

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Saat ini sudah banyak program jahat yang mengganggu keamanan sistem komputer. Bahkan, komputer saat ini tidak luput dari program jahat sekecil apapun. Contohnya virus ganas pernah menyerang Indonesia bulan September 2006. Dari total 1271 kasus, penyerangan virus ter ganas mendalangi 461 kasus [7]. Menurut Kaspersky sekitar 52,03% komputer di Indonesia terinfeksi malware [11]. Angka tersebut menempatkan Indonesia dalam ranking ke-17 dunia dalam tingkat infeksi malware. Sayangnya di Indonesia sendiri belum memiliki data statistik yang akurat tentang penyebaran malware di Indonesia. Yang memiliki data statistik malware di Indonesia justru pihak luar. Terutama para vendor antivirus seperti Kaspersky. Untuk mengatasi polemik tersebut, ID-CERT berinisiatif menggagas survey malware yang bertujuan untuk mendapatkan data real dari jenis malware yang tersebar di Indonesia, dengan merancang sebuah server pendukung survey malware berbasis *mail server*.

Metode yang digunakan yaitu mencari relawan yang ingin ikut serta dalam kegiatan survey malware. Relawan diminta melakukan pendeteksian malware (*scanning*) pada komputer atau laptop yang dimiliki dengan aplikasi pihak ketiga yang dikhususkan untuk melakukan pendeteksian malware. Setelah pendeteksian malware selesai, relawan diminta mengirimkan hasil *scanning (log report)* ke email ID-CERT. Kemudian secara otomatis sistem server melakukan proses *parsing* terhadap laporan malware yang diterima dan memasukan hasil parsing tersebut ke *database*.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka rumusan masalahnya adalah :

1. Bagaimana membangun mail server untuk pendukung kegiatan survey malware ID-CERT?
2. Bagaimana cara membangun aplikasi parser untuk melakukan parsing data dari email responden?

1.3 Tujuan

Adapun tujuan dari proyek akhir ini yang diharapkan tercapai ialah sebagai berikut:

1. Membangun mail server pendukung kegiatan survey malware ID-CERT.
2. Membangun aplikasi parser untuk melakukan parsing data dari email relawan.

1.4 Batasan Masalah

Untuk menghindari meluasnya pokok pembahasan, maka pengerjaan penelitian ini terbatas pada :

1. Sistem operasi yang digunakan adalah FreeBSD.
2. Mengimplementasikan *mail server* untuk menerima laporan berupa *log* yang dikirimkan oleh relawan.
3. *Tools* tambahan pendukung yaitu iRedMail sebagai perangkat lunak *mail server*, dan PHP sebagai dasar bahasa pemrograman yang digunakan untuk aplikasi *parser*.
4. Pembahasan dititik tekankan pada *mail server* dan *parser*.
5. Aplikasi Parser digunakan untuk mengolah email dari relawan berupa *log report*.

6. Data yang telah berhasil didapatkan akan dimasukkan kedalam database *survey*.
7. Aplikasi hanya mem-*parsing* data berupa mailform, timestamp, dan nama malware dari email yang diterima.
8. Data yang digunakan adalah laporan dari relawan *survey malware*.

1.5 Definisi Operasional

1. *Server* atau peladen merupakan sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. ^[4]
2. *Malware* merupakan singkatan dari *malicious software* adalah perangkat lunak berbahaya yang dirancang untuk merusak sebuah komputer independen atau sebuah jaringan komputer. ^[1]
3. Dalam ilmu komputer, istilah *parsing* digunakan dalam komputasi *linguistic* untuk melakukan sebuah proses analisis terhadap serangkaian simbol, kalimat atau string lain dalam bahasa alami atau dalam bahasa komputer, sesuai dengan aturan tata bahasa secara formal. ^[2]
4. *Mail Server* merupakan sebuah komputer yang berfungsi sebagai kantor pos elektronik untuk *email*. Pesan yang dipertukarkan di jaringan berlalu antara *mail server* yang menjalankan software yang dirancang khusus. Perangkat lunak ini dibangun pada protokol yang disepakati, standar untuk menangani pesan dan file data (seperti foto, multimedia atau dokumen) yang mungkin melekat kepada mereka. ^[8]

1.6 Metode Pengerjaan

Langkah yang akan dikerjakan dalam menyelesaikan proyek akhir ini antara lain:

1. Studi Literatur

Dilakukan pengumpulan data-data yang berkaitan dengan server pendukung survey malware. Data dapat bersumber dari *website*, buku, wawancara atau penelitian yang pernah dilakukan sebelumnya.

2. Analisis Kebutuhan

Pencarian referensi berhubungan mail server dan pembuatan aplikasi parser.

3. Perancangan Sistem

Tahap perancangan sistem dengan membuat skema arsitektur server pendukung survey malware.

4. Implementasi Sistem

Untuk implementasi pembangunan *mail server*, dilakukan dengan melakukan instalasi sebuah komputer *server* menggunakan FreeBSD dan mengintegrasikan aplikasi parser dengan *mail server*.

5. Pengujian Sistem

Pengujian dilakukan dengan menjalankan serangkaian *step* seperti yang dilakukan oleh relawan. Mengirimkan sebuah log *report malware* ke email ID-CERT, *mail server* yang dimiliki telah diintegrasikan dengan aplikasi parser. Kemudian akan didapatkan hasil *parsing* lalu dimasukkan ke dalam *database* pada *server*.

6. Pembuatan Laporan

Mencatat dan menyusun laporan tentang proyek akhir yang dikerjakan selama pengerjaan proyek akhir tersebut.

1.7 Jadwal Pengerjaan

Tabel 1.1 Jadwal Pengerjaan

No	Kegiatan	Waktu Pelaksanaan Tahun 2017																			
		Januari				Februari				Maret				April				Mei			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur	■	■	■	■																
2	Analisis Kebutuhan		■	■	■	■															
3	Perancangan Sistem					■	■	■	■	■											
4	Implementasi Sistem									■	■	■	■	■	■	■	■	■	■		
5	Pengujian Sistem																	■	■	■	■
6	Pembuatan Laporan			■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■