**“KEAMANAN PADA JARINGAN WORLD WIDE WEB”**

**Oleh : Wydyanto**

**Dosen : Universitas Biasa Universitas, Palembang**

Email : Widiwidyanto@yahoo.com

**ABSTRAK**

Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi di dalam perusahaan tersebut. Internet yang mulai populer saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan komputer yang terhubung dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat. Tetapi dalam beberapa hal terhubung dengan internet bisa menjadi suatu ancaman yang berbahaya, banyak serangan yang dapat terjadi baik dari dalam maupun luar seperti virus, trojan, maupun hacker. Pada akhirnya security komputer dan jaringan komputer akan memegang peranan yang penting dalam kasus ini.

**A. LATAR BELAKANG MASALAH**

World Wide Web (WWW atau Web1) merupakan salah satu “killer applications” yang menyebabkan populernya Internet. Kehebatan Web adalah kemudahannya untuk mengakses informasi, yang dihubungkan satu dengan lainnya melalui konsep*hypertext*.

Informasi dapat tersebar di mana-mana di dunia dan terhubung melalui *hyperlink*. Informasi lebih lengkap tentang WWW dapat diperoleh di web W3C .

 Pembaca atau peraga sistem WWW yang lebih dikenal dengan istilah *browser* dapat diperoleh dengan mudah, murah atau gratis. Contoh browser adalah Netscape, Internet Explorer, Opera, kfm (KDE file manager di sistem Linux), dan masih banyak lainnya.

 Kemudahan penggunaan program

browser inilah yang memicu populernya WWW. Sejarah dari browser ini dimulai dari browser di sistem komputer NeXT yang kebetulan digunakan oleh Berners-Lee. Selain browser NeXT itu, pada saat itu baru ada browser yang berbentuk text (text-oriented) seperti “line mode” browser. Berkembangnya WWW dan Internet menyebabkan pergerakan sistem informasi untuk menggunakannya sebagai basis. Banyak sistem yang tidak terhubung ke Internet tetapi tetap menggunakan basis Web sebagai basis untuk sistem informasinya yang dipasang di jaringan Intranet. Untuk itu, keamanan sistem informasi yang berbasis Web dan teknologi Internet 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 :

**a. Asumsi dari sisi pengguna**

1. Server dimiliki dan dikendalikan oleh organisasi yang mengaku memiliki  server tersebut.
2. Dokumen yang ditampilkan bebas dari virus, trojan horse, atau itikad jahat lainnya. Bisa saja seorang yang nakal memasang virus di web nya. Akan tetapi ini merupakan anomali.
3. 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.
4. Pelanggaran terhadap asumsi ini sebetulnya melanggar privacy. Jika hal ini dilakukan maka pengunjung tidak akan kembali ke situs ini.

**b. Asumsi dari penyedia layanan (web master)**

1. Pengguna tidak beritikad untuk merusak server atau mengubah isinya (tanpa ijin).
2. Pengguna hanya mengakses dokumen-dokumen atau informasi yang diijinkan diakses. Seorang pengguna tidak mencoba-coba masuk ke direktori yang tidak diperkenankan (istilah yang umum digunakan adalah “*directory traversal*”).
3. 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.

**c. Asumsi dari kedua belah pihak**
 Jaringan komputer (network) dan komputer bebas dari penyadapan pihak ketiga. Informasi yang disampaikan dari server ke pengguna (dan sebaliknya) terjamin keutuhannya dan tidak dimodifikasi oleh pihak ketiga yang tidak berhak.

Asumsi-asumsi di atas bisa dilanggar sehingga mengakibatkan adanya  masalah keamanan.

**C. TUJUAN**

Tujuan dari makalah ini adalah :

1. Mengetahui metode keamanan seperti apa yang tepat untuk layanan WWW ini.

2. Membuktikan melalui metode keamanan yang didapat terhadap jawaban  dari apa yang diasumsikan diatas.

**D. LANDASAN TEORI**

 Internet merupakan jaringan global yang menghubungkan suatu network dengan network lainya di seluruh dunia. TCP/IP menjadi protocol penghubung antara jaringan-jaringan yang beragam di seluruh dunia untuk dapat berkomunikasi. World Wide Web (WWW) merupakan bagian dari internet yang paling cepat berkembang dan paling populer

WWW bekerja merdasarkan pada tiga mekanisme berikut:

•    **Protocol** standard aturan yang di gunakan untuk berkomunikasi pada computer networking, Hypertext Transfer Protocol (HTTP) adalah protocol untuk WWW.

•     **Address**     WWW memiliki aturan penamaan alamat web yaitu: URL(Uniform

Resource Locator) yang di gunakan sebagai standard alamat internet.

•    **HTML** digunakan untuk membuat document yang bisa di akses melalui web. HTML merupakan standard bahasa yang digunakan untuk menampilkan documentweb.

•    Mengontrol tampilan dari web page dan contentnya.

•    Mempublikasikan document secara online sehingga bisa di akses.

•    Membuat online form yang bisa di gunakan untuk menangani pendaftaran,

transaksi secara online.

        Menambahkan object-object seperti image, audio, video dan juga java appletdalam document HTMLBrowser merupakan software yang di install di mesin client yang berfungsi untukmenterjemahkan tag-tag HTML menjadi halaman web. Browser yang sering digunakan biasanya Internet Explorer, Netscape Navigator, Opera, Mozilla dan masih banyak yang lainya.

**E. IMPLEMENTASI**

-     **KEAMANAN SERVER**

Server WWW 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 lubang keamanan di sistem WWW dapat dieksploitasi dalam bentuk yang beragam, antara lain:

**•**    Informasi yang ditampilkan di server diubah sehingga dapat mempermalukan perusahaan atau organisasi anda (dikenal dengan istilah *deface*1);

**•**    Informasi yang semestinya dikonsumsi untuk kalangan terbatas (misalnya laporan keuangan, strategi perusahaan anda, atau database client anda) ternyata berhasil disadap oleh saingan anda (ini mungkin disebabkan salah setup server, salah setup router / firewall, atau salah setup authentication);

**•**    Informasi dapat disadap (seperti misalnya pengiriman nomor kartu kredit untuk membeli melalui WWW, atau orang yang memonitor kemana saja anda melakukan *web surfing*);

**•**   Server diserang (misalnya dengan memberikan *request* secara bertubi-tubi)

sehingga tidak bisa memberikan layanan ketika dibutuhkan (*denial of service* *attack*);

**•**    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*).

**Strategi Implementasi**

**a. Membatasi akses melalui Kontrol Akses**

Sebagai penyedia informasi (dalam bentuk berkas-berkas), sering diinginkan pembatasan akses. Misalnya, diinginkan agar hanya orang-orang tertentu yang dapat mengakses berkas (informasi) tertentu. Pada prinsipnya ini adalah masalah kontrol akses. Pembatasan akses dapat dilakukan dengan:

•  Membatasi domain atau nomor IP yang dapat mengakses;

•  Menggunakan pasangan userid & password;

•  Mengenkripsi data sehingga hanya dapat dibuka (dekripsi) oleh orang yang memiliki kunci pembuka.

**b. Proteksi halaman dengan menggunakan password**

Salah satu mekanisme mengatur akses adalah dengan menggunakan pasangan *userid* (*user identification*) dan *password*. Untuk server Web yang berbasis Apache1, akses ke sebuah halaman (atau sekumpulan berkas yang terletak di sebuah directory di sistem Unix) dapat diatur dengan menggunakan berkas “.htaccess”.

**c. Secure Socket Layer**

Salah satu cara untuk meningkatkan keamanan server WWW adalah dengan menggunakan enkripsi pada komunikasi pada tingkat socket. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari/ke server WWW. Salah satu mekanisme yang cukup populer adalah dengan menggunakan *Secure Socket Layer* (SSL) yang mulanya dikembangkan oleh *Netscape*.

**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 WWW 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.

-     **KEAMANAN CLIENT WWW**

Dalam bagian terdahulu dibahas masalah yang berhubungan dengan server WWW. Dalam bagian ini akan dibahas masalah-masalah yang berhubungan dengan keamanan client WWW, 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 paparan diatas dapat disimpulkan sebagai berikut :

      Sistem keamanan WWW dibagi kedalam dua aspek, yaitu aspek dari Server dan aspek dari Client.

      Untuk sisi server ada mekanisme tertentu untuk mengambil file / berkas yang ada dalam server

      Beberapa strategi untuk memberikan keamanan server diantaranya adalah batasan kontrol aksesn, proteksi halaman dengan password, SSL (Security SocketLayer)

      Sedangkan yang harus diperhatikan dalam strategi pengamanan untuk client diantaranya adalah masalah privacy dan trojan house.

**G. DAFTAR PUSTAKA**

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

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

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