BAB III

LANDASAN TEORI

3.1. Pengertian dan Sejarah Virus Komputer

Pengertian virus komputer adalah suatu program yang menempel dan menjadi bagian dari rutinitas program lainnya dengan keistimewaan dapat menggandakan dirinya (Sutarman, 2009). Pengertian virus komputer secara umum, virus adalah suatu jenis program yang memiliki kemampuan menduplikasikan diri di mana hasil duplikasinya berbeda dengan aslinya tergantung jenis virusnya dan membutuhkan tempat untuk memperbanyak diri

Awal ditemukannya istilah virus dalam dunia komputer ialah pada tahun 1949 berangkat dari seorang pakar di bidang komputer, John Von Neumann dengan teori self altering automata. Hal ini menjadi inspirasi bagi para programmer di Lab BELL (AT&T) pada tahun 1960 dengan mencoba membuat suatu jenis program permainan yang dapat memperbanyak dirinya dan menghancurkan semua program buatan lawannya. Program yang dapat bertahan dan juga menghancurkan semua program lain, maka akan dianggap sebagai pemenangnya. Permainan ini menjadi jenis game yang favorit di setiap laboratorium komputer. Akan tetapi, semakin lama program ini semakin berbahaya karena dapat menghapus program yang tidak saja terlibat dalam permainan tersebut, akan tetapi juga pada program lain yang berguna.

Istilah virus komputer kemudian dikenalkan oleh seorang peneliti Asisten Professor di Universitas Cincinati, Ohio (Amerika Serikat), Fred Cohen pada tahun 1984 dalam makalahnya Computer Viruses-Theory and Experiments yang

kemudian disambut baik oleh peserta. Cohen menjelaskan virus komputer dan menggambarkan eksperimen yang dilakukannya untuk membuktikan eksistensi virus komputer dalam rangka menyusun disertasi untuk meraih gelar Ph.D.

Berdasarkan metode penyebaran virus komputer dan cara melakukan infeksi pada organisasi lain yang serupa dengan virus pada istilah kesehatan maka menjadi pembicaraan serius. Dalam waktu dekat kemudian bermunculan pemrograman lain yang membuat program sejenis dengan variasi dan cara penyerangan yang berbeda-beda.

Dalam Sejarahnya, awal mula kemunculan virus tidak bertujuan untuk merugikan orang lain. Namun, perkembangan selanjutnya virus dijadikan sebagai ajang untuk balas dendam terhadap sistem atau kelompok pengguna komputer tertentu, sekedar bercanda untuk mengganggu sistem orang lain, eksperimen untuk mengetahui apakah virus bekerja dengan baik atau tidak. Penggunaan virus yang semulanya hanya dijadikan permainan (game), malah digunakan untuk merugikan orang lain dengan merusak sistemnya.

3.2 Jenis-jenis Virus Komputer

Sejalan dengan perkembangan kemampuan orang menguasai suatu bidang bahasa pemrograman, maka semakin banyak jenis jenis virus komputer yang beredar di masyarakat (Pratikno, 2008). Beberapa jenis jenis virus komputer yang umum beredar pada saat ini.

1. Jenis Virus Makro

Jenis virus ini ditulis dengan bahasa pemrograman dari suatu aplikasi bukan dengan bahasa pemrograman dari suatu operating system. Jenis virus komputer ini dapat berjalan apabila aplikasi pembentuknya dapat berjalan dengan baik, jenis virus ini biasanya menempel pada file aplikasi berbasis dokumen, antara lain pengolah kata (ekstensi .doc pada Ms. Word), pengolah spreedsheet (ekstensi .xls pada Ms. Excel) dan lainnya. Contoh virus komputer ini :

- Varian W97M. Panther dengan panjang 1234 bytes, akan menginfeksi NORMAL.DOT dan menginfeksi dokumen apabila dibuka.
- WM.Twno.A, TW dengan panjang 41984 bytes, yang akan menginfeksi dokumen Ms. Word dengan menggunakan bahasa makro, biasanya berekstensi *.DOT dan *.DOC.

2. Jenis Virus Boot Sector

Jenis virus komputer ini yaitu berkemampuan menggandakan dirinya dan memindahkan atau menggantikan boot sector asli dengan booting virus. Pada saat terjadi booting, virus akan di-load ke memori dan selanjutnya virus komputer ini akan mempunyai kemampuan mengendalikan hardware standar (contoh : monitor, printer) dan dari memori ini pula virus akan menyebar ke seluruh drive yang ada dan yang terhubung ke komputer. Contoh virus komputer ini : Varian virus wyx, wyx.C(B), jenis virus yang menginfeksi boot record dan floopy dengan panjang 520 bytes; karakteristik : memory resident dan terenkripsi.

3. Jenis Virus Stealth Virus

Jenis virus komputer ini berkemampuan untuk mengendalikan instruksi-instruksi level DOS dan biasanya mereka tersembunyi sesuai namanya, baik secara penuh atupun sesuai ukurannya. Contoh virus komputer ini : Vmem(s) menginfeksi file file *.EXE, *.SYS dan *.COM panjang file 3275 bytes, menetap dimemori, ukurannya tersembunyi, dienkripsi.

4. Jenis Virus Polymorphic

Jenis virus komputer ini berkemampuan untuk mengecoh program dari antivirus, dalam hal ini berarti bahwa virus tersebut selalu berusaha agar tidak dikenali oleh antivirus dengan cara selalu mengubah-ubah strukturnya setiap kali selesai menginfeksi file atau program lain (Kurniawan, 2010). Contoh virus komputer ini : Nightfall yang menginfeksi file *.EXE dan *.COM, panjang file 1963 bytes, menetap di memori, ukuran dan virus tersebut tersembunyi, terenkripsi dan dapat berubah ubah strukturnya.

5. Jenis Virus File atau Program

Jenis virus komputer ini menginfeksi file-file yang dapat dieksekusi langsung dari sistem operasi, baik itu file *.EXE maupun *.COM. Biasanya juga hasil infeksi dari virus komputer ini dapat diketahui dengan berubahnya ukuran file yang diserangnya.

6. Jenis Virus Partition

Jenis virus komputer ini merupakan gabungan dari jenis virus boot sector dan jenis virus file. Artinya, pekerjaan yang dilakukan berakibat dua, yaitu dapat menginfeksi file-file *.EXE atau *.COM dan juga menginfeksi boot sector.

3.3 Komputer *Server*

Komputer *server* adalah salah satu infrastruktur yang paling penting dalam organisasi mana pun. *Server* adalah sebuah komputer yang mengatur lalu lintas data yang terjadi pada sebuah jaringan. Aplikasi yang disimpan di komputer ini dan terminal komputer lain terhubung dapat mengaksesnya. *Server* merupakan induk dari segala komputer yang terhubung pada sebuah jaringan yang berfungsi sebagai pengatur sistem jaringan, misalnya untuk pembatasan akses dan melakukan control data.

Fungsi *server* secara umum dilakukan oleh sebuah komputer adalah

a. menyimpan aplikasi dan *database* yang di butuhkan oleh komputer yang terhubung.

b. menyediakan fitur keamanan komputer.

c. melindungi semua komputer yang terhubung menggunakan firewall.

d. menyediakan *IP Address* untuk mesin komputer terhubung.

Server yang dipilih untuk sebuah organisasi harus memenuhi kondisi tertentu antara lain:

a. Dibutuhkan ukuran memori atau RAM yang cukup besar untuk menampung jumlah query yang dijalankan oleh komputer yang terhubung. Hal ini dikarenakan komputer *server* memberikan layanan kepada sejumlah besar komputer maka dibutuhkan memori yang besar untuk mendukung tugas utamanya.

b. Aspek berikutnya adalah dibutuhkan untuk mengelola, adalah kecepatan prosesor. Kecepatan prosesor biasanya di ukur dalam *Giga Hertz*. Kemampuan prosesor adalah menjalankan semua perintah yang dimioleh mesin. Hal ini sangat diperlukan bahwa server harus memiliki kecepatan prosesor yang optimal, oleh karena itu prosesor yang digunakan adalah kemampuannya memberikan fasilitas *multitasking.*

c. Kapasitas penyimpanan *hard drive* dari komputer *server*, haruslah besar untuk dapat menyimpan semua data. Dalam sebuah jaringan, pengguna komputer umumnya menyimpan informasi yang dibutuhkan oleh komputer *client*.

Berbagai jenis-jenis komputer *server* dapat dikategorikan dalam dua kategori utama.

1. Dedicated Server

Jenis *server* yang melakukan fungsi tertentu, seperti web hosting. ada berbagai layanan *web hosting*, yang menggunakan *dedicated server* untuk situs *web hosting*. Perusahaan tertentu juga telah mendedikasikan *server* komputer untuk menyimpan situs *web* mereka sendiri. Jenis *server* ini sangat kuat karena harus menangani lalu lintas *web* yang mencoba untuk mengakses halaman *web* yang terkandung di dalamnya.

2. *Non - dedicated server* (*Server* Bersama)

Sebuah komputer *server* bersama adalah *server* biasa, yang digunakan dalam jaringan komputer untuk beberapa pengguna. Sejumlah besar aplikasi, database disimpan di dalamnya. Pengguna yang berbeda terhubung ke *server*, mengakses *server* tergantung pada kebutuhan mereka. *Server* ini tidak perlu disesuaikan seperti *dedicated server*. Contoh yang paling umum untuk jenis *server* ini adalah *server* aplikasi. Sebuah *server* aplikasi menyimpan semua informasi yang diperlukan oleh orang-porang dalam jaringan.

3.4. Windows *Server* 2008

Windows *Server* 2008, adalah sebuah versi baru Windows *Server*, yang dirilis pada tanggal 27 Februari 2008. Pada saat pengembangannya, Windows *Server* memiliki nama kode "*Windows Server Codenamed Longhorn."* Windows *Server* 2008 dibangun di atas beberapa keunggulan teknologi dan keamanan yang pada awalnya diperkenalkan dengan Windows Vista, dan ditujukan agar bisa lebih modular secara signifikan, ketimbang pendahulunya, Windows *Server* 2003.

Windows *Server* 2008 dikembangkan dari Windows *Server* 2003 R2 yang sudah terbukti cukup andal dan aman, untuk membantu meringankan tekanan tersebut, dengan mengotomatisasikan tugas pengelolaan harian, memperketat pengamanan, meningkatkan efisiensi dan keandalan sistem (Utama, 2008).

Feature utama yang menjadi keunggulan Windows *Server* 2008 ini adalah penyederhanaan tugas administrasi, karena riset internal Microsoft, sekitar 70 persen anggaran belanja TI dihabiskan untuk tugas pengelolaan harian.

3.4.1. Kelebihan Windows *Server* 2008

1. Windows *Server* 2008 dapat beroperasi tanpa tampilan grafis atau *graphical user interface* (GUI) dengan adanya teknologi *powershell.*
2. Pengguna dapat memilih fungsi-fungsi yang dibutuhkannya saja atau menambah fungsi lainnya jika membutuhkan sewaktu-waktu tanpa melakukan instalasi ulang.
3. Kemampuan virtualisasi bahkan *embedded* (menyatu) dengan Windows *Server* 2008.
4. Windows *Server* 2008 mampu mengatur besar bandwidth yang dapat dipakai setiap aplikasi maupun komputer yag terhubung ke jaringan.
5. Windows *Server* 2008 juga sanggup mengontrol keamanan jaringan dengan fitur *Network Access Protection*.
6. *Server* juga dapat mengatur setiap akses identitas ke jaringan agar aman dan praktis dengan adanya fitur *read only domain controller*.
7. Melalui powershell, administrator tetap dapat memantau komputer di jaringan dari jarak jauh.
8. Lebih aman dalam mengendalikan laju informasi.
9. Peningkatan Kapasitas *Server* untuk melayani lebih Simultan Koneksinnya.
10. Driver disk yang fault toleran yang mendukung disk mirroring dan disk stripping dengan parity (RAID 1 dan RAID 5).
11. Bebas dari Kode 16 Bit milik MS-Dos,mendukung operasi 32 bit dan semua Fitur yang ditawarkan oleh Microprosesor 32 bit seperti dapat mengamati memori hingga 4 Gb dan Terproteksi.

12. Di Desain agar kompatibel dengan Sistem Operasi terdahulu seperti MS-Dos,IBM OS/2.
13. Peningkatan kemampuan layanan server TCP/IP seperti DHCP,WNS dan DNS.
14. Tool untuk mengintegrasikan Netware dan memonitoring Jaringan.
15. Model keamanan berbasis Domain penuh.
16. Terdapat Layanan untuk Macintosh.
17. Bisa Membooting jarak jauh untuk client.
18. Terintegrasi Paket Back Office.
19. Terdapat *Network Client Administrator.*
20. Fitur pengendalian yang lebih baik (*more control*).

3.4.2. Kekurangan Windows Server 2008:

1. Browser yang digunakan sebagai sistem dasar pada sistem perangkat bantu administrasi banyak menggunakan Javascript dan Active X, ternyata mengakibatkan proses sangat lambat. Hal yang sama dengan PC yang menggunakan processor 300 MHz AMD dan 128 MB SDRAM serta 100 MHz Bus tidak bisa diharapkan bekerja dengan lancar seperti yang diharapkan.
2. Pengubahan konfigurasi yang mendasar jarang dapat dilakukan dengan berhasil. Hal ini berlaku untuk nilai default, Format file Log yang bersifat propritary dan juga pilihan default-indeks, yang kesemuanya secara standar selalu harus disimpan pada drive C. Administrator dalam hal ini

harus melakukan pekerjaan yang tak perlu, hingga sistem keseluruhan berjalan sebagaimana mestinya, sebelum dapat melakukan perubahan.

3. Dokumentasi online, yang praktis tidak diperlukan, ketika sistem keamanan tertinggi Active X telah dipilih menyebabkan strategi keamanan yang kurang baik pada IIS.
4. Dibutuhkan pengubahan konfigurasi yang sangat kompleks untuk ISS *Server,* yang dapat dikatakan sangat sulit dan merepotkan sekali. Dari pihak administrator berpendapat kegiatan perubahan file Registry adalah pekerjaan yang relatif berat untuk sistem yang menggunakan Windows NT sebagai sistem operasinya.

3.5. *Symantec Endpoint Protection Manager*

Dalam memilih program antivirus untuk komputer seharusnya memilih yang terbaik karena kita berharap banyak darinya dalam rangka mengawal komputer dari awal sampai akhir dari serangan virus. Ada beberapa antivirus dunia yang hadir di pasaran baik itu berbayar maupun gratis. Salah satunya adalah produk keluaran *Symantec* terbaru yaitu *Symantec Endpoint Protection 12.1* yang merupakan antivirus terdepan dan handal, untuk melindungi komputer dari serangan berbagai virus yang terus berkembang setiap harinya.

Dengan mengusung tagline: *"Unrivaled security, Blazing performance, Built for virtual environments"*, tidak diragukan lagi *Symantec Endpoint Protection* 12.1 semakin unggul dan terdepan yang mampu bekerja cepat juga powerful dalam melindungi user dari serangan virus physical ataupun virtual pada sistem komputer. *Symantec Endpoint* juga sangat mudah dalam

pengimplementasian dan integrasi tools security kedalam satu paket program, serta monitoring ratusan bahkan ribuan *client* hanya dengan *single console*. *Endpoint Protection* menyediakan proteksi kelas dunia tanpa memperlambat kinerja sistem perusahaan.

Adapun beberapa keunggulan dari *Symantec Endpoint Protection* 12.1 adalah :

1. Perlindungan terhadap virus dan spyware
2. Perlindungan terhadap ancaman serangan virus yang sulit terdeteksi sekalipun (i.e., zero-day threats)
3. Memberikan perlindungan lebih terhadap insfrastruktur jaringan.
4. *Antivirus, antispyware, desktop firewall, IPs, browser protection, device & application control, network access control* kesemuanya dapat dikerjakan oleh *single agent* dan di-manage melalui *single console*).
5. Proses otomatisasi dan sentralisasi management yang simple dan akurat.

Beberapa fitur terbaru dari *Symantec Endpoint Protection* 12.1 yang terbaru yang membuat *Symantec endpoint* menjadikan pilihan terdepan yang berkelas dunia di dalam menyediakan produk *security, storage* dan *system management. Symantec endpoint protection* 12.1 merupakan salah satu product *security* yang menawarkan berbagai perlindungan yang menjamin sistem keamanan di perusahaan terhadap bermacam-macam serangan virus yang selalu berkembang baik itu *spyware, worm, Trojan* maupun *rootkit*.

Fitur tersebut diantaranya adalah :

1. *Insight* (Sebuah teknologi revolusioner, bisa dikatakan teknologi yang langsung melakukan proses scaning secara online)
2. *Real time SONAR (Symantec Online Network for Advanced Response)*, scaning program selagi berjalan
3. *Browser protection* (Lebih aman dalam menjelajah internet)
4. *Built for virtual environments* (Melindungi infrastruktur virtual Anda)
    - Dapat di-manage untuk scan virtual image file
    - Scan image file secara random dan melakukan update terjadwal
    - Mengurangi beban bandwidth dalam melakukan scan virtual client
    - Symantec Endpoint Protection Manager secara otomatis dapat mengidentifikasi dan me-manage virtual clients
    - Melakukan scan terhadap image file offline
5. Support untuk Apple OS X® and Linux®
6. Central console yang cepat dan akurat
7. Terjadwal
8. Lebih cepat dalam proses *deployment*
9. *Symantec Endpoint Protection Manager* telah teritegrasi dengan *Symantec™ Protection Center 2.0*
10. Melakukan *reporting* dan *analytics* secara tepat dan akurat