Tugas Bahasa Indonesia

Semester 100

Membuat Jurnal

Vidyatama Kurnia

5235127270

Pendidikan Teknik Informatika dan Komputer

(Non Reguler)

UNIVERSITAS NEGERI JAKARTA (Kampus A)
Jl. Rawamangun Muka Jakarta Timur 13220
Telp. (021) 4890046, Fax (021) 4893726
Email : unj@unj.ac.id, Website : www.unj.ac.id

KEAMANAN KOMPUTER PADA JARINGAN INTERNET

ABSTRAK

Nowadays computer networks have mushroomed all over the world. Almost every company, offices, BANK systems, and so there is a computer network to facilitate information on the company. Internet is gaining popularity today is a giant computer network that can connect and interact with each other. Rapid technological developments is the trigger. However, in practice a lot of something evil or dangerous threats threats such as viruses, hackers, fraud and so forth. So it takes kmputer security and computer networks in order to overcome this problem.

A. LATAR BELAKANG MASALAH

WWW atau *World Wide Web* atau yang lebih dikenal dengan WEB adalah salah satu yang menyebabkan popularitas internet. WEB dapat memudahkan untuk mengakses informasi yang dihubungkan satu dengan yang lainnya melalui HTML. suatu alat atau software yang dapat digunakan untuk membuka sistem WEB ata yang lebih dikenal sebagai *browser* dapat diperoleh degan mudah dan gratis. Contoh dari *browser* antara lain seperti Google Chrome, Internet Explorer, Mozilla Firefox dan lain sebagainya. Kemudahan dari penggunaan *browser* inilah yang memicu perkembangan WEB.

Berkembangnya WEB menyebabkan pergerakan sistem informasi untuk menggunakannya sebagai basis. Untuk itu keamanan sistem informasi yang berbasi WEB dan teknologi unternet bergantung kepada keamanan sistem WEB tersebut. Arsitektur sistem Web terdiri dari dua sisi: server dan client. Keduanya dihubungkan dengan jaringan komputer (computer network). Selain menyajikan data-data dalam bentuk statis, sistem Web dapat menyajikan data dalam bentuk dinamis dengan menjalankan program. Program ini dapat dijalankan di server (misal dengan CGI, servlet) dan di client (applet, Javascript).

B. RUMUSAN MASALAH

Munculnya masalah keamanan ini didasarkan atas beberapa asumsi yang datang dari berbagai kalangan baik dari kalangan / pihak User, dari pihak Web Master atau dari Sistem Web itu sendiri, sehingga beberapa asumsi dapat disimpulkan sebagai berikut :

1. Asumsi dari sisi pengguna
   - *Server* dikendalikan oleh organisasi pemilik *server* tersebut.
   - File file yang ditampilkan bebas dari virus atau kejahatan pada internet.

VIDYATAMA KURNIA
PTIK NR (5235127270)

- Server tidak mendistribusikan informasi mengenai pengunjung (user yang melakukan browsing) kepada pihak lain. Hal ini disebabkan ketika kita mengunjungi sebuah web site, data-data tentang kita (nomor IP, operating system, browser yang digunakan, dll.) dapat dicatat.
- Pelanggaran terhadap asumsi ini sebenarnya melanggar *privacy.* Jika hal tersebut dilakukan maka pengunjung tidak bisa kembali mengakses situs tersebut.

2. Asumsi dari penyedia layanan (*WEB Master*)
   - Pengguna tidak bisa mengubah isi atau merusak server tanpa ijin dari penyedia layanan.
   - Pengguna hanya dapat mengakses *file file* yang diperkenankan untuk diakses.
   - Identitas pengguna benar. Banyak situs web yang membatasi akses kepada user-user tertentu. Dalam hal ini, jika seorang pengguna "login" ke web, maka dia adalah pengguna yang benar tidak dengan cara membobol atau masuk tanpa ijin.

Asumsi asumsi tersebut dapat dilanggar oleh oknum sehingga dapat mengakibatkan masalah keamanan pada jaringan internet.

C. TUJUAN

1. Mengetahui sistem keamanan yang cocok untuk layanan WEB.
2. Membuktikan dengan metode keamanan yang dari apa yang diasumsikan diatas.

D. LANDASAN TEORI

Internet merupakan jaringan yang terdiri dari milyaran komputer yang ada di seluruh dunia. Internet melibatkan berbagai jenis komputer serta topology jaringan yang berbeda. Dalam mengatur integrasi dan komunikasi jaringan, digunakan standar protokol internet yaitu TCP/IP. WEB merupakan bagian dari internet yang berkembang paling cepat dan paling populer.

E. IMPLEMENTASI

1. Keamanan *Server*

Server WEB menyediakan fasilitas agar client dari tempat lain dapat mengambil informasi dalam bentuk berkas (*file*), atau mengeksekusi perintah (menjalankan program) di server. Fasilitas pengambilan berkas dilakukan dengan perintah "GET", sementara mekanisme untuk mengeksekusi perintah di server dapat dilakukan dengan "CGI" (Common Gateway Interface), Server Side Include (SSI), Active Server Page (ASP), PHP, atau dengan menggunakan servlet (seperti pernggunaan Java Servlet). Kedua jenis servis di atas (mengambil berkas biasa

maupun menjalankan program di server) memiliki potensi lubang keamanan yang berbeda.

Adanya celah keamanan pada distem WEB dapat dieksploitasi dalam bentuk yang beragam, antara lain :

- Informasi atau *file* yang ditampilkan *server* diubah atau diganti sehingga dapat menjatuhkan perusahaan atau organisasi.
- Informasi atau *file* yang seharusnya untuk kalangan terbatas ternyata berhasil dibajak oleh orang lain (mungkin terjadi karena *setup server*, salah setup *router/firewall*, atau salah *setup authentication*)
- Untuk server web yang berada di belakang firewall, lubang keamanan di server web yang dieksploitasi dapat melemahkan atau bahkan menghilangkan fungsi dari firewall (dengan mekanisme *tunneling*).

a. Membatasi Akses melalui Akses Kontrol

Sebagai penyedia layanan informasi (*file*), pemilik web biasanya menginginkan hanya orang orang tertentu yang dapat mengakses *file* tertentu. Pada dasarnya adalah masalah *control* akses. Pembatasan *control* akses dapat dilakukan dengan :

- Membatasi domain atau *IP Address* yang dapat mengakses
- Penggunaan *login* dengan *User ID* dan *Password*
- Mengenkripsi data dehingga hanya data yang dibuka (deskripsi) oleh orang yang memiliki kunci pembuka.

b. Proteksi Halaman dengan menggunakan Password

Salah satu cara untuk mengatur keamanan akses adalah dengan login yang menggunakan *User ID* dan *Password* . Sehingga hanya orang yang sudah memiliki ID yang valid yang hanya dapat ngeakses

c. Secure Socket Layer

Salah satu cara untuk meningkatkan keamanan server WEB adalah dengan menggunakan enkripsi pada komunikasi pada tingkat socket. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari/ke server WEB**.**

d. Mengetahui Jenis Server

Informasi tentang web server yang digunakan dapat dimanfaatkan oleh perusak untuk melancarkan serangan sesuai dengan tipe server dan operating system yang digunakan. Seorang penyerang akan mencari tahu software dan versinya yang digunakan sebagai web server, kemudian mencari informasi di Internet tentang kelemahan web server tersebut. Informasi tentang program server yang digunakan sangat mudah diperoleh. Cara yang paling mudah adalah dengan

menggunakan program “telnet” dengan melakukan telnet ke port 80 dari server web tersebut, kemudian menekan tombol return dua kali. Web server akan mengirimkan respon dengan didahuli oleh informasi tentang server yang digunakan.

e. Keamanan Program CGI

Common Gateway Interface (CGI) digunakan untuk menghubungkan sistem WEB dengan software lain di server web. Adanya CGI memungkinkan hubungan interaktif antara user dan server web. CGI seringkali digunakan sebagai mekanisme untuk mendapatkan informasi dari user melalui “*fill out form*”, mengakses *database*, atau menghasilkan halaman yang dinamis.

2. Keamanan Client WEB

Dalam bagian terdahulu dibahas masalah yang berhubungan dengan server WEB. Dalam bagian ini akan dibahas masalah-masalah yang berhubungan dengan keamanan client WEB, yaitu pemakai (pengunjung) biasa. Keamanan di sisi client biasanya berhubungan dengan masalah privacy dan penyisipan virus atau trojan horse.

a. Pelanggaran Privacy

Ketika kita mengunjungi sebuah situs web, browser kita dapat “dititipi” sebuah “*cookie*” yang fungsinya adalah untuk menandai kita. Ketika kita berkunjung ke server itu kembali, maka server dapat mengetahui bahwa kita kembali dan server dapat memberikan setup sesuai dengan keinginan (*preference*) kita. Ini merupakan servis yang baik. Namun data-data yang sama juga dapat digunakan untuk melakukan tracking kemana saja kita pergi. Ada juga situs web yang mengirimkan script (misal *Javascript)* yang melakukan interogasi terhadap server kita (melalui *browser*) dan mengirimkan informasi ini ke server. Bayangkan jika di dalam komputer kita terdapat data-data yang bersifat rahasia dan informasi ini dikirimkan ke server milik orang lain.

b. Penyisipan Trojan Horse

Cara penyerangan terhadap client yang lain adalah dengan menyisipkan virus atau trojan horse. Bayangkan apabila yang anda *download* adalah virus atau trojan horse yang dapat menghapus isi harddisk anda. Salah satu contoh yang sudah terjadi adalah adanya web yang menyisipkan trojan horse *Back Orifice* (BO) atau Netbus sehingga komputer anda dapat dikendalikan dari jarak jauh. Orang dari jarak jauh dapat menyadap apa yang anda ketikkan, melihat isi direktori, melakukan *reboot*, bahkan memformat harddisk.

F. KESIMPULAN

Dari penjelasan tersebut dapat disimpulkan sebagai berikut :

1. Sistem keamanan WEB dibagi ke dalam dua aspek, yaitu aspek dari Server dan *Aspek* dari *Client.*
2. Untuk sisi *server* ada mekanisme tertentu untuk mengambil *file*/berkas yang ada dalam *server*.
3. Beberapa strategi untuk memberikan keamanan server diantaranya adalah batasan kontrol akses, proteksi halaman dengan password.
4. Sedangkan yang harus diperhatikan dalam strategi pengamanan untuk client diantaranya adalah masalah *privacy trojan horse*

G. DAFTAR PUSTAKA

Richard H. Baker, “Network Security: how to plan for it and achieve it,” McGraw-Hill International, 1995.

Steven M. Bellovin, “Security Problems in TCP/IP Protocol Suite,” Computer Communication Review, Vol. 19, No. 2, pp. 32-48, 1989.

Tim Berners-Lee, “Weaving the Web: the past, present and future of the world wide web by its inventor,” Texere, 2000.