DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

ABSTRAK i

ABSTRACT iii

KATA PENGANTAR iv

DAFTAR ISI vi

DAFTAR TABEL xii

DAFTAR GAMBAR xiii

DAFTAR SIMBOL xv

DAFTAR LAMPIRAN xvii

BAB I PENDAHULUAN

1.1. Latar Belakang Masalah 1

1.2. Identifikasi Masalah 2

1.3. Maksud dan Tujuan 3

1.4. Batasan Masalah 3

1.5. Metodologi Penelitian 4

1.6. Sistematika Penulisan 6

BAB II LANDASAN TEORI

2.1. Sejarah Worm Komputer 8

2.2. Perbedaan Worm Dan Virus 10

2.2.1 Definisi 12

2.2.1.1 Virus..... 12
2.2.1.2 Worm 12
2.2.2 Cara Penyebaran 13
2.2.2.1 Virus..... 13
2.2.2.2 Worm 13
2.3 Kemampuan dasar Worm..... 15
2.3.1 Kemampuan Reproduksi Dan Distribusi 16
2.3.2 Kemampuan Rekayasa Sosial 16
2.3.3 Kemampuan Menyembunyikan Diri 17
2.3.4 Kemampuan Mendapatkan Informasi..... 17
2.3.5 Kemampuan Mengadakan Manipulasi 17
2.4 Siklus Hidup Worm 17
2.4.1 Propagation Phase (Fase Penyebaran)..... 18
2.4.2 Dormant Phase (Fase Istirahat/Tidur) 18
2.4.3 Trigerring Phase (Fase Aktif) 18
2.4.4 Execution Phase (Fase Eksekusi)..... 18
2.5 Metode File Name Scanning 18
2.6 Metode String Scanning 19
2.7 Perkembangan Worm Non Lokal 19
2.5.1 Christma Exec..... 19
2.5.2 Morris 20
2.5.3 Happy99 20
2.5.4 Melisa 21

2.5.5 Pretty Park 22
2.5.6 Explore Zip 22
2.5.7 Bubble Boy 23
2.5.8 Love Letter 24
2.5.9 Hybris 25
2.5.10 Anna Kournikova 25
2.5.11 Sadmind 25
2.5.12 Code Red 26
2.5.13 Nimda 27
2.5.14 BadTrans.B 28
2.5.15 Slammer 29
2.5.16 Bagle 29
2.5.17 Netsky 30
2.8 Perkembangan Worm Lokal 31
2.6.1 I-Worm Perksa 31
2.6.2 Pesin 31
2.6.3 Tabaru 32
2.6.4 Kangen 32
2.6.5 Kumis 33
2.6.6 Decoil 33
2.6.7 Rontokbro 34
2.6.8 Nobron 34
2.6.9 Runitis 34

2.6.10 Bluefantasi 35
2.9 Diagram Arus Data (*Data Flow Diagram*) 36
2.10 Diagram Konteks 38
2.11 Data Flow Diagram Fisik 38
2.12 Data Flow Diagram Logika 39
2.13 Jaringan Semantik 39
2.14 MS. Visual Basic 6.0 39
BAB III ANALISIS DAN PERANCANGAN
3.1. Analisis Masalah 43
3.2. Langkah-Langkah Penyelesaian Masalah 44
3.3. Analisis Metode 47
3.3.1 Analisis Metode File Name Scanning 47
3.3.2 Analisis Metode String Scanning 48
3.4 Analisis Karateristik Worm 49
3.5 Analisis Pengenalan File Worm 51
3.5.1 File Name Scanning 51
3.5.2 String Scanning 52
3.6 Analisis Kerugian 53
3.6.1 Spionase Dan Pengumpulan Data 53
3.6.2 Pengrusakan Data 53
3.6.2 Pengrusakan Hardware 53
3.7 Analisis Keakuratan Metode 54
3.8 Analisis Kecepatan 54

3.9 Analisis Kebutuhan Non Fungsional 54
3.9.1 Analisis Perangkat Keras 54
3.9.2 Analisis Perangkat Lunak 55
3.9.3 Analisis Kebutuhan Pengguna 55
3.10 Analisis Basis Data 55
3.11 Analisis Kebutuhan Fungsional 56
3.11.1 Diagram Konteks 56
3.11.1.1 DFD Level 0 57
3.11.1.2 DFD Level 1 Proses 2 58
3.11.1.3 DFD Level 2 Proses 2.1 58
3.11.1.4 DFD Level 3 Proses 2.1.1 59
3.11.1.5 DFD Level 3 Proses 2.1.2 59
3.11.1.6 DFD Level 4 Proses 2.1.1.2 60
3.11.1.7 DFD Level 4 Proses 2.1.2.2 60
3.12 Spesifikasi Proses 61
3.13 Perancangan Struktur Menu 69
3.14 Perancangan Antar Muka 70
3.15 Perancangan Pesan 73
3.16 Jaringan Semantik 74

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi 76
4.1.1 Perangkat Lunak Pembangun 76
4.1.2 Perangkat Keras Pembangun 76

4.1.3 Implementasi Antarmuka 77
4.1.3.1 Antarmuka Menu Utama 77
4.1.3.2 Antarmuka Sub Menu File 77
4.1.3.3 Antarmuka Menu Scan 78
4.1.3.4 Antarmuka Info Worm 78
4.1.3.5 Antarmuka Chart 79
4.1.3.6 Antarmuka Profile 79
4.2 Pengujian 80
4.2.1 Rencana Pengujian 80
4.2.2 Kasus Dan Hasil Pengujian Alpha 82
4.2.2.1 Pengujian File Name Scanning 82
4.2.2.2 .....
Pengujian String Scanning 83
4.3 Pengujian Waktu File Name Scanning 84
4.4 Pengujian Waktu String Scanning 85
4.5 Kesimpulan Hasil Uji 88
4.6 Kasus dan Hasil Pengujian Betha 88
4.7 Kesimpulan Hasil Pengujian Betha 93
BAB V KESIMPULAN DAN SARAN
5.1 Kesimpulan 94
5.2 Saran 94
DAFTAR PUSTAKA 96