BAB II
LANDASAN TEORI

2.1 Keylogger

Berikut akan dijelaskan berbagai hal mengenai *keylogger.*

2.1.1 Definisi Keylogger

Keystroke Logger atau yang lebih dikenal dengan *keylogger* merupakan sebuah perangkat, baik perangkat keras atau perangkat lunak yang digunakan untuk memantau penekanan tombol *keyboard*. Sebuah *keylogger* biasanya akan menyimpan hasil pemantauan penekanan tombol *keyboard* tersebut ke dalam sebuah berkas log/catatan/rekaman. Hasil rekaman tersebut kemudian akan dikirim kepada orang yang membutuhkan data-data tersebut melalui berbagai media, diantaranya melalui *email*, jaringan *local area network,* jaringan *wireless,* dan lain-lain. *Keylogger* dapat digunakan untuk kepentingan yang baik atau bahkan bisa digunakan untuk kepentingan yang jahat. Kepentingan yang baik antara lain untuk memantau produktivitas karyawan, untuk penegakan hukum dan pencarian bukti kejahatan.

2.1.2 Jenis-jenis *keylogger*

Keylogger terbagi menjadi dua jenis :

a. *Keylogger* berbasis perangkat lunak

Keylogger berbasis perangkat lunak adalah salah satu dari jenis *keylogger* yang dapat merekam ketukan *keyboard* melalui suatu program aplikasi.

Berdasarkan perspektif teknis, *keylogger* terbagi menjadi lima metode:

1) *Hypervisior-based*

Hypervisior disebut juga *Virtual Machine Monitor* (VMM) yang memungkinkan beberapa sistem operasi untuk bekerja secara bersamaan pada komputer host. *Keylogger* yang menggunakan metode ini secara teori berada pada *malware hypervisior* dimana *keylogger* tersebut bekerja dibawah sistem operasi.

2) *Kernel-based*

Kernel adalah suatu perangkat lunak yang menjadi bagian utama dari sistem operasi. Kernel bertugas untuk melayani bermacam-macam program aplikasi untuk mengakses perangkat keras pada komputer. Metode jenis ini memungkinkan *keylogger* sulit dideteksi terutama para pengguna awam. Metode ini sering diimplementasikan sebagai rootkit yang dapat merubah kernel sistem operasi sehingga dapat mengakses perangkat keras tanpa izin. Sebagai contoh, *keylogger* yang menggunakan metode ini dapat bertindak sebagai sebuah driver *keyboard*, dengan demkian semua informasi yang diketikkan pada *keyboard* dapat diketahui.

3) *Hook-based*

Metode ini bekerja seperti pengait, dimana metode ini menggunakan fungsionalitas yang disediakan oleh sistem operasi sehingga *event* yang terjadi pada *keyboard* dapat diketahui. Sistem operasi akan memberitahu *keylogger* setiap kali tombol *keyboard* ditekan.

4) *Passive Methods*

Metode ini menggunakan *Application Programming Interface* (API) dari sistem operasi, seperti: *GetAsyncKeyState* (), *GetForegroundWindow* () dan lain-lain, untuk mendapatkan informasi ketukan pada *keyboard*.

5) *Form Grabber based*

Metode ini bekerja pada web form dengan cara merekam fungsi *onSubmit* pada web browser. Perekaman informasi dilakukan sebelum data di enkripsi dan di kirim melalui internet.

Pengaksesan data pada *keylogger* berbasis perangkat lunak terbagi menjadi empat cara, yaitu:

1) Data diupload ke situs web, database atau akun ftp
2) Data dikirimkan melalui email secara berkala
3) Data ditransmisikan melalui suatu sistem perangkat keras yang terpasang
4) Data log disimpan pada mesin target

b. *Keylogger* berbasis perangkat keras

Keylogger berbasis perangkat keras adalah salah satu dari jenis *keylogger* yang dapat merekam ketukan keyboard melalui perangkat keras yang terpasang pada komputer target.

Jenis-jenis *keylogger* berbasis perangkat keras

1. *Regular Hardware Keylogger*

   Merupakan rangkaian perangkat keras yang dibutuhkan untuk melakukan proses perekaman *keyboard* yang dipasang antara *keyboard* dan komputer, alat tersebut biasanya dipasang bersamaan dengan konektor kabel *keyboard*. Tetapi ada juga yang dipasang kedalam *keyboard* tersebut sehingga alat tersebut tidak terlihat. Hasil ketukan dari alat tersebut akan disimpan kedalam memori internal yang sewaktu-waktu dapat diakses.

2. *Wireless Keylogger Sniffers*

   Alat yang digunakan untuk melakukan pengumpulan paket-paket data antara *keyboard wireless* dengan alat penerimanya *(receiver).*

3. *Firmware-based*

   BIOS-level firmware yang bertugas menangani *event* pada *keyboard*, setelah dimodifikasi maka dapat merekam proses atau event yang terjadi pada *keyboard*. Pada metode ini diperlukan akses root untuk dapat mengakses perangkat lunak yang dibutuhkan oleh BIOS agar dapat mengakses perangkat keras yang sedang berjalan.

4. *Keyboard overlay*

   Tombol palsu yang diletakkan diatas tombol yang sebenarnya, sehingga apabila tombol asli ditekan maka tombol palsu juga akan ikut tertekan dan secara otomatis semua hasil ketukan pada tombol asli akan sama pada tombol palsu.

Salah satu keuntungan yang didapat dari penggunaan *keylogger* berbasis perangkat keras adalah Proses perelaman ketukan keyboard tidak dipengaruhi oleh sistem operasi yang digunakan oleh target.

2.2 Antarmuka Pemrograman Aplikasi Windows

Berikut akan dijelaskan mengenai berbagai hal mengenai Antarmuka Pemrograman Aplikasi Windows.

2.2.1 Definisi

Antarmuka Pemrograman Aplikasi Windows (*Windows Application Progamming Interface*) yang juga sering disebut sebagai WinAPI atau Windows API adalah sekumpulan antarmuka pemrograman aplikasi yang dibuat oleh *Microsoft* dalam inti sistem operasi *Microsoft Windows* buatannya. Semua program Windows, kecuali program konsol, harus berinteraksi dengan Windows API tanpa melihat dengan bahasa apa ia dibuat. Akses terhadap elemen sistem operasi yang lebih rendah, seperti halnya yang dibutuhkan oleh device driver, tidak disediakan oleh Windows API, tapi disediakan oleh *Windows Driver Foundation* atau *Native API* dalam versi-versi baru Windows.

2.2.2 Versi-Versi Windows API

a) Win16 API

Windows 16 API atau Win16 API merupakan API yang digunakan pertama kali pada versi Windows 16-bit. Pada awalnya, Win16 API disebut dengan Windows API, tapi kemudian diubah menjadi Win16 dalam usaha *Microsoft*

untuk membedakannya dengan versi Windows API yang lebih baru yang berjalan pada Windows 32-bit, Win32 API. Fungsi-fungsi Win16 API umumnya terdapat di dalam berkas-berkas inti sistem operasi: kernel.exe (krnl286.exe pada Windows for 286 atau krnl386.exe pada Windows yang berjalan pada Enhanced 386), user.exe, dan gdi.exe. Meskipun memiliki ekstensi EXE, sebenarnya mereka bukanlah berkas yang dapat dieksekusi (*executable*), melainkan mereka adalah DLL (*Dynamic Linking Library*).

b) Win32 API

Win32 API merupakan antarmuka pemrograman yang terdapat di dalam sistem operasi Windows 32-bit modern. Seperti halnya Win16 API, Win32 API juga sama mengimplementasikan fungsi-fungsi di dalam DLL sistem operasi. DLL inti yang dimiliki oleh Win32 API antara lain kernel32.dll, user32.dll, dan gdi32.dll. Win32 pertama kali muncul pada tahun 1993, saat Windows NT diluncurkan. Windows 95 juga menggunakan Win32 API, dan pada awalnya dikenal dengan sebutan Win32c, di mana huruf "c" di sana merujuk kepada "*compatibility*", tapi istilah ini akhirnya ditinggalkan oleh *Microsoft* demi konsistensi nama "*Win32*".

Dalam Windows NT 4.0 dan para penerusnya (termasuk di antaranya versi-versi terbaru Windows), panggilan-panggilan Win32 dieksekusi oleh dua modul, yakni csrss.exe (*Client/Server Runtime SubSystem*) di dalam modus pengguna dan Win32K.sys di dalam modus kernel.

c) Win32s API

Win32s API merupakan sebuah ekstensi untuk keluarga Windows 3.1x yang mengimplementasikan sekumpulan kecil dari Win32 API untuk sistem-sistem tersebut, yang merupakan sistem operasi 16-bit. Huruf "s" di sana merupakan singkatan dari "*subset*".

d) Win32 for 64-bit Windows

Win32 for 64-bit Windows, yang sebelumnya dikenal dengan sebutan Win64, merupakan sebuah versi Windows API yang ditargetkan untuk digunakan oleh Windows versi 64-bit, yakni Windows XP Professional x64 Edition dan Windows Server 2003 x64 Edition (untuk prosesor-prosesor x86-64) dan Windows XP 64-bit Edition *dan* Windows Server 2003 for Itanium-series (untuk prosesor-prosesor IA-64). Dengan kemunculan Win64, Windows NT pun akhirnya masuk ke dalam pasar komputasi 64-bit, dan kompatibilitas aplikasi 32-bit pun masih terjaga. Akan tetapi, memang semua pointer memori dialamatkan dengan menggunakan alamat 64-bit, sehingga kode sumber program harus dicek ulang untuk melihat apakah ada masalah kompatibilitas dengan pointer aritmetika 64-bit dan jika perlu ditulis ulang, tidak ada penambahan fungsi-fungsi baru yang spesifik ditambahkan ke dalam Windows versi 64-bit.

2.2.3 Fungsionalitas

Fungsionalitas yang ditawarkan oleh Windows API dapat digolongkan menjadi 8 kategori, yaitu:

1. Base Services

Menyediakan akses terhadap beberapa sumber daya fundamental yang tersedia di dalam sebuah sistem yang menjalankan sistem operasi *Microsoft Windows*. Fungsi-fungsi ini terdapat dalam kernel.exe, krnl286.exe, atau krnl386.exe (dalam Windows 16-bit) dan kernel32.dll serta advapi32.dll dalam Windows 32-bit. Subkomponen yang terdapat pada golongan ini antara lain:

a. File System FAT12, FAT16, FAT32, CDFS, UDFS dan NTFS
b. Devices
c. Process and threads
d. Error handling

2. Advanced Services

Menyediakan akses terhadap fungsionalitas yang berada di luar kernel sistem operasi Windows. Fungsionalitas yang termasuk di dalam kategori ini adalah akses *registry Windows*, *shutdown* (*turn-off, restart, hibernate*, atau *standby*) *Windows*, manajemen *Windows service*, hingga manajemen akun pengguna. Fungsi-fungsi ini terdapat di dalam advapi32.dll, dan hanya terdapat pada versi Windows 32-bit.

3. Graphics Device Interface (GDI)

Menyediakan fungsionalitas untuk mengeluarkan tampilan grafik ke monitor, printer dan beberapa perangkat keluaran lainnya. Dalam Windows 16-bit, GDI ditangani oleh GDI.EXE, atau GDI32.DLL dalam Windows 32-bit.

4. User Interface

Menyediakan fungsionalitas untuk membuat dan mengatur layar jendela dan sebagian besar kontrol dasar, seperti tombol (*button*), baris geser (*scroll bar*), hingga menerima input dari pengguna melalui *keyboard* atau *mouse*. Dalam Windows 16-bit, fungsionalitas user interface ditangani oleh USER.EXE, atau User32.DLL dalam Windows 32-bit. Saat Windows XP dirilis, kontrol-kontrol dasar Windows digabungkan ke dalam ComCtl32.DLL, bersama-sama dengan *Common Control Library*.

5. Common Dialog Box Library

Menyediakan fungsionalitas untuk membuat kotak dialog untuk membuka dan menutup berkas, memilih warna, huruf (font) dan lain sebagainya. Antarmuka ini terdapat pada sebuah berkas dengan nama Commdlg.dll pada Windows 16-bit, atau Comdlg32.dll pada Windows 32-bit. Meskipun demikian, fungsionalitas ini dimasukkan dalam kategori User Interface.

6. Windows Shell

Komponen Windows API yang mengizinkan aplikasi untuk mengakses fungsionalitas yang disediakan oleh shell sistem operasi dan juga mengubah atau bahkan meningkatkannya. Komponen ini terdapat di dalam DLL Shell.DLL dalam Windows 16-bit, sementara dalam Windows 32-bit terdapat

di dalam Shell32.DLL. Windows 95 juga menawarkan sebuah DLL yang disebut sebagai ShlWApi.DLL. Ini juga dikelompokkan ke dalam kategori User Interface di dalam API.

7. Network Services

Mengizinkan aplikasi agar dapat mengakses kemampuan jaringan di dalam sistem operasi. Komponen ini memeliki beberapa subkomponen, yakni:

a. *Network Basic Input Output System* (NetBIOS)
b. *Windows Socket*(Winsock)
c. *Network Dynamic data Exchange* (NetDDE)
d. *Remote Procedure Call* (RPC)

2.3 Jaringan Komputer

Berikut akan dijelaskan berbagai hal mengenai jaringan komputer.

2.3.1 Definisi

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama.

Tujuan dari jaringan komputer adalah:

1. Membagi sumber daya
2. Komunikasi
3. Akses informasi

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang meminta layanan disebut klien (*client*) dan yang memberikan layanan disebut pelayan (*server*). Arsitektur

ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

2.3.2 Jenis-Jenis Jaringan Komputer

Jaringan komputer dapat dibedakan berdasarkan cakupan geografisnya menjadi 4, yaitu:

a. LAN (*Local Area Network*)

   LAN digunakan untuk meenghubungkan komputer yang berada didalam suatu area kecil, misalnya didalam gedung perkantoran atau kampus. Jarak antar komputer yang dihubungkannya bisa sampai 5 sampai 10 km. Suatu LAN biasanya bekerja dengan kecepatan mulai dari 10 Mbps sampai 100 Mbps. LAN menjadi popular karena memungkinkan banyak pengguna untuk memakai sumber daya secara bersama-sama.

b. MAN (*Metropolitan Area Network*)

   MAN merupakan suatu jaringan yang cakupannya meliputi suatu kota. MAN menghubungkan LAN-LAN yang lokasinya berjauhan. Jangkauan MAN bisa mencapai 10 km sampai beberapa ratus km. Suatu MAN biasanya bekerja pada kecepatan 1.5 sampai 150 Mbps.

c. WAN (*Wide Area Network*)

   WAN dirancang untuk menghubungkan komputer-komputer yang terletak pada suatu cakupan geografis yang luas, seperti hubungan dari suatu kota ke kota lain di dalam suatu negara. Cakupan WAN meliputi 100 km sampai

1000 km dan kecepatan antar kota bisa bervariasi antara 1,5 Mbps sampai 2,4 Mbps.

d. GAN (*Global Area Network*)

GAN merupakan suatu jaringan yang menghubungkan negara-negara di seluruh dunia. Kecepatan GAN bervariasi mulai dari 1,5 Mbps sam[ai 100 Gbps dan cakupannya meliputi ribuan kilometer.

2.3.3 Topologi Jaringan

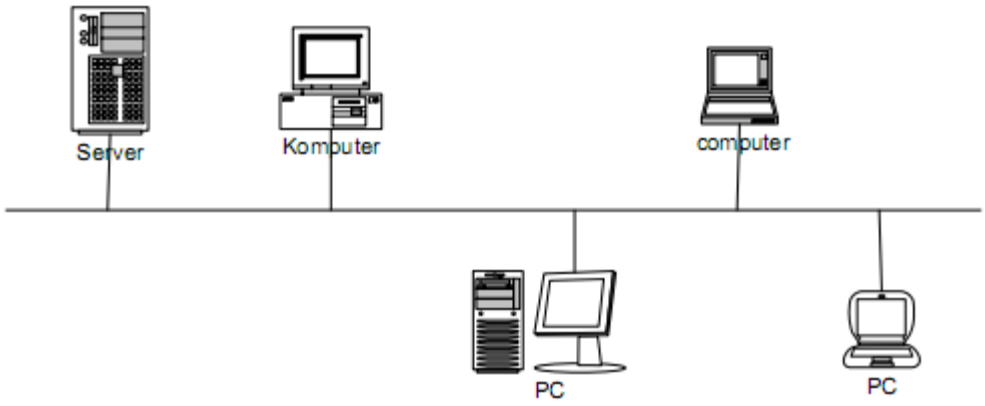
Topologi jaringan adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Topologi secara fisik dari suatu jaringan local adalah merujuk kepada konfigurasi kabel, komputer, dan perangkat lainnya.

2.3.3.1 Tipe-Tipe Utama Topologi Fisik

Berikut ini akan dijelaskan mengenai topologi fisik yang digunakan di dalam jaringan local diantaranya:

a. Topologi Garis Lurus *(Linear Bus)*

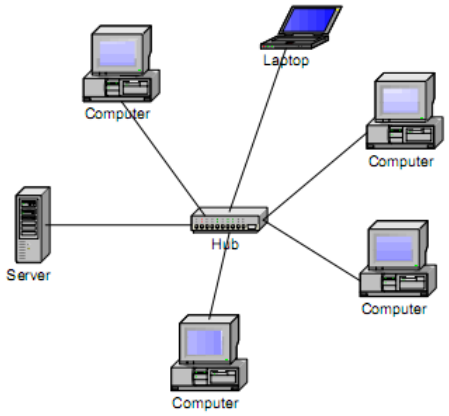
Topologi Garis Lurus *(Linear Bus)* terdiri terdiri dari satu jalur kabel utama dimana pada masing-masing ujungnya diberikan sebuah *terminator*. Semua nodes pada jaringan terkoneksi pada sebuah kabel utama (*backbone*).



Gambar 2.1 Topologi Garis Lurus *(Linear Bus)*

b. Topologi Jaringan Bintang *(Star)*

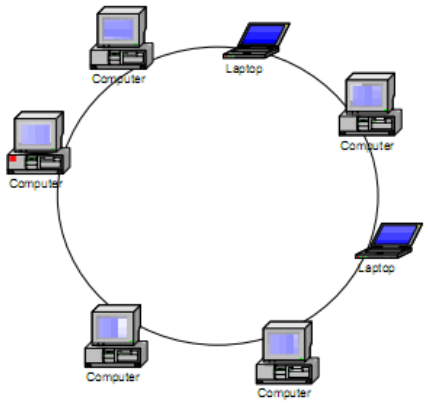
Topologi ini dirancang dimana semua node (*file server*, *workstation,* dan perangkat lainnya) terkoneksi ke jaringan melewati sebuah *concentrator*.



Gambar 2.2 Topologi Jaringan Bintang

c. Topologi Jaringan Cincin *(Ring)*

Topologi cincin menggunakan teknik konfigurasi yang sama dengan topologi bintang tetapi pada topologi ini terlihat bahwa jalur media transmisi menyerupai suatu lingkaran tertutup menyerupai cincin (lingkaran), sehingga diberi nama topologi bintang dalam lingkaran.

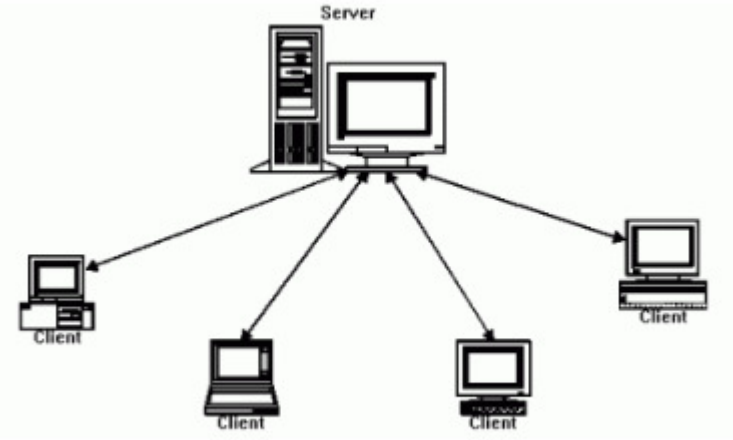


Gambar 2.3 Topologi Jaringan Cincin *(Ring)*

Berdasarkan fungsinya maka jaringan komputer terabagi menjadi 2 jenis, yaitu:

a. Client-Server

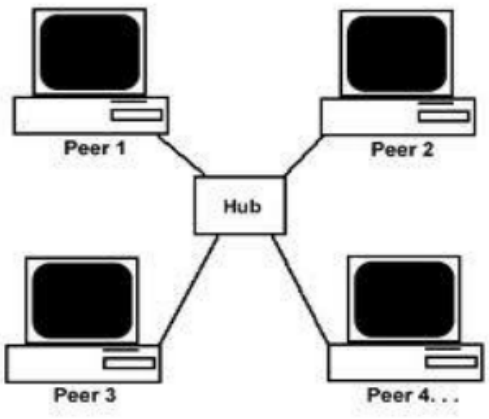
Model hubungan *client-server* memungkinkan jaringan untuk mensentralisasi fungsi dan aplikasikepada satu atau dua *dedicated file server*. Model hubungan ini menyediakan mekanisme untuk mengintegrasikan seluruh komponen yang ada di jaringan.



Gambar 2.4 *Client-Server*

b. Peer-to-peer

Model hubungan peer-to-peer memungkinkan user membagi sumber daya yang ada dikomputernya baik itu berupa file, layanan printer, dan lain-lain. Di dalam model ini seluruh komputer adalah sama, dimana mempunyai komampuan yang sama untuk memakai sumber daya yang tersedia dan model jaringan ini di desain untuk jaringan berskala kecil dan menengah.



Gambar 2.5 *Peer-to-Peer*

2.3.4 IP Address

Internet Protocol address atau IP address adalah alamat numerik yang ditetapkan untuk sebuah komputer yang berpartisipasi dalam jaringan komputer yang memanfaatkan *Internet Protocol* untuk komunikasi antara *node*-nya. Untuk mempermudah proses pembagiannya, IP address dikelompokkan dalam kelas-kelas. Dasar pertimbangan pembagian IP address kedalam kelas-kelas adalah untuk memudahkan pendistribusian pendaftaran IP address. IP address ini dikelompokkan dalam lima kelas, yaitu: Kelas A, Kelas B, Kelas C, Kelas D dan Kelas E. Perbedaan pada tiap kelas tersebut adalah pada ukuran dan jumlahnya. IP address Kelas A dipakai oleh sedikit jaringan namun jaringan ini memiliki anggota yang besar. Kelas C dipakai oleh banyak jaringan namun anggota masing-masing jaringan sedikit. Kelas D diperuntukkan bagi jaringan *multicast* dan Kelas E digunakan untuk keperluan eksperimental.

Pembagian kelas-kelas IP address didasarkan pada dua hal yaitu *network ID* dan *host ID* dari suatu IP address. Setiap IP address selalu merupakan sebuah pasangan dari *network ID* dan *host ID. Network ID* ialah bagian dari IP address yang digunakan untuk menunjukkan jaringan tempat komputer berada, sedangkan *host ID* ialah bagian dari IP address yang digunakan untuk menunjukkan *workstation*, *server*, *router* dan semua *host* TCP/IP lainnya dalam jaringan tersebut.

Berikut ini adalah kelas-kelas IP address, yaitu:

a. Kelas A

   Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit pertama : 0

Panjang Net ID : 8 bit

Panjang Host ID : 24 bit

Byte pertama : 0-127

Jumlah : 126 Kelas A

Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

Jumlah IP : 16.777.214 IP address pada tiap kelas A

IP address kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar. Bit pertama dari IP address kelas A selalu dipasang nilai nol sehingga byte terdepan dari IP address kelas A selalu bernilai antara angka 0 dan 127. Pada IP address kelas A, *network ID* ialah 8 bit sedangkan *host ID* ialah 24 bit berikutnya.

b. Kelas B

Format : 10nnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit pertama : 10

Panjang Net ID : 16 bit

Panjang Host ID : 16 bit

Byte pertama : 128 - 191

Jumlah : 16.184 Kelas B

Range IP : 128.0.xxx.xxx sampai 191.255.xxx.xxx

Jumlah IP : 65.532 IP address pada tiap kelas B

IP address kelas B biasanya dialokasikan untuk jaringan berukuran sedang dan besar. Dua bit pertama dari IP address kelas B selalu dipasang dengan nilai satu dan nol sehingga byte terdepan dari IP address kelas B selalu bernilai antara 128 – 191. Pada IP address kelas B, *network ID* ialah 16 bit pertama sedangkan *host ID* adalah 16 bit berikutnya.

c. Kelas C

Format : 110nnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit pertama : 110

Panjang Net ID : 24 bit

Panjang Host ID : 8 bit

Byte pertama : 192 - 223

Jumlah : 2.097.152 Kelas C

Range IP : 192.0.0.xxx sampai 191.255.255.xxx

Jumlah IP : 254 IP address pada tiap kelas C

IP address kelas C awalnya digunakan untuk jaringan berukuran kecil (misalnya pada LAN). Tiga bit pertama dari IP address kelas C selalu berisi 110. 21 bit selanjutnya (untuk melengkapi tiga oktet pertama) akan membentuk sebuah network identifier. 8 bit sisanya (sebagai oktet terakhir) akan merepresentasikan host identifier. Ini memungkinkan pembuatan total 2,097,152 buah network, dan 254 host untuk setiap network-nya.

d. Kelas D

Format : 1110mmmm.mmmmmmmm.mmmmmmmm.
mmmmmmmm

4 bit pertama : 1110

Bit Multicast : 28 bit

Byte Inisial : 224 - 247

Deskripsi : kelas D adalah ruang alamat multicast

IP address kelas D digunakan untuk keperluan IP multicasting. 4 bit pertama IP address kelas D adalah dipasang 1110. Bit-bit berikutnya diatur sesuai keperluan multicast group yang menggunakan IP ini.

e. Kelas E

Format : 1111rrrr.rrrrrrrr.rrrrrrrr.rrrrrrrr

4 bit pertama : 1111

Bit Multicast : 28 bit

Byte Inisial : 248 - 255

Kelas E adalah ruang alamat yang dicadangkan untuk keperluan eksperimental. IP address tidak digunakan untuk umum.

2.3.5 Port Jaringan Komputer

Dalam protokol jaringan TCP/IP, sebuah *port* adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasikan

aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server. Port dapat dikenali dengan angka 16-bit (dua byte) yang disebut dengan Port Number dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam Port TCP dan Port UDP. Karena memiliki angka 16-bit, maka total maksimum jumlah port untuk setiap protokol transport yang digunakan adalah 65536 buah.

Dilihat dari penomorannya, port UDP dan TCP dibagi menjadi tiga jenis, yakni sebagai berikut:

1. *Well-Known Port*

   Port yang pada awalnya berkisar antara 0 hingga 255 tapi kemudian diperlebar untuk mendukung antara 0 hingga 1023. Port number yang termasuk ke dalam well-known port, selalu merepresentasikan layanan jaringan yang sama, dan ditetapkan oleh *Internet Assigned Number Authority* (IANA). Beberapa di antara port-port yang berada di dalam range *Well-known port* masih belum ditetapkan dan direservasikan untuk digunakan oleh layanan yang bakal ada di masa depan. *Well-known port* didefinisikan dalam *RFC 1060*

2. *Registered Port*

   Port-port yang digunakan oleh vendor-vendor komputer atau jaringan yang berbeda untuk mendukung aplikasi dan sistem operasi yang mereka buat. Registered port juga diketahui dan didaftarkan oleh IANA tapi tidak

dialokasikan secara permanen, sehingga vendor lainnya dapat menggunakan port number yang sama. *Range registered port* berkisar dari 1024 hingga 49151 dan beberapa port di antaranya adalah *Dynamically Assigned Port*.

3. *Dynamically Assigned Port*

   merupakan port-port yang ditetapkan oleh sistem operasi atau aplikasi yang digunakan untuk melayani request dari pengguna sesuai dengan kebutuhan. *Dynamically Assigned Port* berkisar dari 1024 hingga 65536 dan dapat digunakan atau dilepaskan sesuai kebutuhan.

Tabel 2.1 Pengelompokan Port Komputer

No	Protokol	Label Port	Nama Port	Keterangan
19	tcp/udp	chargen	Character Generation	Generator karakter ini mengembalikan deretan karakter-karakter. Walaupun layanan yang ada sekarang terbatas ke 512 byte, namun bisa dijumpai server yang mengirimkan karakter secara terus-menerus sampai hubungan ke port ini diputuskan. Seringkali diserver-server lama, jika jumlah klien yang membuka hubungan mencapai ratusan secara sekaligus, CPU time akan terkonsumsi secara besar-besaran, sehingga membuat server menjadi lambat

20/21	tcp	ftp	File Transfer Protocol	Protokol untuk menangani pentransferan file-file dari satu komputer ke komputer lainnya. Protokol ini menggunakan dua saluran, yang satu sebagai saluran untuk mengendalikan lalulintas data, sedangkan yang satu lagi untuk dilintasi data itu sendiri.
23	tcp	telnet	Telnet	Metode login jarak jauh yang paling populer, walupun tidak seaman ssh (data yang melintasi tidak dienkripsi secara otomatis).
25	tcp	mail	Simple Mail Transfer	Protokol pentransferan pesan sederhana, dan merupakan standar *de facto* untuk internet.
48	tcp/udp	auditd	Digital Audit Daemon	Digunakan oleh *daemon* audit komputer-komputer digital untuk menjalankan tugas-tugas administrasi.
53	tcp/udp	dns	Domain Name Server	Salah satu layanan yang cukup vital, dijalankan diserver-server, dan berfungsi untuk memberikan informasi berbentuk layanan IP xxx.xxx.xxx.xxx untuk setiap permintaan penterjemahan dari nama-nama domain.
79	tcp	finger	Finger Daemon	*Daemon* yang bertugas memberikan informasi mengenai pengguna-pengguna suatu sistem

				kepada sang peminta.
80/ 8000/ 8080/	tcp	http	HyperText Transfer Procotol	Protokol pentransferan data berformat HTML (webpage) dari server kepada publik.
110	tcp/udp	pop3	Post Office Protocol v3	Protokol standar pemeriksaan email jarak jauh. Biasanya user atau program e-mail *client* user me-*logon* untuk memeriksa dan mengambil pesan e-mail yang diterima lewat mailbox server.
111	tcp/udp	sunrpc	Sun Remote Procedure Call	Beberapa portscanner mentargetkan port ini dan terdapat beberapa program yang mengeksploit port ini (mesin-mesin sun/solaris)
139	tcp/udp	netbiossn	NetBIOS Session Service	Port inilah yang digunakan sebagai sarana komunikasi dengan atau antara mesin-mesin Microsoft (NT/95/98).
143	tcp/udp	imap2	Interactive Mail Access Protocol	Salah satu protokol pengaksesan mail.
443	tcp	https	HyperText Transfer Protocol Secure	Daemon penerima permintaan tipe http yang berjalan diatas *secure layer.*
512	tcp	exec	Remote Process Execution	Menginzinkan eksekusi proses jarak jauh dengan sistem autentifikasi berdasar file.
513	tcp	rlogin	Remote Login Protocol	Port inilah yang digunakan jika melakukan *rlogin* ke suatu host, dengan *rlogin,* user di host A tidak perlu

				melewati proses login lewat telnet ke host B seperti biasa, namun bisa masuk ke *home directory*-nya host B (tanpa password).

2.4 Diagram Arus Data (*Data Flow Diagram*)

DFD atau singkatan dari *Data Flow Diagram* merupakan representasi grafik dari suatu sistem yang menunjukan proses atau fungsi, aliran data, tempat penyimpan data dan *entitas eksternal*. DFD juga digunakan untuk menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan. Dengan menggunakan DFD, rancangan yang akan kita buat akan lebih terarah dan lebih rinci. Sehingga kita tidak akan mengalami kesulitan dalam melakukan perancangan. *Data flow diagram* memiliki empat komponen, antara lain akan dijelaskan dibawah ini.

1. *Terminator (external exitity)*

   Terminator mewakili *entity external* yang berkomunikasi dengan sistem yang sedang dikembangkan. *Terminator* merupakan kesatuan dilingkungan sistem. Biasanya terminator ini dikenal dengan nama entitas (*external*) sumber atau tujuan (*source* dan *sink*). Terminator dapat juga berupa departemen, divisi atau sistem diluar sistem yang berkomunkasi dengan sistem yang dikembangkan.

2. Proses

   Proses sering dikenal dengan nama *Bubble*, fungsi atau informasi. Komponen proses menggambarkan bagian dari sistem yang mentransformasikan *input* ke

output, atau dapat dikatakan bahwa komponen proses menggambarkan transformasi satu *input* atau lebih menjadi *output.* Setiap proses harus diberikan penjelasan yang lengkap sebagai berikut :

a. Identifikasi Proses

umunya berupa angka yang menunjukan nomor dari proses atau ditulis pada bagian atas simbol proses.

b. Nama Proses

Menunjukan apa yang dikerjakan oleh proses tersebut. Nama proses harus jelas dan lengkap menggambarkan bagian prosesnya nama proses diletakan dibawah identifikasi proses.

3. Penyimpanan data *(data store)*

Data store digunakan sebagai sarana untuk mengumpulkan data. Data store disimbolkan dengan dua garis horizontal yang paralel dimana tertutup pada salah satu ujungnya atau dua garis horizontal saja. *Data store* ini biasanya berkaitan dengan penyimpanan-pemyimpanan seperti *file* atau *database* yang berkaitan dengan penyimpanan secara komputerisasi, contohnya *file* pita magnetic, *file* disket atau *file harddisk*. *Data store* juga berkaitan dengan pemyimpanan data.

4. Alur Data *(Data Flow)*

Suatu data *flow* atau alur data dapat dipresentasikan dengan anak panah yang menunjukan arah menuju ke dan keluar dari suatu proses. Alur data ini digunakan untuk menerangkan perpindahan data atau satu paket data atau informasi dari suatu bagian sistem ke bagian lainnya. Selain menunjukan

arah, alur data pada model yang dibuat dapat merepresentasikan bit, karakter, pesan, formulir, bilangan *real* dan macam-macam informasi yang berkaitan dengan komputer.

Ada tiga tipe DFD, yaitu *context diagram* (diagram konteks), *data flow diagram fisik*, dan *data flow diagram logika*.

2.4.1 Diagram Konteks

Diagram Konteks adalah bagian dari DFD yang berfungsi memetakan model model lingkungan, yang dipresentasikan dengan lingkaran tunggal yang mewakili keseluruhan sistem. Diagram ini adalah diagram *level* tertinggi dari DFD. Diagram konteks menyoroti sejumlah karateristik penting sistem, yaitu :

1. Kelompok Pemakai, organisasi atau sistem lain dimana sistem melakukan komunikasi (sebagai terminator).
2. Data Masuk, yaitu data yang diterima sistem dari lingkungan dan harus diproses dengan cara tertentu.
3. Data Keluar, yaitu data yang dihasilkan sistem dan diberikan kedunia luar.
4. Penyimpanan Data (*storage*), yaitu digunakan secara bersama antara sistem dengan terminator. Data ini dapat dibuat oleh sistem dan digunakan oleh lingkungan atau sebaliknya dibuat oleh lingkungan dan digunkan oleh sistem. Hal ini berarti pembuatn simbol *data storage* dalam diagram konteks dibenarkan, dengan syarat simbol tersebut merupakan bagian dari dunia diluar sistem.
5. Batasan, antara sistem dan lingkungan.

2.4.2 *Data Flow Diagram* Fisik

Data flow diagram fisik adalah representasi dari sebuah sistem yang menunjukan *entitas-entitas internal* dan *eksternal* dari sistem tersebut, *Entitas-entitas internal* adalah *personal,* tempat atau mesin dalam sistem tersebut yang *mentransformasi* data. Maka data *flow* diagram fisik tidak menunjukkan apa yang dilakukan, tetapi menunjukan dimana, bagaimana, dan siapa proses-proses dalam sebuah sistem dilakukan.

2.4.3 *Data Flow Diagram Logika*

Data flow diagram logika digunakan untuk menggambarkan sistem yang akan diusulkan (sistem yang baru). *Data flow diagram logika* tidak menekankan pada bagaimana sistem diterapkan, tetapi penekanannya hanya pada logika pada kebutuhan-kebutuhan sistem, yaitu proses-proses apa secara logika yang dibutuhakan oleh sistem.

2.5 Jaringan Semantik

Model jaringan sematik merupakan grafik, yang terdiri dari simpul-simpul yang merepresentasikan objek fisik atau objek konsep, dan busur-busur yang menunjukan relasi antara simpul-simpul tersebut. Jaringan semantik merupakan alat efektif untuk merepresentasikan pemetaan data, yang bertujuan mencegah terjadinya duplikasi data.

2.6 MS. Visual Basic 6.0

BASIC, adalah singkatan dari *Beginners' All-purpose Symbolic Instruction Code* adalah sebuah kelompok bahasa pemrograman tingkat tinggi. Secara harfiah, BASIC memiliki arti "kode instruksi simbolis semua tujuan yang dapat digunakan oleh para pemula". Memang, istilah "Bahasa BASIC" di sini juga bisa diartikan menjadi bahasa untuk pemula, atau dengan kata lain, disebut sebagai bahasa dasar, tapi hal tersebut dirasa kurang tepat, mengingat BASIC dapat juga digunakan oleh para pemrogram ahli.

BASIC pertama kali dikembangkan pada tahun 1963 oleh John George Kemeny dan Thomas Eugene Kurtz yang berasal dari Dartmouth Collage, untuk mengizinkan akses terhadap komputer bagi para mahasiswa jurusan selain jurusan ilmu eksakta. Pada waktu itu, hampir semua komputer membutuhkan perangkat lunak, dan waktu itu belum ada perangkat lunak yang dijual secara bebas, sehingga hanya orang-orang tertentulah yang dapat menggunakan komputer, yakni para matematikawan dan ilmuwan, karena mereka dapat membangun perangkat lunak sendiri. Bahasa BASIC, setelah diciptakan menjadi menjamur dan banyak dimodifikasi. Bahasa BASIC menjadi bahasa yang paling populer digunakan pada komputer mikro pada akhir tahun 1970-an dan komputer rumahan pada tahun 1980-an. Dan hingga saat ini, menjadi bahasa yang dialeknya beberapa kali berevolusi.

Bill Gates, pendiri Microsoft, memulai bisnis softwarenya dengan mengembangkan interpreter bahasa Basic untuk Altair 8800, untuk kemudian ia ubah agar dapat berjalan di atas IBM PC dengan sistem operasi DOS.

Perkembangan berikutnya ialah diluncurkannya BASICA (basic-advanced) untuk DOS. Setelah BASICA, Microsoft meluncurkan Microsoft QuickBasic dan Microsoft Basic (dikenal juga sebagai Basic Compiler).

Sejarah BASIC di tangan Microsoft sebagai bahasa yang diinterpretasi (BASICA) dan juga bahasa yang dikompilasi (BASCOM) membuat Visual Basic diimplementasikan sebagai gabungan keduanya.

Programmer yang menggunakan Visual Basic bisa memilih kode terkompilasi atau kode yang harus diinterpretasi sebagai hasil executable dari kode VB. Sayangnya, meskipun sudah terkompilasi jadi bahasa mesin, DLL bernama MSVBVMxx.DLL tetap dibutuhkan. Namun karakteristik bahasa terkompilasi tetap muncul (ia lebih cepat dari kalau kita pakai mode terinterpretasi).

Microsoft Visual Basic (sering disingkat sebagai VB saja) merupakan sebuah bahasa pemrograman yang bersifat event driven dan menawarkan Integrated Development Environment (IDE) visual untuk membuat program aplikasi berbasis sistem operasi Microsoft Windows dengan menggunakan model pemrograman Common Object Model (COM). Visual Basic merupakan turunan bahasa BASIC dan menawarkan pengembangan aplikasi komputer berbasis grafik dengan cepat, akses ke basis data menggunakan Data Access Objects (DAO), Remote Data Objects (RDO), atau ActiveX Data Object (ADO), serta menawarkan pembuatan kontrol ActiveX dan objek ActiveX. Beberapa bahasa skrip seperti Visual Basic for Applications (VBA) dan Visual Basic Scripting

Edition (VBScript), mirip seperti halnya Visual Basic, tetapi cara kerjanya yang berbeda.

Para programmer dapat membangun aplikasi dengan menggunakan komponen-komponen yang disediakan oleh Microsoft Visual Basic Program-program yang ditulis dengan Visual Basic juga dapat menggunakan Windows API, tapi membutuhkan deklarasi fungsi eksternal tambahan.

Dalam pemrograman untuk bisnis, Visual Basic memiliki pangsa pasar yang sangat luas. Dalam sebuah survey yang dilakukan pada tahun 2005, 62% pengembang perangkat lunak dilaporkan menggunakan berbagai bentuk Visual Basic, yang diikuti oleh C++, JavaScript, C#, dan Java.

Visual Basic merupakan bahasa yang mendukung OOP, namun tidak sepenuhnya. Beberapa karakteristik objek tidak dapat dilakukan pada Visual Basic, seperti *Inheritance* tidak dapat dilakukan pada class module. *Polymorphism* secara terbatas bisa dilakukan dengan mendeklarasikan *class module* yang memiliki *Interface* tertentu. Visual Basic (VB) tidak bersifat case sensitif.