1. PENDAHULUAN

5.1 Latar Belakang Masalah

Serangan virus, *spyware* dan program membahayakan lainnya semakin meningkat kuantitas maupun kualitasnya. Hal tersebut terjadi karena semakin berkembangnya ilmu tentang *security* komputer dan kelemahan – kelemahan yang ditemukan dalam sebuah sistem.

Spyware adalah program yang mampu memata-matai aktivitas pengguna komputer, dimana salah satunya adalah dapat merekam ketukan *keyboard* yang disebut *keylogger*. Pembuat *keylogger* berargumentasi betapa produk yang mereka buat sangat berguna untuk mencegah kerugian namun lebih banyak yang menganggap *keylogger* sebagai ancaman.

Keylogger merupakan sebuah perangkat, baik perangkat lunak maupun keras, bekerja di belakang layar atau tidak akan diketahui oleh user, yang menyebabkan setiap penekanan tombol akan dicatat. *Keylogger* dapat merekam apa saja yang user ketik, baik itu *username*, *password*, *email*, dokumen, dan lainnya.

Perangkat keras *keylogger* merupakan benda berwujud yang dapat disentuh, diraba, dan dipegang. Perangkat keras *keylogger* dipasang pada ujung kabel *keyboard* yang berperan sebagai perantara *keyboard* dengan *Central Processing Unit* (CPU). Berbeda dengan perangkat keras, perangkat lunak *keylogger* sama seperti perangkat lunak lainnya, yang harus diinstal terlebih dahulu sebelum digunakan.

Ada lima metode yang banyak digunakan oleh perangkat lunak *keylogger* diantaranya *hypervisor-based*, *kernel-based*, *hook-based*, *passive-method*, dan *form grabber based*. Kemudian di antara lima metode tersebut *passive method* adalah teknik yang paling banyak digunakan oleh pembuat *keylogger*. Metode ini banyak menggunakan fungsi Windows API (*Appication Programming Interface*) di antaranya dengan memanfaatkan fungsi *GetAsyncKeyState(), GetForegroundWindow(), GetWindowText(), GetCapsState(), dan GetShiftState()*. Fungsi tersebut digunakan untuk merekam segala aktivitas *keyboard* yang nantinya akan disimpan ke dalam file log tertentu dan dikirim ke sebuah alamat FTP Server atau Email seseorang.

Jika *keylogger* tersebut digunakan untuk aktivitas positif, misalnya seorang administrator jaringan yang ingin mengetahui aktivitas apa saja (monitoring) yang dilakukan oleh user dalam *Local Area Network* (LAN) dimana dalam LAN tersebut memiliki jumlah komputer yang cukup banyak dan dengan asumsi LAN tersebut tidak terkoneksi langsung dengan internet maka fungsi pengiriman file log tersebut ke sebuah FTP Server atau Email seseorang menjadi sia – sia. Selain itu administrator harus mempunyai akses secara langsung ke komputer target monitoring untuk mengambil file lognya. Jika keadaannya demikian maka proses monitoring akan menjadi sangat lama.

Salah satu solusi media pengiriman file log selain FTP dan Email adalah menggabungkan *control keylogger* dengan *spy agent*. *Spy agent* akan sengaja dijalankan di semua komputer client dalam LAN. *Spy agent* ini akan melakukan

tugasnya sebagai *keylogger* yang akan merekam segala aktivitas *keyboard* user. *Spy agent* tidak akan membuat file log dalam komputer client karena memungkinkan user untuk menghapusnya jika file log tersebut secara tidak sengaja ditemukan oleh user. *Spy agent* ini hanya akan menyimpan semua aktivitas *keyboard* user dalam memori komputer. Selain itu *spy agent* harus diberikan kemampuan bertahan seperti mampu menggandakan diri (file ganda) agar mampu saling mengawasi dan bertahan dari serangan antivirus. Sedangkan *control keylogger* dapat menghubungi *spy agent* mana yang akan diambil file lognya. File log ini nantinya akan disimpan di dalam komputer server yang lebih aman.

Dalam implementasinya dibutuhkan *windows socket* yang akan menghubungkan *control keylogger* dengan *spy agent*. Dengan mekanisme ini proses monitoring aktivitas *keyboard* user diharapkan akan menjadi lebih cepat untuk studi kasus LAN yang mempunyai cukup banyak komputer dan LAN tersebut tidak terkoneksi internet secara langsung.

5.2 Perumusan Masalah

Dalam tugas akhir ini terdapat beberapa rumusan masalah sebagai berikut :

1. Bagaimana membuat perangkat lunak (*spy agent*) yang bertujuan untuk monitoring aktivitas *keyboard* user dalam jaringan LAN.
2. Teknik bertahan seperti apa yang digunakan oleh *spy agent* agar tidak mudah ditemukan dan dilumpuhkan baik oleh antivirus maupun user.
3. Bagaimana memanfaatkan Microsoft Winsock Control untuk menghubungkan *control keylogger* dengan *spy agent* menjadi satu sistem yang terintegrasi.

Dengan batasan masalah dalam tugas akhir ini adalah sebagai berikut :

1. Aktivitas keyboard user yang akan di-*monitoring* meliputi data *keyboard state*, c*aption window*, dan data *clipboard*.
2. Sistem yang dibuat dirancang untuk berjalan dalam LAN berbasis Windows XP.
3. *Control keylogger* akan dijalankan pada komputer server dan *spy agent* akan sengaja dijalankan pada komputer client.
4. Sistem berjalan pada jaringan lokal yang tidak terkoneksi internet.

5.3 Tujuan

Tujuan dari tugas akhir ini adalah :

1. Membuat perangkat lunak *control keylogger* dan *spy agent* yang dapat merekam aktivitas *keyboard* dengan metode file ganda sebagai teknik bertahan *spy agent* dan memanfaatkan Microsoft Winsock Control sebagai media penghubung antara *control keylogger* dan *spy agent*.
2. Menganalisis cara kerja antivirus dan *firewall* dalam menemukan dan menghapus *spy agent*.

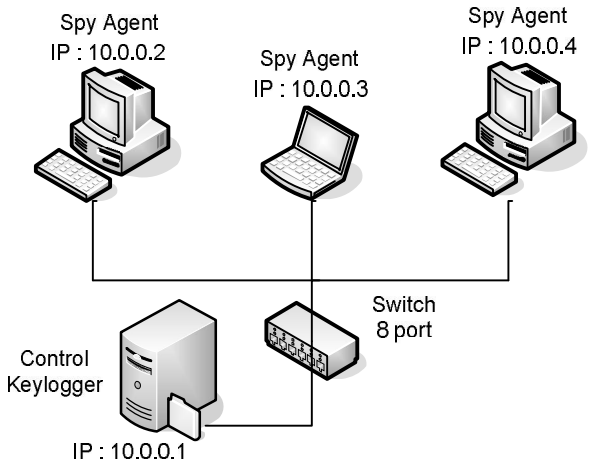
5.4 Metodologi Penyelesaian Masalah

Metodologi yang digunakan adalah sebagai berikut :

1. Identifikasi masalah
   Memanfaatkan Microsoft Winsock Control sebagai media penghubung *control keylogger* dan *spy agent* agar file log hasil monitoring aktivitas *keyboard* dapat dikirim melalui LAN.

2. Studi literatur
   Mencari dan memelajari mengenai teknik – teknik bertahan yang digunakan oleh *keylogger*, memanfaatkan Windows API untuk keperluan merekam data *keyboard state*, serta memahami jaringan komputer berbasis Windows XP.

3. Analisis dan perancangan
   - Menganalisis kebutuhan sistem terhadap perangkat lunak yang dibuat, dalam hal ini *control keylogger* dan *spy agent.*
   - Merancang bentuk topologi yang digunakan untuk pengujian. Untuk memudahkan implementasi maka topologi yang digunakan adalah Star dengan bentuk sebagai berikut :



Gambar 1. Desain Topologi Jaringan

Jumlah komputer yang ada di LAN ada 4 unit, 1 sebagai server, tempat dimana *control keylogger* akan dijalankan, dan 3 unit yang lain sebagai client yang di dalamnya akan dijalankan *spy agent.* Semua sistem operasi yang akan digunakan adalah Windows XP.

4. Implementasi
   Implementasi dari hasil perancangan yang sudah ada ke dalam bahasa pemrograman Visual Basic 6 (VB6) karena VB6 dapat berjalan dengan baik pada sistem operasi Microsoft Windows.

5. Pengujian Sistem

Melakukan pengujian terhadap perangkat lunak yang dibuat berdasarkan skenario pengujian. Skenario pada komputer client :

- *Spy agent* akan dijalankan disetiap komputer client.
- User akan diminta melakukan aktivitas yang menggunakan *keyboard* seperti mengetik sebuah dokumen.
- Komputer client yang menjadi target *spy agent* akan diinstal antivirus yang berbeda – beda.

Sedangkan skenario pada komputer server :

- *Control keylogger* akan dijalankan pada komputer server.
- *Control keylogger* akan melakukan koneksi dengan salah satu komputer client dan me-*request* terhadap file log yang telah direkam sebelumnya oleh *spy agent*.
- File log yang telah berhasil dikirim oleh *spy agent* akan disimpan di komputer server sehingga mudah untuk dikelola.

Kemudian akan dilakukan analisis hasil pada faktor – faktor berikut ini :

- Melihat kemampuan bertahan *spy agent* pada komputer yang terinstal antivirus.
- Melihat mampu tidaknya *spy agent* dalam merekam aktivitas *keyboard* kemudian mengirimnya lewat LAN.
- Hasil dari analisis tersebut kemudian akan dibandingkan dengan hipotesis awal seperti yang telah dijelaskan dalam tujuan penelitian.

6. Penyusunan laporan

Membuat laporan tugas akhir yang memuat kesimpulan dan saran terhadap sistem yang dibuat.

5.5 Sistematika Penulisan

Tugas akhir ini ditulis dengan sistematika sebagai berikut :

1 : Pendahuluan

Bab ini berisi latar belakang, perumusan masalah dan batasan masalah, tujuan, metodologi penyelesaian masalah dan sistematika penulisan.

2 : Dasar Teori

Bab ini berisi penjelasan mengenai konsep *spyware*, *keylogger*, *watcher method*, Windows-32 API, dan Windows Socket API.

3 : Analisis dan Perancangan Sistem

Bab ini berisi penjelasan mengenai gambaran umum sistem yang dibuat, analisis kebutuhan sistem yaitu penjelasan fungsi – fungsi API apa saja yang digunakan, analisis kebutuhan *control keylogger*

dan *spy agent*. Selanjutnya akan dipaparkan perancangan sistem yang dibuat serta perancangan antarmuka aplikasinya.

4 : Implementasi dan Pengujan Sistem
Bab ini berisi penjelasan mengenai lingkungan implementasi sistem dan rencana pengujian. Setelah itu sistem diuji berdasarkan skenario pengujian yang telah ditentukan. Hasil pengujian tersebut akan dilihat berdasarkan parameter uji apakah telah sesuai dengan tujuan penelitian.

5 : Kesimpulan dan Saran
Bab ini berisi kesimpulan dan saran terhadap sistem yang dibuat.