda tangan di bawah ini menyatakan bahwa Laporan Tugas Akhir dari mahasiswa berikut ini :

Nama : Eka Difa Andika

NIM : 01502-021

Fakultas : Ilmu Komputer

Program Studi : Teknik Informatika

Judul : Analisa dan Perancangan Aplikasi Antivirus untuk Backdoor Menggunakan Visual Basic 6.0".

Yang bertanda tangan di bawah ini, menyatakan bahwa Laporan Tugas Akhir dari mahasiswa tersebut di atas, telah diuji dan dipresentasikan pada sidang tugas akhir serta telah disetujui dan disahkan sebagai Laporan Tugas Akhir.

Menyetujui,

(Raka Yusuf, ST,. MKom)
Pembimbing

Mengesahkan,

(Devi Fitrianah, S,.Kom MTI)
Koordinator Tugas Akhir

Mengetahui,

(Abdusy Syarif, ST,. MT)
Ketua Program Studi
Teknik Informatika

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Eka Difa Andika

NIM : 01502-021

Fakultas : Ilmu Komputer

Program Studi : Teknik Informatika

Menyatakan bahwa Laporan Tugas Akhir dengan judul :

Analisa dan Perancangan Aplikasi Antivirus untuk Backdoor Menggunakan Visual Basic 6.0".

Adalah hasil dari penelitian yang dilakukan oleh penulis sendiri, dan bukan merupakan jiplakan, kecuali kutipan-kutipan yang berasal dari sumber-sumber yang tercantum pada Daftar Pustaka.

Jakarta, Agustus 2009

Eka Difa Andika

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan hidayah dan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul "Aplikasi Antivirus Backdoor Menggunakan Visual Basic 6.0" dengan baik. Laporan Tugas Akhir ini ditulis untuk melengkapi persyaratan mencapai gelar sarjana strata satu (S1) Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Mercu Buana.

Dalam menyelesaikan laporan Tugas Akhir ini, penulis banyak mendapat bantuan berupa dukungan, sumbangan pikiran dan bimbingan yang sangat besar artinya. Untuk itu dalam kesempatan ini penulis mengucapkan terima kasih kepada :

1. Kedua orang tua tercinta hususnya ibu yang tanpa henti mengalirkan do'a untuk keselamatan dan keberhasilan penulis serta memberikan dukungan dan semangat baik spiritual, moril dan materil sehingga tugas ini dapat selesai pada waktunya.
2. Untuk adikku tercinta Didi Prayudi yang selalu memberikan dukungan dan semangat supaya penulis bisa menyelesaikan laporan tugas akhir.
3. Bapak Abdusy Syarif, ST., MT selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana.

4. Bapak Raka Yusuf, ST., MKom selaku Dosen Pembimbing Tugas Akhir yang telah banyak membantu penyusun dalam membuat laporan tugas akhir ini sampai selesai.
5. Untuk Yuli Yanti penulis ucapkan terima kasih telah membantu dan memberikan dukungan supaya penulis dapat menyelesaikan laporan tugas akhir ini.
6. Untuk teman - teman seperjuangan Teknik Informatika angkatan 2002, yoko, candra, ardi, dede, sofi, rian dan anak kosan belakang terima kasih atas dukungannya.

Semoga Allah SWT memberikan dan melimpahkan rahmat dan karunia-Nya atas segala bantuan yang telah diberikan kepada penulis. Akhir kata penulis mengharapkan tulisan ini dapat memberikan manfaat bagi penulis khususnya dan pembaca pada umumnya. Penulis menyadari bahwa tulisan ini tidak lepas dari kekurangan. Atas saran dan kritik yang membangun penulis mengucapkan terima kasih.

Jakarta, Agustus 2009

Eka Difa Andika

DAFTAR ISI

Halaman

JUDUL i

LEMBAR PENGESAHAN DOSEN ii

LEMBAR PERNYATAAN iii

ABSTRAK iv

ABSTRACT v

KATA PENGANTAR vi

DAFTAR ISI viii

DAFTAR GAMBAR xii

DAFTAR TABEL xiv

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Ruang Lingkup 2

1.3 Tujuan Pembahasan 3

1.4 Batasan Masalah 3

1.5 Metodologi 4

1.6 Sistematika Penulisan 5

BAB II LANDASAN TEORI

2.1 Model Sekuensial Linier 6

2.2 Unified Modelling Language (UML) 8

2.2.1 Diagram Use Case 9

2.2.2 Diagram Sekuensial 12

2.2.3 Diagram Aktifitas 14

2.3 Malware (*Malicious Software*) 15

2.4 Backdoor Komputer 16

2.4.1 Struktur Backdoor 17

2.4.2 Kemampuan Dasar Backdoor 19

2.4.3 Siklus Hidup Backdoor 21

2.5 Anti Virus 22

2.5.1 Program Removal 24

2.5.1.1 Launcher File Removal 26

2.5.1.2 Infector File Removal 27

2.5.2 Definition File 29

2.6 Registry 30

2.6.1 Struktur Dasar Registry 31

2.6.2 Bagian Registry dan Fungsinya 32

2.6.3 Value 33

BAB III ANALISIS DAN PERANCANGAN

3.1 Analisis 35

3.1.1 Diagram Use Case 36

3.1.2 Diagram Aktifitas 42

3.1.2.1 Diagram Aktifitas Untuk Use Case Melakukan Pendeteksian 43

3.1.2.2 Diagram Aktifitas Untuk Use Case Mengelola Data Signature 47
3.1.2.3 Diagram Aktifitas Untuk Use Case Melakukan Pencegahan dan Penggagalan 49
3.1.3 Diagram Sekuensial 53
3.1.3.1 Diagram Sekuensial Untuk Use Case Melakukan Pendeteksian 53
3.1.3.2 Diagram Sekuensial Untuk Use Case Mengelola Data Signature 54
3.1.3.3 Diagram Sekuensial Untuk Use Case Melakukan Pencegahan dan Penggagalan..... 55
3.2 Perancangan Tampilan 56
3.2.1 Rancangan Menu Pendeteksian 56
3.2.2 Rancangan Menu Signature..... 58
3.2.3 Rancangan Menu Option..... 59
3.2.4 Rancangan Tampilan Form CRC 59
3.2.5 Rancangan Tampilan Form Report..... 60
3.2.6 Rancangan Tampilan Form Konfigurasi Windows..... 61
3.2.6 Rancangan Tampilan Form Lihat Registry..... 62

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi 63
4.1.1 Pengkodean..... 63
4.1.2 Antarmuka..... 76

4.2 Pengujian 80

4.2.1 Metode Pengujian 82

4.2.2 Pengujian 81

4.2.3 Hasil Pengujian 84

4.2.4 Analisis Hasil Pengujian 90

BAB V PENUTUP

5.1 Kesimpulan 92

5.2 Saran 92

Lampiran L1

DAFTAR GAMBAR

Gambar 2.1 Model Sekuensial Linier..... 8

Gambar 2.2 Taksonomi program-program jahat..... 15

Gambar 2.3 Gambaran proses umum komponen backdoor..... 19

Gambar 2.4 Bagian struktur registry dalam *regedit*..... 32

Gambar 3.1 Diagram use case aplikasi antivirus..... 36

Gambar 3.2 Diagram aktivitas untuk use case melakukan pendeteksian 45

Gambar 3.3 Diagram aktifitas untuk use case mengelola data signature..... 48

Gambar 3.4 Diagram aktifitas untuk use case melakukan pencegahan dan penggagalan..... 51

Gambar 3.6 Diagram sekuensial untuk use case mengelola data signature... 55

Gambar 3.8 Rancangan menu pendeteksian dari aplikasi..... 57

Gambar 3.9 Rancangan menu *signature* dari aplikasi..... 58

Gambar 3.10 Rancangan menu *option* dari aplikasi..... 59

Gambar 3.11 Rancangan tampilan form CRC dari aplikasi..... 59

Gambar 3.12 Rancangan tampilan form *report* dari aplikasi..... 60

Gambar 3.13 Rancangan tampilan form konfigurasi windows dari aplikasi... 61

Gambar 3.14 Rancangan tampilan form lihat registry dari aplikasi..... 62

Gambar 4.1 Tampilan menu pendeteksian..... 77

Gambar 4.2 Tampilan aplikasi ketika pengguna menekan tombol browse pada menu pendeteksian..... 77

Gambar 4.3 Tampilan menu *signature*..... 78

Gambar 4.4 Tampilan form CRC..... 78

Gambar 4.5 Tampilan menu *option*..... 79

Gambar 4.6 Tampilan form konfigurasi windows ketika pengguna menekan tombol konfigurasi windows..... 79

Gambar 4.7 Tampilan form lihat registry ketika pengguna menekan tombol ok pada form konfigurasi windows..... 80

Gambar 4.8 Tampilan menu pendeteksian ketika menemukan file backdoor. 85

Gambar 4.9 Tampilan menu pendeteksian ketika pengguna menekan tombol delete tetapi tidak ada file yang dipilih..... 86

Gambar 4.10 Tampilan menu pendeteksian ketika pengguna menekan tombol reload..... 86

Gambar 4.11 Tampilan form CRC yang menampilkan nilai CRC dari file yang dipilih..... 87

Gambar 4.12 Tampilan menu signature ketika pengguna mengisi data signature backdoor..... 87

Gambar 4.13 Tampilan menu signature setelah pengguna menekan tombol add..... 88

Gambar 4.14 Tampilan file scan.dat yang mengalami perubahan setelah pengguna menekan tombol save..... 88

Gambar 4.15 Tampilan form konfigurasi windows setelah backdoor menginfeksi. 89

Gambar 4.16 Tampilan form lihat registry setelah backdoor memanipulasi registry..... 90

DAFTAR TABEL

Tabel 2.1. Jenis diagram resmi UML versi 2..... 9

Tabel 2.2. Notasi pemodelan diagram use case..... 10

Tabel 2.3. Notasi pemodelan diagram sekuensial..... 13

Tabel 2.4. Simbol-simbol pada diagram aktifitas..... 14

Tabel 3.1 Kebutuhan sistem, aktor dan use case pada aplikasi antivirus..... 36

Tabel 3.2 Mencari aktifitas di aliran utama dan alternatif pada use case melakukan pendeteksian..... 43

Tabel 3.3 Mengelola data signature dari dokumen use case..... 47

Tabel 3.4 Mencari aktifitas di aliran utama dan alternatif pada use case melakukan pencegahan dan penggagalan..... 49

Table 4.1 Tabel skenario pengujian 83

Table 4.2 Tabel hasil pengujian..... 84